



Finanziert von der
Europäischen Union
NextGenerationEU

Gefördert durch:



Bundesministerium
für Wirtschaft
und Energie

aufgrund eines Beschlusses
des Deutschen Bundestages

31.12.2025

Schlussbericht

Security-Umfänge

Autoren: Patrick Wagner (Institutsprojektleitung), Magdalena Bertram, Dr. Alexander Giehl, Fabian Kügler, Lukas Lautenschlager, Nikolai Lenski, Veronique Momeu, Sebastian N. Peters, Nikolai Puch, Tudor Soroceanu, Dr. Stefan Tatschner, Benjamin Zengin und weitere Institutsmitarbeitende

Laufzeit: 01.01.2022 – 30.06.2025

Zuwendungsempfänger:

Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung eingetragener Verein;
Ausführende Stelle: Fraunhofer-Institut für Angewandte und Integrierte Sicherheit AISEC

Förderkennzeichen: 19A21048D

Inhaltsverzeichnis

1	Kurzdarstellung	12
1.1	Aufgabenstellung und Zielsetzung	12
1.1.1	Methode Security-Risikoanalyse	12
1.1.2	Übergreifender Vergleich von ISO/SAE 21434, ISO/IEC 27000 Familie und IEC 62443 Reihe	13
1.1.3	Vergleichende Analyse der regulatorischen Anforderungen an die Cybersicherheit im Automobilbereich	14
1.1.4	Technologien zum Schutz der Privatsphäre für vernetzte Automobilumgebungen	15
1.1.5	Einschätzung zu den Auswirkungen des EU AI Act auf ATLAS-L4	16
1.1.6	Sicherheit vernetzter Fahrzeugtechnologien im Nutzfahrzeugsektor	17
1.1.7	Testen von Resilienzeigenschaften in Ethernet-Netzwerken	17
1.1.8	Sicherheitsanforderungen von Industrial Ethernet Protokollen	18
1.1.9	Group Key Agreement auf Bussen von Cyber-physischen Systemen	19
1.1.10	Relevanz des OWASP MASVS für die Automobilindustrie	20
1.1.11	Sicherheit von Ortungsdiensten	21
1.1.12	Bereichsübergreifendes Security-Risikomanagement in der Automobilindustrie: Anforderungen und aktuelle Praktiken	22
1.1.12.1	Standards und Experteninterviews	22
1.1.12.2	Usability	22
1.1.13	Prototypisches Werkzeug für ein bereichsübergreifendes Security-Management	22
1.1.14	Entwicklung öffentlich verfügbarer Testtools für Fahrzeugdiagnose	24
1.1.15	Entwicklung eines Testsystems für Ladekommunikation in E-Fahrzeugen	24
1.1.16	Entwicklung eines Test-Frameworks für V2X	25
1.1.17	Modul-Baukasten Woodpecker zur statischen Code Analyse	25
1.1.18	Security-Risikoanalyse eines automatisierten Fahrsystems	26
1.1.19	Security-Risikoanalyse eines Control Centers	26
1.2	Voraussetzungen	27
1.3	Planung und Ablauf des Vorhabens	27
1.4	Stand der Wissenschaft und Technik zu Projektbeginn	28
1.4.1	Methode Security-Risikoanalyse	28
1.4.2	Übergreifender Vergleich von ISO/SAE 21434, ISO/IEC 27000 Familie und IEC 62443 Reihe	29

1.4.3	Vergleichende Analyse der regulatorischen Anforderungen an die Cybersicherheit im Automobilbereich	31
1.4.4	Technologien zum Schutz der Privatsphäre für vernetzte Automobilumgebungen	32
1.4.5	Einschätzung zu den Auswirkungen des EU AI Act auf ATLAS-L4	32
1.4.6	Sicherheit vernetzter Fahrzeugtechnologien im Nutzfahrzeugsektor	33
1.4.6.1	Grundlagen von V2V/V2X	33
1.4.6.2	Grundlagen von In-Vehicle Netzwerken	34
1.4.7	Testen von Resilienzeigenschaften in Ethernet-Netzwerken	35
1.4.8	Sicherheitsanforderungen von Industrial Ethernet Protokollen	36
1.4.9	Group Key Agreement auf Bussen von Cyber-physischen Systemen	37
1.4.10	Sicherheit von Ortungsdiensten	38
1.4.11	Bereichsübergreifendes Security-Risikomanagement in der Automobilindustrie: Anforderungen und aktuelle Praktiken	40
1.4.11.1	Standards und Experteninterviews	40
1.4.11.2	Usability	41
1.4.12	Prototypisches Werkzeug für ein bereichsübergreifendes Security-Management	47
1.4.13	Entwicklung öffentlich verfügbarer Testtools für Fahrzeugdiagnose	48
1.4.14	Entwicklung eines Testsystems für Ladekommunikation in E-Fahrzeugen	49
1.4.15	Entwicklung eines Test-Frameworks für V2X	50
1.4.16	Modul-Baukasten Woodpecker zur statischen Code Analyse	52
1.4.17	Security-Risikoanalyse eines automatisierten Fahrsystems	53
1.4.18	Security-Risikoanalyse eines Control Centers	54
	Verwendete Fachliteratur	55
1.5	Zusammenarbeit mit anderen Stellen	67
1.5.1	Zusammenarbeit mit den Partnern	68
1.5.2	Zusammenarbeit mit Forschungsinstituten und Hochschulen	68
1.5.3	Sonstige Zusammenarbeit	68
2	Eingehende Darstellung der erzielten Ergebnisse	69
2.1	Erzielte wissenschaftlich-technische Ergebnisse	69
2.1.1	Methode Security-Risikoanalyse	69
2.1.1.1	Anpassungen an den ATLAS-L4 Kontext und sonstige Erweiterungen	69
2.1.1.2	Usability	72
2.1.2	Übergreifender Vergleich von ISO/SAE 21434, ISO/IEC 27000 Familie und IEC 62443 Reihe	74
2.1.2.1	Kurzfassung	74

2.1.2.2	Geltungsbereich und Terminologie.....	75
2.1.2.3	Organisatorisches Cybersecurity-Management.....	76
2.1.2.4	Cybersicherheits-Risikomanagement	80
2.1.2.5	Zusammenführung und Handlungsempfehlungen	88
2.1.2.6	Fazit	90
2.1.3	Vergleichende Analyse der regulatorischen Anforderungen an die Cybersicherheit im Automobilbereich	91
2.1.3.1	Kurzfassung	91
2.1.3.2	Globale Regulierungsrahmen für die Cybersicherheit von Fahrzeugen	92
2.1.3.3	Vergleich der Regulierungsansätze.....	98
2.1.3.4	Kritische Bewertung und Lücken der Vorschriften	100
2.1.3.5	Indirekte Einflüsse und angrenzende Vorschriften	103
2.1.3.6	Fazit	105
2.1.4	Technologien zum Schutz der Privatsphäre für vernetzte Automobilumgebungen	106
2.1.4.1	Use Case 3: Sichere Netzwerkkommunikation Autonomer Fahrzeuge	109
2.1.4.2	Zuordnung von PETs auf vertrauliche Daten	110
2.1.4.3	Zusammenfassung.....	113
2.1.5	Einschätzung zu den Auswirkungen des EU AI Act auf ATLAS-L4	114
2.1.5.1	Klassifizierung der Systeme	114
2.1.5.2	Resultierende Pflichten	115
2.1.5.3	Handlungsempfehlungen für eine EU AI Act-konforme Umsetzung.....	117
2.1.5.4	Zusammenfassung der Bewertungen des EU AI Act bezüglich Innovation und Schutz der Privatsphäre.....	118
2.1.6	Sicherheit vernetzter Fahrzeugtechnologien im Nutzfahrzeugsektor	119
2.1.6.1	V2V/V2X.....	119
2.1.6.2	In-Vehicle Netzwerke.....	125
2.1.7	Testen von Resilienzeigenschaften in Ethernet-Netzwerken	128
2.1.8	Sicherheitsanforderungen von Industrial Ethernet Protokollen.....	132
2.1.8.1	Kurzfassung	132
2.1.8.2	Sicherheitsbewertung	132
2.1.8.3	Fallstudie zur Authentifizierung von Nachrichten	134
2.1.8.4	Bewertung	135
2.1.8.5	Diskussion.....	137
2.1.8.6	Fazit	138
2.1.9	Group Key Agreement – GRACYBUS.....	138

2.1.10	Relevanz des OWASP MASVS für die Automobilindustrie	142
2.1.10.1	Zielsetzung und Struktur des OWASP MASVS	142
2.1.10.2	Relevanz des MASVS im automobilen Kontext	143
2.1.10.3	Herausforderungen und Abgrenzungen	143
2.1.10.4	Fazit	144
2.1.11	Sicherheit von Ortungsdiensten	144
2.1.12	Bereichsübergreifendes Security-Risikomanagement in der Automobilindustrie: Anforderungen und aktuelle Praktiken	148
2.1.12.1	Kurzfassung	148
2.1.12.2	Cybersicherheitsstandards mit Relevanz für Cybersicherheitsrisikomanagement in der Automobilindustrie.....	148
2.1.12.3	Experteninterviews zu bereichsübergreifendem Cybersicherheitsrisikomanagement	152
2.1.12.4	Fazit	162
2.1.12.5	Usability	162
2.1.13	Prototypisches Werkzeug für ein bereichsübergreifendes Security-Management.....	165
2.1.13.1	Kurzfassung	165
2.1.13.2	Konzept und Architektur	165
2.1.13.3	Umsetzung in SharePoint und Power Automate	166
2.1.13.4	Umsetzung weiterer Anforderungen aus Standards, Interviews und Usability-Analyse	170
2.1.14	Entwicklung öffentlich verfügbarer Testtools für Fahrzeugdiagnose.....	175
2.1.15	Entwicklung eines Testsystems für Ladekommunikation in E-Fahrzeugen.....	179
2.1.16	Entwicklung eines Test-Frameworks für V2X.....	182
2.1.17	Modul-Baukasten Woodpecker zur statischen Code Analyse.....	183
2.1.18	Security-Risikoanalyse eines automatisierten Fahrsystems.....	189
2.1.18.1	Kurzfassung	189
2.1.18.2	Methode	189
2.1.18.3	Security-Risikoanalyse eines automatisierten Fahrsystems des Level 4.....	190
2.1.18.4	Grundsätze für die Durchführung von Security-Risikoanalysen für automatisierte Fahrsysteme	294
2.1.19	Security-Risikoanalyse eines Control Centers	294
2.1.19.1	Kurzfassung	294
2.1.19.2	Methode	295
2.1.19.3	Security-Risikoanalyse eines Control Centers für Lkw mit Level 4 Autonomiegrad.	296
2.2	Wichtige Positionen des zahlungsmäßigen Nachweises	423

2.3	Darstellung der Notwendigkeit und Angemessenheit der geleisteten Arbeit	423
2.4	Nutzen und Verwertbarkeit der Ergebnisse.....	424
2.5	Bekannt gewordener Fortschritt auf dem Gebiet des Vorhabens bei anderen Stellen ..	425
2.6	Erfolgte oder geplante Veröffentlichungen	425

Tabellenverzeichnis

Tabelle 1: Vergleich der Kandidaten nach theoretischem Aufwand.	37
Tabelle 2: Übersicht über die Aspekte des Regulierungsvergleichs.....	92
Tabelle 3: Klassifizierung von Fahrzeugtypen gemäß EU-Kategorien [149].....	93
Tabelle 4: Vergleich der Regulierungsrahmen für die Cybersicherheit von Fahrzeugen (EU, China, USA)	97
Tabelle 5: Wichtigste regulatorische Lücken nach Region mit Auswirkungen und Empfehlungen	102
Tabelle 6: Bewertung der Identifizierbarkeit der Datenpunkte je Domäne.	107
Tabelle 7: Vertraulichkeits-Scoring Matrix.	108
Tabelle 8: Risikobewertung der Datenpunkte.	108
Tabelle 9: Privacy Framework nach Taxonomie von Heurix et al.	111
Tabelle 10: Taktzyklusanzahl von NewHope1024 im CPA-Modus auf AURIX und Cortex M4 [172].	122
Tabelle 11: Taktzyklusanzahl von den gitterbasierten Verfahren CRYSTALS-KYBER, Saber und NTRU im CCA-Modus auf AURIX [177].	124
Tabelle 12: Protokollanforderungen für ein ideales sicheres GKA auf CPS-Bussen.	139
Tabelle 13: Themen und induktive Codes mit Häufigkeiten für den Status quo.....	155
Tabelle 14: Themen und induktive Codes mit Häufigkeiten für Anforderungen und Machbarkeit	157
Tabelle 15: Themen und induktive Codes mit Häufigkeiten für Chancen und Risiken	159
Tabelle 16: Funktionen des automatisierten Fahrsystems. Wenn Dx oder Nx in Spalte Architektur eingetragen ist, bedeutet dies, dass das Datum Dx oder der Datenfluss Nx für die Funktion relevant sind. Dies ist auch der Fall, wenn die ID einer Komponente, z. B. CC, aufgeführt ist.	191
Tabelle 17: Daten des automatisierten Fahrsystems	192
Tabelle 18: Komponenten des automatisierten Fahrsystems	193
Tabelle 19: Kommunikationstechnologien des automatisierten Fahrsystems	194
Tabelle 20: Kommunikationsflüsse des automatisierten Fahrsystems.....	196
Tabelle 21: Schadensszenarien für das automatisierte Fahrsystem; Auswirkungsklassen: S-Sicherheit, F-Finanziell, O-Betrieb, P-Datenschutz; Auswirkungsgrade: 0-Vernachlässigbar, 1-Mäßig, 2-Erheblich, 3-Schwerwiegend.....	205
Tabelle 22: Schutzziele für das automatisierte Fahrsystem; Auswirkungsklassen: S-Sicherheit, F-Finanziell, O-Betrieb, P-Datenschutz; Auswirkungsgrade: 0-Vernachlässigbar, 1-Mäßig, 2-Erheblich, 3-Schwerwiegend.	207

Tabelle 23: Annahmen für das automatisierte Fahrsystem.....	217
Tabelle 24: Schutzmaßnahmen für das automatisierte Fahrsystem	221
Tabelle 25: Bedrohungsszenarien und Risiken für das automatisierte Fahrsystem; SZ _v /SZ _n - Schadensszenarien vor/nach Schutzmaßnahmen; AG _v /AG _n -Auswirkungsgrad vor/nach Schutzmaßnahmen, V-Vernachlässigbar, M-Mäßig, E-Erheblich, S- Schwerwiegend; AM _v /AM _n -Angriffsmachbarkeit vor/nach Schutzmaßnahmen, SG-Sehr gering, G-Gering, M-Mittel, H-Hoch; R _v /R _n -Risikowert vor/nach Schutzmaßnahmen; Hinweis: Wenn in den Spalten SZ _v /SZ _n zwei durchgezogene Linien vorhanden sind, ist dies so zu interpretieren, dass oberhalb der ersten Linie die Schadensszenarien ohne Berücksichtigung von Annahmen, darunter die durch Annahmen entfernten oder transformierten Schadensszenarien und ganz unten die Schadensszenarien unter Berücksichtigung von Annahmen aufgeführt sind.	230
Tabelle 26: Funktionen des Control Centers. Wenn Dx oder Nx in Spalte Architektur eingetragen ist, bedeutet dies, dass das Datum Dx oder der Datenfluss Nx für die Funktion relevant sind. Dies ist auch der Fall, wenn die ID einer Komponente, z. B. CC, aufgeführt ist.	296
Tabelle 27: Daten des Control Centers	297
Tabelle 28: Komponenten des Control Centers	298
Tabelle 29: Kommunikationstechnologien des Control Centers	299
Tabelle 30: Kommunikationsflüsse des Control Centers.....	301
Tabelle 31: Schadensszenarien für das Control Center; Auswirkungsklassen: S-Sicherheit, F- Finanziell, O-Betrieb, P-Datenschutz; Auswirkungsgrade: 0-Vernachlässigbar, 1- Mäßig, 2-Erheblich, 3-Schwerwiegend.	323
Tabelle 32: Schutzziele für das Control Center; Auswirkungsklassen: S-Sicherheit, F-Finanziell, O-Betrieb, P-Datenschutz; Auswirkungsgrade: 0-Vernachlässigbar, 1-Mäßig, 2- Erheblich, 3-Schwerwiegend.	324
Tabelle 33: Annahmen für das Control Center.....	334
Tabelle 34: Schutzmaßnahmen für das Control Center	340
Tabelle 35: Bedrohungsszenarien und Risiken für das Control Center; SZ _v /SZ _n - Schadensszenarien vor/nach Schutzmaßnahmen; AG _v /AG _n -Auswirkungsgrad vor/nach Schutzmaßnahmen, V-Vernachlässigbar, M-Mäßig, E-Erheblich, S- Schwerwiegend; AM _v /AM _n -Angriffsmachbarkeit vor/nach Schutzmaßnahmen, SG-Sehr gering, G-Gering, M-Mittel, H-Hoch; R _v /R _n -Risikowert vor/nach Schutzmaßnahmen; Hinweis: Wenn in den Spalten SZ _v /SZ _n zwei durchgezogene Linien vorhanden sind, ist dies so zu interpretieren, dass oberhalb der ersten Linie die Schadensszenarien ohne Berücksichtigung von Annahmen, darunter die durch Annahmen entfernten oder transformierten Schadensszenarien und ganz unten die Schadensszenarien unter Berücksichtigung von Annahmen aufgeführt sind.	353

Abbildungsverzeichnis

Abbildung 1: Existierende schützenswerte Datentypen laut OECD-Report [10].	15
Abbildung 2: Vernetzung in modernen Anlagen.	19
Abbildung 3: Beispielhafte C-ITS Warnung für ein stehendes Fahrzeug [35].	25
Abbildung 4: Unterschiedliche Kommunikationsmöglichkeiten in V2X: V2V, V2P, V2I, V2C.	34
Abbildung 5: U- und C-plane in LTE.	39
Abbildung 6: Reduzierter Signal-/Frequenzsuchraum mit A-GNSS-Hilfsdaten. Alle Hilfsdaten wie Position, Zeit und Almanach reduzieren den Frequenzsuchraum. Zur Reduzierung des Codeverzögerungssuchraums ist eine präzise Zeitangabe erforderlich [108].	39
Abbildung 7: Protokollstapel der High-Level Ladekommunikation im ISO/OSI Schichtenmodell.	50
Abbildung 8: C-ITS Frequenzband	51
Abbildung 9: C-ITS Protokoll Stack mit den zugehörigen ETSI Standards [127].	51
Abbildung 10: C-ITS-Vertrauensmodellarchitektur [128].	52
Abbildung 11: Schnittstellen zwischen Fahrzeug-CSMS, ISMS und Produktions-Cybersecurity-Management nach ISO/SAE 21434.	77
Abbildung 12: Einbettung des ISMS in andere Managementsysteme nach ISO/IEC 27001/27003.	78
Abbildung 13: Koordination von IACS-Security-Programm und ISMS nach IEC 62443-2-1.	79
Abbildung 14: Kernaspekte des Risikomanagements nach ISO/SAE 21434 und Übertragung von Cybersecurity-Claims und -Anforderungen auf externe Systeme und Managementsysteme.	81
Abbildung 15: Kernaspekte des Risikomanagements nach ISO/IEC 27005 und Harmonisierung von Risikokriterien und -prozessen über CSMS, ISMS und IACS-Security-Programm hinweg.	83
Abbildung 16: Cybersecurity Risikomanagement im IACS-Kontext nach IEC 62443-3-2.	85
Abbildung 17: Darstellung des WAVE Referenzmodells mit den Security Services, die sich über den gesamten Stack erstrecken. Quelle: [79].	120
Abbildung 18: Authenticated key exchange [174, 173].	123
Abbildung 19: Prozessorientierte Sicht auf das modulare Testsystem von der Beschreibung von Datenflüssen bis zur Testausführung.	129
Abbildung 20: Entdeckung der Netzwerktopologie mithilfe von LLDP über NETCONF. In Schritt 1 entdeckt das RTS den ersten angeschlossenen Netzwerkknoten. Schritt 2 zeigt das Auslesen von LLDP-Informationen und Schritt 3 das Entdecken von weiteren Netzwerkknoten. Das Verfahren wird iterativ wiederholt, bis keine neuen Knoten mehr entdeckt werden.	130

Abbildung 21: Beispielhafter Ablauf des technologieunabhängigen Tests für 1-Link-Failures. Die verschiedenen Farben zeigen das Einschleusen des Datenverkehrs von RTS zur Test Source, das produktive Verhalten von Test Source zur Test Sink und das Extrahieren der Testdaten von Test Sink zu RTS mittels VBSR. Zur Fehlerinduzierung wird in Schritt 1 die entsprechende VLAN-ID entfernt, wodurch es in Schritt 2 zu einem Ausfall der Verbindung kommt.	131
Abbildung 22: Referenzarchitektur für OT-Netzwerke.	133
Abbildung 23: Ergebnisse für 100-Megabit/s-Netzwerke.	136
Abbildung 24: Ergebnisse für 1-Gigabit/s-Netzwerke.	136
Abbildung 25: Systemmodell - Bussystem mit den angeschlossenen Geräten A, B und C. Gerät J tritt dem Bus bei. Gerät X verlässt den Bus abrupt. Der Angreifer T hat physischen Zugriff auf den Bus.....	138
Abbildung 26: Konzept des Test-Frameworks.	145
Abbildung 27: Beobachteter PSDS-Server für verschiedene Geräte. ? kennzeichnet Geräteeigenschaften, die wir nicht testen konnten.	145
Abbildung 28: Liste der für SUPL getesteten Mobilgeräte. Die Tests mit ? wurden aufgrund der fehlenden erforderlichen Laborausstattung nicht durchgeführt.	146
Abbildung 29: Vergleich von Methoden zur Erfassung des Datenverkehrs für Android.	146
Abbildung 30: Unsere Vermutung für den Algorithmus zur Ableitung des Standorts für Google FLP.....	147
Abbildung 31: Einbeziehung von Informationen und Kenntnis der Vorschriften in den verschiedenen Bereichen	160
Abbildung 32: Wahrgenommene Vorteile und Herausforderungen	161
Abbildung 33: Bedeutung einer einheitlichen Terminologie und Datenstandardisierung	161
Abbildung 34: Auszug des Power-Automate-Flows „Import MoRA Files“ zur automatisierten Übernahme der MoRA-Risikobewertungen aus Excel in die SharePoint-Listen des prototypischen bereichsübergreifenden Security-Management-Werkzeugs.	167
Abbildung 35: SharePoint-Seite „Risk Assessments“ des prototypischen Werkzeugs mit TOE-Auswahl (oben) und den automatisch aus den MoRA-Dateien befüllten Listen zum Systemmodell und den Risikoartefakten (unten).....	169
Abbildung 36: Die Tools in gallia können verwendet werden, um ECUs und deren Funktionalitäten zu scannen.	175
Abbildung 37: Überblick über die Software-Architektur von gallia	177
Abbildung 38: Control Pilot Schaltkreis nach IEC 61851-1 [34].....	180
Abbildung 39: Proximity Pilot Schaltkreis nach IEC 61851-1 [34].	180
Abbildung 40: Render der designten Platine in KiCad	181

Abbildung 41: Aufbau des Testsystems. Im Projekt entwickelte oder erweiterte Komponenten sind rot eingefärbt.	182
Abbildung 42: Raspberry Pi Setup mit einem Atheros miniPCle-HAT und zwei Antennen.....	183
Abbildung 43: Gefilterte Liste an Findings.	186
Abbildung 44: False positive Finding (Kind: Pass).	187
Abbildung 45: True positive Finding (Kind: Fail).....	188
Abbildung 46: Hauptaktivitäten von MoRA, entnommen aus [1] mit Anpassungen an die Terminologie von ISO/SAE 21434. Die Risikomatrix für unsere CRA ist in der unteren rechten Ecke dargestellt.	190
Abbildung 47: ADS Diagramm, das die Komponenten und ihre Verbindungen zeigt. IPC steht für Interprozesskommunikation.	195
Abbildung 48: Sequenzdiagramm des automatisierten Fahrsystems	205
Abbildung 49: Control Center Diagramm, das die Komponenten und ihre Verbindungen zeigt.	300
Abbildung 50: Sequenzdiagramm des Control Centers	322

1 Kurzdarstellung

1.1 Aufgabenstellung und Zielsetzung

Im Teilvorhaben „Security-Umfänge“ wurden alle cybersicherheitsrelevanten Fragestellungen des Verbundprojekts ATLAS-L4 gebündelt. Ziel war es, für das Gesamtsystem aus L4-fähigem Nutzfahrzeug und cloudbasiertem Control Center Security-by-Design sicherzustellen und die gesetzlichen sowie normativen Anforderungen (u. a. UN R155, ISO/SAE 21434, ISO/IEC-27000-Familie, IEC-62443) fundiert umzusetzen.

Hierzu wurden

- eine auf das ATLAS-L4-Szenario zugeschnittene Methode zur Security-Risikoanalyse entwickelt (weiterentwickeltes MoRA),
- die relevanten Cybersecurity-Standards und Regulierungen über die Bereiche Fahrzeug, Backend/IT und Produktion hinweg analysiert und aufeinander bezogen,
- ein prototypisches Werkzeug für bereichsübergreifendes Security-Management konzipiert und umgesetzt sowie
- konkrete Security-Risikoanalysen für das automatisierte Fahrsystem (Lkw) und das Control Center erstellt.

Flankierend wurde eine Vielzahl von Spezialthemen wie Privacy-Enhancing Technologies, Security vernetzter Fahrzeugtechnologien, Testsysteme für Ladekommunikation und V2X, statische Code-Analyse oder die Auswirkungen des EU AI Act auf ATLAS-L4 bearbeitet. Die auf diese Weise gewonnenen Security-Anforderungen flossen in die technische Auslegung der ATLAS-L4-Architektur und in die Prozesse der Konsortialpartner ein.

Die nachfolgenden Unterabschnitte 1.1.1 bis 1.1.19 konkretisieren für die jeweiligen Einzelthemen die spezifische Aufgabenstellung und Zielsetzung innerhalb dieses Teilvorhabens.

1.1.1 Methode Security-Risikoanalyse

Für die Entwicklung des ATLAS-L4-Gesamtsystems – bestehend aus L4-Truck mit automatisiertem Fahrsystem (ADS) und einem Cloud-basierten Control Center – mussten Security-Anforderungen frühzeitig, nachvollziehbar und normkonform abgeleitet werden. Ziel des Arbeitsschritts „Methode Security-Risikoanalyse“ war es daher, eine bestehende, bei MAN bereits eingesetzte Methode zur Security-Risikoanalyse so weiterzuentwickeln, dass sie (i) ISO/SAE-21434-konform ist, (ii) sowohl klassische Automotive-E/E-Systeme als auch IT-/Cloud-Systeme des Control Centers abdeckt und (iii) als gemeinsame Basis für die in ATLAS-L4 durchgeführten Risikoanalysen dient.

Als Methodenkern wurde Modular Risk Assessment (MoRA) gewählt, da MoRA in der Lkw-Entwicklung bereits zur Ableitung von Security-Anforderungen für Steuergeräte und Funktionen eingesetzt wird, auf einem modellbasierten Ansatz beruht und sich eng an ISO/SAE 21434 orientieren lässt [1, 2]. In mehreren Workshops zwischen Fraunhofer AISEC und MAN wurden Terminologie, Bewertungsmodell und Werkzeugunterstützung für den ATLAS-L4-Kontext abgestimmt. Die Projektpartner einigten sich im Wesentlichen auf die Begriffswelt von ISO/SAE 21434, um eine direkte Anschlussfähigkeit an TARA-basierte Herstellerprozesse und an UN R155 zu gewährleisten.

Auf dieser Basis wurden das Impact-/Attack-Feasibility-Modell, Schadenskriterien sowie Annahmen-, Bedrohungs- und Maßnahmenkataloge an die Spezifika vollautomatisierter Hub-to-Hub-Lkw und des Control Centers angepasst. Neben den in ISO/SAE 21434 geforderten Impact-Kategorien Safety, Financial, Operational und Privacy wurden zusätzliche Kriterien eingeführt, um OEM-spezifische Aspekte (z. B. Vertragsstrafen, Gewährleistungskosten, Flottenverfügbarkeit) abbilden zu können. Die Angriffsmachbarkeit wird in Anlehnung an die Common Evaluation Methodology (CEM) attack-potential-basiert über Faktoren wie benötigte Zeit, Expertise, Systemkenntnis, Gelegenheit und Ausrüstung bewertet.

Alle methodischen Bausteine wurden in ein überarbeitetes MoRA-Excel-Werkzeug überführt, das im Projekt sowohl für die Security-Risikoanalyse des ADS (Abschnitt 2.1.18) als auch des Control Centers (Abschnitt 2.1.19) eingesetzt wurde. Damit konnten Security-Anforderungen für Truck und Control Center konsistent und wiederholbar abgeleitet sowie in MAN-interne Cybersecurity Concepts und Specifications überführt werden.

Begleitend zur Weiterentwicklung der Methode zur Security-Risikoanalyse wurde untersucht, wie gut sich das MoRA-Excel-Template im ATLAS-L4-Kontext praktisch nutzen lässt und welche strukturellen Anforderungen sich aus Usability-Sicht ergeben. Ziel war nicht eine vollumfängliche Gebrauchstauglichkeitsstudie, sondern die Identifikation von übergreifenden Verbesserungsbedarfen (z. B. hinsichtlich Automatisierung, Strukturierung der Tabellenblätter, Nachvollziehbarkeit von Verweisen und kontextsensitiver Unterstützung), die in die weitere Werkzeuftpflege einfließen können. Kleinere Optimierungen des aktuellen Entwicklungsstands – etwa Farbwahl, Spaltenbreiten oder die konkrete Anordnung einzelner UI-Elemente – wurden bewusst nicht vertieft, da sie mit geringem Aufwand angepasst werden können und keinen Einfluss auf den methodischen Kern der Security-Risikoanalyse haben.

1.1.2 Übergreifender Vergleich von ISO/SAE 21434, ISO/IEC 27000 Familie und IEC 62443 Reihe

Moderne Fahrzeugarchitekturen – insbesondere im Kontext hochautomatisierter Nutzfahrzeuge – basieren auf einem Verbund aus fahrzeugseitigen E/E-Systemen, IT-Backends und vernetzten Produktionsanlagen. Für diese Teilbereiche existieren etablierte, aber jeweils domänenspezifische Cybersicherheitsstandards: ISO/SAE 21434 für Straßenfahrzeuge [21], die ISO/IEC-27000-Familie für Informationssicherheits-Managementsysteme (ISMS) [22, 73, 174, 175] und die IEC-62443-Reihe für industrielle Automatisierungs- und Steuerungssysteme (IACS) [23, 176, 177]. In der Praxis müssen alle drei Normenwelten simultan berücksichtigt werden, etwa wenn ein Level-4-Lkw im CSMS nach ISO/SAE 21434 entwickelt, in einer IEC-62443-konformen Fertigungslinie produziert und über eine ISO/IEC-27001-konforme Backend-Infrastruktur betrieben wird.

Ziel dieses Arbeitsschritts war ein übergreifender, normtextnaher Vergleich dieser drei Standardfamilien und die Ableitung von Konsequenzen für Automobilhersteller. Analysiert wurden

- Geltungsbereich und Zielsetzung der Normfamilien,
- zentrale Begriffe (Risiko, Bedrohung, Schwachstelle, Schaden) und deren Ausprägungen,
- Anforderungen an Managementsysteme (CSMS, ISMS, IACS-Security-Programm) und deren Schnittstellen sowie
- Gemeinsamkeiten und Unterschiede im Risikomanagement.

Die Ergebnisse dienen als fachliche Grundlage für weitere Arbeiten im Projekt, insbesondere für das in Abschnitt 2.1.12 beschriebene bereichsübergreifende

Cybersicherheits-Risikomanagement (Fahrzeug – Backend – Produktion). Für die ATLAS-L4-Partner werden daraus konkrete Empfehlungen abgeleitet, wie CSMS, ISMS und IACS-Security-Programm harmonisiert und gemeinsame Risiko- und Bewertungsmaßstäbe etabliert werden können.

1.1.3 Vergleichende Analyse der regulatorischen Anforderungen an die Cybersicherheit im Automobilbereich

Moderne Fahrzeuge sind in hohem Maße auf miteinander verbundene elektronische Systeme angewiesen. Dazu gehören zahlreiche elektronische Steuergeräte (ECUs), die über Kommunikationsprotokolle wie Controller Area Network (CAN), Ethernet, Bluetooth, Wi-Fi und Mobilfunknetze miteinander verbunden sind. Dies erhöht sowohl die Funktionalität als auch die Anzahl potenzieller Angriffsflächen. Durch die Integration von Infotainment-Systemen, mobilen Geräten und Cloud-Diensten sind Fahrzeuge anfällig für verschiedene Arten von Cyberangriffen geworden [3]. Dazu gehören physische Schnittstellen wie On-Board Diagnostics II (OBD-II) und Universal Serial Bus (USB) sowie Fernzugriff über kompromittierte Firmware-Updates, heruntergeladene Anwendungen oder Verbindungen zu mobilen Geräten. Wichtige Komponenten wie die Headunit, das Gateway und sicherheitskritische Aktoren können zum Ziel werden. Typische Angriffsmethoden sind das Ausnutzen von Software-Schwachstellen, das Einschleusen von Schadcode und das Abfangen von Benutzerdaten. Diese Risiken unterstreichen die Notwendigkeit von Sicherheitsmechanismen über alle internen und externen Schnittstellen hinweg. Während technische Lösungen für die Cybersicherheit im Automobilbereich aktiv entwickelt werden, mangelt es nach wie vor an einheitlichen, weltweit verbindlichen Regulierungsstandards. Verschiedene Länder haben unterschiedliche rechtliche und regulatorische Ansätze mit jeweils eigenem Geltungsbereich, eigenen Anforderungen und eigenem Durchsetzungsgrad verabschiedet. Diese fragmentierte Regulierungslandschaft wirft mehrere Fragen auf: Wie unterscheiden sich die führenden Regulierungsrahmen in ihrer Behandlung der Cybersicherheit im Automobilbereich? Welche Verpflichtungen erlegen sie Herstellern und Zulieferern auf? Und wo bestehen noch Regulierungslücken? Dieser Artikel bietet einen Überblick über die einflussreichsten Regulierungsansätze, die die Cybersicherheitslandschaft im Automobilbereich prägen. Dazu gehören die verbindlichen Regelungen Nr. 155 und 156 der Wirtschaftskommission der Vereinten Nationen für Europa (UNECE), die von der Europäischen Union, Südkorea und Japan übernommen wurden [4], das nationale Rahmenwerk GB 44495-2024 in China und die unverbindliche Richtlinie der National Highway Traffic Safety Administration (NHTSA) in den Vereinigten Staaten. Das Papier soll deren jeweiligen Geltungsbereich, Kernanforderungen und praktische Auswirkungen für Originalgerätehersteller (OEMs) und Zulieferer hervorheben [5, 6, 7]. Andere Länder sind dabei, solche Vorschriften zu entwickeln. So hat Indien kürzlich einen Entwurf der AIS 189 [8] veröffentlicht, der jedoch noch nicht endgültig ist und daher aus diesem Vergleich ausgeschlossen wird. Angesichts der globalen Bedeutung der Automobilindustrie in der EU, den USA und China konzentriert sich dieses Papier auf diese Länder als repräsentative Fälle. Der Aufbau dieses Kapitels ist wie folgt: Nach einer Übersicht über die relevante Literatur im Bereich der Cybersicherheit im Automobilbereich wird im Kern des Papiers eine strukturierte Darstellung der drei ausgewählten Rahmenwerke UNECE R155/R156 (EU), GB 44495-2024 (China) und der NHTSA-Richtlinien (USA) gegeben. Anschließend folgt eine vergleichende Analyse, in der die Gemeinsamkeiten und Unterschiede zwischen den Ansätzen hervorgehoben werden. Darüber hinaus bietet der Artikel eine kritische Bewertung der Wirksamkeit der Richtlinien und der Herausforderungen bei ihrer Umsetzung. Schließlich analysiert der Artikel auch angrenzende, nicht automobilbezogene Vorschriften, wie das Cyber-Resilienz-Gesetz der EU, die Datenschutz-Grundverordnung (DSGVO) und das chinesische Cybersicherheitsgesetz,

die technische und rechtliche Verpflichtungen auferlegen, die zunehmend das Cybersicherheitsdesign im Automobilsektor prägen.

1.1.4 Technologien zum Schutz der Privatsphäre für vernetzte Automobilumgebungen

Moderne Fahrzeuge sind mit manchmal über 100 elektronischen Steuergeräten (ECUs) ausgestattet, bei denen es sich um kleine, eingebettete Computer handelt, die potenziell Daten über die Fahrzeugnutzer sammeln könnten [9]. Trotz des zunehmenden Bewusstseins für Datenschutzfragen im Automobilsektor mangelt es nach wie vor an systematischen Ansätzen, um zu bestimmen, welche Daten intelligente Fahrzeuge sammeln und welche Datentypen spezifische Vertraulichkeitsgarantien erfordern.

In dem wissenschaftlichen Papier mit dem Titel: „SoK: Technologien zum Schutz der Privatsphäre für vernetzte industrielle, intelligente Gebäude- und Automobilumgebungen“ werden Use Cases aus den Bereichen Industrial, Smart Home und Automotive vorgestellt. Jeder Use Case hat eigene, spezifische Anforderungen hinsichtlich des Schutzes der personenbezogenen Daten und der proprietären Daten, wie z. B. dem Schutz des geistigen Eigentums, die sich daraus ableiten. In unserem Paper haben wir uns hauptsächlich auf nicht-öffentliche Daten, also Daten, die sich nicht mit der blauen Farbe kreuzen, fokussiert. Die Klassifizierung der OECD aller schützenswerten Daten ist in Abbildung 1 ersichtlich.

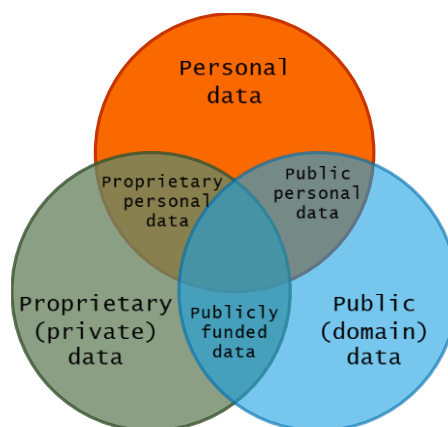


Abbildung 1: Existierende schützenswerte Datentypen laut OECD-Report [10].

Die Wichtigkeit für den Schutz proprietärer, persönlicher Daten ergibt sich aus der Vielzahl an rechtlich vorgeschriebenen Cybersecurity Frameworks und Standards, wie:

- der Network and Information Security NIS-2-Richtlinie¹
- dem EU Cybersecurity Act²
- und Cyber Resilience Act (CRA)³

aber auch aus Privacy spezifischen Regulatorien, wie:

- der Datenschutz-Grundverordnung (DSGVO, oder GDPR)⁴

¹ <https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng>

² <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019R0881&qid=1764250598816>

³ <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R2847&qid=1764250598816>

⁴ <https://www.datenschutz.org/eu-datenschutzgrundverordnung/>

und aus für den Automotive Sektor spezifischen Regulatorien, wie:

- der UN Regulation Nr. 155 und 156⁵
- und den internationalen Automotive Standards ISO/SAE 21434, ISO PAS 5112, und ISO 24089⁶

Privacy Enhancing Technologies (PETs) können Unternehmen helfen, richtlinienkonform zu bleiben [Richter‘25]⁷. Anonymisierung und Pseudonymisierung tragen zur Datenminimierung bei (DSGVO Art. 5), verschiedene Verschlüsselungs-PETs, wie zum Beispiel Homomorphic Encryption, tragen zum Integritätsschutz bei, indem verschlüsselte Berechnungen stattfinden (DSGVO Art. 5) und die Entscheidung PETs als Teil des Systemdesigns zu integrieren, gewährleistet die von der DSGVO geforderte Privacy-by-Design-Maßnahme (DSGVO Art. 25).

Für den ATLAS-L4 Kontext haben wir einen besonderen Fokus auf die Anwendbarkeit von Privacy-Enhancing Technologies zum Schutz von proprietären und persönlichen Daten innerhalb von Fahrzeugen (Intra-Vehikel-Netzwerken) gelegt. Dafür haben wir zunächst definiert, an welchen Stellen innerhalb eines Fahrzeugnetzes vertrauliche Daten anfallen und wie diese zu bewerten sind. Anschließend haben wir als Use Case die kritischste Domäne identifiziert und daraus Anforderungen abgeleitet. Diese Anforderungen bieten zusammen mit generischen Anforderungen, die unter anderem aus relevanten Standards extrahiert werden, eine Grundlage für die Auswahl von geeigneten Privacy Enhancing Technologies (PETs). PETs wurden geclustert und systematisch nach unserem festgelegten Schema beschrieben und bezüglich ihrer Reife und Anwendbarkeit für unsere Use Cases bewertet. Anschließend wurde der Use Case auf zwei in der Literatur existierende Privacy Engineering Frameworks (Heurix et al. [11] und Kunz et al. [12]) abgebildet. Die Abweichungen, die durch die Anwendung der Frameworks entstanden sind, führten uns schließlich zur Ableitung eines eigenen Ansatzes. Diese Ableitung vervollständigte das Ziel unseres Papers, die Auswahl geeigneter Privacy Enhancing Technologies für unsere Use Cases. Abschließend wurde das Paper in der Schlussfolgerung resümiert.

1.1.5 Einschätzung zu den Auswirkungen des EU AI Act auf ATLAS-L4

Im Zusammenhang mit dem automatisierten Transport zwischen Logistikzentren auf Level 4 und der im Projekt durchgeführten Analyse relevanter Standards ist eine kurze Untersuchung der aktuellen ML-Technologien und infrastrukturellen Voraussetzungen geplant, um festzustellen, inwieweit die neuen Standards und Regularien des EU AI Act den Einsatz solcher Technologien unterstützen oder angepasst werden müssen. Darauf aufbauend werden Empfehlungen für mögliche zusätzliche regulatorische Maßnahmen (z. B. im Kontext des Schutzes der Privatsphäre) erarbeitet, um die Integration autonomer Verkehrssysteme im Einklang mit den Zielen des EU AI Act voranzutreiben.

Im Mittelpunkt standen das in ATLAS-L4 eingesetzte Automated Driving System (ADS) sowie das projektierte Control Center als integrierter Bestandteil des Gesamtsystems. Ziel war es,

⁵ <https://unece.org/sites/default/files/2021-03/R155e.pdf> und <https://unece.org/sites/default/files/2021-03/R156e.pdf>

⁶ <https://www.iso.org/standard/70918.html> und <https://www.iso.org/standard/80840.html> und <https://www.iso.org/standard/77796.html>

⁷ <https://techgdp.com/blog/discover-how-privacy-enhancing-technologies-pets-help-organizations-achieve-gdpr-compliance-by-safeguarding-personal-data-reducing-risks-and-enhancing-confidentiality-through-encryption-anonymiza/>

- die im Projekt geplanten KI-basierten Komponenten (insb. Perception, Prediction, Planning, Mission Control und Control Center) mit den Definitionen und Anforderungen des EU AI Act abzugleichen,
- die Systeme zu klassifizieren (insb. Hochrisiko-Einstufung) und daraus resultierende Pflichten für Anbieter und Betreiber herauszuarbeiten,
- anhand der vorhandenen Projektdokumente (Vorhabensbeschreibung, Meilensteinberichte, SRA Lkw, SRA Control Center) den bereits erreichten Umsetzungsgrad zu bewerten und Lücken zu identifizieren,
- mögliche zusätzliche Maßnahmen insbesondere im Bereich Datenschutz/Privatsphäre, Robustheit und erklärbarer KI abzuleiten,
- sowie Bewertungen des EU AI Act bezüglich Innovation und Schutz der Privatsphäre zusammenzufassen.

1.1.6 Sicherheit vernetzter Fahrzeugtechnologien im Nutzfahrzeugsektor

Die fortschreitende Integration vernetzter Fahrzeugtechnologien in den Nutzfahrzeugsektor stellt einen bedeutenden Fortschritt für die Sicherheit und Effizienz des Güterverkehrs dar. Insbesondere die Technologie des Driver-Assistive Truck Platooning (DATP), die auf der Fahrzeug-zu-Fahrzeug-Kommunikation (V2V) basiert, ermöglicht es mehreren Lkw, in enger Formation zu fahren und dabei Informationen über die Fahrzeugleistung auszutauschen. Diese Form der kooperativen adaptiven Geschwindigkeitsregelung (CACC) bietet nicht nur das Potenzial zur Reduktion von Kraftstoffverbrauch und CO₂-Emissionen, sondern trägt auch zur Verringerung von Auffahrunfällen bei.

Mit zunehmender Komplexität der elektrischen und elektronischen Systeme in Fahrzeugen, die durch eine Vielzahl von vernetzten Steuergeräten (ECUs) und Sensoren geprägt ist, werden robuste Kommunikationsnetzwerke unerlässlich. Der Einsatz standardisierter Kommunikationssysteme und -protokolle, wie das Controller Area Network (CAN) und

SAE J1939, hat sich bewährt, um eine effiziente Kommunikation zwischen verschiedenen Systemen zu gewährleisten. Neuere Entwicklungen, wie Ethernet-basierte Kommunikationsprotokolle und Time Sensitive Networking (TSN), zeigen das Potenzial, die Bandbreitenanforderungen moderner Anwendungen zu erfüllen, insbesondere im Hinblick auf sicherheitskritische Funktionen und die Unterstützung von Fahrerassistenzsystemen.

Angesichts der zunehmenden Bedrohung durch Quantencomputer, die in der Lage sind, konventionelle kryptographische Verfahren zu brechen, ist die Integration von Post-Quantum-Kryptografie (PQC) in diese Technologien von entscheidender Bedeutung. Der Einsatz von PQC wird als notwendiger Schritt gesehen, um die langfristige Sicherheit der Kommunikationssysteme in der Nutzfahrzeugindustrie zu gewährleisten. Dieses Dokument bietet eine Übersicht über die Herausforderungen und Möglichkeiten der Integration von PQC in verschiedene Systeme vernetzter Fahrzeugtechnologien.

1.1.7 Testen von Resilienzeigenschaften in Ethernet-Netzwerken

Moderne Netzwerke sind hochkomplexe Umgebungen, welche eine Konfiguration unterschiedlichster Protokolle zur Funktion benötigen. Die Resilienz dieser Netzwerke ist besonders kritisch für den reibungslosen Betrieb in verteilten Systemen, wie sie heutzutage in Fahrzeugen, industriellen Anlagen und Rechenzentren zu finden sind. Moderne Netzwerkarchitekturen verwenden

schon Netzwerkresilienzprotokolle, wie zum Beispiel Protokolle der Time-Sensitive Networking (TSN)-Protokollfamilie, jedoch wird die korrekte Konfiguration im Netzwerk selten validiert. Testverfahren basieren häufig auf manuellen Tests, welche einen hohen Aufwand, dediziertes Testwerkzeug sowie menschliche Intervention benötigen. Um korrektes Resilienzverhalten in operativen Netzwerken effizient zu validieren, soll ein Testsystem zur automatisierten Resilienzmessung in Ethernet-Netzwerken auf der Sicherungsschicht entwickelt und erprobt werden.

Die Aufgabenstellung ist, unterschiedliche Resilienzklassen in bestimmten Fehlerszenarien zu quantifizieren. Dabei sollen produktivnahe Tests eingesetzt werden, welche möglichst automatisiert unterschiedliche Datenflüsse im Netzwerk abtesten können. Weitere Faktoren wie möglichst breite Einsatzmöglichkeiten (z. B. durch Umsetzung nach verbreiteten Standards) sowie möglichst geringe Auswirkungen auf den operativen Betrieb sollten berücksichtigt werden.

Zielsetzung dieses Vorhabens ist die Konzeption und prototypische Umsetzung eines automatisierten Verfahrens zur Validierung und Quantifizierung von Resilienzeigenschaften in produktionsnahen Ethernet-/TSN-Netzen. Das Verfahren führt unter realitätsnahen Bedingungen kontrollierte, temporäre Störungen (z. B. Verbindungsausfall) entlang der relevanten Pfade ein, misst dabei Resilienz, zum Beispiel in Form der Erreichbarkeit oder des Paketverlusts. Weiterhin arbeitet das Verfahren minimalinvasiv, kommt ohne die Stimulation von Endgeräten und ohne zusätzliche Verkabelung aus und nutzt standardnahe Managementschnittstellen, um sich möglichst gut für den operativen Einsatz zu eignen. Die Tests werden aus einer abstrakten Fluss-/Zielbeschreibung automatisch geplant, ausgeführt, ausgewertet und dokumentiert, sodass sie reproduzierbar und skalierbar auf unterschiedliche Topologien und Schutzkonzepte anwendbar sind.

1.1.8 Sicherheitsanforderungen von Industrial Ethernet Protokollen

In den letzten Jahren ist das Bewusstsein der Betreiber von Betriebstechnologie (OT) für die entscheidende Bedeutung der Sicherheit in industriellen Umgebungen gewachsen [13]. Die Sicherheit von Industrial-Ethernet-Protokollen (IE), die mit einem Marktanteil von 71 % dominieren [14], gibt weiterhin Anlass zu erheblicher Sorge. Diese Protokolle, die häufig in industriellen Netzwerken verwendet werden, weisen oft keine robusten Sicherheitsfunktionen auf, wodurch die Systeme anfällig für verschiedene Cyber-Bedrohungen sind [15]. Diese Sorge ist im Kontext kleiner und mittlerer Unternehmen (KMU) noch ausgeprägter, wo die OT-Sicherheit innerhalb der organisatorischen Prioritäten noch kein weit verbreitetes Thema ist [16].

Die aktuellen Risiken, denen OT-Betreiber und OT-Umgebungen ausgesetzt sind, resultieren aus der zunehmenden Vernetzung von Fertigungssystemen und Maschinen [17]. Dies wird in Abbildung 2 veranschaulicht. Auf der linken Seite von Abbildung 2 ist eine Anlage mit den entsprechenden Betriebsebenen gemäß [18] und anderen verwandten Normen dargestellt. Auf der untersten Ebene findet der physische Fertigungsprozess statt. Dieser physische Prozess stellt die Herstellung des eigentlichen Produkts dar, der in den meisten Fällen entweder einen diskreten oder einen kontinuierlichen Fertigungsprozess mit seinen Sensoren und Aktoren umfasst. Darüber befindet sich die Fertigungssteuerungsebene. Hier befinden sich Geräte wie speicherprogrammierbare Steuerungen (SPS). In dieser Ebene werden die meisten SCADA-Aktivitäten (Supervisory Control and Data Acquisition) ausgeführt. Über dieser Ebene befindet sich die nächste Ebene, die für die Gesamtsteuerung des Anlagenbetriebs zuständig ist. Diese Ebene kombiniert die Eingaben der verschiedenen SCADA-Aktivitäten, um einen umfassenden Überblick über den aktuellen Zustand der Anlage zu bieten. Die oberste Ebene in Abbildung 2 zeigt die letzte Ebene, die die OT der Anlage

mit der IT der Fabrik und dem zugehörigen Unternehmen integriert (d. h. hier ist der Übergang vom Fertigungsbereich zum Bürobereich abgeschlossen).

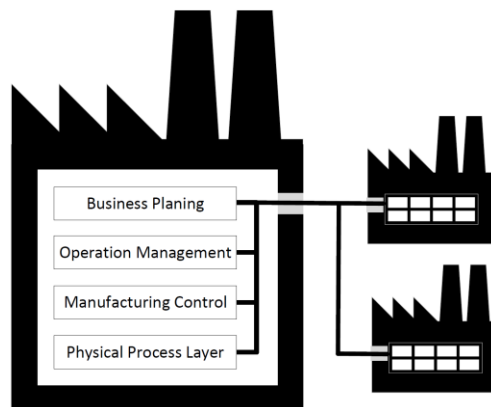


Abbildung 2: Vernetzung in modernen Anlagen.

Die verschiedenen Schichten sind über verschiedene Bus-Technologien miteinander verbunden. In modernen Anlagen basieren diese zunehmend auf IE-Technologien, die schnellere Datenübertragungsraten ermöglichen [15]. In einer traditionellen Konfiguration für die OT-Kommunikation werden die verschiedenen Schichten, abgesehen von der Verwendung anderer Technologien wie Modbus oder CAN, einzeln miteinander verbunden, d. h., es findet keine Verbindung zwischen den Schichten statt [19]. Im modernen Fertigungsparadigma von Industrie 4.0 nimmt die Vernetzung zwischen den Schichten jedoch zu und durchdringt die einzelnen Schichten des Anlagenbetriebs [20]. Wie in Abbildung 2 dargestellt, setzt sich dieser Trend in Richtung einer Vernetzung von Anlagen untereinander über öffentliche Netzwerke fort wie beispielsweise das Internet. Aus Sicht der Sicherheit erhöht dies die Angriffsfläche einer einzelnen Anlage erheblich [21].

Dieses Papier befasst sich mit der dringenden Notwendigkeit verbesserter Sicherheitsmaßnahmen in industriellen Systemen. Es erörtert, wie Sicherheitsprobleme innerhalb von Industrial-Ethernet-Protokollen identifiziert und Strategien zu ihrer Minderung umgesetzt werden können. Das Papier veranschaulicht dies anhand einer detaillierten Fallstudie zu einem sicherheitsrelevanten Thema, die nicht nur häufige Schwachstellen aufzeigt, sondern auch praktische Lösungen zu deren Behebung vorschlägt.

Unsere Beiträge in diesem Artikel lassen sich wie folgt zusammenfassen: Zunächst zeigen wir, wie sichere industrielle Netzwerke mit einem systematischen Ansatz aufgebaut werden können, der auf die Entwicklung sicherer industrieller Netzwerke und deren spezifische Anforderungen in Bezug auf branchenspezifische Umgebungen zugeschnitten ist. Zweitens veranschaulichen wir, wie häufige Sicherheitsprobleme identifiziert werden können. Schließlich zeigen wir anhand von Beispielen aus der Praxis und unserer Erfahrung im Bereich OT-Sicherheit, wie praktische Maßnahmen zur Sicherung von Systemen, die an industrielle Ethernet-Busse angeschlossen sind, ergriffen werden können. Das Ziel dieses Artikels ist es, als Referenz für OT-Fachleute und industrielle Netzwerkingenieure zu dienen und aufzuzeigen, wie robuste und sichere Netzwerkarchitekturen für den Einsatz in industriellen Betrieben entwickelt werden können.

1.1.9 Group Key Agreement auf Bussen von Cyber-physischen Systemen

Aufgabenstellung. In modernen Cyber-Physischen Systemen (CPS), wie Automotive- oder industriellen Busumgebungen (z. B. CAN, PROFIBUS, Automotive/Industrial Ethernet) müssen zahlreiche eingebettete Geräte über Broadcast- und teils half-duplex Links sicher miteinander

kommunizieren. Für die Integrität und Authentizität der Busnachrichten werden gruppenweit geteilte Schlüssel für Message Authentication Codes (MACs) benötigt. Klassische Ansätze mit fest vorverteilten Schlüsseln oder Trust-on-First-Use (TOFU) sind hierfür zu unsicher; paarweise Protokolle wie Transport-Layer-Security (TLS) skalieren in Gruppen nicht und widersprechen dem Broadcast-Paradigma. Die Aufgabe besteht daher darin, ein authentifiziertes, vollständig verteiltes Group Key Agreement (GKA) zu ermöglichen, das unter typischen CPS-Busrestriktionen funktioniert. Dazu werden ein buszentriertes Systemmodell und konkrete Sicherheits- und Praktikabilitätsanforderungen abgeleitet, existierende GKA-Ansätze systematisiert und gegen diese Anforderungen bewertet.

Zielsetzung. Ziel ist die Entwicklung, Implementierung und Evaluation eines GKA-Protokolls, das ohne zentrale Dienste auskommt, Bus-agnostisch ist und für größere Gruppen effizient skaliert. Das Protokoll soll:

- Die Authentizität der Gruppenteilnehmer sicherstellen und den Integritätsschutz von Nachrichten via MACs ermöglichen.
- Dynamische Gruppenoperationen (Beitreten und Verlassen) unter Broadcast-Bedingungen unterstützen.
- Forward Secrecy (FS) und Post-Compromise Security (PCS) erreichen.
- Kryptografische Agilität bieten, um über den Lebenszyklus die kryptografischen Verfahren wechseln zu können.
- Ressourcenbedarf (Rechenzeit, Speicher, Bandbreite) minimieren und auf den Einsatz in kostensensitiven, langlebigen CPS passen.

Neben dem Nachweis der technischen Machbarkeit unter realistischen Busrestriktionen wird die Sicherheitswirkung gegenüber dem Dolev-Yao-Modell analysiert.

1.1.10 Relevanz des OWASP MASVS für die Automobilindustrie

Die zunehmende Digitalisierung und Vernetzung moderner Fahrzeuge führt zu einer erheblichen Ausweitung sicherheitskritischer Systemkomponenten. Mobile Anwendungen fungieren heute als zentrale Schnittstelle zwischen Fahrzeug, Backend-Infrastruktur und Nutzer und übernehmen Funktionen, die von der Abfrage diagnostischer Daten über die Verwaltung digitaler Schlüssel bis zur Fernsteuerung von Komfort- und Sicherheitsfunktionen reichen [22]. Vor diesem Hintergrund wird die Absicherung dieser mobilen Applikationen zu einem integralen Bestandteil der übergreifenden automobilen Sicherheitsarchitektur.

Die technologische Entwicklung hin zu vernetzten und softwaredefinierten Fahrzeugen sorgt zugleich dafür, dass mobile Endgeräte und die darauf ausgeführten Applikationen zunehmend als funktionale Erweiterung des Fahrzeugs betrachtet werden. Sicherheitslücken in mobilen Anwendungen können unmittelbare Auswirkungen auf Fahrzeugfunktionen und den Schutz personenbezogener Daten haben. Ein systematisches und standardisiertes Vorgehen zur Absicherung dieser Anwendungen ist daher notwendig, um Risiken entlang der gesamten digitalen Fahrzeugkette zu minimieren.

Ziel dieses Dokuments ist es zu betrachten, inwieweit der Open Worldwide Application Security Project (OWASP) Mobile Application Security Verification Standard (MASVS) [23] für den Einsatz in der Automobilindustrie relevant ist. Dabei wird untersucht,

- welche inhaltlichen Anforderungen der MASVS abdeckt,

- wie diese Anforderungen typische Risiken mobiler Automotive-Anwendungen adressieren,
- wie der MASVS in sicherheitstechnische Prozesse der Fahrzeugindustrie eingebettet werden kann,
- und welche Grenzen bei seiner Anwendung bestehen.

Die Betrachtung trägt dazu bei, die Rolle des MASVS im Zusammenspiel von Fahrzeug, Backend-Systemen und mobilen Anwendungen nachvollziehbar darzustellen.

1.1.11 Sicherheit von Ortungsdiensten

Standortdienste sind heute elementarer Bestandteil zahlreicher Anwendungen, von Navigation-Diensten über Tracking in der Logistik bis hin zu Assistenz- und Automatisierungsfunktionen. Gleichzeitig häufen sich Stör- und Spoofing-Vorfälle bei GNSS in sicherheitskritischen Bereichen, wie z. B. in der Luftfahrt über dem Nahen Osten und der Schwarzmeer-Region. Dabei besteht bei GNSS eine zentrale Herausforderung: Zivil genutzte GNSS-Signale sind öffentlich spezifiziert, unverschlüsselt und nicht authentisiert. Ein Angreifer kann daher mit vergleichsweise geringem Aufwand stärkere oder manipulierte Signale aussenden und die Entfernungs- und Zeitmessungen verfälschen. Die Folge sind falsche Positionslösungen.

Gleichzeitig verlassen sich moderne Endgeräte nicht mehr ausschließlich auf GNSS. Sie berechnen Positionen in der Regel aus mehreren Informationsquellen, wie GNSS, Mobilfunk-/WLAN-Fingerprints, und Sensorik. Diese Daten werden durch proprietäre Fusionslogiken zusammengeführt. Auf Android ist der empfohlene Anbieter der Google Fused Location Provider (FLP). Dessen konkrete Entscheidungs- und Priorisierungslogik ist nicht öffentlich dokumentiert und funktioniert für externe Beobachter als „Black Box“. Die zentrale Problemstellung lautet daher: Wie vertrauenswürdig ist die von handelsüblichen, netzwerkfähigen Geräten gelieferte Position im Hinblick auf Manipulation und sicherheitskritische Anwendungen?

Ziel der Arbeit ist es, diese Black Box systematisch zu beleuchten. Dazu wird ein Testbed entwickelt, das sowohl GPS-Spoofing als auch den Betrieb eigener GPRS- und LTE-Testnetze ermöglicht. Mit diesem Aufbau sollen

- (1) die praktische Umsetzbarkeit von GNSS- und Netz-Spoofing demonstriert werden
- (2) die Protokoll- und Traffic-Nutzung von A-GNSS auf Android (insbesondere SUPL auf der User Plane sowie chipherstellerspezifische PSDS/XTRA-Downloads) analysiert werden
- (3) die grundlegende Quellenpriorisierung und Entscheidungslogik des FLP empirisch abgeleitet werden
- (4) die resultierende Vertrauenswürdigkeit der Positionsangabe bewertet werden

Begleitend werden Sicherheits- und Datenschutzimplikationen (u. a. IMSI-Übertragung, TLS/Cipher) untersucht und wirksame Gegenmaßnahmen eingeordnet.

Aus diesen Zielen leiten sich die zentralen Forschungsfragen ab:

- Wie einfach ist es, Mobilfunknetze und GNSS-Standorte zu manipulieren?
- Wie und in welchem Zusammenhang werden Protokolle des Assisted Global Navigation Satellite System (A-GNSS) in Android-Smartphones eingesetzt?
- Haben diese Protokolle Auswirkungen auf den Datenschutz oder die Sicherheit?

- Wie ermittelt Google Fused Location Provider die angegebene Position und wie zuverlässig ist diese?
- Welche Gegenmaßnahmen zum Schutz vor Standortmanipulationen gibt es?

1.1.12 Bereichsübergreifendes Security-Risikomanagement in der Automobilindustrie: Anforderungen und aktuelle Praktiken

1.1.12.1 Standards und Experteninterviews

Die Integration neuer Technologien in moderne Fahrzeuge erfordert die Zusammenarbeit mehrerer Bereiche. Ein Paradebeispiel ist die sichere Over-the-Air-Softwareaktualisierung für elektrische und elektronische (E/E) Systeme [24, 25]:

- Die Fahrzeugentwicklung erstellt das Software-Update.
- Der Backend-Services-Bereich verwaltet die Paketierung, digitale Signatur und Verteilung des Updates.
- Die Produktion überwacht die sichere Generierung und den Import von kryptografischem Schlüsselmaterial in E/E-Systeme während der Fertigung, um die Signaturprüfung in der Betriebsphase des Fahrzeugs zu ermöglichen [26].

Solche bereichsübergreifenden Prozesse und ständigen technologischen Fortschritte bringen neue Cyberrisiken mit sich, die systematisch gemanagt werden müssen. Zu diesem Zweck bietet ISO/SAE 21434 [27] Leitlinien für die Cybersicherheit in E/E-Systemen, während die ISO/IEC 27000 [28] und IEC 62443 [29] sich jeweils mit der Backend-Infrastruktur und den Produktionssystemen befassen [30]. Diese Normen bieten jedoch keine umfassenden Richtlinien für die Koordinierung des Cybersicherheitsrisikomanagements über Automobilsparten hinweg, sodass eine Lücke in der praktischen spartenübergreifenden Beratung besteht. Um diese Lücke zu schließen, untersucht dieser Artikel sowohl die Anforderungen als auch die aktuellen Praktiken des bereichsübergreifenden Cybersicherheitsrisikomanagements im Automobilsektor. Zunächst werden bestehende Normen analysiert, um relevante bereichsübergreifende Aspekte in Abschnitt 2.1.12.2 hervorzuheben. Anschließend werden die Ergebnisse von halbstrukturierten Interviews mit Cybersicherheitsrisikomanagementbeauftragten bei sechs verschiedenen Original Equipment Manufacturers (OEMs) vorgestellt, die reale Praktiken, Herausforderungen und Anforderungen in Abschnitt 2.1.12.3 aufzeigen. Abschließend werden wichtige Erkenntnisse und Prioritäten für zukünftige Forschungsarbeiten in Abschnitt 2.1.12.4 zusammengefasst.

1.1.12.2 Usability

In diesem Unterabschnitt sollen Erkenntnisse und Empfehlungen gesammelt werden, welche die Entwicklung eines SharePoint-basierten Tools für bereichsübergreifendes Risikomanagement unterstützen, indem Aspekte der Usability in den Vordergrund gerückt werden. Zu diesem Zweck sollen Anforderungen sowie Empfehlungen basierend auf existierender Literatur aufgeführt sowie aus Experteninterviews abgeleitet werden. Die Ergebnisse dieser Untersuchungen sollen helfen, die Weiterführung des Prototyps in eine vollständige Implementierung nach ATLAS-L4 in eine nutzendenfreundliche Richtung zu leiten.

1.1.13 Prototypisches Werkzeug für ein bereichsübergreifendes Security-Management

Die in den vorangegangenen Arbeitsschritten gewonnenen Erkenntnisse zur Methode der Security-Risikoanalyse (Abschnitt 1.1.1), zum Zusammenspiel von ISO/SAE 21434, ISO/IEC-27000-Familie und IEC-62443-Reihe (Abschnitt 1.1.2) sowie zu bereichsübergreifendem Security-Risikomanagement (Abschnitt 1.1.12) zeigen, dass Cybersicherheitsrisiken im automobilen Umfeld nur dann konsistent gesteuert werden können, wenn Fahrzeug-CSMS, Backend-ISMS und Produktions-Security-Programme gemeinsam betrachtet werden. In der Praxis beruhen die zugrunde liegenden Risikoanalysen jedoch häufig auf verteilten Excel-Templates, In-sellösungen in einzelnen Bereichen und nicht integrierten Werkzeugen.

Ziel des Arbeitsschritts „Prototypisches Werkzeug für ein bereichsübergreifendes Security-Management“ war es daher, ein initiales, praxisnahes Werkzeug zu entwickeln, das

- die im Projekt eingesetzte MoRA-Methode nicht nur als Excel-Template, sondern als gemeinsam nutzbare Datenbasis abbildet,
- Ergebnisse aus Security-Risikobewertungen für unterschiedliche Targets of Evaluation (TOE) vergleichbar und nachverfolgbar macht,
- Verantwortlichkeiten (z. B. Risk Owner, Control Owner) bereichsübergreifend sichtbar und über das Unternehmens-Active-Directory zuweisbar macht und
- darüber hinaus die Erfüllung regulatorischer und normativer Anforderungen (u. a. UN R155, ISO/SAE 21434, ISO/IEC 27001:2022, IEC 62443) unterstützt.

Ein zentrales Ziel bestand darin, dieses Werkzeug bewusst frühzeitig – also noch vor einer vollständigen, detaillierten Anforderungsspezifikation – als Prototyp aufzubauen. So sollte es den Experteninterviewpartnern als ein greifbares Artefakt zur Verfügung stehen, das den Mehrwert eines bereichsübergreifenden Security-Managements unmittelbar erfahrbar macht und gleichzeitig als Diskussionsgrundlage zur weiteren Anforderungsgewinnung dient.

Als technische Basis wurde Microsoft 365 mit SharePoint Online, Power Apps und Power Automate gewählt. Diese Plattform ist im industriellen Umfeld verbreitet, erlaubt die modellbasierte Abbildung komplexer Domänen in Listenstrukturen, integriert sich nahtlos in das bestehende Active Directory und stellt mit Power Automate eine Low-Code-Umgebung für Workflows zur Verfügung. Für ATLAS-L4 sollte damit geprüft werden, inwieweit eine solche Standardplattform ausreicht, um ein CSMS-nahes, bereichsübergreifendes Werkzeug aufzubauen, ohne zunächst eine dedizierte Spezialsoftware einzuführen.

Fachlich sollte der Prototyp drei Ebenen zusammenführen:

- die MoRA-Artefakte der Security-Risikoanalysen für ADS und Control Center (Funktionen, Daten, Komponenten, Datenflüsse, Schadensszenarien, Schutzziele, Bedrohungen, Maßnahmen, Annahmen, Risiken),
- TOE-bezogene Verantwortlichkeiten und Perspektiven (z. B. pro TOE verantwortliche Personen, persönliche Übersichten „My Risks“) sowie
- normbasierte Compliance-Anforderungen (z. B. ausgewählte Anforderungen aus UN R155, ISO/SAE 21434, ISO/IEC 27001, IEC 62443) inklusive deren Zuordnung zu TOEs und Verantwortlichen.

Auf dieser Grundlage sollte ein zentrales „Cockpit“ entstehen, in dem Security-Verantwortliche für einen ausgewählten TOE die relevanten Architektur- und Risikoartefakte einsehen, bereichsübergreifende Abhängigkeiten nachvollziehen und sowohl Risiko- als auch Compliance-Status pflegen können. Ergänzend sollten personalisierte Sichten (z. B. „My Risks“, „My Compliance“) entstehen.

Rollen wie Risk Ownern oder Process Ownern erlauben, ihre jeweils eigenen Aufgaben über das gleiche Werkzeug zu verwalten.

Begleitend war vorgesehen, Erkenntnisse aus den Experteninterviews zum bereichsübergreifenden Security-Risikomanagement (Abschnitt 1.1.12) sowie aus der Usability-Analyse (Abschnitt 1.1.12.2 und 1.4.11.2) systematisch in Gestaltung und Bedienkonzept des Prototyps einfließen zu lassen. Der Arbeitsschritt sollte somit nicht nur ein technisches Artefakt liefern, sondern auch aufzeigen, wie ein praxisnahes, nutzendenfreundliches Werkzeug als Enabler für ein harmonisiertes CSMS/ISMS/IACS-Security-Programm dienen kann.

1.1.14 Entwicklung öffentlich verfügbarer Testtools für Fahrzeugdiagnose

Methoden und Tools müssen nicht nur für das Risikomanagement während der Design- und Entwicklungsphasen von autonomen Lkw eingesetzt werden, um holistische Security zu erreichen, sondern auch in den Testphasen. Das Fraunhofer AISEC entwickelte in vorangegangenen Projekten das öffentlich verfügbare und quelloffene Testsystem gallia [31] für Steuergeräte in automobilen Fahrzeugen basierend auf dem herstellerübergreifenden Unified Diagnostic Services (UDS) Standard gemäß ISO 14229 [32]. Auf diesem Protokoll basiert auch das für Nutzfahrzeuge vorgeschriebene WWH-OBd Diagnoseprotokoll gemäß ISO 27145 [33].

Im Rahmen des Projekts sollte das Testtool um weitere Funktionen erweitert werden, um unter anderem die Unterstützung für die Diagnose von Nutzfahrzeugen zu verbessern. Dazu sollten zusätzliche Diagnosetransportprotokolle implementiert oder deren bestehende Implementierung erweitert werden, um den Umfang an unterstützten Fahrzeugen und Bussystemen zu erweitern. Zusätzlich sollten im Rahmen des Projekts auch Teile des Codes erneuert werden, um zukünftig leichter Testskripte zu entwickeln, welche mehrere Tests programmatisch und strukturiert verbinden können, wodurch etwa die Automatisierung von Testabläufen vereinfacht wird. Die im Rahmen des Projekts erfolgten Änderungen sollten dabei auch wieder an das Open-Source Projekt zurückgespielt und damit für die Öffentlichkeit zugänglich gemacht werden.

1.1.15 Entwicklung eines Testsystems für Ladekommunikation in E-Fahrzeugen

Der Verkehrssektor gilt als einer der Hauptemittenten von klimaschädlichen Gasen. Entsprechend ist die Elektrifizierung des Straßenverkehrs ein wesentlicher Faktor auf dem Weg zur Klimaneutralität. Die Entwicklung hin zu batterieelektrischen Antrieben betrifft dabei Fahrzeuge aller Größen, von PKWs über Busse, hin zu Trucks.

Da sich die entsprechenden Schnittstellen, d. h. die Ladebuchsen, an der Außenhaut der Fahrzeuge befinden, können sie von Angreifern als potenzielles Einfallstor zum restlichen Fahrzeugsystem genutzt werden, um sich dort auszubreiten. Auch über kompromittierte Ladestellen können sich Angreifer Zugang zu dieser Schnittstelle verschaffen. Folglich ist sicherzustellen, dass die digitale Ladeschnittstelle keine ungeschützten Dienste exponiert und dass die Implementierungen der Ladesysteme resistent gegen böswillig erzeugte Nachrichten sind. Um diese Kriterien zu überprüfen, werden Testsysteme benötigt, welche ähnlich einem potenziellen Angreifer, über die Ladeschnittstelle mit dem Fahrzeug kommunizieren und dieses dabei auf potenzielle Schwachstellen untersuchen. Etwa indem analog zu etablierten Testvorgängen in IT-Systemen, dessen Funktionalitäten enumeriert werden, um Testern einen Überblick über die Angriffsoberfläche zu geben.

Da derartige Testsysteme zum Projektbeginn nicht existierten, war es ein Ziel innerhalb des Forschungsprojektes ein Tool zu erstellen, mit welchem Tests bezüglich der IT-Sicherheit von

Ladeschnittstellen von elektrischen Fahrzeugen durchgeführt werden können, um so Schwachstellen identifizieren und folglich die Sicherheit der Systeme verbessern zu können.

Ferner war es ein Ziel, das Testsystem mit realen Fahrzeugen zu evaluieren. Um auch Tests, welche mehrere Ladevorgänge erfordern, abdecken zu können, musste eine Platine entwickelt werden, welche neben der in IEC 61851 [34] beschriebenen Signalisierung der Verwendung von High-Level Kommunikation, auch ein programmatisches Ein- und Ausstecken des Ladesteckers ermöglicht.

1.1.16 Entwicklung eines Test-Frameworks für V2X

V2X-Kommunikation findet zunehmende Verbreitung in modernen vernetzten Fahrzeugen. Sie erlaubt den Austausch von Echtzeit-Informationen zwischen Fahrzeugen und Infrastruktur, um den Verkehrsfluss zu steuern oder Teilnehmer zu warnen. Während dies offensichtlich Vorteile für den Verkehr bietet, eröffnet es gleichzeitig eine neue Angriffsfläche bei Fahrzeugen oder Road Side Units (RSU).



Abbildung 3: Beispielhafte C-ITS Warnung für ein stehendes Fahrzeug [35]

Bisher existieren jedoch keine Test-Frameworks, die es erlauben aus der Security Sicht mit C-ITS zu interagieren und On-Board-Units (OBUs) und RSUs zu analysieren. Daher war es ein Ziel innerhalb des Forschungsprojektes ein Test-Framework für C-ITS zu entwickeln, um aktive Sicherheitsanalysen durchzuführen und damit die Sicherheit von V2X-Komponenten zu erhöhen.

1.1.17 Modul-Baukasten Woodpecker zur statischen Code Analyse

Mit der steigenden Komplexität der Software auf Steuergeräten in autonomen Lkw nimmt auch die Anzahl potenzieller Schwachstellen zu. Ein frühes Erkennen ist daher essenziell. Die Integration von Analyse-Tools in die Entwicklungs-Toolchain und das Durchführen von Security Code Reviews bereits in der Implementierungsphase sind zentrale Maßnahmen. Das Fraunhofer AISEC hat hierfür den Modul-Baukasten Woodpecker ([s.fhg.de/woodpecker](https://www.fhg.de/woodpecker)) entwickelt, der öffentlich verfügbare Static Application Security Testing (SAST) Tools bündelt und für eingebettete Systeme optimiert. Damit leistet Woodpecker im Arbeitspaket Security von ATLAS-L4 einen direkten

Beitrag zur frühzeitigen Identifikation von Schwachstellen und damit zur sicheren Umsetzung einer L4-tauglichen Fahrzeugarchitektur.

Vorarbeiten: Woodpecker wird über mehrere Jahre am AISEC entwickelt und liegt in einer funktionsfähigen Version vor. Zur Unterstützung des Review-Prozesses existiert ein VS-Code-Plugin zur Visualisierung der Findings.

Ziele im Kontext von ATLAS-L4:

- Nutzbarmachung für die Automotive-Domäne, u. a. durch domänenspezifische CWE-Kategorien.
- Unterstützung von Windows als Plattform, wie sie in der Automotive-Entwicklung verbreitet ist.
- Demonstration der Umsetzung an relevanten Open-Source-Projekten (mbedtls, COVESA vsomeip).

Durch diese Zielsetzungen wird Woodpecker konkret auf die Anforderungen der Automotive-Domäne zugeschnitten und damit für die Entwicklung sicherer, automatisierter Lkw nutzbar gemacht.

1.1.18 Security-Risikoanalyse eines automatisierten Fahrsystems

Derzeit wird intensiv an der Nutzung von automatisierten Fahrsystemen (Automated Driving Systems, ADS) geforscht [36, 37]. Insbesondere im Lkw-Bereich scheint der Einsatz von ADS der Stufe 4 gemäß SAE J3016 [38] unvermeidlich, da die Zahl der Lkw-Fahrer in den letzten Jahren stark zurückgegangen ist [39]. In Deutschland wurde 2021 ein Gesetz verabschiedet, das den Betrieb autonomer Fahrzeuge in zugelassenen Verkehrsbereichen unter bestimmten Bedingungen erlaubt, beispielsweise unter der technischen Aufsicht durch ein autonomes Control Center (CC) [40].

Der Einsatz neuer Technologien bringt neue Cyberrisiken mit sich. Die UN-Regelung Nr. 155 [41] und die internationale Norm ISO/SAE 21434 [42] bieten einen grundlegenden Rahmen für den Umgang mit diesen Cyberrisiken im Automobilbereich. Es fehlen jedoch konkrete Leitlinien dazu, wie ADS der Stufe 4 vor Cyberangriffen geschützt werden sollten, insbesondere im Hinblick auf den Hub-to-Hub-Transport und vernetzte und autonome Lkw. Wir möchten diese Lücke schließen, indem wir die Ergebnisse einer Cybersicherheits-Risikoanalyse (Cybersecurity Risk Assessment, CRA) vorstellen, die wir für ein CC-überwachtes ADS der Stufe 4 für Lkw unter Verwendung der modularen Risikobewertungsmethode (Modular Risk Assessment, MoRA) [1] durchgeführt haben.

Zu diesem Zweck geben wir in Abschnitt 2.1.18.2 eine Einführung in die MoRA-Methode. Anschließend präsentieren wir in Abschnitt 2.1.18.3 die Ergebnisse unserer CRA, beginnend mit der Definition des Systemmodells. Anschließend werden Schadensszenarien beschrieben, die durch Cyberangriffe auf das Systemmodell verursacht werden können. Darüber hinaus werden Annahmen zum Umfang und zum Angreifer-Modell sowie zu Schutzmaßnahmen und deren Auswirkungen detailliert beschrieben. Anschließend stellen wir die Risiken vor und zeigen, welche Schutzmaßnahmen implementiert werden sollten, um diese auf ein akzeptables Maß zu reduzieren. Abschließend fassen wir unsere Ergebnisse zusammen und beschreiben in Abschnitt 2.1.18.4 die Prinzipien, die wir aus unserer CRA abgeleitet haben und die auf andere CRAs von ADSs angewendet werden können.

1.1.19 Security-Risikoanalyse eines Control Centers

Aufbauend auf der in Abschnitt 1.1.1 beschriebenen, für ATLAS-L4 angepassten MoRA-Methode wurde eine detaillierte Security-Risikoanalyse für das cloudbasierte Control Center durchgeführt. Ausgangspunkt war ein gemeinsam mit MAN und weiteren Partnern erarbeitetes Systemmodell, das Komponenten wie Vehicle Adapter Service, Command Service, Routing- und Flottenmanagement, Control-Center-Frontend, Backend-Services sowie deren Anbindung an die AWS-Cloud und externe Partner abbildet.

Für diese Architektur wurden Schadensszenarien, Schutzziele und Bedrohungsszenarien identifiziert und bewertet. Besondere Aufmerksamkeit galt dabei Risiken, die den Betrieb der Fahrzeugflotte, die Auslösung von MRMs oder die Routenplanung beeinflussen, sowie die Offenlegung von Video- und Bewegungsdaten betreffen. Auf Basis der Bewertung wurden technische und organisatorische Schutzmaßnahmen abgeleitet (z. B. Ende-zu-Ende-Authentisierung und -Verschlüsselung, Härtung internetexponierter Dienste, Resilienzkonzepte), mit denen sich die Risiken auf ein akzeptables Niveau reduzieren lassen und die als Security-Anforderungen in die Control-Center-Architektur und das Betriebsmodell einfließen.

1.2 Voraussetzungen

Das Vorhaben konnte unter sehr günstigen fachlichen und organisatorischen Voraussetzungen durchgeführt werden. Auf Seiten des Fraunhofer AISEC standen langjährige Erfahrungen in den Bereichen Automotive-Security, Industrial/OT-Security, Kryptographie und Security-Engineering zur Verfügung, einschließlich etablierter Methoden wie Modular Risk Assessment (MoRA) sowie vorhandener Werkzeuge (u. a. gallia, Woodpecker, OT-Testbeds).

Durch die enge Zusammenarbeit mit MAN und weiteren ATLAS-L4-Partnern lagen frühzeitig Systemkonzepte, Architekturentwürfe und Use-Case-Beschreibungen für den L4-Lkw und das Control Center vor, die als Grundlage für die Risikoanalysen genutzt werden konnten. Die erforderliche technische Infrastruktur (Labore, Entwicklungs- und Testumgebungen, Zugriff auf Cloud-Ressourcen) war vorhanden. Regulatorischer und normativer Rahmen (UN R155/R156, ISO/SAE 21434, ISO/IEC 27001/27005, IEC 62443, EU-Digitalregulierung) war zum Projektstart weitgehend bekannt, sodass konkrete Bezüge hergestellt werden konnten.

1.3 Planung und Ablauf des Vorhabens

Das Teilvorhaben „Security-Umfänge“ war in vier inhaltliche Phasen gegliedert, die zeitlich teilweise überlappten und überwiegend unabhängig voneinander bearbeitet werden konnten. Zwischen einzelnen Phasen bestanden gezielte inhaltliche Abhängigkeiten.

In **Phase 1** wurden die methodischen Grundlagen erarbeitet. Dazu zählten insbesondere die Weiterentwicklung der MoRA-Methode für den ATLAS-L4-Kontext (inkl. Bewertungsmodell, Schadenskriterien sowie Annahmen-, Bedrohungs- und Maßnahmenkatalogen) und die Aufarbeitung des Stands der Wissenschaft und Technik zu Security-Risikoanalysen im Automotive-Umfeld.

Parallel hierzu adressierte **Phase 2** den organisatorischen und regulatorischen Kontext. Schwerpunkte waren der vergleichende Standard- und Regulierungsvergleich (u. a. ISO/SAE 21434, ISO/IEC-27000-Familie, IEC-62443-Reihe, UNECE R155/R156, GB 44495-2024, NHTSA-Guidelines), die Analyse bereichsübergreifender Security-Risikomanagement-Praktiken (inkl. Experteninterviews) sowie Arbeiten zu querliegenden Themen wie Datenschutz und EU AI Act.

Auf den Ergebnissen von Phase 2 **baute Phase 3** auf: Hier wurde das prototypische Werkzeug für ein bereichsübergreifendes Security-Management konzipiert und in einer Microsoft-365-

Umgebung (SharePoint, Power Apps, Power Automate) umgesetzt. Die Erkenntnisse aus Standardvergleich, Interviews und Usability-Analyse flossen in Struktur, Datenmodell und Workflows des Prototyps ein.

In **Phase 4** wurden schließlich die in Phase 1 entwickelten Methoden praktisch angewendet. Kern waren die Security-Risikoanalysen für das automatisierte Fahrsystem und das Control Center sowie darauf aufbauende Security-Anforderungen für die ATLAS-L4-Partner. Die MoRA-Weiterentwicklung aus Phase 1 diente dabei als methodische Grundlage; die Nutzung des Werkzeugs aus Phase 3 und die Ergebnisse aus Phase 2 erfolgten punktuell unterstützend, ohne dass eine enge prozessuale Kopplung der Phasen notwendig war.

1.4 Stand der Wissenschaft und Technik zu Projektbeginn

Die Arbeiten im Teilvorhaben bauten auf einem breiten, bereits vor Projektbeginn vorhandenen Stand der Wissenschaft und Technik in den Bereichen Automotive-Security, Informationssicherheits-Management, OT-Security, Kryptographie sowie Privacy-Engineering auf. Im Rahmen von ATLAS-L4 wurde dieser Stand systematisch aufgearbeitet, um Lücken für L4-Nutzfahrzeuge mit Control Center zu identifizieren und gezielt adressieren zu können.

Die Literaturrecherche erfolgte überwiegend über Scopus, Web of Science und Google Scholar, ergänzt durch fachspezifische Dienste wie IEEE Xplore, ACM Digital Library und SpringerLink. Berücksichtigt wurden vor allem peer-reviewte Konferenz- und Zeitschriftenbeiträge aus den Bereichen Security & Privacy, Automotive, Cyber-Physical Systems und Internet of Things sowie einschlägige Normen und Regulierungstexte. Die folgenden Unterkapitel (1.4.1–1.4.18) fassen den für die jeweiligen Themen relevanten Stand von Wissenschaft und Technik zusammen und dienen als Referenzrahmen für die in Kapitel 2 beschriebenen Projektergebnisse. Am Ende von Kapitel 1.4 ist die Verwendete Fachliteratur aufgeführt, auf die im weiteren Verlauf des Berichts Bezug genommen wird.

1.4.1 Methode Security-Risikoanalyse

Zu Projektbeginn war Security-Risikoanalyse im Automotive-Umfeld bereits gut erforscht, jedoch überwiegend aus Sicht einzelner Domänen und häufig ohne durchgängige, modellbasierte Unterstützung. Klassische Ansätze wie Bedrohungsbäume, STRIDE-basierte Analysen oder Risiko-Frameworks nach ISO 31000/ISO/IEC 27005 liefern generische Konzepte, sind aber für die Anwendung auf komplexe Fahrzeug- und Backend-Systeme nur bedingt konkretisiert. Im Automobilbereich wurden in den letzten Jahren verschiedene sicherheitsspezifische Methoden vorgeschlagen, u. a. RACE [43] und SARA [44], SAHARA [45] oder FMVEA [46]. Diese Ansätze kombinieren HARA-/FMEA-Denken mit Threat Modeling, fokussieren aber meist einzelne Schichten (z. B. E/E-Architektur oder Kommunikationsprotokolle) und behandeln die Integration in OEM-interne Entwicklungsprozesse nur am Rande.

Parallel dazu haben Normen und Regulierung die Notwendigkeit systematischer Security-Risikoanalysen deutlich verschärft. ISO/SAE 21434 fordert TARA-basierte Analysen über den gesamten Produktlebenszyklus [27]; UN R155 macht ein wirksames Cybersecurity-Risikomanagement zur Zulassungsvoraussetzung [5]. IEC 62443 verlangt risikobasierte Zonierung und Security Levels für OT-Systeme [47], und die ISO/IEC-27000-Familie etabliert generische Prozesse für Informationssicherheits-Risikomanagement [48]. Diese Vorgaben lassen jedoch bewusst offen, mit welchen konkreten Methoden OEMs Risiken modellieren und bewerten sollen – insbesondere dort, wo Fahrzeug-, IT- und OT-Domänen ineinandergreifen.

Vor diesem Hintergrund wurde am Fraunhofer AISEC das Modular Risk Assessment (MoRA) entwickelt und in mehreren Publikationen beschrieben [1, 2]. MoRA verfolgt einen modellbasierten Ansatz, bei dem das „System under Development“ (SUD) zunächst als Zusammenspiel von Funktionen, Daten, Komponenten und Datenflüssen beschrieben wird. Darauf aufbauend werden Security-Goals (Schutzziele für Assets), Damage Scenarios (Schadensszenarien in den Kategorien Safety, Financial, Operational, Privacy), Threats (Bedrohungen), Controls (Maßnahmen) und Annahmen in einem einheitlichen Metamodell erfasst. Das Risiko ergibt sich – im Sinne von ISO/SAE 21434 – aus der Kombination von Impact-Bewertungen und Attack-Feasibility-Ratings.

Die Besonderheit von MoRA liegt in der expliziten Abbildung der Abhängigkeiten zwischen diesen Elementen: Schutzziele können voneinander abhängen, Threats setzen sich aus vorbereitenden und eigentlichen Angriffsschritten zusammen, Controls und Annahmen wirken auf Threats und/oder transformieren Schadensszenarien. Angermeier et al. zeigen, dass sich diese Zusammenhänge als gerichteter, azyklischer Graph modellieren lassen, auf dem Risk-Bewertungen lokal getroffen und dann konsistent über das Modell fortgeschrieben werden können [2]. Dadurch werden einerseits typische Lücken (vergessene Assets, unvollständige Pfade) reduziert, andererseits bleibt die Methode nahe an den Artefakten der Systementwicklung (Architektur, Datenflüsse, Funktionslisten).

In der Praxis wurde MoRA vor ATLAS-L4 bereits bei einem OEM im Nutzfahrzeugbereich eingesetzt, allerdings primär für Steuergeräte und klassische Fahrzeugfunktionen. Eine systematische Erweiterung auf ein L4-ADS mit Control-Center-Anbindung, Cloud-Infrastruktur und Office-/Backend-IT lag zum Projektstart noch nicht vor. Ebenso fehlten katalogisierte Annahmen, Bedrohungen und Maßnahmen, die sowohl Automotive-E/E- als auch IT-/Cloud-Domänen abdecken und sich zugleich in ISO/SAE-21434-konforme TARA-Prozesse integrieren lassen.

Das ATLAS-L4-Projekt knüpft genau an diese Lücke an: Die vorhandene MoRA-Methode wurde an die Normlandschaft (insb. ISO/SAE 21434 und ISO/IEC 27005) angeglichen, auf den Kontext „L4-Truck plus Control Center“ zugeschnitten und so erweitert, dass sie als durchgängige, wiederverwendbare Vorgehensweise für die in ATLAS-L4 durchgeführten Security-Risikoanalysen dienen konnte.

1.4.2 Übergreifender Vergleich von ISO/SAE 21434, ISO/IEC 27000 Familie und IEC 62443 Reihe

Zu Projektbeginn lagen mit ISO/SAE 21434, der ISO/IEC-27000-Familie und der IEC-62443-Reihe drei weit verbreitete, aber historisch getrennt gewachsene Normenwelten vor, die jeweils unterschiedliche Teile des automobilen Ökosystems adressieren.

- **ISO/SAE 21434** [27] wurde 2021 veröffentlicht und adressiert explizit die Cybersicherheit im Engineering von elektrischen/elektronischen (E/E-) Systemen in Straßenfahrzeugen. Die Norm definiert Anforderungen an ein Cybersecurity-Managementsystem (CSMS), an TARA-basierte Risikoanalysen und an den gesamten Produktlebenszyklus. Systeme außerhalb des Fahrzeugs – etwa Backend-Server oder Produktionsanlagen – werden zwar als „operational environment“ berücksichtigt, fallen aber nicht in den eigentlichen Normumfang. Über die UN-Regelung Nr. 155 ist ISO/SAE 21434 indirekt typgenehmigungsrelevant.
- **Die ISO/IEC-27000-Familie** [28, 49, 50, 48] stellt seit Anfang der 2000er-Jahre den faktischen Standard für Informationssicherheits-Managementsysteme dar. ISO/IEC 27001 definiert generische Anforderungen an ein ISMS, während ISO/IEC 27002, 27003 und 27005 u. a. Schutzmaßnahmen, Implementierungsleitlinien und ein strukturiertes Vorgehen zum Management

von Informationssicherheitsrisiken beschreiben. Die Normen sind bewusst branchenneutral formuliert und können auf beliebige Organisationen und Informationswerte angewendet werden, von Backend-Infrastrukturen über Office-IT bis hin zu datengetriebenen Mobilitätsdiensten.

- **Die IEC-62443-Reihe** [29, 47, 51] adressiert die Sicherheit von Industrial-Automation- and-Control-Systemen (IACS) – also OT-Umgebungen wie Fertigungsanlagen, Prozessleitsysteme und deren Vernetzung mit Unternehmens-IT. IEC 62443-2-1 beschreibt Anforderungen an ein IACS-Security-Programm für „asset owners“, IEC 62443-3-2 liefert eine Methode zur Risikobewertung und Zonierung von IACS-Systemen. Die Normen schreiben u. a. die Bildung von „Zonen“ und „Conduits“, Security Levels und eine klare Trennung zwischen IACS- und Nicht-IACS-Bereichen vor.

In der wissenschaftlichen Diskussion lagen bereits erste Übersichten und Vergleiche von Cybersicherheitsstandards vor. Schmittner und Macher [30] ordnen ISO/SAE 21434 u. a. gegenüber IEC 62443 ein, fokussieren aber primär auf automotiv E/E-Systeme und deren Konnektivität. Costantino et al. [52] analysieren ISO/SAE 21434 im Vergleich zu anderen Normen und zeigen insbesondere deren Verknüpfung zu ISO 26262 und UN R155. Djebbar und Nordström [53] sowie Taherdoost [54] vergleichen verschiedene industrielle Cybersecurity-Frameworks, ohne jedoch die spezifische Kombination ISO/SAE 21434 – ISO/IEC 27000 – IEC 62443 im automobilen Kontext detailliert zu betrachten.

Parallel dazu formulierten die Standards bereits explizite oder implizite Anforderungen an **bereichsübergreifende Managementsysteme**:

- ISO/SAE 21434 verlangt u. a. die Abstimmung des CSMS mit einem vorhandenen Qualitätsmanagementsystem (z. B. IATF 16949/ISO 9001) und verweist für Produktionsprozesse beispielhaft auf IEC 62443-2-1 [27]. Teilweise wird explizit gefordert, Arbeitsergebnisse gemäß einem Informationssicherheits-Managementsystem zu verwalten.
- ISO/IEC 27001/27003 fordern, beim Aufbau eines ISMS den Kontext der Organisation, bestehende Managementsysteme und Schnittstellen zu anderen Organisationsteilen zu berücksichtigen. Die Risikokriterien sollen organisationsweit harmonisiert werden, um Risiken aus verschiedenen Geschäftsbereichen vergleichen und aggregieren zu können [49, 50].
- IEC 62443-2-1 schreibt vor, dass ein IACS-Security-Programm mit einem bestehenden ISMS koordiniert werden muss, um eine abgestimmte Verteidigungsstrategie zwischen IT und OT zu erreichen. Annex A und B der Norm verweisen explizit auf ISO/IEC 27001 und NIST-Rahmenwerke und fordern eine abgestimmte unternehmensweite Risikobetrachtung [51].

Trotz dieser Hinweise bestand zu Projektbeginn eine **Forschungslücke**: Es fehlte eine systematische, auf die Automobilindustrie zugeschnittene Gegenüberstellung der drei Normwelten, insbesondere

- eine harmonisierte Terminologie (z. B. Risiko, Bedrohungsszenario, Schaden/Damage Scenario) über alle Standards hinweg,
- ein klarer Vergleich der Risikobegriffe ($\text{Risk} = f(\text{Attack-Feasibility}, \text{Impact})$ in ISO/SAE 21434 vs. $\text{Risk} = f(\text{Likelihood}, \text{Consequence})$ in ISO/IEC 27005 und IEC 62443),
- eine strukturierte Darstellung der expliziten „cross-domain“- und „cross-management-system“-Anforderungen (z. B. verbindliche Schnittstellen zwischen CSMS, ISMS und IACS-Security-Programm) und

- darauf aufbauende konkrete Handlungsempfehlungen für OEMs und Zulieferer mit komplexen Backend- und Produktionslandschaften.

Bestehende Arbeiten zum bereichsübergreifenden Risikomanagement im Automobilsektor (vgl. Abschnitt 1.4.11 und [30, 55]) erkannten diese Lücke, boten aber noch keine fein granulierte Normenanalyse speziell dieser drei Standardfamilien. Vor diesem Hintergrund war es Ziel des hier vorgestellten Arbeitsschritts, erstmals einen **übergreifenden, normtextnahen Vergleich von ISO/SAE 21434, ISO/IEC-27000-Familie und IEC-62443-Reihe** zu erarbeiten und daraus konkrete Integrationspfade für die ATLAS-L4-Systemlandschaft abzuleiten.

1.4.3 Vergleichende Analyse der regulatorischen Anforderungen an die Cybersicherheit im Automobilbereich

Dieser Abschnitt bietet einen Überblick über bestehende akademische und technische Beiträge zu Vorschriften für die Cybersicherheit im Automobilbereich. Die Literatur lässt sich in drei Hauptkategorien unterteilen: Grundlagenarbeiten mit Schwerpunkt auf Normen, Forschung zu Implementierung und Tests sowie Erkenntnisse aus Industrie und Praxis. Ein zentraler Bezugspunkt für die Cybersicherheit im Automobilbereich ist die Norm ISO/SAE 21434. Obwohl es sich um eine unverbindliche Norm handelt, spielt sie eine grundlegende Rolle bei der Gestaltung von Rechtsrahmen in verschiedenen Regionen. Die USA verweisen in offiziellen Dokumenten auf ISO/SAE 21434 [56], die EU nimmt in der UN-Regelung R155 ausdrücklich darauf Bezug, und Chinas GB 44495-2024 zeigt eine konzeptionelle Übereinstimmung mit UNECE R155, die ihrerseits von den Grundsätzen der ISO/SAE 21434 beeinflusst ist. Die ISO/SAE 21434 wurde gemeinsam von der Internationalen Organisation für Normung (ISO) und der Society of Automotive Engineers (SAE) entwickelt und 2021 offiziell veröffentlicht. Sie definiert technische Anforderungen an die Cybersicherheit während des gesamten Lebenszyklus eines Fahrzeugs, vom Konzept über die Entwicklung bis hin zur Produktion, zum Betrieb und zur Stilllegung [57]. In vergleichenden Analysen wurde ISO/SAE 21434 neben der UNECE-Regelung R155 untersucht. Eine Studie hebt wichtige konzeptionelle Unterschiede hervor und kommt zu dem Schluss, dass ISO/SAE eine „Security-by-Design“-Philosophie betont, während UNECE R155 einen risikobasierten Regulierungsansatz verfolgt [58]. Über die Interpretation von Normen hinaus schlagen mehrere Beiträge konkrete Umsetzungsstrategien vor. Ein bemerkenswertes Beispiel ist Bohara et al., die sich mit der Unklarheit in den UNECE-Vorschriften befassen, insbesondere mit der Cyber Security Management System (CSMS) und Software Update Management System (SUMS), indem sie eine detaillierte Lösung für die Systemarchitektur vorschlagen, die die regulatorischen Anforderungen erfüllt und erweitert, mit Mechanismen zur Sicherung der Software-Lieferkette [59]. Eine weitere technische Perspektive bieten Han et al., die sich auf Cybersicherheitstests konzentrieren, die sowohl mit UNECE R155 als auch mit ISO/SAE 21434 übereinstimmen. Ihre Arbeit skizziert einen Testprozess, der auf die regulatorischen Anforderungen während der Fahrzeugentwicklung und der Typgenehmigungsphase zugeschnitten ist [60]. Neben technischen Beiträgen bieten einige Publikationen auch Branchenperspektiven. Der Artikel von Köllner für Springer [61] interpretiert beispielsweise die regulatorischen Auswirkungen von UNECE R155 auf OEMs und bietet eine praktische Branchenperspektive, die die akademischen und technischen Diskussionen ergänzt. Diese Perspektive wird im Bewertungsteil dieses Artikels erneut aufgegriffen. Neben begutachteten Arbeiten tragen auch öffentlich zugängliche Ressourcen zur Diskussion bei. So bietet beispielsweise ein Blog-Artikel von Kanmaz (2025), der auf der Plattform diconium veröffentlicht wurde [62], einen allgemeinen Überblick über globale und regionale Cybersicherheitsvorschriften. Er deckt zwar ein breites Spektrum an Standards und Rahmenwerken ab, bleibt jedoch

oberflächlich und lässt vergleichende Tiefe oder Kritik an der Umsetzung vermissen. Zusammenfassend lässt sich sagen, dass zwar mehrere Beiträge spezifische Rahmenwerke untersuchen oder Umsetzungsleitlinien anbieten, es der Literatur jedoch an einer vergleichenden und kritischen Analyse der Art und Weise mangelt, wie verschiedene Regionen Vorschriften zur Cybersicherheit im Automobilbereich umsetzen und durchsetzen. Dieser Beitrag zielt darauf ab, diese Lücke zu schließen, indem er einen strukturierten, regionenübergreifenden Vergleich liefert und operative Herausforderungen hervorhebt, die in der Praxis auftreten.

1.4.4 Technologien zum Schutz der Privatsphäre für vernetzte Automobilumgebungen

Der geplante Beitrag wird als Systematization of Knowledge (SoK) publiziert, wodurch der Hauptteil die relevante Fachliteratur zusammenfasst und diskutiert. Dadurch wird der Stand der Wissenschaft detailliert in den erzielten wissenschaftlich-technischen Ergebnissen dargestellt.

Unser Beitrag soll das Potenzial von PETs in der Domäne Automotive hervorheben. In modernen Fahrzeugen fällt eine Vielzahl von sensiblen Daten an, die einen entsprechenden Schutz benötigen. Grundlegende Paper zu dieser Thematik finden sich bereits in der bestehenden Literatur. Die Arbeit von Garrido et al untersuchte dazu industrielle Use Cases entlang der automobilen Wertschöpfungskette und gliedert deren Charakteristika mit den Fähigkeiten existierender PETs und Open-Source-Werkzeuge ab [63]. Das SoK-Paper von Bahrami et al bietet einen umfassenden Überblick über technische, rechtliche und ethische Herausforderungen bei der Monetarisierung von Fahrzeugdaten, inklusive Bedrohungsmodellen und Governance-Fragen [64].

Ergänzend fasst die Publikation von Yuca et al den Stand zu kryptographischen Verfahren wie Secure Multi-Party Computation und Homomorphic Encryption in unterschiedlichen automobilen Anwendungskontexten zusammen und zeigt sowohl Potenziale als auch bestehende Forschungslücken auf. In ihrem Forschungspapier wurde die Anwendbarkeit von SMPC in verschiedenen Use Cases analysiert. Jedoch fehlt ihnen die Betrachtung von Datenflüssen, die wir als besonders kritisch betrachtet haben [65].

Das Forschungspapier von Pape et al. zum Privatsphäre Management im Automotive Bereich, empfiehlt den Einsatz eines so genannten „Privacy Managers“, als generisches, anwendungsübergreifendes Konzept. Jedoch erläutern sie selbst, dass es für sie eine große Herausforderung war, ihren Privacy Manager anzuwenden, da es sehr Use Case spezifisch ist, welche Art des Betriebsmodus er einnehmen soll [66].

In der von unserer angestrebten Publikation wird abgrenzend dazu der aktuelle Forschungsstand der PETs für den Schutz von Daten in Fahrzeugen diskutiert. Dafür werden bestehende Taxonomien aus dem Bereich Datenschutz genutzt, um kritische Stellen der Datenverarbeitung im Fahrzeug zu identifizieren. Für diese Stellen werden geeignete PETs zum Schutz der Daten vorgeschlagen.

1.4.5 Einschätzung zu den Auswirkungen des EU AI Act auf ATLAS-L4

Hierzu wird im Folgenden der wissenschaftliche und technische Kontext skizziert, an den mit der im Rahmen des Arbeitsschritts verknüpften Analyse angeknüpft wird.

Der EU AI Act als zentrales Dokument des Arbeitsschrittes ist 2024 in Kraft getreten und etabliert einen EU-weit geltenden horizontalen Rechtsrahmen für den Einsatz von KI-Systemen, der insbesondere Hochrisiko-Anwendungen durch spezifische Anforderungen an Sicherheit, Transparenz,

Aufsicht und Governance adressiert [67]. Zentrales Leitprinzip ist dabei ein risikobasierter Ansatz: Der Umfang der regulatorischen Pflichten hängt vom jeweiligen Gefährdungspotenzial für Gesundheit, Sicherheit und Grundrechte ab, wobei insbesondere sicherheitskritische Anwendungen – wie automatisierte Fahrfunktionen – als Hochrisiko-KI klassifiziert werden. Einzelne Technikbereiche werden weiterhin durch sektorspezifische Regelwerke wie die Verordnung (EU) 2019/2144 zur Typgenehmigung von Kraftfahrzeugen und sicherheitsrelevanten Systemen konkretisiert, die u. a. Anforderungen an automatisierte und vollautomatisierte Fahrfunktionen formuliert und damit einen zentralen Bezugspunkt für die Einstufung fahrzeugseitiger KI-Komponenten bildet [68].

Parallel zur regulatorischen Entwicklung haben sich in Forschung und Industrie mehrere Rahmenwerke für die Bewertung und das Management von KI-Risiken herausgebildet. Systematische Übersichtsarbeiten zeigen, dass bereits eine breite Palette an AI-Risk-Assessment-Frameworks existiert, welche konkret im industriellen Kontext zum Einsatz kommen, und unterschiedliche Dimensionen von Risiko (z. B. Sicherheit, Robustheit, Fairness) adressieren [69]. Ergänzend existieren AI-Risk-Management-Frameworks wie das NIST AI RMF [70], Risk-Assessment Methoden wie MoRA [71]. Zudem sind mit der Verabschiedung des EU AI Act neue Methoden entstanden, welche die Einhaltung dieser Regularien durch entwickelte und eingesetzte KI-Systeme gewährleisten sollen [72, 73], teils wiederum unter Einsatz von generativer KI [74].

In dieses Umfeld reiht sich die vorliegende Arbeit ein, indem sie die abstrakten Vorgaben exemplarisch auf ein konkretes System – das ATLAS-L4-Lkw- und Control Centers-System – anwendet.

Schließlich wird der EU AI Act in der öffentlichen Diskussion auch mit Blick auf seine Auswirkungen auf Innovation und Schutz der Privatsphäre bewertet. Medien- und Verbandsbeiträge analysieren Chancen und Risiken des EU AI Act, diskutieren insbesondere mögliche Wettbewerbsnachteile für europäische Unternehmen durch umfangreiche Protokollierungs- und Dokumentationspflichten sowie dem Schutz von personenbezogenen Daten [75, 76, 77].

1.4.6 Sicherheit vernetzter Fahrzeugtechnologien im Nutzfahrzeugsektor

1.4.6.1 Grundlagen von V2V/V2X

Moderne Fahrzeuge besitzen heutzutage dank fortschreitender Kommunikationstechnologien weitreichende Möglichkeiten zur Kommunikation mit ihrer Umgebung. Dabei können Fahrzeuge nicht nur mit anderen Fahrzeugen kommunizieren, sondern auch mit Infrastruktur, Fußgängern, oder Cloud-Computing basierten Diensten. Der allgemeine Oberbegriff für diese Art von Kommunikation wird als Vehicle-to-everything (V2X) bezeichnet, bei dem alle Entitäten dazugerechnet werden, die ein Fahrzeug beeinflussen kann, beziehungsweise die von einem Fahrzeug beeinflusst werden können. V2X setzt sich aus zahlreichen Netzwerktechnologien zusammen, wie vor allem Vehicle-to-vehicle (V2V) für die Kommunikation unter Fahrzeugen, Vehicle-to-pedestrian (V2P) für die Kommunikation von Fahrzeugen mit Fußgängern, Vehicle-to-infrastructure (V2I) für die Kommunikation mit Infrastruktur, oder Vehicle-to-cloud (V2C) für die Kommunikation mit Cloud-basierten Diensten. Abbildung 4 veranschaulicht die unterschiedlichen Bestandteile von V2X.

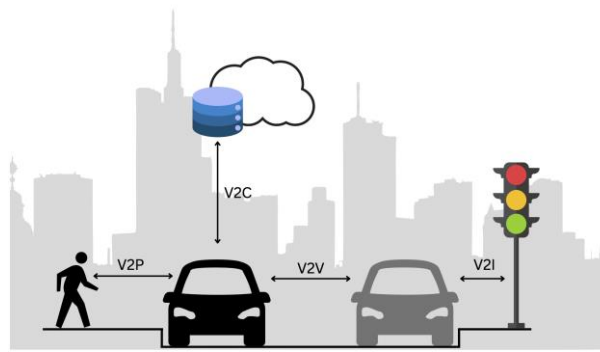


Abbildung 4: Unterschiedliche Kommunikationsmöglichkeiten in V2X: V2V, V2P, V2I, V2C.

Für V2X existieren unterschiedliche Standards und Spezifikationen, die sich in erster Linie durch die eingesetzten zugrundeliegenden Technologien unterscheiden. V2X kann entweder basierend auf WLAN-Technologie oder basierend auf Mobilfunknetzen (cellularV2X, C-V2X) umgesetzt werden. WLAN-basiertes V2X wird unter anderem vom Institute of Electrical and Electronics Engineers (IEEE) standardisiert. Für WLAN basiert V2X auf dem IEEE Standard 802.11p [78] und ist in dem IEEE Standard 1609.x [79] standardisiert. V2X basierend auf Mobilfunknetzen wird von einem Zusammenschluss von Standardisierungsorganisationen 3GPP vorangetrieben und benutzt LTE als Grundlage zur Kommunikation. Im Folgenden werden wir die beiden Standards kurz beschreiben und auf die technischen Unterschiede eingehen.

WLAN V2X Die auf IEEE 802.11p basierenden und in IEEE 1609.x beschriebenen Standards benutzen WLAN-Technologie als Grundlage. Dabei werden Ad-hoc Netzwerke erstellt, sobald mindestens zwei V2X Kommunikationspartner in ausreichender Nähe zueinander sind. Die V2X-Kommunikationsansätze sind dabei Dedicated Short Range Communication (DSRC) [80] in den Vereinigten Staaten und C-ITS [81] in Europa sowie ITS Connect in Japan [82]. Diese IEEE 802.11p-basierte V2X-Kommunikationstechnologie ist ausgereift und wird bereits verbreitet eingesetzt. Die verwendeten Kommunikationsformen für V2X-Kommunikation sind hauptsächlich Broadcast und Unicast/Multicast als Informationsnachrichten [83] und eignen sich daher für ein breites Spektrum von V2X-Anwendungen wie Verkehrsoptimierung, kooperative Tempokontrolle, Spurwechselwarnungen usw. Für bestimmte Anwendungen (z. B., Aktualisierungen von Software/Sicherheitsinformationen, Verkehrs- und Kraftstoffmanagement, nicht sicherheitsrelevante Anwendungen wie Infotainment-/Multimedia-Streaming usw.) kann die Verbindung mit Infrastrukturkomponenten (Road-Side Units, RSUs), dazu verwendet werden die Kommunikationsreichweite und die Konnektivität zu Backend-Infrastrukturen und dem Internet zu verbessern.

LTE C-V2X Im Gegensatz zu WLAN-V2X benutzt C-V2X Mobilfunknetze als Übertragungsgrundlage. Die Standardisierung wird von 3rd Generation Partnership Project (3GPP) vorangetrieben. Dabei hat C-V2X vor allem zwei Operationsmodi: Device-to-Device (V2V oder V2I) und Device-to-Network (V2N) [84]. Device-to-Device Kommunikation für V2X erlaubt den Austausch von Nachrichten über eine kurze Distanz und nutzt das PC5 Interface, wobei keine Basisstationen benötigt werden. Für Device-to-Network werden die üblichen Uplink und Downlink Verbindungen zu den Basisstationen im Mobilfunk verwendet. Im Gegensatz zu V2X basierend auf DSRC und C-ITS, ist der C-V2X Standard noch nicht so ausgereift und in der Nutzung verbreitet [85].

1.4.6.2 Grundlagen von In-Vehicle Netzwerken

Wie Neumann et al. [86] darstellen, gewinnen elektrische und elektronische Systeme in der Automobilindustrie zunehmend an Bedeutung, insbesondere für Innovationen im Bereich der

Fahrzeugkommunikation. Die Vernetzung innerhalb von Fahrzeugen, bekannt als In-Vehicle-Kommunikation, ist entscheidend für die Integration und Interaktion verteilter Steuerungsfunktionen und Benutzerinteraktionen. Diese Netzwerke ermöglichen den Austausch von Sensordaten und reduzieren die Kabelmenge im Vergleich zu paralleler Verkabelung, was zu Kosteneinsparungen, geringerem Gewicht und damit weniger Kraftstoffverbrauch führt.

In modernen Fahrzeugen sind zahlreiche elektronische Steuergeräte mit Sensoren und Aktoren verbunden. Bereits vor zehn Jahren waren in Personenkraftwagen etwa 70 ECUs vorhanden, die rund 2500 Signale verarbeiteten. Diese Zahl ist weiter gestiegen. Seit den späten 1980er Jahren werden standardisierte serielle Kommunikationsprotokolle zur Vernetzung dieser Systeme genutzt, was Interoperabilität zwischen Subsystemen verschiedener Hersteller ermöglicht.

Für die In-Vehicle-Kommunikation existieren verschiedene Netzwerktechnologien, darunter das CAN (ISO 11898-2), das Local Interconnect Network (LIN, ISO 17987-1 bis -7) und FlexRay. CAN bietet eine lineare Bustopologie und ist weit verbreitet für Anwendungen wie Motorsteuerung und Diagnose. LIN wird für kleinere Netzwerke mit geringem Bandbreitenbedarf eingesetzt, während FlexRay für sicherheitskritische Anwendungen wie X-by-wire Technologien entwickelt wurde.

In Nutzfahrzeugen, insbesondere bei Lkws, sind die Kommunikationsanforderungen komplexer aufgrund der Notwendigkeit, unterschiedliche Anhängervorrichtungen und Aufbauten zu integrieren. Diese erfordern eine flexible und erweiterbare Netzwerkarchitektur, da die Kombinationen aus Zugmaschine und Anhänger häufig variieren und somit eine dynamische Kommunikationsstruktur erfordern. Das CAN-basierte SAE J1939-Protokoll ist weit verbreitet für die Kommunikation zwischen den zahlreichen Steuergeräten, die in Lkws typischerweise für Antrieb, Fahrgestell und Aufbauten erforderlich sind. Mit der zunehmenden Elektrifizierung von Zusatzaggregaten wie Kompressoren und Pumpen in Lkws steigt die Anzahl der Kommunikationsknoten erheblich an, was die Anforderungen an Bandbreite und Flexibilität der Netzwerktechnologien erhöht. Die Integration von Ethernet-basierten Technologien, wie BroadR-Reach®, könnte helfen, diesen steigenden Anforderungen gerecht zu werden, indem sie eine höhere Datenübertragungsrate und eine robustere Skalierbarkeit bieten.

Die Anforderungen an die In-Vehicle-Kommunikation variieren je nach Anwendung. Fahrerassistenzsysteme legen beispielsweise Wert auf Determinismus und funktionale Sicherheit, während Infotainmentsysteme eine hohe Datenübertragungsrate erfordern. Die Netzwerkinfrastruktur besteht daher aus einer heterogenen Mischung von Technologien, die miteinander verbunden sind.

In anderen Branchen, wie der industriellen Automatisierung, werden auf Ethernet basierende Technologien erfolgreich eingesetzt. Auch im Fahrzeugbereich gibt es Bestrebungen, Ethernet-basierte Protokolle zu integrieren, um die Leistungsfähigkeit der Netzwerke zu verbessern. Die Einführung von Ethernet in Fahrzeugen könnte ein Weg sein, um den steigenden Anforderungen an Bandbreite und Datenmanagement gerecht zu werden, insbesondere mit der Entwicklung von Technologien wie Time Sensitive Networking, die Echtzeitkommunikation unterstützen.

Die Zukunft der In-Vehicle-Kommunikation könnte durch die Integration von Ethernet und dynamischen Informationsmodellen, wie OPC UA, gestaltet werden. Solche Modelle ermöglichen eine flexible Informationsverarbeitung und könnten die Grundlage für zukünftige Anwendungen und Funktionen im Fahrzeugbereich bieten.

1.4.7 Testen von Resilienzeigenschaften in Ethernet-Netzwerken

Mechanismen und Protokolle zur Steigerung der Resilienz von Ethernet-Netzwerken wurden schon in der Vergangenheit vielfach entwickelt. Zum Beispiel entwickelten Lindner et al. [87] einen 1+1-Protection-Switching-Mechanismus für einen P4-Switch zur programmierbaren Steigerung der Netzwerkresilienz. Yu [88] zeigte einen praktischen Ansatz zur Implementierung für Hochverfügbarkeitsprotokolle, um nahtlose Redundanz gegenüber Ausfällen von Verbindungen in optischen Netzwerken zu demonstrieren. Li et al. [89] entwickelten schon im Jahre 2009 hochverfügbare Systeme auf Basis von Heartbeat-Protokollen. Der Unterschied zu dem im Zuge dieses Forschungsprojektes erarbeiteten Vorhaben besteht darin, dass die hier dargelegten Werke sich auf die Implementierung spezifischer Protokolle zur Steigerung der Resilienz fokussieren, wobei das vorliegende Vorhaben konkret ein Testwerkzeug bereitstellt, welches automatisiert in realen Netzwerken Resilienzeigenschaften durch induzierte Fehlerfälle überprüft.

Weiterhin gibt es Werke, welche versuchen, eine Testbarkeit der Netzwerkresilienz zu erreichen. Li et al. [90] beschreiben eine generelle Methode zum Testen der Verlässlichkeit von Netzwerkapplikationen. Calle et al. [91] evaluieren die Leistung eines MPLS-basierten 1:1 Protection Switching Algorithmus, welcher aufgrund eines wahrscheinlichkeitstheoretischen Fehlermodells Verbindungsfehler induziert. Arendt et al. [92] beschreiben ein Framework für Lasttests für kabellose Kommunikationssysteme. Hierbei kommen dedizierte und räumlich verteilte Lastgeräte zum Einsatz. All diese Ansätze beschreiben einzelne Aspekte einer Resilienztestumgebung. Ihr praktischer Einsatz ist darauf limitiert, dass sie schwer automatisierbar sind, proprietäre Systeme verwenden oder nicht in operativen Umgebungen eingesetzt werden können.

Ein erstes gesamtheitliches Konzept für das Testen von verteilten Systemen auf Basis von wahrscheinlichkeitstheoretischen Fehlermodellen wurde durch Chang et al. [93] geschaffen. Hierbei werden Fehler mit Hilfe von Mechanismen von softwaredefinierten Netzwerken induziert, um die Resilienz zu überprüfen. Dieses System hilft bei der Entdeckung von Systemfehlern in homogenen Rechenzentrumsumgebungen. Die Unterschiede zu dem hier entwickelten Verfahren liegen vor allem in der Erzeugung des Datenverkehrs, der eingesetzten Technologie zur Fehlerinduktion sowie der Homogenität der Umgebung.

1.4.8 Sicherheitsanforderungen von Industrial Ethernet Protokollen

In unserer früheren Arbeit haben wir die Anwendbarkeit der Implementierung von Sicherheitsprotokollen für Industrial Ethernet untersucht [15]. Insbesondere haben wir das Powerlink-Protokoll und seine entsprechende Open-Source-Implementierung untersucht.

Seitdem scheinen einige Arbeiten zur Verbesserung der Sicherheit von Industrial-Ethernet-Protokollen durchgeführt worden zu sein. In [94] diskutiert der Autor mehrere Sicherheitsverbesserungen und -kontrollen für das Profinet-Protokoll. Im Hinblick auf Profinet werden mehrere Ziele des Informationsschutzes diskutiert, wobei für jedes der diskutierten Schutzziele mögliche Sicherheitserweiterungen angegeben werden. Die Arbeit ist ferner mit Profinet-Arbeitsgruppen verbunden und zielt auf die Einhaltung der Normen IEC 62443 ab [95]. In [96] liefern die Autoren eine formale Verifizierung des Industrial-Ethernet-Protokolls EtherCAT. In ihrer Arbeit identifizieren und untersuchen die Autoren drei Man-in-the-Middle-Angriffe, nämlich das Wiederholen von Nachrichten, das Abhören und das Manipulieren von Nachrichteninhalten. Andere Angriffe werden in ihrer Analyse nicht untersucht. Darüber hinaus werden Echtzeitanforderungen in ihrer Arbeit nicht berücksichtigt.

In [97] entwickeln die Autoren Monitore für die Analyse des Netzwerkverkehrs auf den Industrial-Ethernet-Protokollen Profinet und Modbus/TCP. Ihre Lösungen zielen darauf ab, den Datenverkehr

aus dem Netzwerk und der Anwendungsschicht zu erfassen. Darüber hinaus testen sie ihre Implementierung im Hinblick auf den OPC-UA-Standard, eine Spezifikation für unter anderem sichere industrielle Kommunikation [16]. In [98] untersuchen die Autoren die Sicherheitseigenschaften der Industrial-Ethernet-Protokolle EtherNet/IP, Profinet, CC-Link IE und RAPIEnet. Ihr Schwerpunkt liegt auf der Untersuchung dieser Protokolle hinsichtlich ihrer Verwendbarkeit für Anomalieerkennungs- und Überwachungsschemata. Sicherheitserweiterungen oder -kontrollen für die genannten Industrial-Ethernet-Protokolle werden von den Autoren weder empfohlen noch diskutiert. Wie zu sehen ist, behandeln die Arbeiten von [97] und [98] Industrial Ethernet in einem breiten Kontext und zielen darauf ab, Lösungen zu skizzieren und bereitzustellen, die auf mehrere Protokolle gleichzeitig angewendet werden können.

1.4.9 Group Key Agreement auf Bussen von Cyber-physischen Systemen

In der Wissenschaft sind bereits verschiedenste GKA-Protokolle mit jeweils unterschiedlichen Eigenschaften bekannt. Zur effizienten Eingrenzung passender Kandidaten haben wir einen Kriterienkatalog mit Protokollanforderungen für ein ideales sicheres GKA auf CPS-Bussen entwickelt. Dieser wird als Teilergebnis in Kapitel 2.1.9 erläutert. Der Kriterienkatalog enthält 12 Anforderungen, u. a. an Authentizität der Teilnehmer, die Möglichkeit der unabhängigen und vollständig verteilten Durchführung aller Protokolloperationen, Bus-Agnostizität, dynamische Mitgliedschaft, Skalierbarkeit, Dolev-Yao-Robustheit, FS/PCS, kryptografische Agilität und Ressourcenschonung.

Analyse existierender GKA-Protokolle. Ausgehend vom Kriterienkatalog für GKA auf CPS und Bus-Systemen wurde der Stand der Technik entlang der Taxonomien von Prantl et al. [99] und Xiong et al. [100] systematisch bewertet. Dabei wurden im ersten Schritt ganze Klassen von Verfahren ausgeschlossen, weil sie den Kernanforderungen widersprechen:

- zentralisierte oder dezentralisierte/leader-basierte Ansätze (z. B. Cluster- oder imbalanced GKAs, LL-CGKA) verletzen die Anforderungen „Vollständig verteilt“ und „Unabhängig“;
- statische GKAs ohne Join/Leave zur Laufzeit verfehlen die Anforderung „Dynamisch“;
- Protokolle, die gruppenweit asymmetrische Schlüssel aushandeln, sind für ressourcenbeschränkte Busgeräte ungeeignet (Anforderung „Ressourcenschonung“).

Übrig bleiben dynamische, verteilte, beitragsbasierte GKAs, deren interne Organisation (Baum vs. Ring vs. flach) die Komplexität bestimmt.

Die Leistungsanalyse zeigt, dass baumbasierte Verfahren mit logarithmischem Aufwand bei Gruppenoperationen für große Bus-Gruppen am besten skalieren. Der Vergleich der verbleibenden Kandidaten ist in Tabelle 1 dargestellt. Insbesondere TGDH, D-OFT und TreeKEM erreichen jeweils $O(\log^2(n))$ für Rechen- und Nachrichtenaufwand; ring- oder flach organisierte GKAs liegen typischerweise bei $O(n)$ und sind daher für >100 Teilnehmer deutlich weniger geeignet. Aufgrund der Standardisierung und Reife von TreeKEM als Kern des IETF Standards *Messaging Layer Security* (MLS) wurde TreeKEM als Basistechnologie ausgewählt. MLS selbst ist im Bus-Kontext allerdings nicht direkt nutzbar, weil es zentrale Dienste für Authentisierung und Zustellung (Authentication Service und Delivery Service) voraussetzt und damit die Anforderungen „Vollständig verteilt“ und „Unabhängig“ verletzt.

Tabelle 1: Vergleich der Kandidaten nach theoretischem Aufwand.

Protokoll	Rechnerischer Aufwand	Nachrichtenaufwand

TGDH [101]	$O(\log_2(n))$	$O(\log_2(n))$
D-OFT [102]	$O(\log_2(n))$	$O(\log_2(n))$
SGRS [103]	$O(n)$	$O(n)$
GDH.2 [104]	$O(n)$	$O(n)$
GDH.3 [104]	$O(n)$	$O(n)$
Dutta & Barua [105]	$O(n)$	$O(n)$
Kim et al. [106]	$O(n)$	$O(n)$
TreeKEM [107]	$O(\log_2(n))$	$O(\log_2(n))$

Fazit. Unter den betrachteten dynamischen, verteilten GKAs ist TreeKEM die geeignetste Grundlage für Bus-Topologien mit strengen Ressourcen- und Broadcast-Bedingungen. Außerdem existieren bereits Protokollimplementierungen, die sich für die Entwicklungen und Evaluation von Prototypen anbieten. Die gezielte Erweiterung von TreeKEM, um sämtliche Anforderungen zu erfüllen, wird in Kapitel 2.1.9 vorgestellt.

1.4.10 Sicherheit von Ortungsdiensten

GNSS-Systeme wie GPS, Galileo, BeiDou und GLONASS liefern Position, Navigation und Zeit über Signale im Bereich ~ 1.2 bis 1.6 GHz. Die Positionsbestimmung erfolgt über die Laufzeitmessung (Triangulation) zu mindestens vier Satelliten sowie Korrektur eines Empfänger-Uhrzeitversatzes. Für einen Fix sind außerdem Ephemeriden (präzise Bahn-/Zeitdaten je Satellit) und ggf. der Almanach (grobe Informationen, für die gesamte Konstellation) erforderlich. Die Startbedingungen beeinflussen die Time to First Fix (TTFF) erheblich. Ohne vorheriges Wissen (Cold Start) müssen alle Konfigurationen iteriert werden und dann alle Informationen aus den Signalen extrahiert werden, was für gewöhnlich etwa 100 Sekunden dauert. Im Vergleich dazu braucht ein Hot Start, wenn alle Informationen plus eine letzte Position bekannt sind, nur rund 2 Sekunden.

Die zivile Nutzung leidet inhärent unter fehlender Authentisierung: Ein Angreifer kann stärkere, zeitlich verzögerte oder manipulierte Signale aussenden und so Pseudorange-Messungen verfälschen. Reale Vorfälle sind dokumentiert (u. a. Luftfahrt), und die weite Verbreitung zivil genutzter Empfänger vergrößert das Risiko exponentiell.

Zur Verkürzung der TTFF und zur Robustheit stehen Assistenzmechanismen zur Verfügung, das so genannte Assisted-GNSS (A-GNSS). Prinzipiell werden hier über andere Informationskanäle die Informationen heruntergeladen:

- Control Plane (C Plane): RRLP (2G/GSM) und LPP (LTE/5G) liefern Hilfsdaten (Zeit, Ephemeriden, Zellinformationen) sowie netzbasierte Verfahren (z. B. Timing Advance, OTDOA, eCID). Die Signalisierung erfolgt über Mobilfunk-Kontrollkanäle.
- User Plane (U Plane): SUPL (OMA) nutzt IP-basierte Kommunikation für dasselbe Ziel; die Implementierung erfolgt häufig über Provider- oder Google-Server (z. B. supl.google.com).

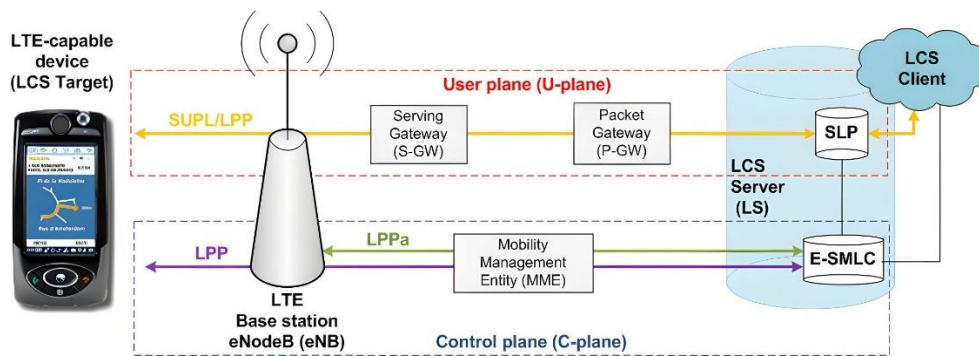


Abbildung 5: U- und C-plane in LTE.

- Hersteller-spezifische Dienste: PSDS/XTRA laden periodisch Bahn-/Zeitdaten (über TLS/HTTPS) direkt vom GNSS-Chiphersteller oder OS-Anbieter (z. B. agnss.goog, xtracloud.net).

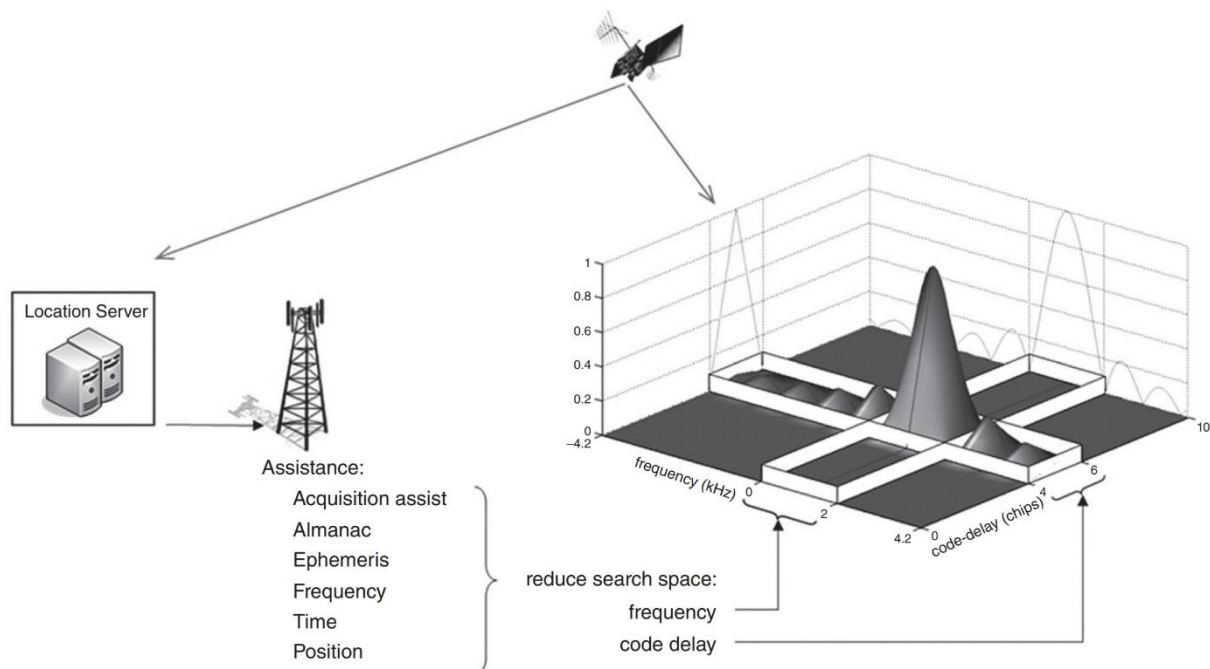


Abbildung 6: Reduzierter Signal-/Frequenzsuchraum mit A-GNSS-Hilfsdaten. Alle Hilfsdaten wie Position, Zeit und Almanach reduzieren den Frequenzsuchraum. Zur Reduzierung des Codeverzögerungssuchraums ist eine präzise Zeitangabe erforderlich [108].

Unabhängig von GNSS dienen Mobilfunk-/WLAN-/Bluetooth-Fingerprints als schnelle, oft indoor robuste Quelle. Geräte lesen Kennungen wie MCC, CellID oder BSSID aus und fragen gegen Crowd-Datenbanken (Google, Apple; offen: Mozilla MLS, CellMapper/OpenCellID) eine Position ab. Vorteile sind Geschwindigkeit und Verfügbarkeit ohne Satellitensicht; Angriffsflächen sind manipulierbare Metadaten durch z. B. gefälschte CellIDs, Rogue-APs.

Vorarbeiten zeigen GNSS-Spoofing gegen Fahrzeuge, Untersuchungen zur Genauigkeit von Netzwerk-Lokalisierung (z. B. WLAN-Fingerprints) und Angriffe über Rogue-Basisstationen [109, 110, 111, 112]. Jedoch fehlt aktuelle, konsolidierte Evidenz zur realen Nutzung und Fusion auf Android (insb. FLP), zu hersteller- und chipabhängigen Unterschieden und zu Privacy-Aspekten von SUPL/PSDS (IMSI-Übertragung, Cipher-Altlasten). Ebenso sind die Priorisierungsentscheidungen in FLP empirisch kaum beschrieben.

1.4.11 Bereichsübergreifendes Security-Risikomanagement in der Automobilindustrie: Anforderungen und aktuelle Praktiken

1.4.11.1 Standards und Experteninterviews

Obwohl sich zahlreiche Arbeiten mit Cybersicherheitsstandards im Automobilbereich befassen, sind die spezifischen Herausforderungen des bereichsübergreifenden Risikomanagements noch nicht ausreichend erforscht. Die meisten bestehenden Studien konzentrieren sich entweder auf Standards, die für einen einzelnen Automobilbereich gelten [30, 52], oder vergleichen Standards, ohne die besonderen strukturellen Merkmale und Kooperationsanforderungen der Automobilindustrie zu berücksichtigen [53, 54].

Schmittner und Macher [30] beispielsweise geben einen umfassenden Überblick über verschiedene Cybersicherheitsstandards und -richtlinien für die Automobilindustrie, wie ISO/SAE 21434, ETSI-Standards und ITU-Empfehlungen. Sie diskutieren zwar Überschneidungen und Lücken zwischen verschiedenen regulatorischen Rahmenwerken, konzentrieren sich jedoch in erster Linie auf die Fahrzeugtechnik und die daraus resultierenden Konnektivitätsprobleme und weniger auf die Wechselwirkungen zwischen verschiedenen Bereichen wie Produktion und Backend-Services.

Arbeiten, die sich mit domänenübergreifendem Risikomanagement befassen, tun dies oft in einem breiteren Kontext außerhalb des rein automobilen Umfelds. So schlagen Ponsard et al. [113] beispielsweise ein metamodellbasiertes Risikomanagement-Framework vor, das standardunabhängig sein soll. Obwohl sie auf verschiedene Standards wie ISO 31000, IEC 62443 und ISO/SAE 21434 verweisen, erfassen diese Bemühungen möglicherweise nicht vollständig die nuancierten Organisationsstrukturen von Automobilherstellern, insbesondere dort, wo sich Konstruktions- und Produktionsprozesse mit vernetzten Fahrzeugökosystemen überschneiden. In ähnlicher Weise unterstreichen die Bemühungen von Urbach et al. [114] und Ramirez et al. [115] die Notwendigkeit einer Zusammenarbeit im Bereich Cybersicherheit über mehrere Geschäftsbereiche hinweg, gehen jedoch nicht auf die branchenspezifischen Probleme der Cybersicherheit im Automobilbereich ein.

In einer aktuellen Veröffentlichung, die sich stärker auf den Automobilbereich konzentriert, zeigen do Carmo und Schlenzog [55], wie wiederholte Bedrohungsanalysen und Risikobewertungen (TARAs) für klassische E/E-Systeme, vernetzte Ökosysteme und Fertigungsanlagen durchgeführt werden können. Sie beschreiben auch, wie ISO/SAE 21434, ISO/IEC 27000 und IEC 62443 in Fertigungskontexten integriert werden können. Obwohl ihre Arbeit grundlegende Einblicke in Multi-Domain-Ansätze liefert, sind praktische bereichsübergreifende Leitlinien noch eher explorativer Natur. Sie erkennen die Notwendigkeit weiterer Forschung darüber an, wie diese Standards gemeinsam umgesetzt werden können, insbesondere auf organisatorischer und prozeduraler Ebene.

Aufbauend auf diesen Grundlagen nimmt die vorliegende Arbeit eine breitere Perspektive ein, indem sie sich auf das bereichsübergreifende Cybersicherheits-Risikomanagement konzentriert und die organisatorischen, verfahrenstechnischen und kommunikativen Lücken, die zwischen Fahrzeugtechnik, Produktion und Backend-Services entstehen, systematisch untersucht. Über die Überprüfung der relevanten Standards aus jedem Bereich und die Extraktion ihrer bereichsübergreifenden Anforderungen hinaus berücksichtigt dieser Artikel empirische Erkenntnisse aus Interviews mit Branchenexperten. Auf diese Weise befasst er sich mit den praktischen

Herausforderungen der Koordinierung des Cybersicherheitsrisikomanagements über unterschiedliche Bereichen hinweg und zielt darauf ab, klarere Richtlinien für die Sicherung von Fahrzeugsystemen und den damit verbundenen Infrastrukturen anzubieten.

1.4.11.2 Usability

Im Folgenden werden Empfehlungen aus der Literatur abgeleitet, welche die nutzenden-freundliche Gestaltung des Risikomanagement-Systems unterstützen sollen. Die hier beschriebenen Anforderungen ergeben sich aus der Erfahrung in der Arbeit mit Nutzenden sowie aus einschlägigen Quellen. Die Quellen können dabei Standards, Heuristiken sowie allgemeinere Guidelines umfassen. Die allgemeinen Anforderungen beziehen sich dabei auf Usability-Anforderungen, die für jedes System relevant sind. Die spezifischen Anforderungen adaptieren solche allgemeinen Regeln für den hier betrachteten Anwendungsfall. Die Literatur deutet darauf hin, dass die Verwendung spezifischer Regeln die Berücksichtigung der allgemeinen Anforderungen nicht ersetzt, und daher sowohl allgemeine als auch spezifische Regeln während der Entwicklung berücksichtigt werden sollten.

Allgemeine Anforderungen

Im Folgenden werden einige Anforderungen an die Usability zusammengefasst, welche für alle Systeme im Allgemeinen gelten. Diese basieren maßgeblich auf den 10 Usability Heuristiken von Jakob Nielsen⁸, welche den Grundstein für benutzbare Gestaltung von Systemen darstellen. Außerdem werden die Prinzipien für Interaktionsgestaltung (Principles of Interaction Design) von Don Norman⁹ berücksichtigt sowie Hinweise zur Barrierefreiheit (Accessibility) gegeben, welche einen entscheidenden Bestandteil der Usability darstellt.

10 Usability Heuristics for User Interface Design (Jakob Nielsen)

1: Visibility of System Status. Nutzende sollten zu jedem Zeitpunkt angebrachtes Feedback über den System-Status erhalten. Dies beinhaltet sowohl die Aktionen des Systems als auch die Folgen von Aktionen der Nutzenden. Ein Beispiel für ein solches Feedback könnte eine Sanduhr sein, welche den Nutzenden mitteilt, dass das System derzeit Berechnungen anstellt und deswegen kurzfristig nicht bedient werden kann.

2: Match Between the System and the Real World: Um das System so einfach und intuitiv verständlich wie möglich zu gestalten, sollte es Konventionen folgen, welche der Zielgruppe bekannt sind. Eine Maßnahme, um dies zu erreichen, ist die Verwendung verständlicher Sprache und dementsprechend die Vermeidung unnötiger Fachbegriffe, welche womöglich nicht allen Nutzenden bekannt sind. Außerdem kann es von Nutzen sein, sich an bekannten Symbolen und Konventionen aus der realen Welt zu orientieren. Die Bedeutung von Designelementen sollte Nutzenden klar sein, ohne, dass sie diese erst erkunden müssen. Ein bekanntes Beispiel hierfür ist die Verwendung einer Diskette als Symbol für das Speichern von Daten.

3: User Control and Freedom. Ein System sollte den Nutzenden einfache Möglichkeiten bieten, Aktionen wieder rückgängig zu machen. Dies erlaubt es den Nutzenden, das System frei zu navigieren und zu testen, ohne Konsequenzen fürchten zu müssen, weil sie einen Fehler begangen haben. Gleichmaßen sollten Nutzende jederzeit in der Lage sein, ungewünschte Prozesse

⁸ <https://www.nngroup.com/articles/ten-usability-heuristics/>

⁹ <https://medium.com/@sachinrekhi/don-normans-principles-of-interaction-design-51025a2c0f33>

wieder abubrechen. Beispiele für diese Heuristik sind übliche „Rückgängig“ und „Wiederherstellen“ Funktionen (wobei „Wiederherstellen“ das „Rückgängig“ machen revidiert), sowie beispielsweise ein „Abbrechen“ Button, um begonnene Prozesse zu beenden. Auch die Tastenkombination „Strg + Z“, welche die „Rückgängig“ Funktion aufruft, wird in den meisten Anwendungen unterstützt.

4: Consistency and Standards. Wo Heuristik Nummer 2 unter anderem Konsistenz mit der realen Welt erfordert, geht es bei dieser Heuristik eher um Konsistenz mit Konventionen und Standards. So sollten intern, aber möglichst auch plattformübergreifend, Vokabular, Funktionen und Interaktions-Möglichkeiten einheitlich gestaltet sein. Solche Konventionen sind oft in Standards oder Gestaltungsregeln (z. B. Design Guidelines, Style Guides, etc.) niedergeschrieben, können aber auch durch den Vergleich mit artverwandten Produkten deutlich werden. Beispiele hierfür stellen unter anderem die Funktionen zum Minimieren, Maximieren und Schließen eines Fensters unter Windows dar, welche sich immer in der rechten oberen Ecke des Fensters befinden und immer die gleichen Symbole verwenden. Auch die Position der Menüleiste am oberen Applikationsrand oder einer Navigation am linken Bildschirmrand sind häufig auftretende Konventionen.

5: Error Prevention. Dass Fehler in einer Anwendung vermieden werden sollten, ist den meisten Entwicklungsteams klar. Bei dieser Heuristik geht es allerdings mehr darum, Nutzende so zu führen, dass ihnen bei der Verwendung der Anwendung keine Fehler unterlaufen. Hierzu kann es hilfreich sein, den Raum möglicher Aktionen des Nutzenden auf die (situationsbedingt) sinnvollen Möglichkeiten einzuschränken, sowie sinnvolle Default-Annahmen zu implementieren. Außerdem sollten Nutzende, wann immer möglich, in ihrer Aufgabe unterstützt werden, zum Beispiel, indem alle notwendigen Informationen einfach zur Verfügung gestellt werden, so dass Nutzende sich an diese nicht selbstständig erinnern müssen. Wo eine fehlerhafte oder versehentliche Aktion von Nutzenden besonders schwere Folgen hätte, sollte dieser außerdem über die Folgen informiert werden und die Aktion anschließend erneut bestätigen müssen. Ein Beispiel für diese Heuristik ist die Bestätigungsabfrage, welche in der Regel vor dem Löschen von Dateien erfordert wird. Aber auch das Ausgrauen von Funktionen, welche in einer bestimmten Situation innerhalb einer Anwendung nicht zur Verfügung stehen, kann ein Beispiel für diese Regel darstellen.

6: Recognition Rather than Recall. Um die Belastung des Gedächtnisses der Nutzenden zu minimieren, sollten zur Verfügung stehende Aktionen und Optionen sowie notwendige Informationen jederzeit sichtbar oder zumindest einfach verfügbar sein. Die Notwendigkeit, sich Dinge zu merken, sollte weitestgehend reduziert werden. Ein klassisches Negativ-Beispiel, das noch immer häufig zu finden ist, sind lange Tutorials beim erstmaligen Öffnen einer Applikation, welche jegliche Funktionen der Anwendung erläutern. Stattdessen sollten Informationen dann zur Verfügung gestellt werden, wenn diese auch benötigt werden.

7: Flexibility and Efficiency of Use. Nicht alle Nutzenden interagieren auf die gleiche Art mit einem System. Um diesen Unterschieden gerecht zu werden, sollte ein System unterschiedliche Möglichkeiten bieten, dasselbe Ziel zu erreichen. Dies erlaubt es den Nutzenden, den Weg zu wählen, welcher ihnen liegt. Solche alternativen Wege können auch genutzt werden, um die Effizienz zu steigern. So können zum Beispiel Tastenkombinationen genutzt werden, um Funktionen schneller aufzurufen, oder es kann andere Möglichkeiten für Experten geben, ein System schneller zu navigieren oder zu nutzen, während für weniger erfahrene Nutzende dennoch einfachere aber weniger effiziente Wege geboten werden. Ein weit verbreitetes Beispiel für eine solche Flexibilität mit effizienterer „Abkürzung“ ist die Tastenkombination „Strg+C“ für die Funktion

„Kopieren“, welche eine Alternative zu dem üblichen Weg anbietet, die Funktion „Kopieren“ aus einem Kontextmenü (üblicherweise durch einen Rechtsklick aufgerufen) zu wählen.

8: Aesthetic and Minimalist Design. Ein Interface, das dieser Heuristik gerecht wird, sollte möglichst nur Informationen enthalten, welche für die gegenwärtige Aufgabe der Nutzenden von Relevanz ist. Selten genutzte Informationen, Funktionen oder Optionen sollten währenddessen verborgen werden. So wird den Nutzenden ermöglicht, benötigte Informationen und Funktionen schnell zu finden, ohne durch irrelevante Interface-Elemente abgelenkt zu werden. Die Schwierigkeit besteht hier meist darin, in jeder Situation zu identifizieren, welche Informationen oder Funktionen benötigt werden und welche nicht. Allerdings sollte auch die Ästhetik hierbei nicht vernachlässigt werden, da diese meist verantwortlich für den Ersteindruck einer Anwendung ist und somit die gesamte Erfahrung prägen kann. Ein Beispiel für diese Heuristik stellt die Google Startseite dar, welche außer der Texteingabe für die Suche nahezu keine weiteren Elemente enthält. Die wichtigsten Einstellungen (z. B. Sprache) sowie Informationen („About“) stehen hier zwar Verfügung, treten aber gegenüber der Suchfunktion in den Hintergrund. Die meisten Optionen (Filter, Art des gesuchten Inhalts, etc.) werden erst nach erfolgter Suche zur Verfügung gestellt.

9: Help Users Recognize, Diagnose, and Recover from Errors. In Heuristik Nummer 5 wurde bereits beschrieben, dass Fehler möglichst zu vermeiden sind. Da dies nicht immer möglich ist, zielt diese Heuristik nun darauf ab, den Einfluss von Fehlern zu minimieren. Um dies zu erreichen, werden gute Fehlermeldungen benötigt. Diese sollten einerseits klar darüber informieren, dass ein Fehler aufgetreten ist, indem üblichen Konventionen gefolgt wird (Verwendung von Symbolen wie Ausrufezeichen, der Farbe Rot, etc.) und der Fehler in einfach verständlicher Sprache erklärt wird (Vermeidung von Fehlercodes und technischer Fachsprache). Andererseits sollten diese Fehlermeldungen aber auch konstruktiv zur Lösung des Problems beitragen, indem beispielsweise die Ursache beschrieben und eine Lösung vorgeschlagen wird. Wenn möglich sollten außerdem direkt „Abkürzungen“ zur Lösung geboten werden. Wenn die Lösung also z. B. erfordert, den Inhalt einer Datei an einer bestimmten Stelle anzupassen, sollten Nutzende aus der Fehlermeldung heraus direkt an diese Stelle der Datei springen können. Klassische Negativ-Beispiele hierfür sind Fehlermeldungen, die lediglich den Inhalt „Ein Fehler ist aufgetreten“ vermitteln. Aber auch beispielsweise die Fehlermeldung „Die Datei kann nicht gelöscht werden, da sie noch geöffnet ist“ könnte verbessert werden, indem man Nutzenden anbietet, direkt aus der Fehlermeldung heraus a) die betroffene Datei zu schließen oder diese b) in den Fokus zu rücken, damit Nutzende diese selbstständig schließen können.

10: Help and Documentation. Im Idealfall ist ein System so selbsterklärend, dass keine weiterführenden Informationen benötigt werden. Da dies aber nicht immer möglich ist, sollte zumindest immer alle Information zur Verfügung stehen, die notwendig ist, um die Ziele der Nutzenden zu erfüllen. Diese Hilfe sollte möglichst genau dann zur Verfügung gestellt werden, wenn Nutzende sie benötigen und sollte kurz sowie einfach zu durchsuchen, verstehen und befolgen sein (z. B. klar zu befolgende Schritte). Nach Möglichkeit sollte diese außerdem direkt im System verfügbar sein und nicht erfordern, dass Nutzende außerhalb nach Informationen suchen. Eine gute Möglichkeit hierfür stellen kontextsensitive Hilfen in digitalen Anwendungen dar, z. B. in Form eines kleinen Fragezeichens an bestimmten Interface-Elementen oder Prozessschritten, welche angeklickt werden können, um Hilfe für genau diesen Schritt oder dieses Element zu erhalten.

Principles of Interaction Design (Don Norman)

Analog zu den 10 Heuristiken aus dem vorangegangenen Abschnitt sollen hier die 6 Prinzipien für Interaktionsgestaltung (Principles of Interaction Design) von Don Norman beschrieben werden. Diese sind sehr artverwandt mit den vorher genannten Heuristiken, können aber womöglich einige weitere Hinweise bieten oder helfen, Missverständnisse aufzuklären. Die Anzahl der genannten Prinzipien kann sich je nach Quelle ein wenig unterscheiden, doch die 6 hier genannten Prinzipien machen immer den Kern der Liste aus und sollten universell anwendbar sein. Dies gilt sogar außerdem der digitalen oder technischen Welt, beispielsweise bei der Gestaltung von Alltagsgegenständen wie Türen.

1: Visibility. Das Prinzip der Sichtbarkeit, oder Visibility, deckt sich weitestgehend mit der Heuristik 8: Aesthetic and Minimalist Design. Es beschreibt den Umstand, dass besser Sichtbare Elemente auch besser wahrgenommen werden, und daher Elemente, welche für die Nutzenden gegenwärtig relevant sind, gut sichtbar sind und entsprechend irrelevante Elemente verborgen werden.

2: Feedback. Nutzende sollten nie im Unklaren gelassen werden, was ihr Handeln bewirkt. Dieses zweite Prinzip beschreibt daher die Anforderung, Nutzenden für jede ihrer Aktionen Feedback zu liefern, welche Aktion ergriffen wurde und welche Konsequenzen diese hat. Dieses Feedback kann verschiedene Modalitäten nutzen, ist aber in der Regel visuell (z. B. ein Licht, eine Farbe o.ä.), auditiv (z. B. ein Warngeräusch, ein Klingelton o.ä.) oder haptisch (z. B. Vibration).

3: Constraints. Wie bereits in der Heuristik 5: Error Prevention beschrieben, empfiehlt auch dieses Prinzip, die möglichen Aktionen auf solche einzuschränken, die für die gegenwärtige Aufgabe oder das Ziel der Nutzenden sinnvoll sind, um so ihr Handeln zu leiten und die Zielerfüllung zu erleichtern.

4: Mapping. Das Prinzip "Mapping" besagt, dass ein klarer Zusammenhang zwischen der Gestaltung von Steuerelementen und ihrer Auswirkung bestehen soll. Dieses „mapping“ soll auf den ersten Blick erkennbar machen, was mit welchem Steuerelement erreicht, bedient werden kann oder was der Effekt ist. So repräsentiert beispielsweise die Position der Knöpfe in einem Aufzug in der Regel auch die Position der dazugehörigen Stockwerke, mit dem Knopf für das niedrigste Stockwerk unten und dem Knopf für das höchste Stockwerk ganz oben an der Steuertafel.

5: Consistency. Dieses fünfte Prinzip deckt sich mit Heuristik 4: Consistency and Standards und empfiehlt, innerhalb der Anwendung aber auch über Anwendungen hinweg konsistente Gestaltung zu verwenden. Dies kann sich beispielsweise auf die Benennung, Position, Aussehen oder Funktionsweise von Interface-Elementen beziehen.

6: Affordance. Das Prinzip „Affordance“ beschreibt, inwiefern die Gestaltung eines Objekts oder eines Elements bereits seine Nutzung diktiert, bzw. inwieweit ihm seine Funktion bereits anzusehen ist. Dies geht häufig mit Prinzip 3: Constraints einher, da eine Einschränkung der Aktionsmöglichkeiten auf ein Minimum häufig auch eine hohe „Affordance“ mit sich bringt. Als Negativ-Beispiel nennt Norman hier gerne Türen. Diese sind oft mit „ziehen“ auf einer Seite und „drücken“ auf der anderen Seite beschriftet, da die Klinke auf beiden Seiten identisch ist und so keinen Hinweis darauf gibt, wie die Tür zu öffnen ist (schlechte „Affordance“). Wäre stattdessen nur an der Seite, an der zu ziehen ist, eine Möglichkeit hierfür angebracht (Klinke, Türknauf, etc.) wäre klar, dass auf dieser Seite gezogen werden muss, während die andere Seite nur gedrückt werden kann.

Barrierefreiheit (Accessibility)

Accessibility, meist als Barrierefreiheit übersetzt, beschreibt in der Regel die Eigenschaft, auch für Personen mit Beeinträchtigungen nutzbar zu sein. Andere Übersetzungen können auch weitergehende Definitionen umfassen. So beschreibt „Zugänglichkeit“ beispielsweise oft die Gebrauchstauglichkeit für eine möglichst weit gefasste Gruppe von Menschen. Selbst wenn jedoch lediglich Barrierefreiheit im oben beschriebenen Sinne betrachtet wird, gilt, dass Maßnahmen zur Verbesserung der Accessibility in der Regel auch die Usability für alle Nutzenden verbessern. Deswegen, und um einen möglichst großen Nutzenden-Kreis abzudecken, stellt die Accessibility einen essenziellen Teil der Usability dar und sollte daher stets von Anfang an mit bedacht werden. In einigen Bereichen ist dies sogar gesetzlich erforderlich. Entsprechende Vorschriften finden sich beispielsweise im Barrierefreiheitsstärkungsgesetz¹⁰ sowie in der Barrierefreie-Informationstechnik-Verordnung¹¹ (BITV 2.0).

Das Thema Barrierefreiheit umfasst in der Regel die vier Prinzipien „Perceivable“, „Operable“, „Understandable“ und „Robust“ (deutsch: Wahrnehmbar, Bedienbar, Verständlich und Robust). Diese umfassen jeweils zahlreiche Regeln, um Bestandteile der Benutzerschnittstelle für Nutzende Wahrnehmbar und Bedienbar aufzubauen und darzustellen sowie Inhalte verständlich und lesbar zu präsentieren und für eine große Auswahl an Benutzeragenten (einschließlich assistierender Techniken) robust interpretierbar zu machen. Da sich diese Regeln nicht so einfach auf wenige, handliche Stichpunkte reduzieren lassen, soll an dieser Stelle nur auf die Bedeutung und Wichtigkeit hingewiesen werden, welche Accessibility in jedem Gestaltungsprozess einnehmen sollte. Um dieser gerecht zu werden, können verschiedene Quellen hilfreich sein. Zum einen ist hier der Teil 20 der ISO-Norm 9241¹² zu nennen. Zum anderen, spezifisch auf Internet-Inhalte ausgerichtet aber auch für andere Bereiche von Nutzen, seien die Web Content Accessibility Guidelines¹³ (WCAG) des World Wide Web Consortiums (W3C) genannt.

Spezifische Anforderungen

In diesem Teilkapitel werden Anforderungen beschrieben, welche durch die Adaption allgemeiner Usability Heuristiken (meist der 10 Usability Heuristiken von Jakob Nielsen) für den spezifischen Gebrauch in Risikomanagement-Systemen und verwandten Anwendungen entstanden sind. Hierfür wurden die „Heuristics for Evaluating IT Security Management Tools“ [116] untersucht. Die Forschungslage zu diesem Anwendungsbereich ist bislang nicht umfassend. Aus diesem Grund ist hier weitere Forschung und besonders auch die Vertestung mit tatsächlichen Nutzenden von besonderer Wichtigkeit.

1: Visibility of Activity Status. Diese Heuristik hat Ähnlichkeiten mit der 1. Heuristik von Nielsen: Visibility of System Status, beschränkt sich aber nicht auf den direkt gegenwärtigen Systemstatus. Stattdessen kann der Status Aspekte beinhalten, welche Räumlich (z. B. auch über Systeme hinweg) oder zeitlich verteilt sind. Um die Heuristik einzuhalten, sollte ein System Nutzende unter anderem über folgende Aspekte des Status informieren: andere beteiligte Nutzende sowie deren Aktionen, die Arbeitsverteilung, einschlägige Regeln, Werkzeuge, Informationen und Materialien

¹⁰ <https://www.bmas.de/DE/Service/Gesetze-und-Gesetzesvorhaben/barrierefreiheitsstaerkungsgesetz.html>

¹¹ https://www.gesetze-im-internet.de/bitv_2_0/BJNR184300011.html

¹² <https://www.dinmedia.de/de/norm/din-en-iso-9241-20/349263418>

¹³ <https://www.w3.org/TR/2023/REC-WCAG21-20230921/>

sowie den Fortschritt. Weiterhin sollten Kommunikationskanäle zum Übertragen dieser Informationen geboten werden.

2: History of Actions and Changes on Artifacts. Um aus vergangenem Vorgehen zu lernen, aber auch um Personen für ihr Handeln zur Verantwortung ziehen zu können, sollte eine Historie der getätigten Aktionen sowie Änderungen an Werkzeugen oder anderen Artefakten (z. B. Logs, Policies, etc.) vorgehalten werden. Für diese sollten außerdem Mittel zur Verfügung gestellt werden, sie sinnvoll zu durchsuchen und historische Informationen analysieren zu können.

3: Flexible Representation of Information. Abhängig von der gegenwärtigen Aufgabe bzw. den gegenwärtigen Zielen der Nutzenden sowie der Zielgruppe können die Anforderungen an die Repräsentation von Informationen variieren. Ein System sollte daher die Möglichkeit bieten, Informationen flexibel je nach Bedarf unterschiedlich darzustellen / Auszugeben. Hierbei sollte auch sichergestellt werden, dass Ein- sowie Ausgaben auch in Kombination mit anderen Systemen nutzbar sind.

4: Rules and Constraints. Vergleichbar mit dem Gestaltungsprinzip der „Constraints“ schreibt diese Heuristik vor, dass mögliche Aktivitäten auf die sinnvollen beschränkt sein sollten, jedoch verschiedene Wege zur Aufgabenerfüllung innerhalb dieser Einschränkungen möglich sein sollten (siehe auch Nielsens Heuristik „Flexibility and Efficiency of Use“). Diese Einschränkungen können beispielsweise von der gegenwärtigen Aufgabe, einer bestimmten Lösungsstrategie für die Aufgabe, sozialen und organisatorischen Strukturen oder der Kompetenz der Nutzenden abhängen. Gemäß Nielsens Heuristik „Error Prevention“ können solche Einschränkungen auch bei der Fehlervermeidung unterstützen.

5: Planning and Dividing Work Between Users. Um Arbeit und Arbeitsteilung effizient gestalten zu können, sollte ein System die Planung und Koordination der Arbeitsteilung bereits inhärent unterstützen. Dies beinhaltet auch, beteiligte Personen schnell involvieren und informieren zu können. Zu diesem Zweck sollten existierende Workflows im System integriert und für neue oder unbekannte Umstände neue Arbeitspläne innerhalb des Systems geplant werden können. Hier sollten auch flexibel neue Nutzende eingebunden werden können.

6: Capturing, Sharing, and Discovery of Knowledge. Diese Heuristik zielt darauf ab, vorliegendes Wissen teilen und neu gewonnenes Wissen dokumentieren zu können. Zu diesem Zweck sollten explizite Mittel zur Dokumentation von Wissen, z. B. in Form von Dokumenten, Webseiten, Notizen, etc., geboten werden. Weiterhin sollten Methoden zum Teilen dieses Wissens sowie zum Auffinden von benötigtem Wissen integriert werden. Bei den aufzufindenden Wissensquellen kann es sich hierbei einerseits um die eben angesprochenen Dokumente, andererseits aber auch um Personen handeln. Bei Personen sollten auch hier Kommunikationskanäle geboten werden, um diese zu kontaktieren.

7: Verification of Knowledge. Diese Heuristik bildet Elemente von Nielsens Heuristiken „User Control and Freedom“ sowie „Error Prevention“ ab. Insbesondere bei kritischen Aktivitäten sollte Nutzenden eine Umgebung zur Verfügung gestellt werden, in der die Aktivitäten frei von Konsequenzen getestet werden können, um ihre Auswirkungen zu validieren. Hier sollten außerdem geplante Aktionen dokumentiert werden können (als Notiz oder sogar als Skript), so dass diese von anderen Nutzenden geprüft werden können. Dies unterstützt außerdem darin, sie anschließend auf dem Produktivsystem einfacher umsetzen zu können.

1.4.12 Prototypisches Werkzeug für ein bereichsübergreifendes Security-Management

Zu Projektbeginn war die Werkzeuglandschaft für Cybersicherheits- und Risikomanagement im Automobilbereich von einer starken Domänentrennung geprägt. Für die fahrzeugseitige TARA nach ISO/SAE 21434 wurden überwiegend Excel-basierte Templates oder Hersteller-eigene Tools eingesetzt; im Backend- und Office-IT-Umfeld kamen klassische ISMS-Werkzeuge (z. B. GRC-Plattformen) zum Einsatz, während in der Produktion OT-spezifische Lösungen auf Basis von IEC-62443-Programmen vorherrschten. Ein durchgängiges, bereichsübergreifendes Werkzeug, das Fahrzeug-CSMS, Backend-ISMS und IACS-Security-Programm integriert, war weder in der Literatur noch in der industriellen Praxis etabliert.

Auch praktikable Ansätze zur Integration bestehender Methoden und Werkzeuge waren nur punktuell vorhanden. MoRA lag vor Projektstart ausschließlich als Excel-Werkzeug vor [1, 2]: Security-Analysten modellierten Funktionen, Daten, Komponenten und Datenflüsse, leiteten daraus Schutzziele, Schadensszenarien, Bedrohungen, Maßnahmen und Annahmen ab und bewerteten Risiken über Impact- und Attack-Feasibility-Ratings. Die Ergebnisse einzelner Risikoanalysen lagen jedoch in separaten Dateien vor, ohne zentrale Ablage und ohne Werkzeuginfrastruktur zur konsolidierten Auswertung, zum Vergleich zwischen TOEs oder zur systematischen Nachverfolgung von Risiken und Maßnahmen über mehrere Bereiche hinweg. Ein explizites Rollen- und Berechtigungskonzept, das Risk Ownern, Control Ownern oder Process Ownern aus unterschiedlichen Unternehmensbereichen zugeschnittene Sichten bereitstellt, war in dieser Form nicht vorgesehen.

Im Bereich der kommerziellen GRC- und ISMS-Werkzeuge existierten zwar Plattformen, die Mehrfachnormen (z. B. ISO/IEC 27001, ISO 9001, teilweise auch IEC 62443) abbilden und generische Risiko- und Compliance-Workflows anbieten. Diese Lösungen waren jedoch in der Regel nicht auf den automobilen Kontext und die spezifische Kombination aus ISO/SAE 21434, UN R155, ISO/IEC 27001 und IEC 62443 zugeschnitten, integrierten sich nur eingeschränkt mit technischen Engineering-Artefakten (z. B. TARA-Excel-Sheets, Architekturmodelle) und waren häufig organisatorisch getrennt von den Werkzeugen der Entwicklungsbereiche angesiedelt.

Parallel dazu war Microsoft SharePoint in vielen Unternehmen bereits als Kollaborationsplattform und Dokumentenablage etabliert. SharePoint-Listen ermöglichen zwar prinzipiell die Modellierung strukturierter Domänen (z. B. „Risiko-Register“ oder „Maßnahmenlisten“), wurden in der Praxis jedoch meist für generische Ticket- oder Aufgabenverwaltung genutzt. Eine spezifische Nutzung von SharePoint als Datenbasis für modellbasierte Security-Risikoanalysen (inklusive Abbildung der MoRA-Artefakte) und als integratives Werkzeug für bereichsübergreifendes Security- und Compliance-Management war zum Projektstart nicht bekannt.

Auch im Bereich Usability für Security-Management-Werkzeuge lag der Schwerpunkt der Forschung eher auf allgemeinen Heuristiken und Guidelines. Jaferian et al. [116] formulierten „Heuristics for Evaluating IT Security Management Tools“, die u. a. Sichtbarkeit von Aktivitäten, Historienführung, flexible Informationsrepräsentation und Unterstützung für Arbeitsteilung adressieren. Konkrete, automotive-spezifische Referenzimplementierungen auf Basis verbreiteter Kollaborationsplattformen fehlten jedoch. Die in Abschnitt 1.4.11 dargestellte Literatur zu bereichsübergreifendem Risikomanagement diskutierte zwar Metamodelle und organisatorische Rahmenbedingungen [113, 114, 115], zeigte aber keine durchgängig implementierten Werkzeuge, die CSMS, ISMS und IACS-Security-Programm in einem gemeinsamen Workspace zusammenführen.

Zusammenfassend stand das ATLAS-L4-Projekt zu Beginn vor der Situation, dass

- MoRA als methodisch ausgereifte, aber Excel-basierte Insel existierte,
- domänenspezifische Managementsysteme (CSMS, ISMS, IACS-Security-Programm) auf unterschiedlichen Werkzeugen und Terminologien beruhten und
- marktgängige Plattformen zwar prinzipiell als Basis für ein bereichsübergreifendes Security-Management geeignet erschienen, aber noch nicht im automobilen Kontext entsprechend genutzt worden waren.

Diese Ausgangslage motivierte den Ansatz, anstelle einer eigenentwickelten Speziallösung zunächst die Möglichkeiten einer bereits breit eingeführten Plattform – konkret Microsoft SharePoint in Kombination mit Power Apps und Power Automate – zu untersuchen und darauf ein prototypisches Werkzeug aufzubauen, das MoRA-Daten, bereichsübergreifende Rollen und Compliance-Anforderungen in einem gemeinsamen Workspace integriert. Dabei sollten die in Abschnitt 1.4.11 beschriebenen Anforderungen an Terminologie, Datenstandardisierung und bereichsübergreifende Kommunikation explizit berücksichtigt werden.

1.4.13 Entwicklung öffentlich verfügbarer Testtools für Fahrzeugdiagnose

Neben der gesetzlich geforderten abgasrelevanten On-Board-Diagnose (OBD) hat sich im Automobilmarkt die im Funktionsumfang erweiterte Diagnose mittels UDS etabliert. Diese spezifiziert eine Vielzahl an Diagnoseservices, welche sowohl das einfache Auslesen einzelner Werte, als auch komplexere Vorgänge, wie die Durchführung von Flashvorgängen der Steuergeräte erlaubt. Zudem werden auch Services zur Authentifizierung spezifiziert, welche den Zugang zu Diagnosefunktionen einschränken können. Im Rahmen der Diagnosekommunikation agieren die Steuergeräte (ECUs) in den Fahrzeugen als Server und stellen je nach Hersteller und Modell unterschiedliche Services zur Verfügung, welche von Diagnosetestern als Clients aufgerufen werden können. In modernen Fahrzeugen liegt dabei zumeist ein Gateway zwischen dem Tester und der ECU, falls die Diagnose nicht direkt an einem Fahrzeugbus, sondern über den OBD-Port durchgeführt wird. Das für Nutzfahrzeuge vorgeschriebene WWH-OBD Diagnoseprotokoll basiert auf dem UDS Standard, fordert jedoch nur einen geringen Umfang an Services, wobei weitere Funktionalitäten optional von den Herstellern angeboten werden können.

Während es eine große Zahl von Protokollimplementierungen im Bereich der automobilen Systeme gibt, existierten in diesem Bereich zu Projektbeginn nur wenige öffentlich verfügbare Testtools mit IT-Sicherheit im Fokus. Scapy [117] ist eine frei verfügbare Bibliothek, welche eine Vielzahl an Protokollen, darunter auch aus dem Automobilbereich, implementiert und dabei programmatisch viele Möglichkeiten zur Paketgenerierung und -manipulation ermöglicht. Zusätzlich sind im Automobilbereich auch einzelne Scanner enthalten. Für die Verwendung der Scanner sind jedoch, mangels aufrufbereiter Programme, Programmierkenntnisse und Einarbeitung in die Funktionalität von Scapy erforderlich, was eine Hürde für potenzielle Nutzer darstellen kann. Sowohl gallia als auch Caring Caribou [118] bieten hingegen einfach auszuführende Skripte, die speziell auf den Automobilbereich ausgerichtet sind. Im Vergleich zu Caring Caribou bot gallia, welches kurz nach Projektbeginn im Rahmen vorangegangener Projekte veröffentlicht wurde, einen höheren Umfang an UDS Service-spezifischen Testskripten und wies eine umfangreichere Implementierung des UDS Standards auf. Weiterhin wurde in gallia auch bereits ein umfangreiches Logging-System integriert, um Testparameter und -ergebnisse nachvollziehbar zu dokumentieren. Da gallia zudem vom Projektteam bereits über mehrere Jahre erfolgreich an einer Vielzahl von realen Testaufbauten und Fahrzeugen entwickelt, getestet und produktiv eingesetzt wurde, und

entsprechend auch die Erfahrungen mit der Architektur und Weiterentwicklung des Tools hier bereits vorhanden waren, wurde gallia unter den evaluierten Alternativen für am besten geeignet für die Weiterentwicklung im Rahmen des Projekts eingestuft.

1.4.14 Entwicklung eines Testsystems für Ladekommunikation in E-Fahrzeugen

Im europäischen Markt hat sich das Combined Charging System (CCS) als wesentliches System zum Laden von Elektrofahrzeugen etabliert. Das aktuell noch gering verbreitete Megawatt Charging System (MCS) ist explizit für hohe Ladeleistungen für schwere Nutzfahrzeuge ausgelegt und soll entsprechend zukünftig in diesem Bereich an Bedeutung gewinnen. Beide Systeme sind, zuletzt im Rahmen der Alternative Fuels Infrastructure Regulation (AFIR), für den europäischen Markt als verbindliche Mindeststandards festgelegt worden. Während sich die maximalen Ladeleistungen und die verwendeten Steckertypen zwischen den Systemen unterscheiden, setzen beide im Kern auf digitale Kommunikation gemäß der internationalen ISO 15118 Normenreihe. Innerhalb der Normenreihe existieren die Standards ISO 15118-2 [119], welcher Anwendungsprotokolle für induktives Laden mit Gleich- oder Wechselstrom spezifiziert, sowie ISO 15118-20 [120], welcher zusätzlich Anwendungsprotokolle für induktives Laden als auch bidirektionales Laden spezifiziert. Ferner existiert mit DIN SPEC 70121 [121] ein weit verbreiteter Standard, welcher lediglich induktives Laden mit Gleichstrom unterstützt und dabei zu ISO 15118 kompatibel ist. Die Standards unterscheiden sich dabei jedoch nicht nur in ihrem Funktionsumfang, sondern auch in Bezug auf Sicherheitsanforderungen. So ist etwa die Absicherung der Kommunikation mit TLS 1.2 bei DIN SPEC 70121 und ISO 15118-2 im Wesentlichen optional, während ISO 15118-20 für alle Anwendungen TLS in der aktuellen Version 1.3 fordert. Das MCS wird gemäß den Vorgaben der AFIR voraussichtlich im Wesentlichen auf ISO 15118-20 setzen, während im CCS, auch aus Kompatibilitätsgründen, alle Standards bis auf Weiteres vertreten sein werden.

Ein weiterer Unterschied besteht in der Wahl des Kommunikationsprotokolls auf den untersten Protokollschichten. Hier setzt das MCS auf Ethernet, während CCS Homeplug Green PHY [122] verwendet. Letzteres ist anfällig für Übersprechen von Kommunikation zwischen Leitungen. So konnten Köhler et al. zeigen, dass Ladevorgänge mithilfe einfacher Hardware aus einigen Metern Entfernung zuverlässig beendet werden können, indem die kabelgebundene Kommunikation zwischen Fahrzeug und Ladestation über Funk gestört wird [123].

Wie in Abbildung 7 dargestellt, basiert die High-Level Kommunikation der betrachteten Systeme auf weit verbreiteten Technologien, etwa einem IPv6/TCP Stack für die Kommunikation der Anwendungsnachrichten nach ISO 15118 und DIN SPEC 70121, mit Ausnahme des SECC Discovery Protokolls (SDP), welches UDP als Transportprotokoll verwendet. Dadurch sind Fahrzeuge und Ladesysteme prinzipiell mit bereits vorhandenen Testtools kompatibel. Diese Kompatibilität wird jedoch dadurch eingeschränkt, dass die entsprechenden IPv6 Endpunkte oft nur während eines laufenden Ladevorgangs adressiert werden können. Entsprechend mühsam können Tests ausfallen, wenn die Ladekommunikation mehrfach manuell neu initiiert werden muss, etwa durch Ein- und Ausstecken des Ladesteckers, und Tests entsprechend iterativ auf mehrere Ladevorgänge aufgeteilt werden müssen.

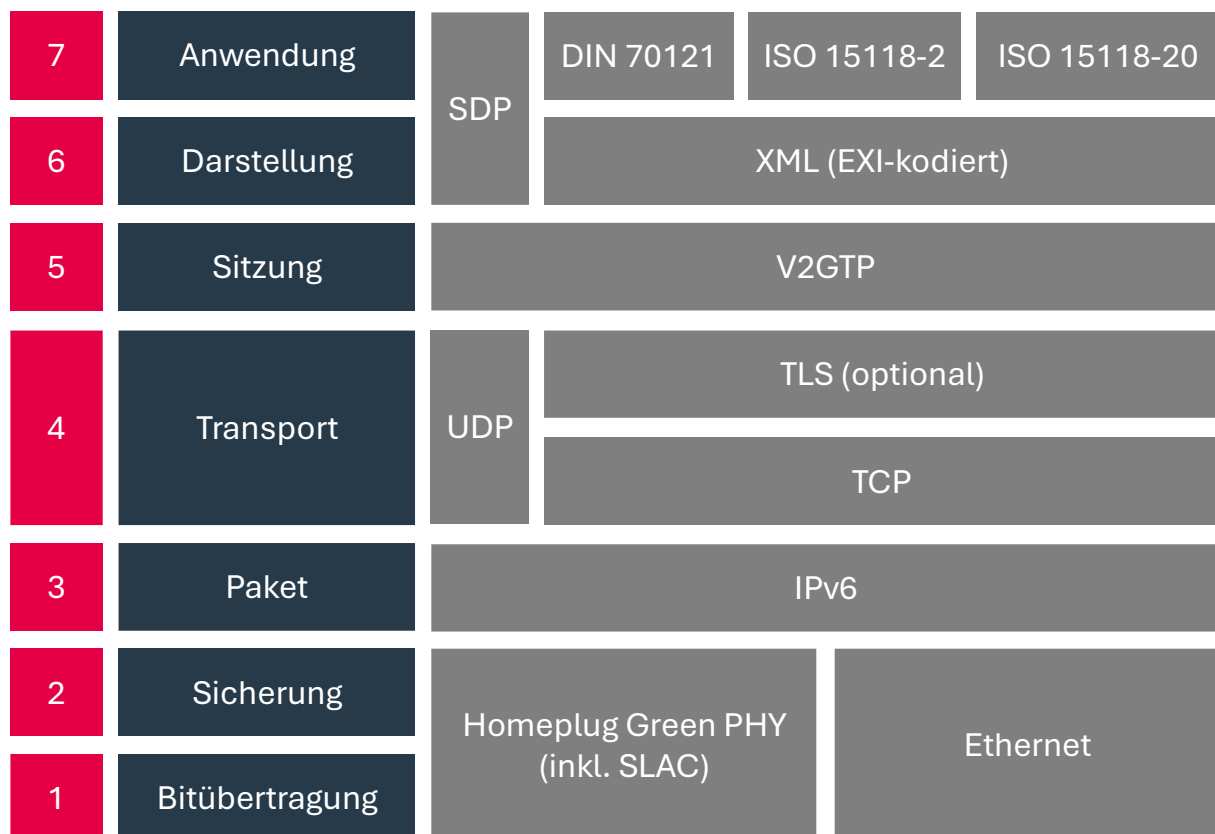


Abbildung 7: Protokollstapel der High-Level Ladekommunikation im ISO/OSI Schichtenmodell.

Zu Projektbeginn existierten bereits Implementierungen der ladespezifischen Protokolle, darunter etwa die von Qualcomm Atheros veröffentlichten open-plc-utils [124], welche Programme zur Verbindung von Fahrzeug und Ladestellen auf den untersten Protokollschichten mithilfe des Signal Level Attenuation Characterization (SLAC) Protokolls enthalten. Weiterhin zu nennen sind öffentlich verfügbare Implementierungen der in DIN SPEC 70121 und ISO 15118-2 und ISO 15118-20 spezifizierten Kommunikation auf den höheren Protokollschichten, etwa Everest [125] oder das in Python programmierte iso15118 [126]. Jedoch ist mit diesen Tools zunächst nur aufwändiges manuelles Testen möglich. Die Programme sind zudem nicht auf Security-Testing ausgelegt, sondern zielen auf standardkonformes Verhalten ab. Frei verfügbare Security-Testtools, speziell für die Ladekommunikation, konnten zum Projektbeginn nicht identifiziert werden.

Auch in Bezug auf die benötigte Hardware konnten zum Projektbeginn keine Produkte identifiziert werden, welche einen flexiblen programmatischen Ansatz zur Kopplung von Ladestelle und Fahrzeug ermöglichen.

Entsprechend zeichnete sich der Bedarf ab, speziell auf diesen Anwendungsfall zugeschnittene Testtools, sowie dafür ausgelegtes Testequipment, im Rahmen des Projekts zu entwickeln.

1.4.15 Entwicklung eines Test-Frameworks für V2X

In der EU ist C-ITS die am weitesten verbreitete V2X-Variante. Der Standard wird von mehreren verschiedenen europäischen Organisationen verwaltet, wie das European Telecommunications Standards Institute (ETSI), die European Standardization Organization (ESO), das European Committee for Standardization (CEN), sowie das CAR 2 CAR Communication Consortium (C2CCC).

Technisch verwendet C-ITS das 5.9 GHz Frequenzband und baut auf dem IEEE 802.11p WLAN-Standard auf.

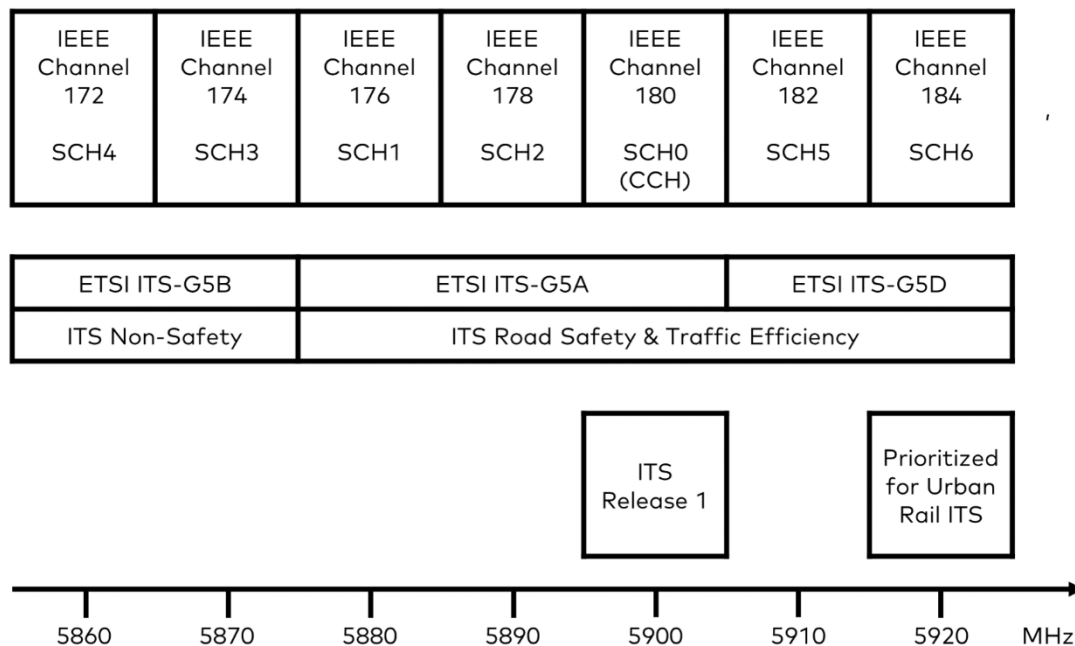


Abbildung 8: C-ITS Frequenzband

Über die Networking- und Transportschichten GeoNet und BTP werden die Nachrichten ausgetauscht. Darauf setzen die Kernfunktionalitäten in der Form von Cooperative Awareness Message (CAM) und Decentralized Environmental Notification Message (DENM) Nachrichten auf. Bei CAM handelt es sich um zyklische Nachrichten, die Informationen über den Zustand des Fahrzeugs, wie etwa seine Position, Geschwindigkeit, Fahrtrichtung und Fahrzeugtyp enthalten. DENMs werden event-basiert ausgelöst und signalisieren beispielsweise ein stehendes Fahrzeug auf der Straße, einen Unfall, gefährliche Straßenverhältnisse (z. B. Eis) oder Baustellen.

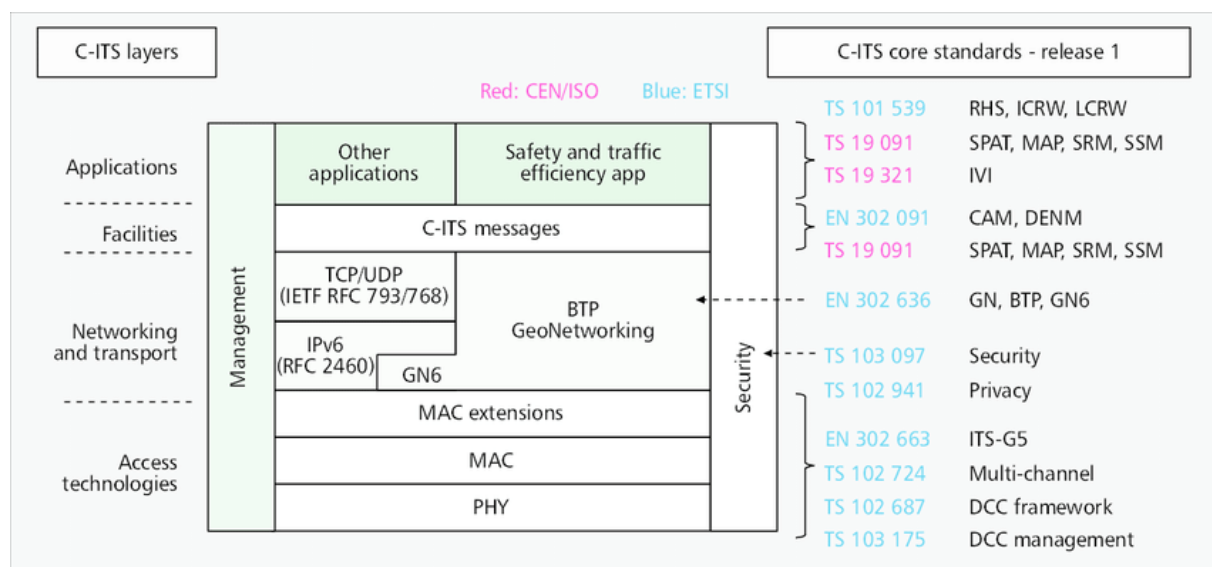


Abbildung 9: C-ITS Protokoll Stack mit den zugehörigen ETSI Standards [127].

Das C-ITS-Sicherheitskonzept basiert auf einer von der Europäischen Kommission verwalteten PKI. Das Vertrauensmodell und die PKI-Architektur sind in Abbildung 10 dargestellt. Die Europäische Kommission führt die European Certificate Trust List (ECTL), eine Liste vertrauenswürdiger Zertifizierungsstellen für C-ITS. Sie definiert drei Konformitätsstufen:

- Level 0 für Test- und Proof-of-Concept-Projekte
- Level 1 für Produktionssysteme mit vorübergehender Konformität
- Level 2 für Produktionssysteme mit vollständiger Konformität

Derzeit betreibt Microsec die einzige PKI, die auf Stufe 1 und 2 akzeptiert ist. Außerdem betreibt das Unternehmen die offizielle C2CCC-Pilot-PKI auf Stufe 0. Der Volkswagen-Konzern nutzt die ECTL-Stufen 1 und 2 noch nicht, sondern verwendet stattdessen eine eigene Vertrauensliste. Um die Kompatibilität zwischen beiden zu gewährleisten, wurde ein gemeinsamer Dienst (Level 1-ready) eingerichtet.

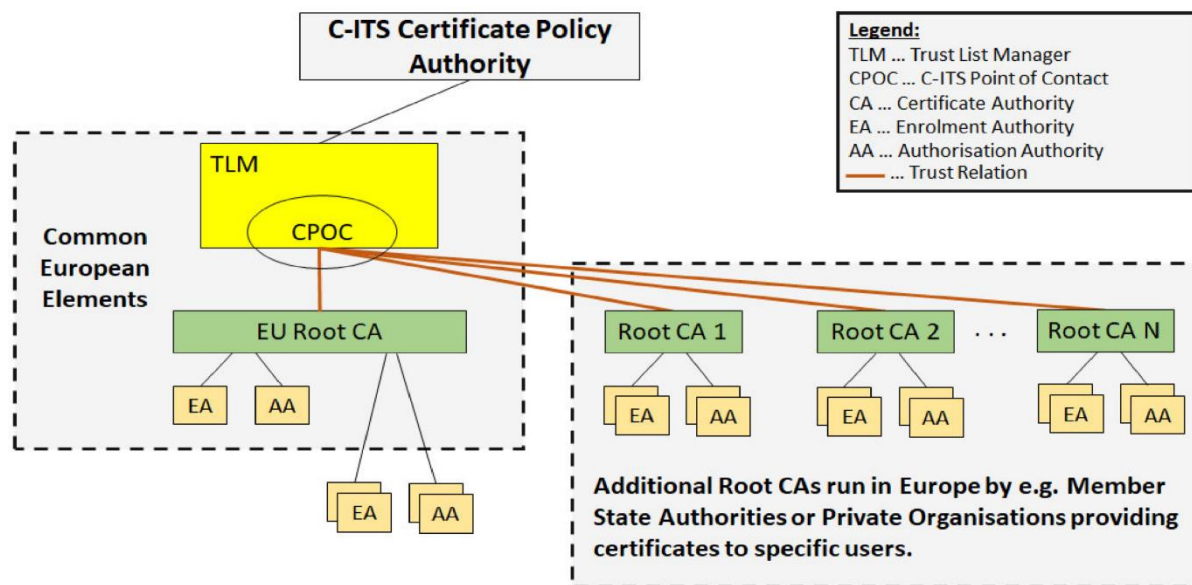


Abbildung 10: C-ITS-Vertrauensmodellarchitektur [128].

Innerhalb der C-ITS-PKI sind verschiedene Rollen definiert, darunter vor allem:

- die *Enrollment Authority*, die langfristige Registrierungszertifikate ausstellt, die die Identität einer Station an ihr Schlüsselmaterial binden, und
- die *Authorization Authority*, die kurzfristige Autorisierungstickets ausstellt, die es einer Station ermöglichen, Nachrichten anonym zu übertragen.

1.4.16 Modul-Baukasten Woodpecker zur statischen Code Analyse

Zu Projektbeginn standen verschiedene leistungsfähige SAST-Tools zur Verfügung, die jedoch schwer zu bedienen sind, unterschiedliche Eingaben und Ausgaben erwarten und erzeugen. Ein verbreitetes Problem sind hohe Raten an False Positives, die Entwicklerinnen und Entwickler bei großen Codebasen schnell überfordern [129, 130, 131].

Die Embedded-/Automotive-Domäne stellt zusätzliche Herausforderungen:

- Hardware-nahe, CPU-architekturspezifische Programmierung.
- Häufig speicherunsichere Sprachen (C/C++).

- Sehr große, modulare Softwareprojekte aus verschiedenen Zulieferungen, teils ohne vollständigen Quellcodezugriff; Analysen oft nur auf Teilmodulen mit unvollständigem Code und fehlenden Abhängigkeiten möglich.
- Proprietäre, Windows-basierte Entwicklungsumgebungen sind verbreitet.
- Oft keine einheitlichen, modernen Build-Umgebungen (kein durchgängiger Offline- oder Docker-Build).

1.4.17 Security-Risikoanalyse eines automatisierten Fahrsystems

Derzeit gibt es kein einheitliches Modell für ein ADS aus Sicherheitsperspektive, aber in der Literatur lassen sich einige gemeinsame Merkmale beobachten. Ein schlankes Modell, bestehend aus Wahrnehmung, Netzwerk und ADS-Anwendung/Steuerung, wird häufig für Risikoanalysen [132] und die Untersuchung von Sicherheits Herausforderungen für ADS [133] verwendet. In detaillierteren Modellen wird ein ADS als Pipeline beschrieben, in der Sensoren wie GPS, LiDAR oder Kameras Umgebungszustände erfassen, die mit zusätzlichen Informationen fusioniert werden können. Diese Daten werden dann für die Objekterkennung/-verfolgung und -lokalisierung verwendet und anschließend für die Bewertung und Verhaltensvorhersage genutzt, was wiederum die Planung und schließlich das Steuermodul zum Betrieb der Aktoren antreibt. Diese Aktionen führen dann zu einem neuen Umgebungszustand und starten somit den Regelkreis von Neuem [134, 135]. Dieses Modell wird häufig um die Fahrzeug-zu-Alles-Kommunikation (Vehicle-to-Everything, V2X) erweitert, wie z. B. Kartenaktualisierungen oder Kommunikation für Platooning [37, 135].

Mehrere Autoren haben die Sicherheit von vernetzten und autonomen Fahrzeugen (CAVs) analysiert, indem sie veröffentlichte Angriffe und Abwehrmaßnahmen untersuchten [37, 133, 36]. Ihre Analyse lässt sich in vier Bereiche unterteilen: Sensorik, Steuerung, fahrzeuginterne Kommunikation und V2X-Kommunikation. Bei Sensorik-Angriffen sind GNSS-Spoofing [136] oder Ultraschall-Störsignale [137] weit verbreitet, und immer mehr Veröffentlichungen konzentrieren sich auf Angriffe auf maschinelle Lernmodelle, die LiDAR- oder Kameradaten interpretieren, um Hindernisse, Verkehrsteilnehmer oder Verkehrszeichen zu erkennen [138, 139, 140]. Im Bereich der Steuerung sind mehrere Angriffe auf elektronische Steuergeräte (ECUs) von Fahrzeugen bekannt, die sich aufgrund ihrer Vernetzung auf Telematik- und Infotainmentsysteme konzentrieren [141]. Die fahrzeuginterne Kommunikation verwendet nach wie vor Protokolle wie CAN, LIN und FlexRay, die nicht unter Berücksichtigung von Sicherheitsaspekten entwickelt wurden. Daher sind die Protokolle anfällig für Angriffe wie Eavesdropping oder Angriffen durch Spoofing oder Manipulation (S/M) von Fahrzeug-zu-Fahrzeug-Kommunikation [142, 143]. V2X umfasst ein breites Spektrum, angefangen bei der Kommunikation zwischen Schlüsselanhängern und Schließsystemen, die bekanntermaßen anfällig sind [144]. Die Ausweitung auf die Fahrzeug-zu-Fahrzeug- oder Fahrzeug-zu-Infrastruktur-Kommunikation eröffnet auch neue Angriffsmöglichkeiten durch Sybil- oder Identitätsdiebstahl-Angriffe [145].

Eine häufig zitierte CRA-Methode ist RACE, die 2015 von Boudguiga et al. [43] vorgeschlagen wurde. Sie erweitern das EVITA-Framework um einen verbesserten Angriffsbaum und Angriffstechniken und beschränken die Angriffsmethoden auf fünf Typen. Das Risiko wird dann als Summe aus Kontrollierbarkeit und dem Produkt aus Schweregrad und Angriffswahrscheinlichkeit berechnet. Sie führen jedoch keine detaillierte Analyse eines CAV durch, sondern gehen in ihrer Folgearbeit [44] näher darauf ein. Park et al. konzentrieren sich auf die Vereinfachung des Risikoanalyseprozesses [146]. Zur Berechnung des Risikos summieren sie die vier Risikokategorien

Wahrscheinlichkeit, Auswirkung, Exposition und Wiederherstellung, die sich wiederum aus drei Risikofaktoren zusammensetzen. Die Faktoren werden gewichtet und anschließend bewertet, um die Punktzahl einer Kategorie zu ermitteln. Ihre Analyse konzentriert sich auf die Hauptfunktionen von CAVs: Over-the-Air-Funktionen (OTA) für das Automobil- und Kollisionsvermeidung. Das anfängliche Risiko in ihrer Methode ist für OTA kritisch, wird jedoch durch die Überprüfung bekannter Schwachstellensignaturen, die Verifizierung von Softwaresignaturen, den Einsatz von Intrusion Detection and Prevention Systems (IDPS) und die Verschlüsselung während der Übertragung auf ein geringes Risiko gesenkt. Für die Kollisionsvermeidungsfunktion ist das anfängliche Risiko gering und wird durch den Einsatz von IDPS, sicherem Flashen und Booten sowie sicherem OTA-Patching auf ein vernachlässigbares Maß reduziert. Cui et al. waren die ersten, die mit ihrer Methode VeRA die menschliche Kontrollfähigkeit und den Automatisierungsgrad des Fahrzeugs berücksichtigten, wobei sie sich zusätzlich auf Effizienz und Benutzerfreundlichkeit konzentrierten [147]. VeRA beschreibt das Risiko als Produkt aus Angriffswahrscheinlichkeit und Schweregrad und fügt die menschliche Kontrolle hinzu. Zur Berechnung der Angriffswahrscheinlichkeit werden die erforderlichen Geräte und Kenntnisse bewertet, und der Schweregrad wird in den Kategorien Sicherheit, Datenschutz, Finanzen und Betrieb bewertet. Bei der menschlichen Kontrolle werden die Erfahrung des Fahrers und der Automatisierungsgrad des Fahrzeugs berücksichtigt. Cui et al. führen eine Fallstudie durch, um VeRA zu testen und mit anderen Methoden zu vergleichen. Es werden drei verschiedene Automatisierungsstufen und zwei Funktionen bewertet: Die erste Funktion, das kognitive Fahrintelligenzsystem, besteht aus sieben Unterfunktionen, für die 116 detaillierte Angriffe analysiert werden. Die zweite Funktion, das Fahrzeugmanipulationssystem, besteht aus drei Unterfunktionen, für die 264 detaillierte Angriffe analysiert werden.

1.4.18 Security-Risikoanalyse eines Control Centers

Control Center für vernetzte und automatisierte Fahrzeuge sind in der Literatur und Praxis bislang vor allem aus Betriebs-, Funktions- und Safety-Perspektive beschrieben worden (z. B. Leitstände für flottenbasierte Logistik, teleoperierte Systeme, Network Operations Center). Arbeiten zu Cybersicherheit fokussieren überwiegend auf generische Backend- und Cloud-Infrastrukturen, ISMS-Ansätze nach ISO/IEC 27001 oder auf sicherheitskritische industrielle Leitstände, jedoch selten auf Control Center, die unmittelbar mit hoch- oder vollautomatisierten Fahrzeugen interagieren.

Bekannte Beiträge adressieren u. a.:

- Security von Backend-Systemen für Connected Cars (Fernzugriff, OTA-Updates, Flottenservices),
- Absicherung cloudbasierter Microservice-Architekturen (Zero Trust, mTLS, Härtung von Internet-Facing Services),
- Teleoperations- und Remote-Assistance-Szenarien, insbesondere Anforderungen an Latenz, Verfügbarkeit und Integrität.

Konkrete, modellbasierte Security-Risikoanalysen für Control Center im Kontext von L4-Lkw – mit expliziter Kopplung an das Fahrzeug-CSMS, an Cloud/IT-Backends und an regulatorische Vorgaben (UN R155, ISO/SAE 21434, ISO/IEC 27001, IEC 62443) – waren zu Projektbeginn jedoch kaum veröffentlicht. Die im Projekt durchgeführte Risikoanalyse schließt diese Lücke, indem sie die Methode MoRA auf ein realistisch dimensioniertes Control-Center-System anwendet und dabei sowohl klassische IT-Bedrohungen (z. B. Web-/API-Angriffe, DDoS, Cloud-Konfigurationsfehler) als

auch die besonderen Safety- und Betriebsrisiken einer flächendeckenden MRM-Auslösung oder falschen Routenplanung berücksichtigt.

Verwendete Fachliteratur

- [1] D. Angermeier, K. Beilke, G. Hansch und J. Eichler, „Modeling security risk assessments,“ 2019.
- [2] D. Angermeier, H. Wester, K. Beilke, G. Hansch und J. Eichler, „Security risk assessments: Modeling and risk level propagation,“ *ACM Transactions on Cyber-Physical Systems*, Bd. 7, Nr. 1, pp. 1-25, 2023.
- [3] S. Kim und R. Shrestha, *Automotive Cyber Security: Introduction, Challenges, and Standardization*, Singapore: Springer, 2020.
- [4] United Nations Economic Commission for Europe, „Three landmark UN vehicle regulations enter into force,“ 2021. [Online]. Available: <https://unece.org/sustainable-development/press/three-landmark-un-vehicle-regulations-enter-force>.
- [5] United Nations Economic Commission for Europe, „UN Regulation No. 155: Uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system: UNECE R155,“ 2021.
- [6] United Nations Economic Commission for Europe, „UN Regulation No. 156: Uniform provisions concerning the approval of vehicles with regards to software update and software updates management system: UNECE R156,“ 2021.
- [7] State Administration for Market Regulation and Standardization Administration of the People's Republic of China, „National Standard of the People's Republic of China: Technical requirements for vehicle cybersecurity: GB 44495-2024,“ 2024.
- [8] Automotive Research Association of India, „Approval of Vehicles with regards to Cyber Security and Cyber Security Management system: AIS-189 Draft D2,“ 2022. [Online]. Available: <https://hmr.araiindia.com/api/AISFiles/Draft%20D2%20AIS%20189%20CSMS%20d03bb4df-a961-4647-ace0-49e298078567.pdf>.
- [9] T. NXP, „Future Advances in Body Electronics,“ 20 November 2015. [Online]. Available: <https://www.nxp.com/docs/en/whitepaper/BODYDELECTRWP.pdf>.
- [1] OECD, „Enhancing Access to and Sharing of Data,“ 2019-11-26.
0]
- [1] J. Heurix, P. Zimmermann, T. Neubauer und S. Fenz, „A taxonomy for privacy enhancing technologies,“ *Computers & Security*, pp. 1-17, 09/2015.
- [1] I. Kunz und A. Binder, „Application-Oriented Selection of Privacy Enhancing Technologies,“
2] 2022, pp. 75-87.
- [1] A. Giehl, N. Wiedermann, M. T. Gholamzadeh und C. Eckert, „Integrating security
3] evaluations into virtual commissioning,“ 2020.
- [1] M. Jansson, „Annual analysis reveals steady growth in industrial network market,“ HMS
4] Networks, 2024.
- [1] A. Giehl und S. Plaga, „Implementing a performant security control for industrial Ethernet,“
5] 2018.

- [1 A. Giehl, M. P. Heint und V. Embacher, „EmuFlex: A Flexible OT Testbed for Security
6] Experiments with OPC UA,“ 2024.
- [1 M. Rocchetto, A. Ferrari und V. Senni, „Challenges and opportunities for model-based
7] security risk assessment of cyber-physical systems,“ in *Resilience of Cyber-Physical Systems: From Risk Modelling to Threat Counteraction*, 2019, pp. 25-47.
- [1 ISA, „Enterprise-Control System Integration – Part 1: Models and Terminology,“ The
8] International Society of Automation, Research Triangle Park, North Carolina, USA, 2010.
- [1 S. Plaga, S. Tatschner und T. Neue, „Logboat — a simulation framework enabling CAN
9] security assessments,“ 2016.
- [2 H. Kagermann, J. Helbig, A. Hellinger und W. Wahlster, „Recommendations for
0] implementing the strategic initiative INDUSTRIE 4.0: Securing the future of German manufacturing industry; final report of the Industrie 4.0 Working Group,“ Forschungsunion, 2013.
- [2 A. Giehl und N. Wiedermann, „Security verification of third party design files in
1] manufacturing,“ 2018.
- [2 J. Deichmann, B. Klein, G. Scherf und R. Stütze, „The race for cybersecurity: Protecting the
2] connected car in the era of new regulation,“ 2019. [Online]. Available: <https://www.mckinsey.com/~media/McKinsey/Industries/Automotive%20and%20Assembly/Our%20Insights/The%20race%20for%20cybersecurity-Protecting-the-connected-car-in-the-era-of-new-regulation.pdf>.
- [2 OWASP Foundation, „OWASP Mobile Application Security Verification Standard (MASVS),“
3] 2024. [Online]. Available: <https://mas.owasp.org/MASVS/>.
- [2 S. Halder, A. Ghosal und M. Conti, „Secure over-the-air software updates in connected
4] vehicles: A survey,“ *Computer Networks*, Bd. 178, p. 107343, 2020.
- [2 International Organization for Standardization, „ISO 24089:2023 Road vehicles – Software
5] update engineering,“ Geneva, 2023.
- [2 I. E. Carvajal-Roca, J. Wang, J. Du und S. Wei, „A Semi-Centralized Dynamic Key
6] Management Framework for In-Vehicle Networks,“ *IEEE Transactions on Vehicular Technology*, Bd. 70, Nr. 10, pp. 10864-10879, 2021.
- [2 International Organization for Standardization and Society of Automotive Engineers,
7] „ISO/SAE 21434:2021 Road vehicles - Cybersecurity engineering,“ Geneva, 2021.
- [2 International Organization for Standardization and International Electrotechnical
8] Commission, „ISO/IEC 27000:2018 Information technology - Security techniques - Information security management systems - Overview and vocabulary,“ Geneva, 2018.
- [2 International Electrotechnical Commission, „IEC/TS 62443-1-1:2009 Industrial
9] communication networks - Network and system security - Part 1-1: Terminology, concepts and models,“ Geneva, 2009.
- [3 C. Schmittner und G. Macher, „Automotive cybersecurity standards - relation and
0] overview,“ Berlin, Heidelberg, 2019.
- [3 „Gallia - Extendable Pentesting Framework,“ [Online]. Available:
1] <https://github.com/Fraunhofer-AISEC/gallia>.
- [3 International Organization for Standardization, „Road vehicles — Unified diagnostic
2] services (UDS) - Part 1: Application layer,“ 2020.

- [3] International Organization for Standardization, „Road vehicles — Implementation of World-
3] Wide Harmonized On-Board Diagnostics (WWH-OBD) communication requirements - Part
3: Common message dictionary,“ 2012.
- [3] International Electrotechnical Commission, „Electric vehicle conductive charging system -
4] Part 1: General requirements,“ 2017.
- [3] Autobahnen- und Schnellstraßen-Finanzierungs-Aktiengesellschaft (ASFINAG), „Mission C-
5] ITS (Deutsch),“ 2023. [Online]. Available:
<https://www.youtube.com/watch?v=Qda83JK6Sho>.
- [3] K. Kim, J. S. Kim, S. Jeong, J. H. Park und H. K. Kim, „Cybersecurity for autonomous vehicles:
6] Review of attacks and defense,“ *Computers & Security*, Bd. 103, 2021.
- [3] C. Gao, G. Wang, W. Shi, Z. Wang und Y. Chen, „Autonomous driving security: State of the
7] art and challenges,“ *IEEE Internet of Things Journal*, Bd. 9, 2022.
- [3] SAE International, „SAE J3016:2021 – Taxonomy and Definitions for Terms Related to Driving
8] Automation Systems for On-Road Motor Vehicles,“ 2021.
- [3] IRU Intelligence Briefing, „Driver shortage global report 2022,“ 2022.
9]
- [4] Federal Ministry for Digital and Transport, „Germany will be the world leader in autonomous
0] driving,“ [Online].
- [4] United Nations Economic Commission for Europe, „UN Regulation No. 155 – Uniform
1] provisions concerning the approval of vehicles with regards to cyber security and cyber
security management system,“ 2021.
- [4] International Organization for Standardization; SAE International, „ISO/SAE 21434:2021 –
2] Road Vehicles – Cybersecurity Engineering,“ 2021.
- [4] A. Boudguiga, A. Boulanger, P. Chiron, W. Klaudel, H. Labiod und J. C. Seguy, „RACE: Risk
3] analysis for cooperative engines,“ 2015.
- [4] J. P. Monteuiis, A. Boudguiga, J. Zhang, H. Labiod, A. Servel und P. Urien, „SARA: Security
4] automotive risk analysis method,“ 2018.
- [4] G. Macher, H. Sporer, R. Berlach, E. Armengaud und C. Kreiner, „SAHARA: A security-aware
5] hazard and risk analysis method,“ 2015.
- [4] C. Schmittner, T. Gruber, P. Puschner und E. Schoitsch, „Security application of failure
6] mode and effect analysis (FMEA),“ in *Computer Safety, Reliability, and Security*, Cham,
Springer International Publishing, 2014, pp. 310-325.
- [4] International Electrotechnical Commission, „IEC 62443-3-2:2020 Security for industrial
7] automation and control systems - Part 3-2: Security risk assessment for system design,“
Geneva, 2020.
- [4] International Organization for Standardization and International Electrotechnical
8] Commission, „ISO/IEC 27005:2022 Information security, cybersecurity and privacy
protection - Guidance on managing information security risks,“ Geneva, 2022.
- [4] International Organization for Standardization and International Electrotechnical
9] Commission, „ISO/IEC 27001:2022 Information security, cybersecurity and privacy
protection - Information security management systems - Requirements,“ Geneva, 2022.
- [5] International Organization for Standardization and International Electrotechnical
0] Commission, „ISO/IEC 27003:2017 Information technology - Security techniques -
Information security management systems - Guidance,“ Geneva, 2017.

- [5] International Electrotechnical Commission, „IEC 62443-2-1:2024 Security for industrial automation and control systems - Part 2-1: Security program requirements for IACS asset owners,“ Geneva, 2024.
- [5] G. Costantino, M. De Vincenzi und I. Matteucci, „In-depth exploration of ISO/SAE 21434 and its correlations with existing standards,“ *IEEE Communications Standards Magazine*, Bd. 6, Nr. 1, pp. 84-92, 2022.
- [5] F. Djebbar und K. Nordström, „A comparative analysis of industrial cybersecurity standards,“ *IEEE Access*, Bd. 11, pp. 85315-85332, 2023.
- [5] H. Taherdoost, „Understanding cybersecurity frameworks and information security standards—a review and comprehensive overview,“ *Electronics*, Bd. 11, Nr. 14, 2022.
- [5] R. do Carmo und A. Schlensog, *Automotive Threat Analysis and Risk Assessment in Practice: A Practical Guide to TARA Following the ISO/SAE 21434 Standard for Automotive Embedded and IT/OT Systems*, 1 Hrsg., Berlin, Heidelberg: Springer Berlin, Heidelberg, 2024.
- [5] U.S. Department of Transportation: National Highway Traffic Safety Administration, „Cybersecurity Best Practices for the Safety of Modern Vehicles,“ 2022. [Online]. Available: <https://www.nhtsa.gov/sites/nhtsa.gov/files/2022-09/cybersecurity-best-practices-safety-modern-vehicles-2022-pre-final-tag%20%200.pdf>.
- [5] ISO and SAE, „Road vehicles - Cybersecurity Engineering,“ Geneva and Warrendale, 2021.
- [5] G. Costantino, M. Vincenzi und I. de Matteucci, „A comparative analysis of UNECE WP.29 R155 and ISO/SAE 21434,“ 2022.
- [5] R. Bohara, M. Ross, S. Rahlfs und S. Ghatta, „Cyber Security and Software Update Management System for Connected Vehicles in compliance with UNECE WP.29, R155 and R156,“ 2023.
- [6] Y. Han, X. Zhao, K. He und Y. Qin, „Automotive cyber security test method for UN-R155 regulation,“ 2022.
- [6] C. Köllner, „Was die Cybersecurity-Richtlinien für die Autobranche bedeuten,“ 2024. [Online]. Available: <https://www.springerprofessional.de/cyber-sicherheit/automobilelektronik---software/was-die-cybersecurity-richtlinien-fuer-die-autobranche-bedeuten/27274236>.
- [6] B. Kanmaz, „Automotive cybersecurity regulations and standards,“ 2025. [Online]. Available: <https://diconium.com/en/blog/automotive-cybersecurity-regulations-and-standards>.
- [6] G. M. Garrido, K. Schmidt, C. Harth-Kitzerow, J. Klepsch, A. Luckow und F. Matthes, „Exploring privacy-enhancing technologies in the automotive value chain,“ 2021.
- [6] E. Bahrami, A. Abdullahi und T. Dargahi, „SoK: Privacy, Security, and Ethical Considerations in Vehicular Data Monetization,“ New York, NY, USA, 2025.
- [6] N. Yuca, N. Matyunin, E. Arzoglou, N. A. Anagnostopoulos und S. Katzenbeisser, „A Survey on Privacy-Preserving Computing in the Automotive Domain,“ New York, NY, USA, 2025.
- [6] S. Pape, S. Syed-Winkler, A. M. Garcia, B. Chah, A. Bkakra, M. Hiller, T. Walcher, A. Lombard, A. Abbas-Turki und R. Yaich, „A Systematic Approach for Automotive Privacy Management,“ in *ACM Computer Science in Cars Symposium*, New York, NY, USA, 2023.
- [6] EU Artificial Intelligence Act, „The AI Act Explorer | EU Artificial Intelligence Act,“ [Online]. Available: <https://artificialintelligenceact.eu/ai-act-explorer/>.

- [6] Europäisches Parlament und Rat der Europäischen Union, „Verordnung (EU) 2019/2144 des
8] Europäischen Parlaments und des Rates vom 27. November 2019 über die
Typgenehmigung von Kraftfahrzeugen und Kraftfahrzeuganhängern sowie von Systemen,
Bauteilen und selbstständigen technischen Einheiten für diese Fahrzeuge im Hinblick auf
ihre allgemeine Sicherheit und den Schutz der Fahrzeuginsassen und von ungeschützten
Verkehrsteilnehmern“, 2019.
- [6] B. Xia, „Towards Concrete and Connected AI Risk Assessment (C²AIRA): A Systematic
9] Mapping Study“, *arXiv*, 24 05 2023.
- [7] E. Tabassi, „Artificial Intelligence Risk Management Framework (AI RMF 1.0)“, Gaithersburg,
0] MD, 2023.
- [7] D. Angermeier, A. Nieding und J. Eichler, „Supporting Risk Assessment with the Systematic
1] Identification, Merging, and Validation of Security Goals“, in *Risk Assessment and Risk-
Driven Quality Assurance (RISK 2016)*, Bd. 10224, Cham, Springer, 2017.
- [7] G. Stettinger, P. Weissensteiner und S. Khastgir, „Trustworthiness Assurance Assessment
2] for High-Risk AI-Based Systems“, *IEEE Access*, Bd. 12, pp. 22718-22745, 2024.
- [7] D. Golpayegani, „AI Cards: Towards an Applied Framework for Machine-Readable AI and
3] Risk Documentation Inspired by the EU AI Act“, *arXiv*, 2024.
- [7] M. Keser, Y. Shoeb und A. Knoll, „How Could Generative AI Support Compliance with the EU
4] AI Act? A Review for Safe Automated Driving Perception“, 2024.
- [7] G. Schmalzried, „Künstliche Intelligenz – AI Act in Kraft: Was stimmt nicht mit Europas KI-
5] Verordnung?“, 2024. [Online]. Available:
[https://www.br.de/nachrichten/netzwerk/kuenstliche-intelligenz-AI-Act-in-kraft-was-
stimmt-nicht-mit-europas-ki-verordnung,UKsMiAJ](https://www.br.de/nachrichten/netzwerk/kuenstliche-intelligenz-AI-Act-in-kraft-was-stimmt-nicht-mit-europas-ki-verordnung,UKsMiAJ).
- [7] Business Reporter, „The Pros and Cons of Regulating AI“, [Online]. Available:
6] <https://www.business-reporter.co.uk/sustainability/the-pros-and-cons-of-regulating-ai>.
- [7] German AI Association, „Position Paper on the EU AI Act: Remaining Issues and Current
7] Discussions in the European Parliament“, 2023. [Online]. Available: [https://ki-
verband.de/wp-content/uploads/2023/04/PositionPaper_AI-Act_German-AI-
Association_April2023.pdf](https://ki-verband.de/wp-content/uploads/2023/04/PositionPaper_AI-Act_German-AI-Association_April2023.pdf).
- [7] IEEE, „IEEE Standard for Information Technology – Telecommunications and Information
8] Exchange Between Systems Local and Metropolitan Area Networks – Specific
Requirements - Part 11: Wireless Local Area Network (LAN) Medium Access Control (MAC)
and Physical Layer (PHY) Specifications“, 2020.
- [7] IEEE, „IEEE Standard for Wireless Access in Vehicular Environments – Security Services for
9] Application and Management Messages“, 2023.
- [8] J. B. Kenney, „Dedicated Short-Range Communications (DSRC) Standards in the United
0] States“, *Proceedings of the IEEE*, Bd. 99, Nr. 7, pp. 1162-1182, 2011.
- [8] A. Festag, „Standards for vehicular communication—from IEEE 802.11p to 5G“, *e & i
1] Elektrotechnik und Informationstechnik*, Bd. 132, Nr. 7, pp. 409-416, 11 2015.
- [8] ITS Connect Promotion Consortium, „ITS Connect“, 2025. [Online]. Available:
2] <https://www.itsconnect-pc.org/en/>. [Zugriff am 12 12 2024].
- [8] C. Suthaputchakun und Z. Sun, „Routing protocol in intervehicle communication systems:
3] a survey“, *IEEE Communications Magazine*, Bd. 49, Nr. 12, pp. 150-156, 2011.
- [8] X. Wang, S. Mao und M. X. Gong, „An Overview of 3GPP Cellular Vehicle-to-Everything
4] Standards“, *GetMobile: Mobile Comp. and Comm.*, Bd. 21, Nr. 3, pp. 19-25, 11 2017.

- [8 NXP Semiconductors, „C-ITS: Three observations on LTE-V2X and ETSI ITS-G5 — A
5] comparison,“ 2018.
- [8 A. Neumann, „Approaches for In-vehicle Communication - An Analysis and Outlook,“ in
6] *Computer Networks - 24th International Conference, CN 2017, Łądek Zdrój, Poland, June 20-23, 2017, Proceedings*, Bd. 718, Springer, 2017, pp. 395-411.
- [8 S. Lindner, D. Merling, M. Häberle and M. Menth, "P4-Protect: 1+1 Path Protection for P4," in
7] *Proceedings of the 3rd P4 Workshop in Europe*, Barcelona Spain, 2020.
- [8 J. T. Yu, „A practical and effective approach to implementing High Availability Seamless
8] Redundancy (HSR),“ in *2017 IEEE Conference on Dependable and Secure Computing*, Taipei, 2017.
- [8 F.-f. Li, X.-z. Yu und G. Wu, „Design and Implementation of High Availability Distributed
9] System Based on Multi-level Heartbeat Protocol,“ in *2009 IITA International Conference on Control, Automation and Systems Engineering (case 2009)*, Zhangjiajie, 2009.
- [9 R. Li, N. Huang, S. Li, R. Kang und S. Chang, „Reliability testing technology for computer
0] network applications,“ in *2009 8th International Conference on Reliability, Maintainability and Safety*, Chengdu, 2009.
- [9 E. Calle, J. L. Marzo and A. Urra, "Protection performance components in MPLS networks,"
1] *Computer Communications*, vol. 27, p. 1220–1228, July 2004.
- [9 C. Arendt, M. Patchou, S. Bocker, J. Tiemann und C. Wietfeld, „Pushing the Limits:
2] Resilience Testing for Mission-Critical Machine-Type Communication,“ in *2021 IEEE 94th Vehicular Technology Conference (VTC2021-Fall)*, Norman, 2021.
- [9 M. A. Chang, B. Tschaen, T. Benson and L. Vanbever, "Chaos Monkey: Increasing SDN
3] Reliability through Systematic Network Destruction," *ACM SIGCOMM Computer Communication Review*, vol. 45, p. 371–372, September 2015.
- [9 K.-H. Niemann, „IT security extensions for PROFINET,“ 2019.
4]
- [9 M. P. Heinl, M. Pursche, N. Puch, S. N. Peters und A. Giehl, „From Standard to Practice:
5] Towards ISA/IEC 62443-Conform Public Key Infrastructures,“ 2023.
- [9 T. Feng, S. Wang, X. Gong und J. Fang, „Formal security evaluation and improvement of
6] industrial Ethernet EtherCAT protocol,“ *Journal of Computer Research and Development*, 2020.
- [9 D. Han, Y. Zhao und Y. Gong, „Design of multi-protocol industrial Ethernet security monitor,“
7] 2021.
- [9 G. Yu und T. Shon, „Security and forensic analysis for industrial Ethernet protocols,“ 2022.
8]
- [9 T. Prantl, T. Zeck, A. Bauer, P. Ten, D. Prantl, A. Yahya, L. Iffländer, A. Dmitrienko, C. Krupitzer
9] und S. Kounev, „A Survey on Secure Group Communication Schemes With Focus on IoT Communication,“ *IEEE Access*, Bd. PP, pp. 1-1, 01 2022.
- [1 H. Xiong, Y. Wu und Z. Lu, „A Survey of Group Key Agreement Protocols with Constant
00 Rounds,“ *ACM Computing Surveys*, Bd. 52, 06 2019.
]
- [1 Y. Kim, A. Perrig und G. Tsudik, „Tree-based group key agreement,“ *ACM Transactions on
01 Information and System Security*, Bd. 7, pp. 60-96, 02 2004.
]

- [1 L. R. Dondeti, S. Mukherjee und A. Samal, „A Distributed Group Key Management Scheme
02 for Secure Many-to-many Communication,“ 1999.
]
- [1 M. Bilal und S.-G. Kang, „A Secure Key Agreement Protocol for Dynamic Group,“ *CoRR*, Bd.
03 abs/1704.02683, 2017.
]
- [1 M. Steiner, G. Tsudik und M. Waidner, „Diffie-Hellman key distribution extended to group
04 communication,“ New York, NY, USA, 1996.
]
- [1 R. Dutta und R. Barua, „Constant Round Dynamic Group Key Agreement,“ 2005.
05
]
- [1 H.-J. Kim, S.-M. Lee und D. H. Lee, „Constant-Round Authenticated Group Key Exchange for
06 Dynamic Groups,“ in *Advances in Cryptology – ASIACRYPT 2004*, Berlin, Heidelberg,
] Springer Berlin Heidelberg, 2004, pp. 245-259.
- [1 K. Bhargavan, R. Barnes und E. Rescorla, „TreeKEM: Asynchronous Decentralized Key
07 Management for Large Dynamic Groups — A protocol proposal for Messaging Layer
] Security (MLS),“ 2018.
- [1 Y. J. Morton, F. van Diggelen, J. J. Spilker, B.-f. W. Parkinson, S. Lo und G. Gao, Position,
08 navigation, and timing technologies in the 21st century: Integrated satellite navigation,
] sensor systems, and civil applications, Bd. 1, John Wiley & Sons, 2021.
- [1 R. Mit, Y. Zangvil und D. Katalan, „Analyzing Tesla's Level 2 Autonomous Driving System
09 Under Different GNSS Spoofing Scenarios and Implementing Connected Services for
] Authentication and Reliability of GNSS Data,“ 2020.
- [1 F. Nedelkov, D.-K. Lee, D. Miralles und D. Akos, „Accuracy and Performance of the Network
10 Location Provider in Android Devices,“ 2020.
]
- [1 R.-P. Weinmann, „Baseband Attacks: Remote Exploitation of Memory Corruptions in
11 Cellular Protocol Stacks,“ 2012.
]
- [1 D. Perez und J. Pico, „A Practical Attack against GPRS/EDGE/UMTS/HSPA Mobile Data
12 Communications,“ *Black Hat DC*, Bd. 2, p. 21, 2011.
]
- [1 C. Ponsard, M. Touzani und V. Ramon, „Méta-modèle des concepts et processus d'analyse
13 des risques selon les normes de cybersécurité,“ Dijon, France, 2022.
]
- [1 N. Urbach und F. Ahlemann, Digitalization as a Risk: Security and Business Continuity
14 Management Are Central Cross-Divisional Functions of the Company, Cham: Springer
] International Publishing, 2019, pp. 85-92.
- [1 R. Ramirez und N. Choucri, „Improving interdisciplinary communication with standardized
15 cyber security terminology: A literature review,“ *IEEE Access*, Bd. 4, pp. 2216-2243, 2016.
]
- [1 P. Jaferian, K. Hawkey, A. Sotirakopoulos, M. Velez-Rojas und K. Beznosov, „Heuristics for
16 evaluating IT security management tools,“ 2011.
]

- [1] „Scapy,“ 2008. [Online]. Available: <https://scapy.net/>.
17
]
- [1] „Caring Caribou,“ 2015. [Online]. Available:
18 <https://github.com/CaringCaribou/caringcaribou>.
]
- [1] International Organization for Standardization, „Road vehicles - Vehicle-to-Grid
19 Communication Interface - Part 2: Network and application protocol requirements,“ 2014.
]
- [1] International Organization for Standardization, „Road vehicles - Vehicle-to-Grid
20 Communication Interface - Part 20: 2nd generation network layer and application layer
] requirements,“ 2022.
- [1] Deutsches Institut für Normung, „Elektromobilität - Digitale Kommunikation zwischen einer
21 Gleichstrom-Ladestation und einem Elektrofahrzeug zur Regelung der Gleichstromladung
] im Verbund-Ladesystem,“ 2014.
- [1] „HomePlug Green PHY Specification Version 1.1.1,“ 2013.
22
]
- [1] S. Köhler, R. Baker, M. Strohmeier und I. Martinovic, „Brokenwire: Wireless Disruption of
23 CCS Electric Vehicle Charging,“ San Diego, CA, USA, 2023.
]
- [1] Qualcomm Atheros, Inc., „open-plc-utils,“ 2023. [Online]. Available:
24 <https://github.com/qca/open-plc-utils>.
]
- [1] LF Energy, „iso15118,“ 2021. [Online]. Available: <https://github.com/EVerest/EVerest>.
25
]
- [1] EcoG-io, „iso15118,“ 2021. [Online]. Available: <https://github.com/EcoG-io/iso15118>.
26
]
- [1] A. Festag, „Cooperative intelligent transport systems standards in Europe,“
27 *Communications Magazine, IEEE*, Bd. 52, pp. 166-172, 12 2014.
]
- [1] European ITS Platform, „Recommendations for continuation of C-ITS deployment,“
28 [Online]. Available: <https://www.its-platform.eu/wp-content/uploads/ITS-Platform/AchievementsDocuments/IntegratingC-ITS/EU%20EIP-44-D8-C-ITS%20Recommendations-v1.0.pdf>.
]
- [1] C. Gentsch, „Evaluation of Open Source Static Analysis Security Testing (SAST) Tools for C,“
29 DLR German Aerospace Center, Jena, 2020.
]
- [1] S. Lipp, „An empirical study on the effectiveness of static C code analyzers for vulnerability
30 detection,“ in *ISSTA 2022: Proceedings of the 31st ACM SIGSOFT International Symposium
] on Software Testing and Analysis*, 2022.
- [1] J. D. Pereira, „On the Use of Open-Source C/C++ Static Analysis Tools in Large Projects,“ in
31 *European Dependable Computing Conference (EDCC)*, 2020.
]

- [1 M. Bakhtina und R. Matulevicius, „Information security analysis in the passenger–
32 autonomous vehicle interaction,“ 2021.
]
- [1 Z. El-Rewini, K. Sadatsharan, D. F. Selvaraj, S. J. Plathottam und P. Ranganathan,
33 „Cybersecurity challenges in vehicular communications,“ *Vehicular Communications*, Bd.
] 23, 2020.
- [1 E. Yurtsever, J. Lambert, A. Carballo und K. Takeda, „A survey of autonomous driving:
34 Common practices and emerging technologies,“ *IEEE Access*, Bd. 8, 2020.
]
- [1 D. Dominic, S. Chhawri, R. M. Eustice, D. Ma und A. Weimerskirch, „Risk assessment for
35 cooperative automated driving,“ 2016.
]
- [1 S. Narain, A. Ranganathan und G. Noubir, „Security of GPS/INS based on-road location
36 tracking systems,“ 2019.
]
- [1 W. Xu, C. Yan, W. Jia, X. Ji und J. Liu, „Analyzing and enhancing the security of ultrasonic
37 sensors for autonomous vehicles,“ *IEEE Internet of Things Journal*, Bd. 5, 2018.
]
- [1 Y. Cao, C. Xiao, B. Cyr, Y. Zhou, W. Park, S. Rampazzi, Q. A. Chen, K. Fu und Z. M. Mao,
38 „Adversarial sensor attack on lidar-based perception in autonomous driving,“ 2019.
]
- [1 Y. Cao, S. H. Bhupathiraju, P. Naghavi, T. Sugawara, Z. M. Mao und S. Rampazzi, „You can't
39 see me: Physical removal attacks on LiDAR-based autonomous vehicles driving
] frameworks,“ 2023.
- [1 S. Pavlitska, N. Lambing und J. M. Zöllner, „Adversarial attacks on traffic sign recognition: A
40 survey,“ 2023.
]
- [1 Tencent Security Keen Lab, „Experimental security assessment of Mercedes-Benz cars“.
41
]
- [1 J. Takahashi, Y. Aragane, T. Miyazawa, H. Fuji, H. Yamashita, K. Hayakawa, S. Ukai und H.
42 Hayakawa, „Automotive attacks and countermeasures on LIN-bus,“ *Journal of Information
] Processing*, Bd. 25, 2017.
- [1 J. Liu, S. Zhang, W. Sun und Y. Shi, „In-vehicle network attacks and countermeasures:
43 Challenges and future directions,“ *IEEE Network*, Bd. 31, 2017.
]
- [1 L. Wouters, B. Gierlichs und B. Preneel, „My other car is your car: Compromising the Tesla
44 Model X keyless entry system,“ *IACR Transactions on Cryptographic Hardware and
] Embedded Systems*, 2021.
- [1 M. N. Mejri, J. Ben-Othman und M. Hamdi, „Survey on VANET security challenges and
45 possible cryptographic solutions,“ *Vehicular Communications*, Bd. 1, 2014.
]
- [1 S. Park und H. Park, „PIER: Cyber-resilient risk assessment model for connected and
46 autonomous vehicles,“ *Wireless Networks*, 2022.
]

- [1 J. Cui und B. Zhang, „VERA: A simplified security risk analysis method for autonomous
47 vehicles,“ *IEEE Transactions on Vehicular Technology*, Bd. 69, 2020.
]
- [1 International Organization for Standardization, „ISO/IEC 18045:2022 – Information security,
48 cybersecurity and privacy protection – Evaluation criteria for IT security – Methodology for IT
] security evaluation,“ 2022.
- [1 European Commission, „EU classification of vehicle types,“ [Online]. Available:
49 <https://alternative-fuels-observatory.ec.europa.eu/general-information/vehicle-types>.
]
- [1 T. Liedtke, *Cybersecurity Management System: Anforderungen - Aufbau - Ziele - Prozesse*,
50 Wiesbaden: Springer Gabler, 2024.
]
- [1 E. Mixon und C. Steele, „OTA-Update (Over-the-Air-Update),“ 2024. [Online]. Available:
51 <https://www.computerweekly.com/de/definition/OTA-Update-Over-The-Air-Update>.
]
- [1 ISAO Standards Organization, „Automotive ISAC,“ 2025. [Online]. Available:
52 <https://www.isao.org/group/automotive-isac/>.
]
- [1 M. Franz, „Porsche Macan erfüllt künftige Vorschriften für Cybersicherheit nicht,“ 2023.
53 [Online]. Available: [https://www.heise.de/news/Porsche-Macan-erfuellt-kuenftige-](https://www.heise.de/news/Porsche-Macan-erfuellt-kuenftige-Vorschriften-fuer-Cybersicherheit-nicht-9575059.html)
] [Vorschriften-fuer-Cybersicherheit-nicht-9575059.html](https://www.heise.de/news/Porsche-Macan-erfuellt-kuenftige-Vorschriften-fuer-Cybersicherheit-nicht-9575059.html).
- [1 D. Shelcuský, „A comprehensive guide to UNECE R155/R156 Compliance,“ 2024. [Online].
54 Available: [https://www.automotive-iq.com/cybersecurity/interviews/a-comprehensive-](https://www.automotive-iq.com/cybersecurity/interviews/a-comprehensive-guide-to-unece-r155r156-compliance)
] [guide-to-unece-r155r156-compliance](https://www.automotive-iq.com/cybersecurity/interviews/a-comprehensive-guide-to-unece-r155r156-compliance).
- [1 C. Gleich, „Cybersicherheits-Vorgaben: Was drin steht,“ 2024. [Online]. Available:
55 [https://www.heise.de/hintergrund/Cybersicherheits-Vorgaben-Was-drin-steht-](https://www.heise.de/hintergrund/Cybersicherheits-Vorgaben-Was-drin-steht-9674259.html)
] [9674259.html](https://www.heise.de/hintergrund/Cybersicherheits-Vorgaben-Was-drin-steht-9674259.html).
- [1 European Parliament and Council of the European Union, „Regulation (EU) 2023/2854 of
56 the European Parliament and of the Council of 13 December 2023 on harmonised rules on
] fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU)
2020/1828: Data Act,“ 2024.
- [1 Federal Office for Information Security, „Cyber Resilience Act: Cybersecurity in the EU,“
57 [Online]. Available: [https://www.bsi.bund.de/EN/Themen/Unternehmen-und-](https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Cyber%20Resilience%20Act/cyber%20resilience%20act%20node.html)
] [Organisationen/Informationen-und-](https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Cyber%20Resilience%20Act/cyber%20resilience%20act%20node.html)
[Empfehlungen/Cyber%20Resilience%20Act/cyber%20resilience%20act%20node.html](https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Empfehlungen/Cyber%20Resilience%20Act/cyber%20resilience%20act%20node.html).
- [1 European Parliament and Council of the European Union, „Regulation (EU) 2024/2847 of
58 the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity
] requirements for products with digital elements and amending Regulation (EU) No
168/2013 and Regulation (EU) 2019/1020 and Directive (EU) 2020/1828: Cyber Resilience
Act,“ 2024.
- [1 European Commission, „Neue Abgasnorm Euro-7: Die Fakten,“ 2022. [Online]. Available:
59 https://germany.representation.ec.europa.eu/neue-abgasnorm-euro-7-die-fakten_de.
]
- [1 European Automobile Manufacturers’ Association, „OBM & Security & Anti-Tampering,“
60 2024. [Online]. Available:
]

<https://www.lobbyregister.bundestag.de/media/28/85/311499/Stellungnahme-Gutachten-SG2406240229.pdf>.

- [1 Deutscher Bundestag, „Euro 7 - Implementierung des sekundären Rechtsaktes zu Cyber
61 Security & Anti Tampering,“ 2024. [Online]. Available:
] <https://www.lobbyregister.bundestag.de/inhalte-der-interessenvertretung/regelungsvorhabensuche/RV0005522/12775>.
- [1 Standing Committee of the National People’s Congress, „Cybersecurity law of the People’s
62 Republic of China: Cybersecurity law (PRC),“ 2017.
]
- [1 European Parliament and Council of the European Union, „Regulation (EU) 2016/679 of the
63 European Parliament and of the Council of 27 April 2016: General Data Protection
] Regulation (GDPR),“ 2016.
- [1 Standing Committee of the National People’s Congress of the People’s Republic of China,
64 „Personal Information Protection Law of the People’s Republic of China: Personal
] Information Protection Law (PIPL),“ 2021.
- [1 California Privacy Protection Agency, „California Consumer Privacy Act Regulations: CCPA
65 Regulations,“ 2023.
]
- [1 D. K. Nilsson, P. H. Phung und U. E. Larson, „Vehicle ECU classification based on safety-
66 security characteristics,“ in *IET Road Transport Information and Control - RTIC 2008*,
] Manchester, 2008.
- [1 G. Kar, S. Jain, M. Gruteser, J. Chen, F. Bai und R. Govindan, „PredriveID: pre-trip driver
67 identification from in-vehicle data,“ in *SEC ’17: IEEE/ACM Symposium on Edge Computing*,
] San Jose, 2017.
- [1 BSI, „bsi.bund.de,“ [Online]. Available:
68 <https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Internet-der-Dinge-Smart-leben/Smart-Home/Digitale-Assistenten/digitale-assistenten.html>.
]
- [1 BfDI, „bfdi.bund.de,“ [Online]. Available:
69 <https://www.bfdi.bund.de/DE/Buerger/Inhalte/Technik/Sprachassistenzsysteme.html>.
]
- [1 OECD, „Emerging privacy-enhancing technologies: Current regulatory and policy
70 approaches,“ OECD Digital Economy Papers, 2023-03-08.
]
- [1 D. Grimm, M. Stang und E. Sax, „Context-Aware Security for Vehicles and Fleets: A Survey,“
71 2021.
]
- [1 T. Fritzmann, J. Vith und J. Sepúlveda, „Post-quantum key exchange mechanism for safety
72 critical systems,“ 2019.
]
- [1 J. Hermelink, „Quantum safe authenticated key exchange protocol for automotive
73 application,“ 2020.
]
- [1 C. de Saint Guilhem, N. P. Smart und B. Warinschi, „Generic Forward-Secure Key
74 Agreement Without Signatures,“ in *Information Security - 20th International Conference*,
]

ISC 2017, Ho Chi Minh City, Vietnam, November 22-24, 2017, *Proceedings*, Bd. 10599, Springer, 2017, pp. 114-133.

- [1 E. Alkim, „NewHope – submission to the NIST post-quantum project (2019),“ 2019.
75
]
- [1 A. Huelsing, „XMSS: eXtended Merkle Signature Scheme,“ 2018.
76
]
- [1 T. Fritzmann, „Post-quantum cryptography for automotive systems,“ *Microprocessors and*
77 *Microsystems*, Bd. 87, p. 104379, 2021.
]
- [1 Q. Hu und F. Luo, „Review of Secure Communication Approaches for In-Vehicle Network,“
78 *International Journal of Automotive Technology*, Bd. 19, Nr. 5, pp. 879-894, 2018.
]
- [1 P. Ravi, „Authentication Protocol for Secure Automotive Systems: Benchmarking Post-
79 Quantum Cryptography,“ 2020.
]
- [1 F. Campos, „Post-quantum cryptography for ECU security use cases,“ 2019.
80
]
- [1 J. W. Bos, „Post-quantum secure over-the-air update of automotive systems,“ 2023.
81
]
- [1 S. Plaga, N. Wiedermann, S. D. Anton, S. Tatschner, H. Schotten und T. Neue, „Securing
82 future decentralised industrial IoT infrastructures: Challenges and free open source
] solutions,“ *Future Generation Computer Systems*, Bd. 93, pp. 596-608, 2019.
- [1 A. Giehl, N. Wiedermann und S. Plaga, „A framework to assess impacts of cyber attacks in
83 manufacturing,“ New York, NY, USA, 2019.
]
- [1 M. Rocchetto und N. O. Tippenhauer, „On attacker models and profiles for cyber-physical
84 systems,“ 2016.
]
- [1 C. Eckert, *IT-Sicherheit: Konzepte–Verfahren–Protokolle*, Oldenbourg Wissenschaftsverlag,
85 2013.
]
- [1 H. Kayan, M. Nunes, O. Rana, P. Burnap und C. Perera, „Cybersecurity of industrial cyber-
86 physical systems: A review,“ *ACM Computing Surveys*, Bd. 54, Nr. 11s, pp. 1-35, 2022.
]
- [1 S. D. Anton, D. Fraunholz, C. Lipps, F. Pohl, M. Zimmermann und H. D. Schotten, „Two
87 decades of SCADA exploitation: A brief history,“ 2017.
]
- [1 P. Wagner, G. Hansch, C. Konrad, K.-H. John, J. Bauer und J. Franke, „Applicability of
88 security standards for operational technology by SMEs and large enterprises,“ 2020.
]

- [1 Federal Office for Information Security (BSI), „Cryptographic Mechanisms:
89 Recommendations and Key Lengths,“ 2024.
]
- [1 M. Runde, C. Tebbe und K.-H. Niemann, „Performance evaluation of an IT security layer in
90 real-time communication,“ 2013.
]
- [1 J. Robert, J.-P. Georges, É. Rondeau und T. Divoux, „Minimum cycle time analysis of
91 Ethernet-based real-time protocols,“ *International Journal of Computers, Communications
] and Control*, Bd. 7, Nr. 4, pp. 743-757, 2012.
- [1 S. Fischer und H. D. Doran, „Embedding real time Ethernet: Ethernet/IP on resource
92 constricted platforms,“ 2011.
]
- [1 A. Almulhim, „Security Risks of Mobile Applications in Electric Vehicles: An Overview,“
93 *Information*, Bd. 14, p. 523, 2023.
]
- [1 United Nations Economic Commission for Europe, „Proposals for Interpretation
94 Documents for UN Regulation No. 155 (Cyber Security and Cyber Security Management
] System),“ 2021.
- [1 International Organization for Standardization, „ISO 26262-3:2018 Road vehicles -
95 Functional safety - Part 3: Concept phase,“ Geneva, 2018.
]
- [1 T. W. Edgar und D. O. Manz, *Research Methods for Cyber Security*, 1 Hrsg., Boston, MA,
96 USA: Syngress, 2017.
]
- [1 G. Guest, A. Bunce und L. Johnson, „How many interviews are enough? an experiment with
97 data saturation and variability,“ *Field Methods*, Bd. 18, Nr. 1, pp. 59-82, 2006.
]
- [1 T. Azungah, „Qualitative research: Deductive and inductive approaches to data analysis,“
98 *Qualitative Research Journal*, Bd. 18, Nr. 4, pp. 383-400, 2018.
]
- [1 J. Corbin und A. Strauss, *Basics of Qualitative Research: Techniques and Procedures for
99 Developing Grounded Theory*, 4 Hrsg., Thousand Oaks, CA: SAGE Publications, 2015.
]
- [2 International Organization for Standardization, „Road vehicles — Diagnostic
00 communication over Internet Protocol (DoIP) - Transport protocol and network layer
] services,“ 2019.
- [2 International Organization for Standardization, „Road vehicles — FlexRay communications
01 system - Part 2: Data link layer specification,“ 2013.
]
- [2 EcoG-io, „pyslac,“ 2023. [Online]. Available: <https://github.com/EcoG-io/pyslac>.
02
]

1.5 Zusammenarbeit mit anderen Stellen

1.5.1 Zusammenarbeit mit den Partnern

Das Teilvorhaben Security war eng mit den übrigen Arbeitspaketen und Partnern des ATLAS-L4-Verbunds verzahnt. Mit MAN erfolgte eine kontinuierliche Abstimmung zu Systemkonzepten, Architekturständen und betrieblichen Anforderungen; MAN stellte die Grundlage für die Systemmodelle von L4-Lkw und Control Center bereit und wirkte an den Risikoanalyse-Workshops aktiv mit. Mit TUM und TU Braunschweig wurden insbesondere Abhängigkeiten zu Safety-Betrachtungen, Fahrfunktionen und Control-Center-Konzepten abgestimmt.

Die Autobahn GmbH brachte Betreiberperspektiven und Anforderungen aus dem Kontext kritischer Infrastrukturen ein, insbesondere für Schnittstellen zwischen Control Center und Straßeninfrastruktur. Weitere Partner (z. B. für V2X, HD-Karten, KI-Methoden) wurden bei Bedarf in die Risikoanalyse-Workshops und Standarddiskussionen einbezogen. Ergebnisse aus den Security-Arbeiten flossen in Form von Anforderungen, Empfehlungen und Tool-Prototypen in die technischen Arbeitspakete (AP 3–AP 9) zurück.

1.5.2 Zusammenarbeit mit Forschungsinstituten und Hochschulen

Neben der Einbindung der universitären Projektpartner (TUM, TU Braunschweig) bestand ein fachlicher Austausch mit weiteren Forschungseinrichtungen und Hochschulen, u. a. über gemeinsame Publikationen und studentische Arbeiten. Eigene Unteraufträge oder formale Kooperationsprojekte außerhalb des ATLAS-L4-Konsortiums wurden für dieses Teilvorhaben nicht vergeben; die Zusammenarbeit erfolgte im Rahmen regulärer Forschungsk Kooperationen und Publikationsaktivitäten.

1.5.3 Sonstige Zusammenarbeit

Eine darüberhinausgehende formelle oder informelle Zusammenarbeit mit externen Stellen (z. B. Standardisierungsgremien, Facharbeitskreisen oder Behörden) erfolgte im Rahmen dieses Teilvorhabens nicht. Externe Dokumente (z. B. Normen, EU-Rechtsakte, Fachveröffentlichungen, Verbandspositionen) wurden ausschließlich als Literatur- und Kontextquellen ausgewertet.

2 Eingehende Darstellung der erzielten Ergebnisse

2.1 Erzielte wissenschaftlich-technische Ergebnisse

Alle in Kapitel 2 dargestellten Ergebnisse sind dem Arbeitspaket AP 2 „Security“ des Verbundprojekts ATLAS-L4 zuzuordnen. Mit den Zuwendungsmitteln wurden dabei sowohl methodische Grundlagen als auch prototypische Werkzeuge und konkrete Risikoanalysen für den sicheren Betrieb eines Level-4-Gesamtsystems aus Lkw und Control Center erarbeitet.

Auf methodischer Ebene wurde die in der Automobilindustrie etablierte MoRA-Methode ISO/SAE-21434-konform weiterentwickelt und an den ATLAS-L4-Kontext (L4-Truck, Control Center, Cloud-/IT-Umgebung) angepasst, einschließlich Bewertungsmodell, Schadenskriterien, Annahmen-, Bedrohungs- und Maßnahmenkatalogen sowie einer überarbeiteten Werkzeugunterstützung (Abschnitt 2.1.1). Ergänzend wurden ein normübergreifender Vergleich von ISO/SAE 21434, ISO/IEC-27000-Familie und IEC-62443 (Abschnitt 2.1.2), eine Analyse der regulatorischen Rahmenbedingungen (UNECE R155/R156, GB 44495-2024, NHTSA, flankierende EU-Regulierungen, Abschnitt 2.1.3), Beiträge zu Privacy-Enhancing Technologies im Fahrzeug (Abschnitt 2.1.4) und eine Einschätzung der Auswirkungen des EU AI Act auf ATLAS-L4 (Abschnitt 2.1.5) erarbeitet. Für das bereichsübergreifende Risikomanagement wurden Anforderungen aus Standards und Industrieinterviews abgeleitet (Abschnitt 2.1.12) und in einem SharePoint-basierten, prototypischen Security-Management-Werkzeug umgesetzt (Abschnitt 2.1.13).

Auf technischer Ebene wurden Security-Fragestellungen vernetzter Fahrzeugtechnologien, insbesondere V2X und Post-Quantum-Kryptographie (Abschnitt 2.1.6), ein Verfahren zum Testen von Resilienzeigenschaften in Ethernet-/TSN-Netzen (Abschnitt 2.1.7) sowie Sicherheitsanforderungen an Industrial-Ethernet-Protokolle (Abschnitt 2.1.8) untersucht. Mit GRACYBUS wurde ein verteiltes Group-Key-Agreement-Protokoll für CPS-Busse entwickelt (Abschnitt 2.1.9). Für mobile Anwendungen im Fahrzeugumfeld wurde die Relevanz des OWASP MASVS analysiert (Abschnitt 2.1.10), die Sicherheit von Ortungsdiensten empirisch untersucht (Abschnitt 2.1.11) und mehrere domänenspezifische Testwerkzeuge weiterentwickelt bzw. neu aufgebaut: Erweiterungen des offenen Diagnose-Frameworks gallia (Abschnitt 2.1.14), ein Testsystem für Ladekommunikation nach ISO 15118/DIN SPEC 70121 (Abschnitt 2.1.15), ein Security-Test-Framework für C-ITS/V2X (Abschnitt 2.1.16) sowie die Automotive-Anpassung des Modul-Baukastens Woodpecker für statische Code-Analyse (Abschnitt 2.1.17).

Als zentrales Anwendungsergebnis wurden mit der weiterentwickelten MoRA-Methode zwei umfassende Security-Risikoanalysen für ein automatisiertes Fahrsystem im Lkw (ADS) und das zugehörige Control Center durchgeführt und in Security-Anforderungen überführt (Abschnitte 2.1.18 und 2.1.19). Die nachfolgenden Unterabschnitte 2.1.1 bis 2.1.19 stellen diese wissenschaftlich-technischen Ergebnisse im Einzelnen dar.

2.1.1 Methode Security-Risikoanalyse

2.1.1.1 Anpassungen an den ATLAS-L4 Kontext und sonstige Erweiterungen

In diesem Abschnitt wird die erreichte Weiterentwicklung der MoRA-Methode für den ATLAS-L4-Kontext dargestellt. Die Ergebnisse bilden die methodische Grundlage für die

Security-Risikoanalysen des automatisierten Fahrsystems (Abschnitt 2.1.18) und des Control Centers (Abschnitt 2.1.19) sowie für die daraus abgeleiteten Cybersecurity-Konzepte.

Zu Beginn des Projekts wurden in gemeinsamen Workshops von Fraunhofer AISEC und MAN die Anforderungen an eine geeignete Security-Risikoanalyse-Methode konkretisiert. Auf Basis der vorhandenen MAN-Praxis wurde Modular Risk Assessment (MoRA) als Kernmethode festgelegt und terminologisch an ISO/SAE 21434 angepasst. System, Daten und Funktionen werden wie in [1, 2] empfohlen als Zusammenspiel von Funktionen, Daten, Komponenten und Kommunikationsbeziehungen beschrieben; darauf aufbauend werden Security-Goals, Schadensszenarien, Threats, Controls und Annahmen in einem einheitlichen Modell erfasst. Als Referenzterminologie dient die ISO/SAE-21434-Begriffswelt (z. B. „Item“, „Damage Scenario“, „Attack Path“), sodass die Methode direkt in TARA-Prozesse eingehängt werden kann.

Das Bewertungsmodell wurde so gestaltet, dass es sowohl den normativen Vorgaben von ISO/SAE 21434 als auch OEM-spezifischen Anforderungen genügt. Die Impact-Bewertung erfolgt entlang der vier Kategorien Safety, Financial, Operational und Privacy; innerhalb jeder Kategorie wurden abgestufte Schadenskriterien definiert, die von vernachlässigbaren bis zu schwerwiegenden Auswirkungen reichen. Für die Finanz- und Betriebsdimension werden dabei explizit Unterschiede zwischen Einzelereignissen (z. B. einzelnes Fahrzeug, einzelner Kunde) und flächendeckenden Vorfällen (z. B. mehrere Fahrzeuge, Flotte, Rückruf) berücksichtigt, ohne die zugrunde liegenden, vertraulichen Schwellenwerte im Bericht offenzulegen. Die Angriffsmachbarkeit wird – im Einklang mit ISO/SAE 21434 und der Common Evaluation Methodology (CEM) [148] – attack-potential-basiert über die Faktoren benötigte Zeit, Expertise, Kenntnis des Systems, Window of Opportunity und erforderliche Ausrüstung eingeschätzt. Die Kombination aus Impact und Attack-Feasibility wird in einer normativen Risikomatrix in diskrete Risikowerte überführt; die konkrete Ausprägung dieser Matrix bleibt intern, die Struktur entspricht jedoch den Beispielen in ISO/SAE 21434.

Aufbauend auf diesem Bewertungsmodell wurden die bestehenden MAN-Kataloge für Annahmen, Bedrohungen, Maßnahmen und Technologien gemeinsam gesichtet, bereinigt und für ATLAS-L4 erweitert. Für das ADS konnten große Teile der Automotive-spezifischen Kataloge (z. B. zu Bussen, Kryptographie, Domänenentrennung, Entwicklungs- und Produktionsumgebung) übernommen werden. Für das Control Center musste der Katalog deutlich in Richtung Office-/Backend-IT und Cloud-Betrieb ausgebaut werden. Hierzu wurden u. a. die Gefährdungslage des BSI-IT-Grundschutz-Kompodiums und die Bedrohungskategorien von ISO/IEC 27005 ausgewertet und in einen generischen Threat-Katalog überführt. Neu eingeführt wurden dabei übergeordnete Bedrohungsklassen wie „Physical threats“ (z. B. Brand, Hitze, Feuchtigkeit, Explosionen), „Natural threats“, „Infrastructure failures“, „Organizational threats“, „Deliberate human actions“, „Accidental human actions“ und „Technical failures“. Diese Klassen bilden den Einstiegspunkt für Control-Center-spezifische Ableitungen (z. B. Stromausfall im Rechenzentrum, Fehlkonfiguration von Cloud-Ressourcen, Fehler externer Dienstleister) und lassen sich mit STRIDE-abgeleiteten anwendungsspezifischen Threats kombinieren.

Im Annahmenkatalog wurden neben generischen Annahmen zu Kryptoverfahren, Entwicklungs- und Produktionssicherheit projekt- und domänenspezifische Annahmen ergänzt. Dazu zählen u. a. Annahmen zur Verantwortlichkeitsverteilung zwischen Cloud-Provider und Control-Center-Betreiber (z. B. physische Sicherheit und Verfügbarkeit der Infrastruktur, Umsetzung von Basis-Schutzmaßnahmen gemäß AWS-Security-Best-Practices) sowie zu nicht sicherheitskritischen minimalen Risikomanövern, die vom Control Center ausgelöst werden. Diese

Annahmen wurden explizit modelliert und in den Risikoanalysen des ADS und des Control Centers genutzt, um Scope und Angreifermodell nachvollziehbar zu fixieren und Schadensszenarien gegebenenfalls zu transformieren (z. B. von sicherheitskritischen zu rein operativen Auswirkungen).

Der Maßnahmenkatalog (Controls) wurde sowohl im Automotive- als auch im IT-/Cloud-Kontext erweitert. Neben etablierten Fahrzeug-Controls (z. B. kryptographisch gesicherte Kommunikation, Domänentrennung, Secure Boot, Intrinsic Safety) wurden insbesondere für das Control Center neue Controls eingeführt, u. a.:

- Absicherung der Kommunikation zwischen Truck und Control Center durch gegenseitig authentifizierte Transportverschlüsselung,
- Ende-zu-Ende-Verschlüsselung und -Authentisierung sensibler Datenströme zwischen Truck, Control Center, Flottenmanagement und externen Partnern,
- Härtung internet-exponierter Komponenten und technischer Aufsichtsarbeitsplätze (minimale Angriffsfläche, Patch-Management, Whitelisting),
- Umsetzung des „Security Pillar“ des AWS Well-Architected Framework (Identity & Access Management, Infrastruktur-Schutz, Monitoring, Incident Response),
- Maßnahmen zur Resilienz bzw. „Security through Diversity“, bei denen besonders kritische Control-Center-Services gezielt heterogen ausgelegt werden, um das Risiko eines Verfügbarkeitsverlusts durch einen einzelnen Exploit zu reduzieren,
- verschlüsselte Speicherung von Truck- und Kundendaten sowie Maßnahmen gegen Piraterie und Reverse Engineering, um geistiges Eigentum zu schützen.

Die vollständige Metamodellierung und die Kataloge wurden in ein überarbeitetes MoRA-Excel-Werkzeug integriert, das bereits vor ATLAS-L4 im Einsatz war und im Projekt strukturell überarbeitet wurde. Funktionen, Daten, Komponenten, Datenflüsse, Schutzziele, Schadensszenarien, Threats, Controls und Annahmen werden in separaten, referenziell verknüpften Tabellen gepflegt. Durch den Einsatz moderner Excel-Funktionen (insb. LET und LAMBDA) konnte die Performance verbessert und die Pflege von Formeln vereinfacht werden. Zudem wurden zusätzliche Blätter ergänzt, etwa zur halbautomatischen Generierung von PlantUML-Eingabestrings für Sequenzdiagramme. Damit lassen sich aus der SRA-Modellierung direkt vereinheitlichte Diagramme erzeugen, die sowohl die Kommunikation im ADS als auch im Control Center visualisieren und die Ergebnisse der Risikoanalyse besser für Fachbereiche und Management vermitteln.

Die weiterentwickelte MoRA-Methode wurde im Projekt in zwei vollständigen, umfangreichen Risikoanalysen eingesetzt: für das automatisierte Fahrsystem im Lkw (Abschnitt 2.1.18) und für das Control Center (Abschnitt 2.1.19). Beide Analysen nutzen dasselbe Bewertungsmodell und große Teile der Kataloge, unterscheiden sich aber naturgemäß in den betrachteten Assets, Bedrohungen und Controls. Für das ADS stehen Safety-nahe Schadensszenarien (z. B. Verlust der ADS-Funktion während der Fahrt, gefährliche Fahrmanöver, Aktivierung außerhalb der ODD) im Vordergrund; für das Control Center dominieren Verfügbarkeits- und Flottenrisiken (z. B. Stillstand der Flotte, falsche Routenplanung, fehlerhafte MRM-Auslösung für mehrere Fahrzeuge) sowie Datenschutzaspekte (z. B. Offenlegung von Videodaten). Die Methode hat sich dabei als ausreichend flexibel erwiesen, um beide Domänen mit einem konsistenten Satz von Skalen, Katalogen und Werkzeugen zu bearbeiten.

2.1.1.2 Usability

Die Usability-Betrachtung konzentrierte sich auf das Excel-Template, mit dem MoRA im Projekt ATLAS-L4 umgesetzt wurde. Grundlage war ein systematischer Durchgang durch das Template aus Sicht zukünftiger Anwenderinnen und Anwender. Die Analyse stellt damit eine frühe Heuristik-Bewertung dar; eine tiefergehende Evaluation mit mehreren Nutzergruppen könnte weitere Anpassungen und Verfeinerungen erforderlich machen. Im Verlauf des Projekts wurden zentrale Ergebnisse dieser Analyse bereits in konkrete Anpassungen des MoRA-Excel-Werkzeugs überführt; andere Empfehlungen wurden bewusst zurückgestellt oder in ein nachgelagertes MoRA-Handbuch ausgelagert.

Ein Schwerpunkt lag auf der **Automatisierung wiederkehrender Schritte**. Die ursprüngliche Empfehlung, IDs generell automatisch zu vergeben, wurde nur dort umgesetzt, wo dies technisch robust möglich ist. Hintergrund ist, dass in der Praxis Tabellenzeilen häufig gelöscht werden. Würden IDs einfach „mitlaufen“, würden sich bei Löschungen die ID-Werte nach oben verschieben und Referenzen aus anderen Blättern ungültig werden. Daher werden IDs heute nur für solche Einträge automatisiert vergeben, bei denen Reihen nicht verschoben oder gelöscht werden und eine stabile Referenzierung gewährleistet ist; in anderen Fällen ist die explizite Vergabe weiterhin erforderlich. Für das Blatt „Function Assignment“ wurde die Bedienung gezielt verbessert: Im Blatt „Data Flows“ kann nun in einer eigenen Spalte direkt angegeben werden, zu welchen Funktionen ein Datenfluss gehört. Auf Basis dieser Information wird automatisch ein Vorschlag generiert, der bei Bedarf noch manuell angepasst werden kann. Damit entfällt ein Teil der zuvor notwendigen manuellen Zwischenschritte. Die Empfehlung, mehrfaches Kopieren von Inhalten auf Knopfdruck zu automatisieren, wurde nur eingeschränkt umgesetzt, da das MoRA-Excel-Tool bewusst ohne Makros auskommen soll (Kompatibilität, Prüfbarkeit, geringere Hürden in IT-Umgebungen). Wo immer möglich werden heute Formelbezüge statt Copy-&-Paste genutzt; weitergehende Automatisierung, die Klick-Buttons oder VBA erfordern würde, wurde dagegen aus Prinzip nicht umgesetzt. Die Idee, Threat-Klassen auf Basis vorhandener Kataloge automatisch vorzuschlagen, wurde als sinnvoll aufgenommen und konzeptionell vorbereitet und ist Kandidat für eine zukünftige Version.

Im Themenfeld **Struktur und Navigation** wurde in der Analyse bemängelt, dass die Vielzahl an Tabellenblättern und ihre wechselseitigen Referenzen für neue Nutzende schwer durchschaubar sind. Anstatt die Struktur im laufenden Projekt radikal umzubauen, wurde dies in ein separates, aktuell noch laufendes Folgeprojekt überführt, in dem ein umfangreicher „MoRA-Leitfaden“ (~60 Seiten) entsteht. Dieser Leitfaden beschreibt den typischen Befüllungsfluss, erklärt die Rolle der einzelnen Blätter, gibt Empfehlungen zu „Hauptblättern“ und dokumentiert, wie und wann zwischen Blättern zu springen sinnvoll ist (inkl. praktischer Tipps wie der Nutzung zweier Excel-Fenster, um verknüpfte Blätter parallel anzuzeigen). Ergänzend existiert im Tool bereits heute das Blatt „Tool explanation“, das die Bedeutung und vorgesehenen Inhalte jeder Spalte beschreibt und damit den Einstieg erleichtert. Die in der Usability-Analyse vorgeschlagene Möglichkeit, aus einer Zelle heraus direkt „zur Quelle zu springen“ (z. B. per Hyperlink auf das referenzierte Blatt) wurde positiv aufgenommen, ist aber noch nicht umgesetzt und wird als Option für künftige Versionen geführt. Eine Reihung und Gruppierung der Blätter entlang des Modellierungsprozesses ist bereits heute über Standard-Excel-Funktionalität möglich (Verschieben/Andocken von Tabs) und wird im MoRA-Handbuch explizit empfohlen, wird aber aus Gründen der Kompatibilität nicht „hart“ im Template vorgegeben.

Beim Aspekt **Ease of Use und Umgang mit IDs/Namen** wurde in der Analyse der Wunsch nach vereinfachter Suche, einheitlichen Benennungen und einem Glossar geäußert. Auf Excel-Ebene wurden hier nur behutsame Anpassungen vorgenommen: Namen können weiterhin direkt aus Katalogblättern kopiert werden, um Doppeleingaben zu vermeiden. Gleichzeitig hat sich in der Praxis gezeigt, dass viele Anwender bewusst sprechende Titel verwenden möchten, die bereits Architekturkontext enthalten (z. B. „mTLS zwischen Vehicle Adapter Service und Mission Control“), so dass eine zu starke Automatisierung der Namen wenig hilfreich wäre. Die weitergehenden Anforderungen an Suche, Fuzzy-Matching und konsistente Wiederverwendung von IDs und Bezeichnungen werden perspektivisch durch das prototypische, SharePoint-basierte Werkzeug adressiert: Dort werden MoRA-Excel-Dateien automatisiert in Listenstrukturen überführt, sodass sich Risiken, Maßnahmen, Annahmen und andere Artefakte systemweit durchsuchen und quer über Projekte hinweg auswerten lassen. Funktionen wie eine „fuzzy search“ oder ein zentrales Glossar lassen sich dort wesentlich eleganter realisieren als im Excel-Template selbst.

Der Bedarf an **Dokumentation und kontextsensitiver Hilfe** wurde in der Analyse sehr deutlich. Schon heute enthält das MoRA-Tool das Blatt „Tool explanation“, in dem für jede Spalte die vorgesehenen Inhalte und Optionen beschrieben sind. Darüber hinaus adressiert das erwähnte MoRA-Handbook genau diese Lücke: Es erläutert nicht nur die Spalten, sondern auch typische Modellierungsmuster, Beispiele und empfohlene Vorgehensweisen (z. B. wie aus Architekturartefakten heraus Funktionen, Datenflüsse und Schutzziele systematisch abgeleitet werden). Kontextsensitiv im engeren Sinne – etwa in Form von Fragezeichen-Symbolen oder eingebetteten Tooltips direkt an kritischen Spalten – ist das Excel-Template bislang nur punktuell; eine breitere Einführung solcher Hilfen würde erneut Makros oder aufwendige Kommentarpflege erfordern und wurde daher im Projektverlauf zurückgestellt. Stattdessen dient das Handbuch als zentrale, versionierbare Referenz, auf die in Schulungen und internen Richtlinien verwiesen werden kann.

Die in der ursprünglichen Analyse angesprochenen **inhaltlichen Unstimmigkeiten und Modellierungsfragen** wurden im weiteren Verlauf differenziert betrachtet. Die Frage, ob Security Goals für Funktionen modelliert werden sollten, wird im MoRA-Handbook explizit adressiert: Der Fokus der Risikoanalyse liegt weiterhin auf Schutzzielen für Assets wie Daten und Komponenten; zusätzlich kann es aber in manchen Kontexten sinnvoll sein, aus Sicht bestimmter Funktionen (z. B. „Ausführen eines MRM“) zusammenfassende Security Goals zu betrachten, etwa für funktionsorientierte Berichte oder zur Kommunikation mit nicht-technischen Stakeholdern. Die Möglichkeit, Security Goals auch an Funktionen anzuknüpfen, ist daher als bewusste Modellierungsoption dokumentiert und nicht als Fehler zu verstehen. Beim Blatt „Risks“ wurde in der Analyse angemerkt, dass die beiden Vergleichsseiten zwar unterschiedliche Risikostände (mit/ohne Maßnahmen) darstellen können, aber stets denselben Satz von Annahmen verwenden. Hierzu existiert bereits eine Variante des MoRA-Excel-Tools, in der Annahmen je Seite getrennt konfiguriert werden können (z. B. zum Vergleich „ohne Annahmen“ vs. „mit Annahmen und Maßnahmen“); diese Variante wurde in ATLAS-L4 jedoch nicht benötigt und daher im Projektkontext nicht weiter eingesetzt. Die methodische Grundlage unterstützt also bereits die in der Usability-Analyse skizzierten Vergleichsszenarien, ihre konkrete Aktivierung hängt vom jeweiligen Anwendungsfall ab.

Insgesamt zeigt sich, dass der methodische Kern von MoRA – die strukturierte Modellierung von Funktionen, Daten, Komponenten, Schadensszenarien, Threats, Controls und Annahmen – im Excel-Template stabil abgebildet ist und im Rahmen von ATLAS-L4 gezielt um Usability-Verbesserungen ergänzt wurde. Wo kurzfristig ohne Makros und größere Strukturbrüche Verbesserungen möglich waren (z. B. automatisierte Vorschläge für „Function Assignment“, teilautomatische ID-Vergabe, bessere Erläuterungen im Template), wurden diese umgesetzt. Wo grundlegendere

Hilfestellungen sinnvoll sind (z. B. Navigationskonzept, Modellierungsempfehlungen, Varianten für Risikovergleiche), wurden sie in ein begleitendes MoRA-Handbuch und in das prototypische, SharePoint-basierte Folgewerkzeug verlagert. Viele der identifizierten Anforderungen sind damit bereits adressiert oder methodisch vorbereitet und können in zukünftigen Werkzeuggenerationen weiter ausgebaut werden.

2.1.2 Übergreifender Vergleich von ISO/SAE 21434, ISO/IEC 27000 Familie und IEC 62443 Reihe

2.1.2.1 Kurzfassung

Die Analyse zeigt, dass ISO/SAE 21434, die ISO/IEC-27000-Familie und die IEC-62443-Reihe drei komplementäre Perspektiven auf Cybersicherheit bieten:

- ISO/SAE 21434 adressiert die **fahrzeugseitige E/E-Entwicklung** und definiert Risiko explizit als Funktion aus **Attack-Feasibility** und **Impact** für Safety-, Financial-, Operational- und Privacy-Auswirkungen [27].
- Die ISO/IEC-27000-Familie bietet ein **generisches Informationssicherheits-Management-system (ISMS)**, in dem Risiko typischerweise als Kombination aus **Likelihood** und **Consequence** verstanden wird [28, 49, 50, 48].
- Die IEC-62443-Reihe fokussiert auf **Industrial-Automation- and-Control-Systeme (IACS)** und führt mit **Security Levels, Zonen** und **Conduits** zusätzliche Konzepte ein, um OT-Netze strukturiert zu segmentieren [29, 47, 51].

Eine detaillierte Begriffsanalyse zeigt, dass viele Konzepte fachlich korrespondieren (Risiko, Threat, Vulnerability, Consequence), aber unter unterschiedlichen Namen und mit abweichenden Definitionen geführt werden. Beispielhaft steht hierfür die Trias

- „**Attack Path**“ (ISO/SAE 21434) – Folge geplanter Aktionen zur Realisierung eines Threat Scenario,
- „**Risk Scenario**“ (ISO/IEC 27005) – Abfolge von Ereignissen vom Auslöser bis zur unerwünschten Folge und
- „**Threat Vector**“ (IEC 62443) – Pfad oder Mittel, über das ein Angreifer Zugang erhält.

Inhaltlich handelt es sich jeweils um eine Kette von Schritten von der Bedrohung bis zur Schädigung. Aus Sicht der beteiligten Domänen sind dies aber unterschiedliche, normativ definierte Begriffe. In interdisziplinären Runden entsteht so leicht der Eindruck, man spreche „über dasselbe“, obwohl man unterschiedliche Formalismen im Hinterkopf hat – oder umgekehrt. Diese terminologische Heterogenität ist eine wesentliche Hürde für ein durchgängiges Risikomanagement über Fahrzeug, Backend und Produktion.

Ähnliches gilt für den Risikobegriff selbst: Während ISO/SAE 21434 Attack-Feasibility und Impact entlang vorgegebener Raster bewertet, lässt ISO/IEC 27005 die Risikokriterien frei definierbar, fordert aber organisationsweite Harmonisierung. IEC 62443 wiederum verankert die Risikoermittlung in Zonierung und Security Levels. Ohne explizite Übersetzungsregeln führt dies dazu, dass ein „hohes Risiko“ im CSMS, ein „hohes Risiko“ im ISMS und ein „Security Level 2 nicht erreicht“ im IACS-Umfeld nicht ohne weiteres vergleichbar sind.

Für das organisatorische Cybersecurity-Management schreiben ISO/SAE 21434 und IEC 62443 explizit vor, bestehende Managementsysteme – insbesondere QMS und ISMS – einzubinden und

klare Schnittstellen zwischen CSMS, ISMS und IACS-Security-Programm zu etablieren. ISO/IEC 27001/27003 formulieren entsprechende Empfehlungen („sollte“) für die Abstimmung mit anderen Managementsystemen.

Im Bereich des **Risikomanagements** konvergieren die Normen auf ein risikobasiertes Vorgehen, unterscheiden sich aber in Detaillierung und Freiheitsgraden. ISO/SAE 21434 gibt Bewertungsrasster für Attack-Feasibility und Impact vor, ISO/IEC 27005 lässt Risikokriterien weitgehend frei definierbar, fordert aber organisatorische Harmonisierung [175], und IEC 62443-3-2 verankert die Risikobetrachtung in der IACS-Zonierung und anwendungsbezogenen Sicherheitsniveaus.

Für ATLAS-L4 bedeutet dies: Die Normen konkurrieren nicht, sie ergänzen sich – ihre **Unterschiede** in Terminologie und Methodik sind aber real und müssen aktiv überbrückt werden. Andernfalls bleiben Risiken domänenspezifisch optimiert, aber quer über Fahrzeug, Backend und Produktion nicht konsistent.

2.1.2.2 Geltungsbereich und Terminologie

Geltungsbereich. Die drei Normenfamilien unterscheiden sich zunächst deutlich in ihrem Scope:

- ISO/SAE 21434 beschränkt sich explizit auf E/E-Systeme in Straßenfahrzeugen. Systeme außerhalb des Fahrzeugs – etwa Backend-Server oder Produktionsanlagen – können zwar „für Cybersicherheitszwecke berücksichtigt“ werden, gehören aber nicht zum unmittelbaren Normumfang.
- *ISO/IEC-27000-Familie* ist organisationsweit anwendbar. ISO/IEC 27001 formuliert Anforderungen an ein ISMS für **alle Organisationstypen** und Informationswerte, vom Quellcode bis zu Kunden- und Personaldaten.
- *IEC-62443-Reihe* fokussiert auf IACS und deren Integration in Unternehmensnetzwerke. Einzelne Normen adressieren dabei unterschiedliche Stakeholder (Asset Owner, Systemintegratoren, Produktlieferanten).

Für ein ATLAS-L4-Szenario bedeutet dies: Das fahrzeugseitige ADS und die vernetzten Steuergeräte fallen in den Geltungsbereich von ISO/SAE 21434; das Control-Center-Backend, Datenplattformen und KI-Trainingsumgebungen gehören in den Geltungsbereich eines ISMS nach ISO/IEC 27001; die OT-Infrastruktur in der Fahrzeugproduktion wird durch IEC 62443 adressiert.

Terminologische Korrespondenzen und ihre Tücken. Auf den ersten Blick lassen sich die Kernbegriffe der drei Normwelten gut einander zuordnen:

- Risk / Risiko
 - ISO/SAE 21434: Effekt von Unsicherheit auf die Fahrzeugsicherheit, ausgedrückt als Kombination von Attack-Feasibility und Impact.
 - ISO/IEC 27000/27005: Effekt von Unsicherheit auf Ziele; Risiko als Kombination von Likelihood und Consequence.
 - IEC 62443: Erwarteter Verlust, ausgedrückt als Likelihood, dass eine Threat eine Vulnerability mit bestimmter Consequence ausnutzt.

Fachlich geht es stets darum, „Wahrscheinlichkeit/Aufwand“ und „Schadensausmaß“ zu verknüpfen. Dennoch sind die Formeln nicht identisch: ISO/SAE 21434 arbeitet mit einem normativ festgelegten Attack-Feasibility-Raster, ISO/IEC 27005 erlaubt große Freiheit bei Likelihood-Skalen, IEC 62443 bindet die Bewertung an Security Levels und Zonen. In der Praxis bedeutet das:

Wenn ein CSMS-Team einen Risk-Wert 4 meldet und ein ISMS-Team ein „hohes Risiko“ dokumentiert, ist nicht automatisch klar, ob dies vergleichbare Größen sind.

Ähnlich verhält es sich mit den **Pfaden vom Angreifer zur Auswirkung**:

- ISO/SAE 21434: „Attack Path“ (konkrete Folge geplanter Aktionen zur Realisierung eines Threat Scenario),
- ISO/IEC 27005: „Risk Scenario“ (Sequenz von Ereignissen vom Auslöser bis zur unerwünschten Folge),
- IEC 62443: „Threat Vector“ (Pfad oder Mittel, über das ein Angreifer Zugang gewinnt).

Alle drei beschreiben im Kern eine Kette von Schritten. Trotzdem sind sie nicht austauschbar: ISO/SAE 21434 verankert Attack Paths eng in der TARA-Methodik und Attack-Feasibility-Bewertung; ISO/IEC 27005 nutzt Risk Scenarios als Träger für Likelihood- und Consequence-Abschätzungen; IEC 62443 verknüpft Threat Vectors mit Zonen und Security Levels. Wenn in einem Meeting „Angriffspfade“ diskutiert werden, müssen die Beteiligten explizit klären, ob sie Attack Paths, Risk Scenarios oder Threat Vectors meinen – sonst laufen Fachbereiche Gefahr, aneinander vorbeizureden.

Weitere Beispiele:

- **Damage Scenario (ISO/SAE 21434) vs. Consequence (ISO/IEC 27005, IEC 62443)** – inhaltlich ähnlich, aber in 21434 klar als fahrzeugbezogenes Schadensszenario verankert.
- **Cybersecurity Control / Control / Countermeasure** – jeweils „risikomindernde Maßnahme“, aber mit unterschiedlichen Katalogen und Bewertungslogiken.
- **Cybersecurity Claim (ISO/SAE 21434) vs. Risk Sharing (ISO/IEC 27005) vs. Tolerable Risk (IEC 62443)** – unterschiedliche Formen, mit verbleibenden oder geteilten Risiken umzugehen.

Dazu kommen normspezifische Begriffe ohne direkter Entsprechung, etwa

- **Risk Owner** (ISO/IEC 27000),
- **Security Level, Zone, Security Perimeter** (IEC 62443),
- **Weakness** (ISO/SAE 21434).

Aus ATLAS-L4-Sicht ist damit klar: Es reicht nicht, intern ein „Glossar“ zu besitzen – zwischen CSMS, ISMS und IACS-SP ist eine **explizite begriffliche Übersetzungsschicht** nötig, damit eine TARA-„Attack Path“ nicht als 27005-„Risk Scenario“ fehlinterpretiert wird oder umgekehrt.

2.1.2.3 Organisatorisches Cybersecurity-Management

ISO/SAE 21434

ISO/SAE 21434 verlangt ein organisationsweites **Cybersecurity-Managementsystem (CSMS)** für die Fahrzeugentwicklung [21]:

- [RQ-05-01] fordert eine Cybersecurity-Policy, die Cybersicherheitsrisiken anerkennt und mit den Zielen und anderen Policies der Organisation verknüpft werden kann.
- [RQ-05-05] verlangt explizit, **Disziplinen im Umfeld der Cybersicherheit** (z. B. IT-Security, funktionale Sicherheit, Privacy) zu identifizieren und **Kommunikationskanäle** zwischen ihnen zu etablieren, u. a. zum Austausch von Bedrohungsszenarien, Safety- und Security-Goals sowie potenziellen Zielkonflikten.

Übersetzungsproblem: Die Flüsse verbinden Domänen, die teilweise **unterschiedliche Begriffe und Risikomodelle** verwenden. Ohne sauber definierte Schnittstellen und Begriffs-Mappings ist eine konsistente Umsetzung der in der Abbildung angedeuteten Cross-Domain- und Cross-MS-Flows kaum möglich.

ISO/IEC 27001 und 27003

ISO/IEC 27001/27003 fordern den Aufbau eines **ISMS**, das auf den Kontext der Organisation zugeschnitten ist:

- externe und interne „Issues“ (z. B. regulatorisches Umfeld, Unternehmensstruktur) sind zu bestimmen (4.1),
- beim Festlegen des Scopes des ISMS sind **Grenzen und Abhängigkeiten** zu anderen Organisationseinheiten und ausgelagerten Funktionen zu berücksichtigen (4.3),
- Kommunikationsbedarfe (z. B. Pläne und Ergebnisse des Risikomanagements, Vorfälle) sind zu definieren (7.4).

ISO/IEC 27003 empfiehlt, beim Aufbau eines ISMS **bestehende Managementsysteme** zu berücksichtigen, Strukturen zu übernehmen und gemeinsame Funktionen (Management-Reviews, Audits) zu kombinieren. Abbildung 12 kondensiert diese Aussagen:

- Das ISMS wird als **horizontale Klammer** um mehrere Managementsysteme (z. B. QMS, CSMS, Umwelt- oder Safety-Management) dargestellt.
- Zwischen dem ISMS und den übrigen Systemen verlaufen **bidirektionale Pfeile**, die die in 27001/27003 geforderten Schnittstellen symbolisieren:
 - Übernahme von Governance-Strukturen,
 - Abstimmung des Scopes (z. B. welche Assets liegen im ISMS, welche im CSMS),
 - Austausch von Risiko- und Vorfallsinformationen.
- Die Abbildung verdeutlicht, dass ISO/IEC 27001 kein reines „IT-Sicherheits-Insel-System“ vorsieht, sondern ein **übergreifendes Managementsystem mit expliziten Anschlussstellen** an andere Domänen.

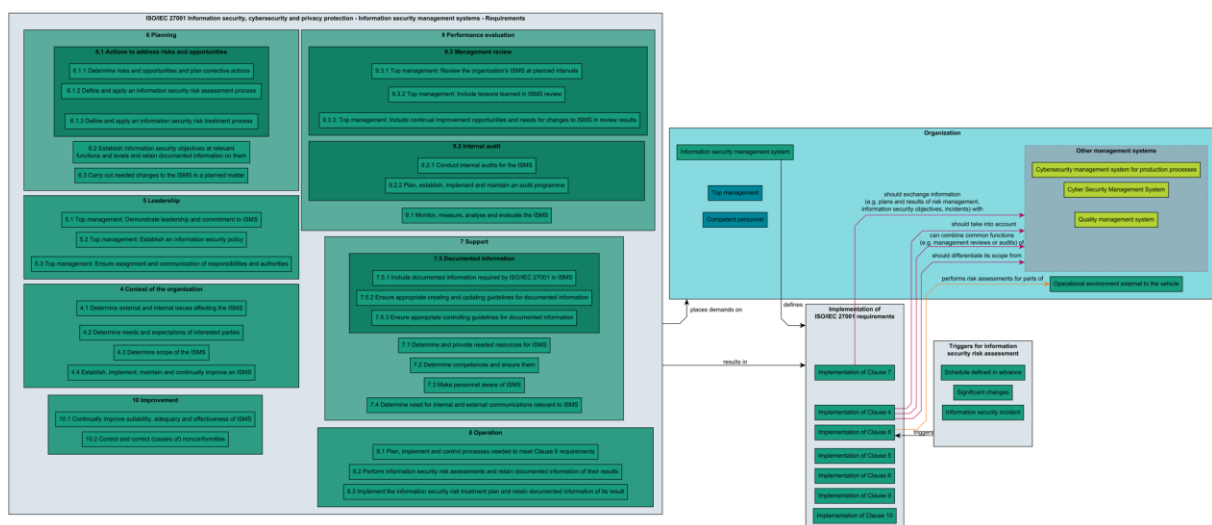


Abbildung 12: Einbettung des ISMS in andere Managementsysteme nach ISO/IEC 27001/27003.

Für ATLAS-L4 bedeutet das: Das ISMS ist nicht nur ein weiteres „Silotool“, sondern soll laut Norm ausdrücklich mit CSMS und weiteren Systemen verzahnt werden – allerdings ohne zu definieren, **wie** z. B. Attack-Feasibility-Skalen in die ISMS-Risikologik einzubetten sind.

IEC 62443-2-1

IEC 62443-2-1 fordert von Asset Ownern ein **IACS-Security-Programm (SP)** und betont dessen Zusammenspiel mit einem bestehenden ISMS:

- Das IACS-SP soll ein ISMS **ergänzen**, um eine koordinierte Betriebs- und Informationssicherheit zu erreichen; vollständige Konsistenz ist wegen unterschiedlicher Verfügbarkeitsanforderungen nicht immer möglich (4.1.2.1).
- Annex A stellt **Cross-References** zu ISO/IEC 27001 und NIST-Rahmenwerken bereit, um eine harmonisierte Umsetzung zu erleichtern (4.1.2.2).
- ORG 1.1 verlangt explizit, dass das IACS-SP mit einem vorhandenen ISMS **koordiniert** wird, inkl. gemeinsamer Gestaltung von IT/OT-Schnittstellen (Firewalls, DMZ, Remote-Access) und Zugriffskonzepten.
- Weitere Anforderungen (z. B. ORG 1.6 Supply-Chain-Security, CM 1.1 Asset-Inventar, NET 1.1/8.2.1 Segmentierung von IACS- und Nicht-IACS-Zonen) adressieren typische OT-Schnittstellen in der Produktion.

Abbildung 13 stellt diese Zusammenhänge grafisch dar:

- Die **IACS-Zone** mit ihrem Security-Programm ist als eigener Block innerhalb der OT-Landschaft dargestellt.
- Das Unternehmens-ISMS bildet eine **übergeordnete Ebene**, mit Pfeilen zum IACS-SP, die gemeinsame Richtlinien, abgestimmte Schutzkonzepte und geteilte Schnittstellen (z. B. DMZ, Remote-Access-Gateways) symbolisieren.
- Weitere Pfeile deuten an, dass das IACS-SP wiederum mit anderen Managementsystemen (z. B. QMS, Safety-Management) interagiert.

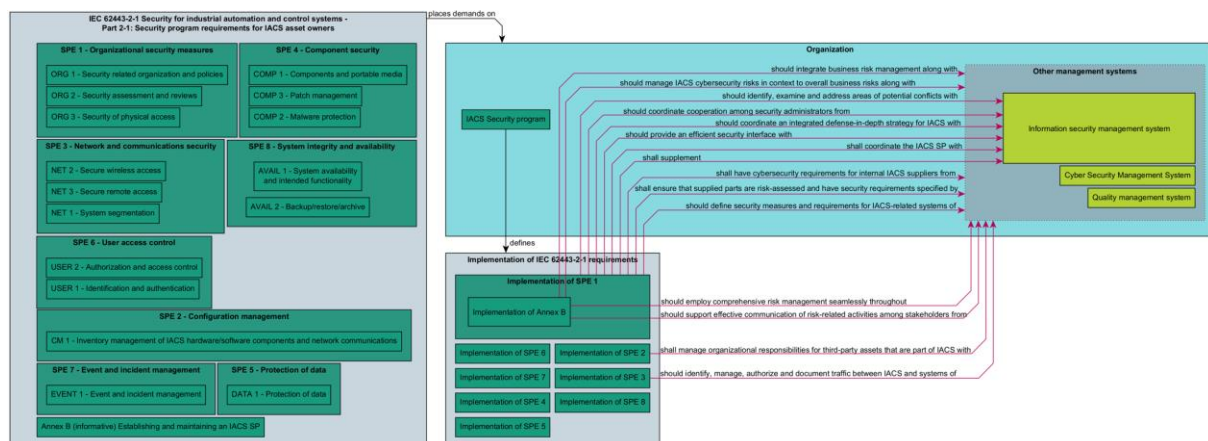


Abbildung 13: Koordination von IACS-Security-Programm und ISMS nach IEC 62443-2-1.

Die Abbildung macht sichtbar, dass IEC 62443 – ähnlich wie ISO/SAE 21434 – zwar primär eine **spezifische Domäne (OT/IACS)** adressiert, aber explizit eine **angekoppelte Governance** an das ISMS fordert. Wie die dort verwendeten Konzepte (Security Levels, Zonen, Conduits) in die Begriffswelt anderer Domänen übersetzt werden sollen, bleibt jedoch offen.

Einordnung für ATLAS-L4. Für ATLAS-L4 ergibt sich daraus ein organisatorisches Zielbild:

- Ein **CSMS nach ISO/SAE 21434** steuert die Security-Aktivitäten für Lkw-E/E-Systeme und ADS.
- Ein **ISMS nach ISO/IEC 27001** deckt u. a. Control-Center, Backend-Plattformen, Datenhaltung und KI-Infrastruktur ab.
- Ein **IACS-Security-Programm nach IEC 62443-2-1** fixiert Sicherheitsanforderungen für Produktions- und OT-Netze.

Die beschriebenen Abbildungen verdeutlichen, dass diese Systeme **nicht isoliert** gedacht sind: Sie sind über cross-domain-Flows (fachliche Anforderungen und Annahmen) und cross-MS-Flows (Policies, Risikoberichte, Vorfallmeldungen) miteinander verbunden. Gleichzeitig zeigen sie, warum die Integration in der Praxis anspruchsvoll ist: Die Managementsysteme sitzen auf **unterschiedlichen Terminologien und Risikomodellen**, deren Übersetzung nicht durch die Normtexte vorgegeben wird und im Unternehmen aktiv gestaltet werden muss.

2.1.2.4 Cybersicherheits-Risikomanagement

ISO/SAE 21434

ISO/SAE 21434 beschreibt in den Klauseln 9 und 15 ein mehrstufiges Vorgehen zur **Threat Analysis and Risk Assessment (TARA)**:

- Die Betriebsumgebung muss so beschrieben werden, dass relevante Threat Scenarios und Attack Paths identifiziert werden können ([RQ-09-02]); Annahmen über externe Abhängigkeiten (z. B. PKI-CAs, Backend-Sicherheit, Produktions-CSMS) sind explizit zu erfassen.
- Das Risiko wird über **Impact Ratings** und **Attack-Feasibility-Ratings** ausgedrückt; beides wird in einer vorgegebenen **Risikomatrix** kombiniert.
 - Impact Ratings: mindestens die vier Impact-Kategorien **Safety, Financial, Operational, Privacy** müssen betrachtet werden. Die Norm gibt hierfür diskrete Bewertungsstufen (z. B. 0–3, „vernachlässigbar“ bis „schwerwiegend“) vor.
 - Attack-Feasibility-Rating (AFR): die Angriffsmachbarkeit wird qualitativ anhand eines normativen Rasters (z. B. Aufwand, Expertise, Kenntnis des Items, Window of Opportunity, benötigte Ausrüstung) bewertet und zu diskreten Feasibility-Stufen zusammengefasst.
 - Die so entstehenden Paare (Impact, Attack-Feasibility) werden auf **diskrete Risikowerte** abgebildet; die Norm spezifiziert zulässige Skalen und Beispiel-Risikomatrizen.
- Safety-bezogene Impact-Ratings sind gemäß ISO 26262-3 abzuleiten ([RQ-15-06]); Safety-Analysen können wiederverwendet werden.
- Wenn Entscheidungen zur Risikobehandlung ein **Risikoteilen oder -beibehalten** beinhalten, sind **Cybersecurity Claims** zu definieren ([RQ-09-06]). Diese Claims dokumentieren u. a.,
 - welche Annahmen über externe Systeme (Backend, Produktion, andere Items) getroffen werden,
 - welches Restrisiko bewusst akzeptiert oder an andere Bereiche „geteilt“ wird,
 - und dienen als Anknüpfungspunkt für kontinuierliche Aktivitäten (Monitoring, Vulnerability Management).
- Cybersecurity-Anforderungen können sowohl das **Produkt** als auch die **Betriebsumgebung** betreffen ([RQ-09-09]); Anforderungen an die Betriebsumgebung (z. B. Backend-Authentisierung, Produktions-CSMS) sind in Validierungsaktivitäten einzubeziehen.

Abbildung 14 stellt diese Mechanik im Detail dar:

- Im **linken Block** ist das „Item“ (z. B. ADS im Lkw) als eigene Domäne dargestellt:
 - Domäneninterne Komponenten (z. B. Steuergeräte, TARA-Prozess) sind als **Domain components** visualisiert.
 - **Domain-interne Flüsse** zeigen den Ablauf der TARA: von der Beschreibung der Betriebsumgebung über die Identifikation von Threat Scenarios und Attack Paths, die Bewertung mittels Impact- und Attack-Feasibility-Ratings bis hin zur Ableitung von Cybersecurity-Zielen und -Anforderungen.
 - Innerhalb dieser Domäne werden **konkret zulässige Werte** verwendet: vordefinierte Impact-Kategorien und -Ratings (z. B. 0–3 pro Kategorie), vordefinierte Attack-Feasibility-Stufen, und daraus abgeleitete diskrete Risikowerte (numerische Klassen gemäß Normbeispiel).
- Im **rechten Bereich** stehen die **domänenexternen Komponenten** („Domain-external components“), etwa:
 - Backend-Systeme (Control Center, Datenplattformen),
 - Produktions-/OT-Systeme,
 - andere Items/Fahrzeuge oder externe PKI-Infrastrukturen.
- Die Grafik unterscheidet klar zwischen:
 - **Cybersecurity-Anforderungen an die Betriebsumgebung:** Pfeile vom Item zu Backend/Produktion, die z. B. Forderungen nach gesicherter Kommunikation, bestimmter Authentisierungs- und Update-Mechanismen oder Produktions-Security-Programmen tragen. Diese werden in der Abbildung als **Cross-domain flows** (fachliche Anforderungen) dargestellt.
 - **Cybersecurity Claims:** weitere Pfeile kennzeichnen Claims, mit denen Risiken explizit **geteilt** oder – auf Basis von Annahmen – **beibehalten** werden. Diese Claims verlassen die Item-Domäne und laufen in Richtung anderer Managementsysteme (z. B. ISMS, IACS-SP). In der Grafik werden sie als **Cross-MS-Flows** gekennzeichnet, da sie nicht nur fachliche, sondern auch managementsystembezogene Artefakte sind.

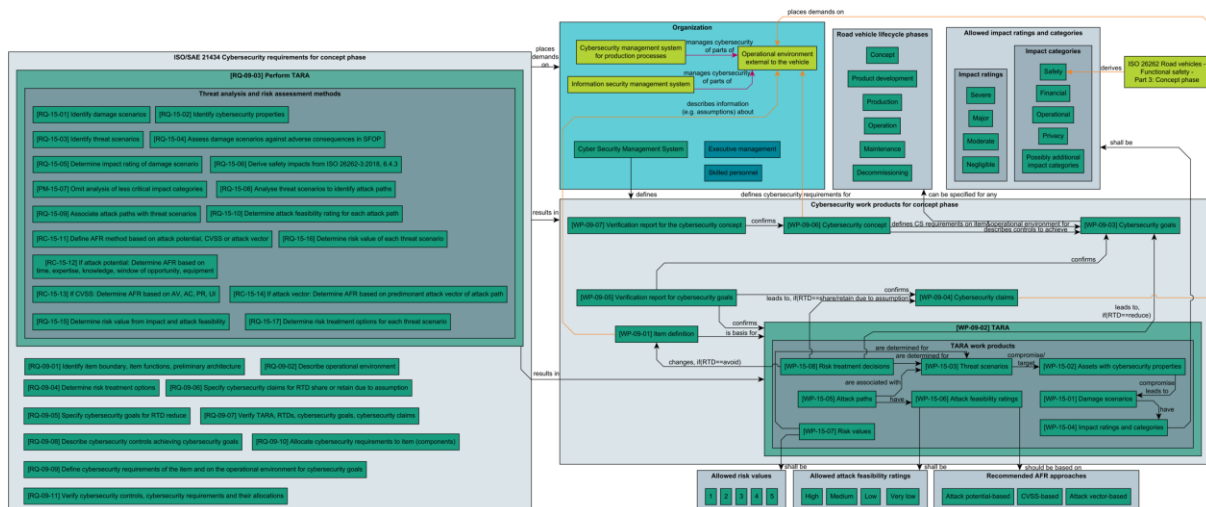


Abbildung 14: Kernaspekte des Risikomanagements nach ISO/SAE 21434 und Übertragung von Cybersecurity-Claims und -Anforderungen auf externe Systeme und Managementsysteme.

Die Abbildung macht sichtbar, dass ISO/SAE 21434 das Risikomanagement **nicht** an der Systemgrenze des Fahrzeugs enden lässt:

- Risiken werden zunächst mit normativ festgelegten Kategorien und Skalen innerhalb des Items bewertet.
- Das Ergebnis (Risikowerte, Anforderungen, Claims) wird anschließend **explizit über die Domänengrenze hinweg** an andere Systeme und Managementsysteme „weitergereicht“.
- Technisch präzise formulierte Anforderungen und Claims treffen dabei auf andere Domänen, die häufig andere Begriffe und Skalen verwenden – genau an diesen Schnittstellen entsteht Übersetzungsbedarf.

ISO/IEC 27005

ISO/IEC 27005 beschreibt einen generischen Prozess zur Bewertung und Behandlung von Informationssicherheitsrisiken:

- Organisationen sollen **Risikokriterien** definieren, einschließlich Akzeptanz-, Konsequenz- und Likelihood-Kriterien (6.4.2, 6.4.3).
- Diese Kriterien sollen **organisationsweit harmonisiert** werden, damit Risiken aus verschiedenen Geschäftsbereichen kommuniziert, verglichen und aggregiert werden können. Dabei betont 27005 ausdrücklich:
- Risiken können **qualitativ oder quantitativ** bewertet werden;
- die konkrete Skala (z. B. 1–5, „low/medium/high“, monetäre Größen) ist **nicht vorgegeben**, sondern von der Organisation zu definieren;
- Konsequenzen, die in verschiedenen Bereichen in unterschiedlichen Maßeinheiten beschrieben werden, sollen auf eine **gemeinsame Referenzskala** abgebildet werden (6.4.3.2).
- Die Wahl der Risikomethoden soll an die allgemeinen Risikomanagementmethoden der Organisation (z. B. ISO 31000) **angeglichen** werden (6.5).
- Bei der Risikobehandlung werden Optionen wie Risikovermeidung, -minderung, **Risikoteilung** und -akzeptanz beschrieben (8.2); im Falle des Risikoteilens bleibt mindestens eine Schutzmaßnahme erforderlich, die Implementierungsverantwortung kann aber an eine andere Partei delegiert werden.

Abbildung 15 zeigt ISO/IEC 27005 als **zentrale Referenzschicht** über mehreren Managementsystemen:

- Am unteren Rand sind mehrere Managementsysteme (z. B. CSMS nach ISO/SAE 21434, ISMS nach ISO/IEC 27001, IACS-Security-Programm nach IEC 62443-2-1) als **separate Blöcke** dargestellt. Jeder Block steht für eine Domäne mit eigenen Risikoanalysen, Tools und Terminologie.
- Darüber ist ISO/IEC 27005 als **gemeinsames Dach** visualisiert. Mehrere Pfeile verbinden diese „Dachschicht“ mit den einzelnen Managementsystemen:
 - Einer dieser Pfeile steht für die Definition und Harmonisierung der Risikokriterien: 27005 verlangt, dass alle Bereiche eine konsistente Definition von „Consequence“ und „Likelihood“ verwenden – unabhängig davon, ob sie letztlich in diskreten Stufen oder monetär ausgedrückt werden. Die Abbildung bringt dies durch einen zentralen Block „Risikokriterien (Konsequenz/Likelihood, Akzeptanzschwellen, Bewertungsmaßstab)“ zum Ausdruck, von dem aus Linien in alle Managementsysteme führen.

- Weitere Pfeile repräsentieren standardisierte Risikoprozesse (Risk Assessment, Risk Treatment, Risk Communication), die in allen Systemen nach denselben Grundprinzipien ablaufen, auch wenn die Detailmethoden variieren dürfen.
- Ein zusätzlicher Pfeil steht für Risk-Sharing-Mechanismen: ISO/IEC 27005 beschreibt, wie Risikoübernahme und -teilung formal zu dokumentieren sind (z. B. durch Benennung von Risk Owners, Vereinbarungen mit Lieferanten, Versicherungen) und wie diese Informationen zwischen Bereichen kommuniziert werden sollen.

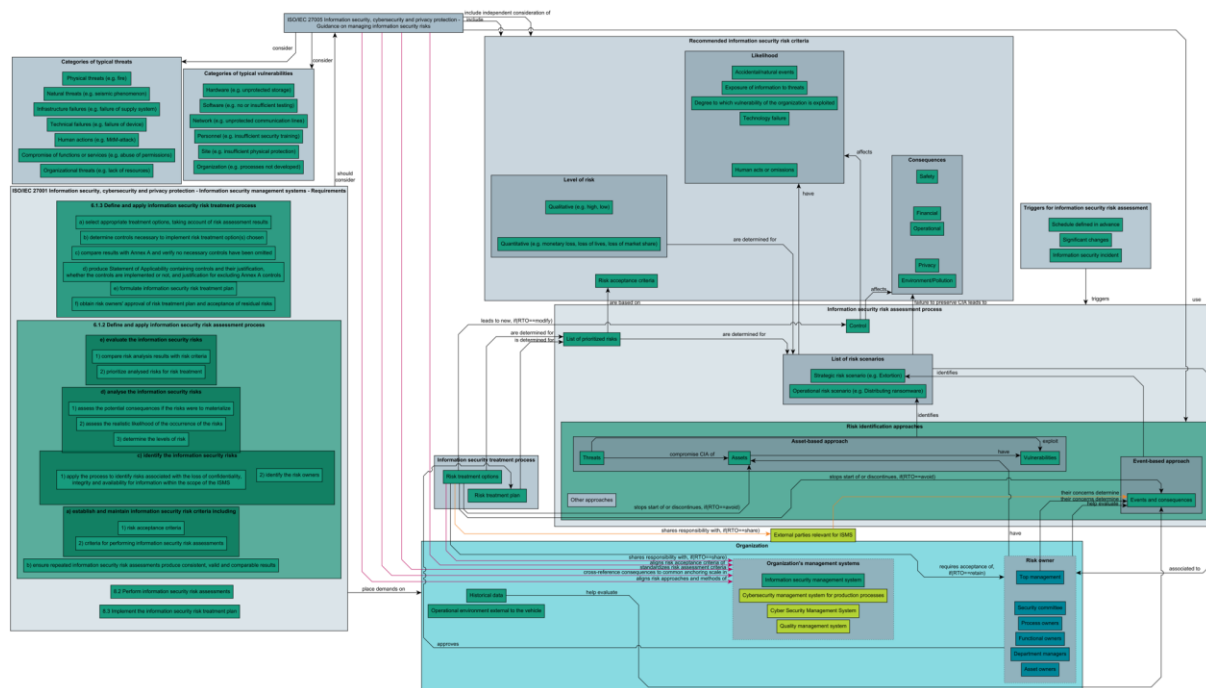


Abbildung 15: Kernaspekte des Risikomanagements nach ISO/IEC 27005 und Harmonisierung von Risikokriterien und -prozessen über CSMS, ISMS und IACS-Security-Programm hinweg.

Die Grafik verdeutlicht, dass ISO/IEC 27005 **keine festen Wertebereiche** vorgibt, sondern die Organisation zwingt,

- eigene **Skalen** für Konsequenz und Likelihood zu definieren und
- diese Skalen **über alle Managementsysteme hinweg zu harmonisieren**.

Damit bildet ISO/IEC 27005 die „Meta-Schicht“, auf der:

- das im CSMS verwendete TARA-Schema (Impact-Kategorien, Attack-Feasibility, diskrete Risikowerte),
- das im ISMS verwendete Risikomodell (z. B. 1–5-Skala, monetäre Schätzungen, qualitative Kategorien),
- und das im IACS-Security-Programm verwendete Modell (z. B. Security Levels, tolerable risk) auf eine **gemeinsame organisationale Referenzskala** abgebildet werden können.

IEC 62443-3-2

IEC 62443-3-2 definiert einen strukturierten Prozess zur **Risikobewertung im IACS-Kontext**:

- Zunächst wird das **System under Consideration (SUC)**, sein Security-Perimeter und alle Zugangspunkte identifiziert (ZCR 1.1).

- IACS-Assets sind in Zonen zu gruppieren, die von Business-Systemen zu trennen sind (ZCR 3.2, 4.4.3).
- Ein initiales Cybersecurity-Risiko wird bestimmt und mit einem organisationsweit definierten „**tolerable risk**“ verglichen (ZCR 4.1, 4.5.2).
- Wenn das initiale Risiko das tolerable Risiko übersteigt, ist eine **detaillierte Risikobewertung** durchzuführen (ZCR 5), wobei Methoden wie ISO 31000, ISO/IEC 27005 oder NIST SP 800-39 explizit als kompatibel genannt werden.
- Bestehende Analysen aus **funktionaler Sicherheit, IT-Security, physischer Sicherheit und Business-Risiko** sollen zur Bestimmung von Konsequenzen herangezogen werden (ZCR 5.3, 5.4).
- Für die Likelihood sind sowohl qualitative als auch quantitative Methoden zulässig; in Ausnahmefällen werden auch **konsequenzbasierte Verfahren** akzeptiert, die Likelihood implizit als „ständig vorhanden“ annehmen (ZCR 5.4/5.5).

Abbildung 16 visualisiert diesen Prozess in Form eines **Phasenmodells**, das zugleich an die beiden anderen Standards anschlussfähig ist:

- Im Zentrum steht das **SUC** als abgegrenzter Block, der von einem **Security Perimeter** umschlossen ist. Der Perimeter markiert die logische/physische Grenze der betrachteten IACS-Assets; an ihm sind sämtliche **Access Points** eingezeichnet, über die Bedrohungen einwirken können (ZCR 1.1).
- Innerhalb des Perimeters sind **Zonen** dargestellt, die die IACS-Assets nach Kriterien wie Funktion, Kritikalität oder verantwortliche Organisation gruppieren. Neben den IACS-Zonen ist eine **separate Business-Zone** angedeutet, getrennt durch eine Boundary mit nur wenigen, kontrollierten Verbindungen (ZCR 3.2, 4.4.3).
- Auf der linken Seite ist ein Block „**Initial Cybersecurity Risk Assessment**“ angeordnet, der vom SUC-Block aus gespeist wird. Er steht für die **erste, grobe Bewertung** des Cyberrisikos.
- Dieses initiale Risiko wird in einem nächsten Schritt mit einem Block „**Tolerable Risk**“ verglichen. Die Grafik zeigt diesen Vergleich explizit als Entscheidungsknoten:
 - „**Initial Risk ≤ Tolerable Risk**“ → es sind keine zusätzlichen detaillierten Analysen erforderlich, das Risiko ist aus Sicht der Organisation akzeptabel.
 - „**Initial Risk > Tolerable Risk**“ → der Pfeil führt weiter zu einem Block „**Detailed Cybersecurity Risk Assessment**“.
- Der Block „**Detailed Cybersecurity Risk Assessment**“ ist über Verweis-Pfeile mit **externen Rahmenwerken** verbunden, etwa **ISO 31000, ISO/IEC 27005** und **NIST SP 800-39**. Diese Pfeile verdeutlichen, dass IEC 62443-3-2 keine eigene, vollständig neue Risikomethodik aufbaut, sondern explizit fordert, dass initiale und detaillierte Bewertungen auf einer **gemeinsamen Risikoskala und einem gemeinsamen Rahmen** basieren (ZCR 5.1, 5.2).
- Aus dem detaillierten Assessment führt ein weiterer Block „**Risk Reduction Measures / Security Levels**“ zurück in die Zonenstruktur:
 - Hier wird symbolisiert, dass die identifizierten Risiken durch **technische und organisatorische Maßnahmen** mitigiert werden, die sich in **Security Levels** und Zonen-/Conduit-Konzepten niederschlagen.
 - Die Grafik stellt damit die Verbindung zwischen abstrakten Risikoergebnissen und konkreter IACS-Architektur (Zonierung, Perimeter, Conduits) her.

- Ergänzend sind an der Seite Verweise auf **bestehende Analysen** (PHA, Safety, IT-Security, Physical Security, Business Risk) angedeutet, die in den Schritt „Determine consequence and impact“ einfließen (ZCR 5.3, 5.4).

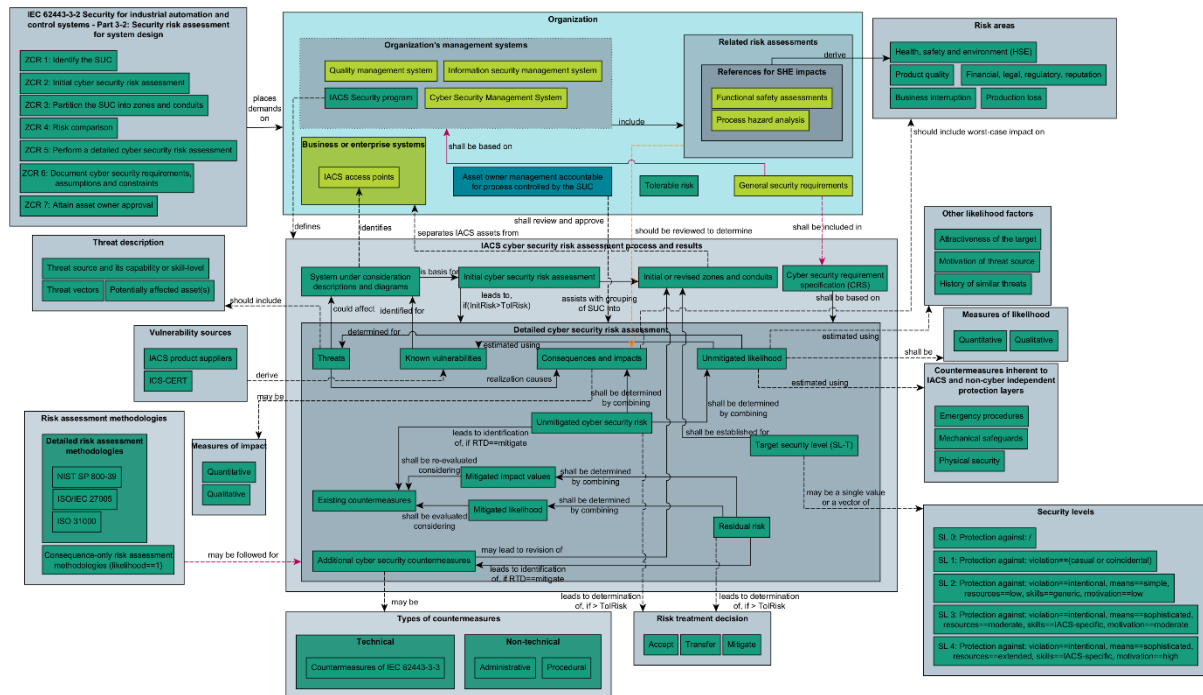


Abbildung 16: Cybersecurity Risikomanagement im IACS-Kontext nach IEC 62443-3-2.

Die Abbildung macht damit drei Spezifika von IEC 62443-3-2 sichtbar:

1. Die **Trennung von initialer und detaillierter Risikobetrachtung**, gesteuert durch das organisationsspezifische „tolerable risk“.
2. Den **Zwang zur Konsistenz** der Risikoskala und des methodischen Rahmens mit allgemeinen Risikostandards (ISO 31000, ISO/IEC 27005 etc.).
3. Die **enge Kopplung von Risikoergebnissen an die IACS-Architektur** (Zonen, Security Levels, Perimeter) und die Möglichkeit, bereits vorhandene Analysen aus anderen Disziplinen wiederzuverwenden.

Für ATLAS-L4 ist wichtig: IEC 62443-3-2 verlangt zwar keine festen numerischen Risikowerte, erzwingt aber, dass initiale und detaillierte Bewertungen derselben **organisationsweiten Skala** folgen. In Kombination mit ISO/IEC 27005 ist das der Hebel, IACS-Risiken so zu bewerten, dass sie mit CSMS- und ISMS-Risiken vergleichbar sind – trotz unterschiedlicher Domänen.

Zusammenspiel der Risikomanagement-Ansätze – normenspezifische Werte vs. offene Gestaltung

Aus den **drei Abbildungen** (ISO/SAE 21434, ISO/IEC 27005, IEC 62443-3-2) und den Normtexten ergibt sich ein gemeinsames Bild – und ein Spannungsfeld:

ISO/SAE 21434: stark vorstrukturierte Werte und Kategorien. ISO/SAE 21434 arbeitet mit einem **eng definierten Risikoschema**, das viele Parameter explizit vorgibt:

- Impact-Kategorien: mindestens **Safety, Financial, Operational, Privacy** müssen betrachtet werden; zusätzliche Kategorien sind möglich, aber nicht zwingend.
- Impact-Ratings: je Kategorie werden **diskrete Stufen** vergeben (z. B. 0–3, „vernachlässigbar“ bis „schwerwiegend“), teils direkt mit ISO 26262 verknüpft.

- Attack-Feasibility: wird über ein normativ vordefiniertes Raster (Aufwand, Expertise, Window of Opportunity, Wissen, erforderliche Ausrüstung etc.) bestimmt und auf **diskrete Feasibility-Stufen** abgebildet.
- Risikomatrix: die Kombination aus Attack-Feasibility-Stufe und Impact-Rating führt zu **vorgegebenen Risikoklassen**; Beispielmatrizen sind Bestandteil der Norm.
- Risikoteilung / -beibehalt: lösen zwingend **Cybersecurity Claims** aus, die als explizite, überprüfbare Aussagen dokumentiert und in den kontinuierlichen Aktivitäten überwacht werden müssen.

Die 21434-Abbildung zeigt das deutlich: TARA erzeugt innerhalb der Fahrzeugdomäne **normativ strukturierte Risikoartefakte** (Threat Scenarios, Attack Paths, Risikowerte, Anforderungen, Claims), die anschließend als **Anforderungen und Claims an externe Systeme und Managementsysteme** (ISMS, IACS-SP) „exportiert“ werden.

ISO/IEC 27005: strukturierte, aber inhaltlich offene Risikomodelle. ISO/IEC 27005 definiert demgegenüber vor allem die **Struktur** des Risikomanagements:

- Risiko besteht aus **Consequence** und **Likelihood**;
- es verlangt definierte **Risikokriterien**, inklusive Akzeptanzkriterien, Skalen für Consequence und Likelihood etc.;
- es fordert, dass diese Kriterien **organisationsweit standardisiert** werden (6.4.3), damit Risiken über Geschäftsbereiche hinweg vergleichbar sind;
- es verlangt, dass unterschiedliche Konsequenzmaße (z. B. Safety-Schweregrade, Euro-Beträge, OT-Klassifizierungen) auf eine **gemeinsame Referenzskala** abgebildet werden (6.4.3.2);
- es schreibt nicht vor, ob Skalen z. B. 1–5, „low/medium/high“ oder quantitativ sein müssen – **die Ausprägung bleibt offen**, solange sie konsistent sind.
- bei der Risikobehandlung werden Optionen wie Avoid, Mitigate, **Share** und Accept beschrieben; Risk-Sharing erfordert mindestens eine Control, deren Umsetzung an Dritte delegiert werden kann (8.2).

Die 27005-Abbildung positioniert ISO/IEC 27005 als **übergreifendes Dach**, das CSMS, ISMS und IACS-SP über gemeinsame **Risikokriterien und Prozesse** verbindet. Sie zeigt: 27005 liefert nicht die „fertige Skala“, sondern zwingt die Organisation dazu, **eigene Skalen zu definieren und zu harmonisieren** – auch für domänenspezifische Schemen wie TARA oder Security Levels.

IEC 62443-3-2: tolerable risk, Zonen und konsistente Skalen im OT-Kontext. IEC 62443-3-2 nimmt eine **OT-spezifische Mittelposition** ein:

- Die Norm verlangt, dass Organisationen ein „**tolerable risk**“ definieren – ein organisationsweit akzeptiertes Risikoniveau für IACS (4.5.2).
- Die **initiale Risikobewertung** liefert einen groben Risikowert, der mit diesem tolerable risk verglichen wird.
- Wird das tolerable risk überschritten, ist eine **detaillierte Risikobewertung** durchzuführen (4.6).
- Für die detaillierte Bewertung dürfen **beliebige Methoden** verwendet werden (z. B. ISO 31000, ISO/IEC 27005, NIST SP 800-39), **unter der Bedingung**, dass initiale und detaillierte Methoden auf demselben Rahmen basieren und eine **konsistente Risikoskala** verwenden (4.6.1).

- Konsequenzen und Impact sollen unter Rückgriff auf bestehende Analysen (PHA, Safety, IT-Security, physische Sicherheit, Business) bestimmt werden (4.6.4).
- Für die Likelihood sind **qualitative und quantitative** Ansätze erlaubt; bei konsequenzbasierten Verfahren wird Likelihood implizit als „ständig vorhanden“ angenommen (4.6.5).

Die IEC-62443-3-2-Abbildung verdeutlicht diese Logik:

- SUC-Perimeter und Access Points definieren den **Scope**,
- initiales Risiko → Vergleich mit **tolerable risk** → ggf. detaillierte Bewertung,
- die detaillierte Bewertung hängt methodisch an **ISO/IEC 27005/ISO 31000**,
- Risikoergebnisse schlagen sich in **Security Levels, Zonen und Conduits** nieder.

IEC 62443-3-2 schreibt damit zwar **keine konkreten Risikowerte oder Bewertungsraster** vor, erzwingt aber, dass OT-Risikobewertungen:

- an einen **allgemeinen Risikorahmen** angekoppelt sind und
- im OT-Kontext auf einer **intern konsistenten Skala** erfolgen, die an „tolerable risk“ ausgerichtet ist.

Konsequenzen für ein Unternehmen mit CSMS, ISMS und IACS-SP. Für ein Unternehmen wie einen Automobilhersteller ergibt sich daraus:

- Im Fahrzeugbereich liefert ISO/SAE 21434 ein **eng geführtes, normativ durchdefiniertes Risikoschema** (Impact-Kategorien, diskrete Ratings, Attack-Feasibility, fixe Risikomatrix, Claims).
- Im ISMS-Bereich verlangt ISO/IEC 27005, dass dieses Schema in eine **organisationsweite Risikowelt** integriert wird, in der auch andere Domänen (IT, OT, Business-Risiken) mit ggf. völlig anderen Skalen arbeiten – und dass alle Skalen über eine **gemeinsame Referenz** vergleichbar gemacht werden.
- Im OT-Bereich verlangt IEC 62443-3-2, dass initiale und detaillierte IACS-Risikoanalysen auf genau diesem **Rahmen** (z. B. ISO/IEC 27005) beruhen und sich an einem **tolerable risk** orientieren, sodass OT-Risiken mit anderen Unternehmensrisiken vergleichbar sind.

Die drei Abbildungen machen damit zusammen **drei Seiten derselben Aufgabe** sichtbar:

1. **ISO/SAE 21434:** erzeugt **strukturierte, aber stark domänenspezifische** Risikoartefakte im Fahrzeugsystem (Risiko = f(Attack-Feasibility, Impact)) und exportiert Claims/Anforderungen an Backend und Produktion.
2. **ISO/IEC 27005:** verlangt, dass sämtliche domänenspezifischen Schemata – einschließlich TARA und IACS-Risikomodelle – auf eine **gemeinsame organisationale Risikoskala** abgebildet und über harmonisierte Kriterien geführt werden.
3. **IEC 62443-3-2:** verankert diese gemeinsame Skala im **IACS-Risikoprozess**, verknüpft sie mit einem **tolerable risk** und mit der OT-Architektur (Zonen, Security Levels).

Praktische Übersetzungsaufgaben. Die eigentliche Integrationsarbeit liegt damit nicht in den Normen, sondern **zwischen** ihnen:

- Attack-Feasibility-Stufen und TARA-Risikowerte aus ISO/SAE 21434 müssen in die **Consequence/Likelihood-Skala** des ISMS übertragen werden, die nach ISO/IEC 27005 organisationsweit gilt.

- Die **Impact-Ratings** (Safety, Financial, Operational, Privacy, 0–3) müssen in eine Referenzskala eingeordnet werden, die auch für IT- und OT-Risiken (z. B. Produktionsstillstand, Datenverlust) gilt.
- Die in IEC 62443-3-2 verwendeten **OT-Risk-Skalen** (z. B. qualitativ, quantitativ oder konsequenzbasiert) müssen so definiert werden, dass initiale und detaillierte IACS-Risikobewertungen mit der ISMS-Skala **kompatibel** sind und klar gegen das **tolerable risk** gespiegelt werden können.
- **Cybersecurity Claims** nach ISO/SAE 21434 müssen im ISMS als **Risk-Sharing-Entscheidungen** im Sinne von ISO/IEC 27005 dokumentiert und mit **Risk Ownern** versehen werden; im IACS-SP müssen sie sich in **konkreten Maßnahmen und Security Levels** niederschlagen.

Ohne ein bewusst gestaltetes Mapping zwischen

- den **normativ festgelegten Werten** von ISO/SAE 21434,
- den **offen gestaltbaren, aber harmonisierungspflichtigen Skalen** der ISO/IEC-27000-Familie und
- den **OT-spezifischen Risiko- und „tolerable risk“-Konzepten** der IEC-62443-3-2-Welt

bleibt genau die Schnittstelle unscharf, an der die drei Abbildungen ansetzen: CSMS, ISMS und IACS-SP liefern jeweils „korrekte“ Ergebnisse in ihrer Normlogik, sind aber **ohne Übersetzung nicht automatisch miteinander kompatibel**.

2.1.2.5 Zusammenführung und Handlungsempfehlungen

Die vorangegangenen Abschnitte haben gezeigt, dass ISO/SAE 21434, die ISO/IEC-27000-Familie und die IEC-62443-Reihe jeweils in ihrem Bereich gut ausgeformte, aber historisch getrennt gewachsene Rahmenwerke bilden. Die Management-Abbildungen machen sichtbar, dass CSMS, ISMS und IACS-Security-Programm strukturell miteinander verbunden sein sollen, während die Risikomanagement-Abbildungen illustrieren, wie domänenspezifische Risikoprozesse und -werte prinzipiell in Beziehung gesetzt werden können. In der Zusammenführung lassen sich drei zentrale Beobachtungen festhalten, aus denen sich konkrete Handlungsempfehlungen für ATLAS-L4 und die Automotive-Praxis ableiten lassen.

Erstens adressieren die drei Normfamilien komplementäre, aber strikt abgegrenzte Teile des automobilien Ökosystems. ISO/SAE 21434 fokussiert auf E/E-Systeme im Fahrzeug und das zugehörige CSMS, die ISO/IEC-27000-Familie auf sämtliche Informationswerte des Unternehmens und damit u. a. Backend- und Control-Center-Systeme, IEC-62443 auf IACS-/OT-Umgebungen der Produktion. Für ein ATLAS-L4-Szenario ergibt sich daraus eine natürliche Aufgabenteilung: Fahrzeugsysteme (ADS, Steuergeräte) werden über ein CSMS nach ISO/SAE 21434 gesteuert, Backend- und Unternehmens-IT über ein ISMS nach ISO/IEC 27001/27005, Produktions-OT über ein IACS-Security-Programm nach IEC 62443-2-1/-3-2. Diese Zuordnung sollte in einer Organisation explizit dokumentiert, organisatorisch verankert und gegenüber allen relevanten Bereichen kommuniziert werden, um Verantwortlichkeiten und Geltungsbereiche klar zu trennen.

Zweitens enthalten alle drei Normen zwar explizite oder implizite Vorgaben für bereichsübergreifende Managementsysteme, überlassen aber die konkrete Ausgestaltung der Schnittstellen den Organisationen. ISO/SAE 21434 fordert u. a. Kommunikationskanäle zu IT-Security, Safety und Privacy ([RQ-05-05]), verweist auf ein QMS mit Change-Management ([RQ-05-11]) und empfiehlt ein eigenes Produktions-CSMS ([RC-05-13]) sowie ein ISMS-konformes Work-Product-Handling ([RC-05-16]). ISO/IEC 27001/27003 verlangen, dass beim Aufbau eines ISMS der organisatorische

Kontext, bestehende Managementsysteme, Schnittstellen und ausgelagerte Funktionen berücksichtigt und gemeinsame Governance-Strukturen genutzt werden. IEC 62443-2-1 schreibt vor, dass ein IACS-Security-Programm mit einem vorhandenen ISMS zu koordinieren ist (ORG 1.1) und verweist in Annex A explizit auf ISO/IEC 27001 und NIST-Rahmenwerke. In Summe ergibt sich daraus, dass CSMS, ISMS und IACS-SP nicht als isolierte „Silos“, sondern als miteinander abgestimmte Systeme betrieben werden sollen. Praktisch bedeutet dies, dass ein übergreifendes Gremium oder Board benötigt wird, das die drei Managementsysteme steuert, Konflikte (z. B. divergierende Verfügbarkeitsziele von IT und OT) moderiert und die Umsetzung der Cross-Domain- und Cross-MS-Vorgaben aus den Normen überwacht.

Drittens unterscheiden sich die Normen deutlich in ihrer Ausgestaltung von Risikobegriffen, Bewertungsrastern und Terminologie. ISO/SAE 21434 legt Impact-Kategorien (Safety, Financial, Operational, Privacy), diskrete Impact-Ratings und Attack-Feasibility-Stufen sowie eine konkrete Risikomatrix vor und erzwingt bei Risikoteilung oder -beibehalt Cybersecurity Claims. ISO/IEC 27005 definiert Risiko strukturell als Funktion aus Consequence und Likelihood, überlässt die konkrete Wahl der Skalen aber der Organisation, verlangt jedoch deren Standardisierung über alle Bereiche hinweg und die Abbildung heterogener Konsequenzmaßstäbe auf eine gemeinsame Referenzskala (6.4.3.2). IEC 62443-3-2 wiederum koppelt die Risikobetrachtung an Zonierung, Security Levels und den organisationsspezifischen Begriff des „tolerable risk“, fordert aber nur, dass initiale und detaillierte Risikobewertung auf einem gemeinsamen Rahmen (z. B. ISO/IEC 27005) und einer konsistenten Risikoskala erfolgen. In der Praxis führt dies dazu, dass ein im Fahrzeugbereich hoch bewertetes Risiko ($\text{Attack-Feasibility} \times \text{Impact}$), ein „hohes Risiko“ im ISMS ($\text{Likelihood} \times \text{Consequence}$) und ein „tolerable risk überschritten“ im IACS-Kontext nicht ohne weiteres miteinander in Beziehung gesetzt werden können.

Aus diesen Beobachtungen lassen sich für ATLAS-L4 mehrere Handlungslinien ableiten. Auf organisatorischer Ebene sollten CSMS, ISMS und IACS-SP formal miteinander gekoppelt werden, indem die in ISO/SAE 21434, ISO/IEC-27001/-27003 und IEC 62443-2-1 geforderten oder empfohlenen Schnittstellen konkretisiert werden. Dazu gehört u. a., dass Annahmen, Anforderungen an die Betriebsumgebung und Cybersecurity Claims aus dem CSMS systematisch in ISMS- und IACS-Prozesse eingespeist werden und dass umgekehrt Änderungen in Backend und Produktion (z. B. neue OT-Anlagen, neue Dienste) als Trigger für Fahrzeug-TARAs und CSMS-Änderungsprozesse definiert werden. Eine übergeordnete Governance-Instanz sollte hierfür klare Rollen (inkl. Risk Owner je Domäne), Eskalationspfade und Review-Zyklen festlegen.

Auf inhaltlicher Ebene ist eine Harmonisierung von Terminologie und Risikokriterien unerlässlich. Abschnitt 2.1.2.2 zeigt, dass viele Begriffe fachlich korrespondieren, aber mit unterschiedlichen Namen und Nuancen benutzt werden. Organisationen sollten daher ein zentrales Cybersecurity-Glossar etablieren, das Kernbegriffe wie Risiko, Bedrohung, Schwachstelle, Schadensszenario/Consequence einheitlich definiert und normenspezifische Begriffe wie Attack Path, Risk Scenario, Threat Vector, Cybersecurity Claim, Security Level, Zone oder Risk Appetite gegeneinander abbildet. Darauf aufbauend sind nach ISO/IEC 27005 organisationsweite Risikokriterien zu definieren, in die die spezifischen Bewertungsrastern der einzelnen Normwelten übersetzbar sind. Konkret bedeutet dies u. a., dass die Attack-Feasibility-Stufen aus ISO/SAE 21434 in eine organisationale Likelihood-Skala eingeordnet werden, die Impact-Ratings (0–3) in eine referenzierte Consequence-Skala transformiert und OT-spezifische Security-Level-/Impact-Betrachtungen aus IEC 62443-3-2 auf dieselbe Skala abgebildet werden. Ergebnis sollte eine gemeinsame Risikomatrix sein, die den domänenspezifischen Matrizen zugrunde liegt, ohne diese zwingend zu ersetzen.

Ein weiterer zentraler Punkt betrifft den normübergreifenden Umgang mit geteilten und verbleibenden Risiken. ISO/SAE 21434 verlangt für Risikoteilung und -beibehalt explizite Cybersecurity Claims, ISO/IEC 27005 beschreibt Risk Sharing als generische Behandlungsoption, IEC 62443-3-2 arbeitet mit dem Begriff des „tolerable risk“. In einer integrierten Sicht sollten Claims aus der Fahrzeugdomäne als Trägerobjekte für Risk-Sharing-Entscheidungen verstanden und im ISMS konsequent mit Risk Ownern, Kontrollverantwortung und Monitoringpflichten hinterlegt werden. Im IACS-SP sind die Claims gegen OT-tolerable-risk-Schwellen zu spiegeln und gegebenenfalls in zusätzliche Controls oder Security-Level-Anforderungen zu übersetzen. Ergänzend empfiehlt sich eine organisationsweite Policy, die festlegt, welche Klassen von Risiken in welcher Domäne verbleiben dürfen, welche zwingend zu mitigieren oder zu teilen sind und wie Abweichungen (z. B. aus Safety- oder Business-Sicht nicht akzeptable OT-Risiken) eskaliert werden.

Schließlich ist die praktische Umsetzung eines bereichsübergreifenden Risikomanagements werkzeug- und prozessseitig zu unterstützen. Aus der Perspektive von ISO/IEC 27005 (6.4.3/6.5) bietet sich entweder ein zentrales Risikoregister oder ein föderiertes Metamodell an, in dem CSMS-TARAs, ISMS-Risikoanalysen und IACS-Risikoanalysen mit einem gemeinsamen Satz von Attributen (Assets, Szenariotypen, Skalenfelder, Status) geführt werden. Wichtig ist, dass jede in ISO/SAE 21434 dokumentierte Annahme, jede Anforderung an die Betriebsumgebung und jeder Claim sich an einer Stelle im ISMS/IACS-SP wiederfindet – und umgekehrt. Ergänzend sollten minimal gemeinsame Datenmodelle und Schnittstellen zwischen den eingesetzten Tools definiert werden, sodass Risiko-Informationen automatisiert übertragen und in den jeweils anderen Domänen verständlich ausgewertet werden können. Eine explizite „Übersetzerrolle“ oder ein kleines, bereichsübergreifendes Team, das die Mappings zwischen Begriffen, Skalen und Tools pflegt und Anwender schult, kann die Nachhaltigkeit dieser Integration sichern.

2.1.2.6 Fazit

Der übergreifende Vergleich von ISO/SAE 21434, der ISO/IEC-27000-Familie und der IEC-62443-Reihe zeigt deutlich, dass die drei Normwelten inhaltlich komplementär sind, aber an entscheidenden Stellen nicht nahtlos ineinandergreifen. ISO/SAE 21434 verankert Security-by-Design und ein TARA-basiertes Risikomanagement in der Fahrzeugdomäne, zwingt zur Beschreibung externer Abhängigkeiten und zur Formulierung von Anforderungen und Claims gegenüber Backend und Produktion. Die ISO/IEC-27000-Familie stellt mit ISMS und ISO/IEC 27005 einen universellen Rahmen bereit, in dem Risikokriterien, Methoden und Akzeptanzschwellen organisationsweit definiert und harmonisiert werden sollen. IEC-62443 schließlich bringt OT-spezifische Konzepte wie Zonen, Conduits, Security Levels und das „tolerable risk“ ein und schreibt die Koordination des IACS-Security-Programms mit einem ISMS ausdrücklich vor.

Gleichzeitig wird deutlich, dass die Normen auf unterschiedlichen Begriffswelten und Risikomodellen operieren. Begriffe wie Attack Path, Risk Scenario und Threat Vector bezeichnen inhaltlich sehr ähnliche Sachverhalte, sind aber normativ jeweils anders definiert und in unterschiedliche methodische Kontexte eingebettet. Der Risikobegriff ist überall eine Kombination aus „Wahrscheinlichkeit/Aufwand“ und „Schadensausmaß“, wird aber einmal als Attack-Feasibility×Impact, einmal als Likelihood×Consequence und einmal eingebettet in Security Levels und tolerable risk operationalisiert. Die Normen fordern die Vernetzung von Managementsystemen und die Harmonisierung von Risikokriterien, liefern aber keine detaillierte Anleitung, wie die heterogenen Begriffe, Skalen und Prozesse in einem konkreten Unternehmen zusammenzuführen sind.

Für ATLAS-L4 lässt sich daraus ableiten, dass kein Standard für sich allein ausreicht, um die Cybersicherheit des Gesamtsystems Lkw–Backend–Produktion abzubilden. Erst in Kombination bilden ISO/SAE 21434, ISO/IEC-27000 und IEC-62443 einen tragfähigen Rahmen, innerhalb dessen CSMS, ISMS und IACS-Security-Programm sinnvoll aufeinander abgestimmt werden können. Die Normen definieren dabei, welche Bausteine vorhanden sein müssen, welche Schnittstellen existieren sollen und wie ein Risikomanagement strukturiert sein sollte; sie nehmen den Organisationen jedoch nicht die notwendige „Übersetzungsarbeit“ ab. Diese Arbeit umfasst die Vereinheitlichung von Begriffen, die Abbildung unterschiedlicher Bewertungsrastern auf eine gemeinsame Risikoskala, die Definition von Prozessen für geteilte und verbleibende Risiken und die Integration der jeweiligen Tools und Datenmodelle.

Die in Abschnitt 2.1.12 dargestellten Interviewergebnisse aus OEM-Praxisprojekten bestätigen, dass genau an diesen Schnittstellen heute Reibungsverluste und Missverständnisse auftreten: Unterschiedliche Terminologien, inkompatible Skalen und isolierte Werkzeuge führen dazu, dass Risiken zwar domänenspezifisch bearbeitet, aber nicht übergreifend gesteuert werden. Der hier vorgelegte Normenvergleich macht sichtbar, wo diese Divergenzen im Text der Standards verankert sind, und bietet eine Grundlage, um sie systematisch anzugehen, statt sie im bereichsübergreifenden Risikomanagement implizit und ad-hoc zu behandeln.

Aus normativer Sicht sind Investitionen in Governance, Harmonisierung und Tool-Integration damit keine „Option“, sondern eine logische Konsequenz aus der gleichzeitigen Anwendung von ISO/SAE 21434, ISO/IEC-27000 und IEC-62443. Die Herausforderung für OEMs und Zulieferer besteht weniger darin, zusätzliche Dokumente zu erzeugen, als vielmehr darin, die von den Normen geforderte Vernetzung der Managementsysteme mit Leben zu füllen und die Übersetzungsleistung zwischen den Domänen explizit zu organisieren.

2.1.3 Vergleichende Analyse der regulatorischen Anforderungen an die Cybersicherheit im Automobilbereich

2.1.3.1 Kurzfassung

Der Automobilsektor befindet sich in einem rasanten digitalen Wandel, wodurch moderne Fahrzeuge zunehmend anfällig für Cybersicherheitsbedrohungen werden. Als Reaktion darauf haben verschiedene Regionen regulatorische Rahmenwerke geschaffen, um die Cyber-Resilienz zu verbessern und Sicherheitspraktiken zu standardisieren. In diesem Beitrag werden drei wichtige Ansätze verglichen: die rechtsverbindlichen Vorschriften der Wirtschaftskommission der Vereinten Nationen für Europa (UNECE), die chinesische Norm GB 44495-2024 und die freiwilligen Richtlinien der US-amerikanischen National Highway Traffic Safety Administration (NHTSA). Jedes Regelwerk wird anhand von sechs Kriterien analysiert, darunter Geltungsbereich, Zertifizierungsanforderungen, Cybersicherheitsmanagementstrukturen, Software-Update-Mechanismen, Risikominderungsstrategien und Überwachungspflichten. Einerseits zeigt die Studie wesentliche Unterschiede bei den Durchsetzungsmechanismen, der technischen Spezifität und den Zertifizierungsprozessen auf. Andererseits identifiziert sie gemeinsame Kernprinzipien wie risikobasiertes Lebenszyklusmanagement und sichere Update-Praktiken. Darüber hinaus identifiziert die Studie wichtige regulatorische Lücken, wie z. B. methodische Unklarheiten, inkonsistente Zertifizierungsansätze sowie Herausforderungen bei der Angleichung nationaler Praktiken, und bewertet deren operative Auswirkungen. Sie hebt auch hervor, wie benachbarte Vorschriften, darunter Datenschutzgesetze und horizontale digitale Gesetzgebung, zunehmend Einfluss auf die

Cybersicherheit von Fahrzeugen nehmen. Die Studie schließt mit gezielten Empfehlungen für verbesserte operative Leitlinien zur Stärkung der langfristigen Widerstandsfähigkeit im Automobilsektor.

2.1.3.2 Globale Regulierungsrahmen für die Cybersicherheit von Fahrzeugen

Dieser Abschnitt bietet einen strukturierten Überblick über ausgewählte internationale Ansätze zur Regulierung und Standardisierung der Cybersicherheit von Fahrzeugen. Insbesondere werden die rechtsverbindlichen Rahmenwerke der Europäischen Union (UNECE-Regelung Nr. 155 (R155) und UN-Regelung Nr. 156 (R156)) und Chinas (GB 44495-2024) sowie die nicht verbindliche Richtlinie der Vereinigten Staaten (NHTSA Best Practices) analysiert. Um Konsistenz und Vergleichbarkeit zu gewährleisten, wird jedes Regulierungsdokument anhand der folgenden sechs Aspekte aus Tabelle 2 geprüft:

Tabelle 2: Übersicht über die Aspekte des Regulierungsvergleichs

Vergleichskategorie	Schwerpunkt des Vergleichs
Anwendungsbereich	Rechtsverbindlichkeit und Zielfahrzeugkategorien
Typgenehmigung und Zertifizierung	Vorhandensein formeller Genehmigungsverfahren und Zertifizierungsanforderungen (z. B. CSMS, SUMS)
Strukturen für das Cybersicherheitsmanagement	Verpflichtungen hinsichtlich organisatorischer Strukturen für das Management von Cybersicherheitsrisiken während des gesamten Lebenszyklus eines Fahrzeugs
Software Update-Management	Anforderungen an sichere Software-Updates, Versionskontrolle, Rollback-Mechanismen und OTA-Prozesse
Umfang der Risikominderung	Explizite Verknüpfung zwischen Bedrohungstypen und erforderlichen Gegenmaßnahmen oder Schutzmaßnahmen
Überwachung und laufende Verpflichtungen	Regulatorische Erwartungen hinsichtlich kontinuierlicher Risikoüberwachung, Meldung von Vorfällen und Aktualisierung der Dokumentation

Europäische Union: UNECE R155, UNECE R156

Die Europäische Union regelt die Cybersicherheit von Fahrzeugen durch rechtsverbindliche Vorschriften, die von der UNECE verabschiedet wurden. Die wichtigsten Instrumente sind die UN-Regelung Nr. 155 (R155) und die UN-Regelung Nr. 156 (R156), die für die Typgenehmigung von Fahrzeugen in allen EU-Mitgliedstaaten verbindlich sind. Diese Vorschriften legen Anforderungen an das Cybersicherheitsmanagement (CSMS) und das Software-Update-Management (SUMS) während des gesamten Lebenszyklus eines Fahrzeugs fest. Beide Vorschriften traten am 1. Juli 2022 für die Typgenehmigung neuer Fahrzeuge in Kraft und sind seit dem 1. Juli 2024 für alle Neuzulassungen verbindlich.

Geltungsbereich

Die UN-Regelung Nr. 155 gilt für Fahrzeuge der Klassen M und N sowie der Klasse O, wenn Anhänger mit mindestens einem Steuergerät ausgestattet sind. Die Klassen L6 und L7 sind ebenfalls eingeschlossen, sofern automatisierte Fahrfunktionen der SAE-Stufe 3 oder höher vorhanden sind. Die Regelung Nr. 156, die sich mit Software-Updates befasst, gilt für Fahrzeuge der Klassen M, N, O, R, S und T. Eine Übersicht über diese Fahrzeugklassen ist in Tabelle 3 enthalten.

Tabelle 3: Klassifizierung von Fahrzeugtypen gemäß EU-Kategorien [149]

Kategorie	Kurzbeschreibung
L6	Leichtes Vierradfahrzeug (max. 350 kg, max. 45 km/h, max. 50 cm ³ Hubraum oder 4 kW Leistung)
L7	Schweres Vierradfahrzeug (max. 400 kg / 550 kg für Güter, max. 15 kW Leistung)
M	Kraftfahrzeuge mit mindestens 4 Rädern, die zur Personenbeförderung verwendet werden
N	Kraftfahrzeuge mit mindestens 4 Rädern, die für den Gütertransport verwendet werden
O	Anhänger (nicht motorisiert, zum Transport von Lasten bestimmt)
R	Landwirtschaftlicher Anhänger (erfordert Zugfahrzeug, Massenverhältnis $\geq 3,0$)
S	Austauschbare gezogene land- und forstwirtschaftliche Geräte (Massenverhältnis $< 3,0$)
T	Motorisiertes land- und forstwirtschaftliches Fahrzeug (mindestens 2 Achsen, ≥ 6 km/h, für Zug- und Arbeitsfunktionen ausgelegt)

Typgenehmigungs- und Zertifizierungsverfahren

Hersteller müssen für jeden Fahrzeugtyp einen Antrag auf Typgenehmigung stellen. Für R155 ist ein gültiges CSMS-Zertifikat erforderlich, für R156 muss ein SUMS-Zertifikat (Software Update Management System) vorgelegt werden. Die Genehmigungsbehörden prüfen die eingereichten Unterlagen und führen Tests durch. Bei unzureichender Risikobewertung Management oder fehlende technische Maßnahmen festgestellt werden, wird die Zulassung verweigert. Beide Zertifikate sind maximal drei Jahre gültig, können jedoch entzogen werden, wenn die Anforderungen nicht mehr erfüllt sind. Nach der Zulassung müssen Fahrzeuge ein internationales Typgenehmigungszeichen tragen.

Cybersicherheits-Managementstrukturen

Um Cybersicherheit zu gewährleisten, müssen Organisationen ein CSMS gemäß UN R155 einrichten und aufrechterhalten. Nach der Definition von Liedtke (2024) ist ein CSMS eine Reihe miteinander verbundener Richtlinien, Verfahren und technischer Mechanismen, die dazu dienen, Cybersicherheitsrisiken in allen Phasen des Produktlebenszyklus zu verwalten. Ein wesentliches Merkmal eines wirksamen CSMS ist seine Rückverfolgbarkeit und Überprüfbarkeit, die es Regulierungsbehörden oder Dritten ermöglicht, die Einhaltung der Vorschriften zu überprüfen. Das System umfasst in der Regel Workflows zur Risikobewertung, Prozesse zum Umgang mit Schwachstellen, Strategien zur Reaktion auf Vorfälle und Überwachungsmechanismen für Lieferanten und Komponenten von Dritten. Verifizierungskriterien können systematisch auf organisatorische Prozesse abgebildet und anschließend in modulare Prozessmodelle gruppiert werden [150]. Diese Abstraktion ist in der Regulierungspraxis besonders wichtig, da sie eine konsistente Umsetzung der Cybersicherheitsanforderungen über verschiedene Betriebsebenen hinweg ermöglicht.

Sichere Software-Update-Prozesse

Um die Softwareintegrität über einen längeren Zeitraum aufrechtzuerhalten, wird von Unternehmen erwartet, dass sie ein SUMS implementieren, das sichere, rückverfolgbare und überprüfbare Software-Updates während des gesamten Fahrzeuglebenszyklus gewährleistet. Dazu gehören die Verwaltung von Versionen, die Überprüfung der Integrität und die Aktualisierungshistorie.

Kritische Updates müssen während der Fahrt nachweislich sicher sein oder erfordern stationäre Bedingungen und Benutzerinteraktion. Ein Schlüsselement ist die RX-Software-Identifikationsnummer (RXSWIN), die bestimmte Softwareversionen mit dem entsprechenden zugelassenen Fahrzeugtyp verknüpft. Sie muss lesbar und vor Manipulationen geschützt sein. Die Vorschriften verlangen außerdem, dass Systeme eine Rollback-Funktionalität oder einen sicheren Fallback-Zustand für den Fall eines fehlgeschlagenen Updates unterstützen.

Umfang der Risikominderung

Anhang 5 unterteilt Bedrohungen in mehrere Gruppen: Backend-Angriffe, Kommunikationskanäle, Aktualisierungsverfahren, menschliches Versagen, externe Schnittstellen und Software-/Hardware-Schwachstellen. Jede Bedrohung (z. B. Man-in-the-Middle-Angriffe, Replay-Angriffe, CAN-Bus-Flooding) wird einer oder mehreren Abhilfemaßnahmen zugeordnet, wie z. B. Nachrichtenauthentifizierung (M10), Zugriffskontrollen (M7), Schutz kryptografischer Schlüssel (M11) oder Erkennungsmechanismen (M13). Diese strukturierte Zuordnung unterstützt die Zulassungsbehörden bei der Überprüfung der Konformität und verpflichtet die Hersteller zur Umsetzung umfassender Sicherheitsmaßnahmen.

Laufende Verpflichtungen und Überwachung

Hersteller müssen regelmäßig Berichte über die Wirksamkeit ihrer umgesetzten Maßnahmen vorlegen und alle identifizierten Sicherheitsprobleme beheben [4]. R156 verlangt, dass alle Over-the-Air (OTA)-Updates dokumentiert werden, einschließlich ihres Zwecks, der betroffenen Systeme, der Dauer, der Voraussetzungen und der Benachrichtigungen an die Benutzer. Ein OTA-Update ist die drahtlose Übertragung von Software, Firmware oder Konfigurationsdaten an Geräte wie Fahrzeuge, wodurch Fernwartung und Funktionsupgrades ohne physische Verbindung möglich sind [151]. Die Nichteinhaltung kann zum Entzug des CSMS- oder SUMS-Zertifikats führen, was wiederum den Widerruf der Typgenehmigung zur Folge haben kann.

China: GB 44495-2024

China regelt die Cybersicherheit von Fahrzeugen durch eine rechtsverbindliche nationale Norm, die von der chinesischen Normungsbehörde herausgegeben wurde. Das wichtigste Dokument ist GB 44495-2024: Technische Anforderungen an die Cybersicherheit von Fahrzeugen, das verbindliche Cybersicherheitsanforderungen für Straßenfahrzeuge festlegt. Diese Norm enthält technische Spezifikationen für die Erkennung von Bedrohungen, die Risikobewertung, Schutzmaßnahmen und das Lebenszyklusmanagement, um die Widerstandsfähigkeit vernetzter Fahrzeuge gegen Cyberbedrohungen zu gewährleisten. GB 44495-2024 trat im August 2024 in Kraft.

Geltungsbereich

Die nationale Verordnung in China gilt für Fahrzeuge der Klassen M und N sowie für Fahrzeuge der Klasse O, die mit mindestens einer ECU ausgestattet sind. Eine Übersicht über diese Fahrzeugklassen ist in Tabelle 3.

Typgenehmigungs- und Zertifizierungsverfahren

Die Typgenehmigung von Fahrzeugen erfordert sowohl dokumentarische Nachweise als auch eine physische Überprüfung. Die Hersteller sind verpflichtet, detaillierte technische Unterlagen vorzulegen, die den Cybersicherheitsstatus eines Fahrzeugs während der Entwicklung und Produktion beschreiben. Diese Unterlagen müssen durch eine formelle Selbsterklärung die

Konsistenz und Rückverfolgbarkeit nachweisen. Darüber hinaus führen die Aufsichtsbehörden Vor-Ort-Inspektionen durch. Es wird eine breite Palette von Systemtests durchgeführt, darunter die Überprüfung der Kommunikationsintegrität, die Bewertung externer Schnittstellen wie USB- und OBD-II-Anschlüsse, die Simulation physischer Manipulationsversuche, OTA-Update-Tests und Bewertungen im Zusammenhang mit der Sicherheit der Vehicle-to-Everything (V2X)-Kommunikation.

Cybersicherheits-Managementstrukturen

Die Verordnung schreibt die Implementierung eines risikobasierten Cybersicherheits-Managementsystems vor, das für alle Phasen des Fahrzeuglebenszyklus gilt. Von den OEMs wird erwartet, dass sie interne Prozesse zur Identifizierung, Klassifizierung und Minderung von Cybersicherheitsrisiken einrichten. Dazu gehören formalisierte Verfahren für das Schwachstellenmanagement, wie beispielsweise Datenerfassung, Bedrohungsanalyse, Vorfallsbearbeitung und koordinierte Offenlegungs- und Freigabeprozesse. Die Überwachung der Cybersicherheit muss spätestens in der Fahrzeugzulassungsphase beginnen und Mechanismen zur Erkennung von Bedrohungen durch Protokollanalyse und Datenüberwachung umfassen. Darüber hinaus verpflichtet die Verordnung die Hersteller, Cybersicherheitsabhängigkeiten entlang der gesamten Lieferkette, einschließlich Subunternehmern und verbundenen Organisationen, zu verwalten. In regelmäßigen Abständen muss überprüft werden, ob die umgesetzten Maßnahmen weiterhin wirksam sind.

Sichere Software-Update-Prozesse

Strenge Anforderungen gelten auch für die Verwaltung von Software-Updates. Die Hersteller müssen den Schutz kritischer Softwarekomponenten wie Bootloader und System-Firmware gewährleisten. Software-Updates, insbesondere OTAs, müssen authentifiziert und nachweislich frei von ungelösten Schwachstellen sein, die in öffentlichen Datenbanken aufgeführt sind. Die Authentizität und Integrität von Update-Paketen muss validiert werden, und alle Update-Aktivitäten müssen auf nachvollziehbare Weise protokolliert werden. Darüber hinaus müssen Update-Mechanismen Rollback- und Fallback-Funktionen bieten, um eine Beschädigung der Software zu verhindern und die Funktionsfähigkeit des Fahrzeugs im Falle eines Update-Fehlers sicherzustellen.

Umfang der Risikominderung

Die Verordnung legt eine Reihe weitreichender Cybersicherheitsanforderungen fest, um die Widerstandsfähigkeit von Fahrzeugen zu verbessern. Zu den Kernmaßnahmen gehören obligatorische Standard-Sicherheitseinstellungen, die Durchsetzung von Zugriffskontrollen für alle internen und externen Schnittstellen sowie die Deaktivierung nicht genutzter Netzwerkports. Eine Netzwerksegmentierung ist erforderlich, um die Ausbreitung von Bedrohungen innerhalb der Fahrzeugarchitektur zu begrenzen. Kryptografische Schutzmaßnahmen sind ein zentraler Bestandteil der Verordnung: Sowohl symmetrische als auch asymmetrische Schlüssel müssen sicher gespeichert werden, und kryptografische Algorithmen müssen international oder national anerkannten Standards entsprechen. Fahrzeuge müssen außerdem in der Lage sein, Cyberangriffe in Echtzeit zu erkennen, sichere forensische Protokolle zu führen und die Authentifizierung für die Fahrzeug-Cloud- und V2X-Kommunikation durchzusetzen. Die Verordnung verlangt außerdem, dass öffentlich bekannt gewordene Schwachstellen innerhalb von sechs Monaten behoben werden müssen.

Laufende Verpflichtungen und Überwachung

Hersteller müssen kontinuierliche Überwachungsroutrinen implementieren und zeitnahe Reaktionen auf Cybersicherheitsvorfälle gewährleisten. Diese Verpflichtungen gehen über die Entwicklung hinaus und umfassen regelmäßige Audits und Tests sowohl unter Laborbedingungen als auch in realen Szenarien. Zu den regulatorischen Schwerpunkten gehören die Widerstandsfähigkeit externer Schnittstellen, die Zuverlässigkeit sicherer Protokollierungsfunktionen und die Stabilität von OTA-Updates unter widrigen Bedingungen. Darüber hinaus müssen Hersteller kritische Datenelemente wie kryptografische Schlüssel und Fahrzeugkennungen (z. B. Fahrzeugidentifikationsnummer (VIN)) schützen und Mechanismen für die autorisierte Löschung personenbezogener Daten bereitstellen. Ein wesentlicher Aspekt der Verordnung ist das Verbot direkter grenzüberschreitender Datenübertragungen, wodurch die Einhaltung nationaler Datenschutzgesetze verstärkt wird.

USA: NHTSA-Richtlinien

Die Vereinigten Staaten schreiben keine verbindlichen Cybersicherheitsvorschriften für Fahrzeuge vor. Stattdessen gibt die National Highway Traffic Safety Administration (NHTSA) unverbindliche Leitlinien als „Cybersecurity Best Practices for the Safety of Modern Vehicles“ (Bewährte Verfahren für die Cybersicherheit moderner Fahrzeuge) heraus. Dieses Dokument enthält freiwillige Empfehlungen, die sich an internationalen Normen wie ISO/SAE 21434 und dem NIST Cybersecurity Framework orientieren. Die neueste Version wurde im September 2022 veröffentlicht.

Geltungsbereich

Die Cybersecurity Best Practices der NHTSA gelten für alle Personen und Organisationen, die an der Entwicklung, Herstellung und Wartung von elektronischen Fahrzeugsystemen und -software beteiligt sind, einschließlich Aftermarket- und Benutzergeräten.

Typgenehmigungs- und Zertifizierungsverfahren

In den Vereinigten Staaten gibt es kein obligatorisches Typgenehmigungs- oder Zertifizierungssystem für die Cybersicherheit von Kraftfahrzeugen. Stattdessen gibt die NHTSA unverbindliche Empfehlungen heraus, deren interne Umsetzung den Herstellern empfohlen wird. Dazu gehören interne Richtlinien, dokumentierte Risikobewertungen und die Umsetzung mehrschichtiger Cybersicherheitsstrategien.

Cybersicherheits-Managementstrukturen

Obwohl die USA kein formelles CSMS vorschreiben, fördert die NHTSA vergleichbare interne Prozesse. Dazu gehören die Rechenschaftspflicht für Cybersicherheit auf Führungsebene, risikobasiertes Engineering, Schwachstellentests und die Kommunikation innerhalb der Lieferkette.

Sichere Software-Update-Prozesse

In den USA gibt es kein formelles SUMS. Dennoch empfiehlt die NHTSA, alle Software-Updates, insbesondere OTAs, durch Authentifizierung, Rollback-Prävention und robuste Dokumentation zu sichern.

Umfang der Risikominderung

Die NHTSA legt Wert auf mehrschichtige Schutzmaßnahmen für Fahrzeugnetzwerke. Die technischen Empfehlungen umfassen sichere Kommunikationsprotokolle, die Isolierung elektronischer Steuergeräte (ECU), den Schutz von Zugangsdaten, Penetrationstests und die Protokollierung. Auch Risiken durch Sensor-Spoofing und Geräte von Drittanbietern werden behandelt.

Laufende Verpflichtungen und Überwachung

Die Hersteller werden aufgefordert, Notfallpläne zu implementieren, Cybersicherheitsaudits durchzuführen und alle Schwachstellen und Abhilfemaßnahmen zu dokumentieren. Regelmäßige interne Überprüfungen und Transparenz sind dabei wichtige Komponenten.

Weitere relevante Aspekte

Die NHTSA legt großen Wert auf den Informationsaustausch und fördert die Zusammenarbeit mit dem Automotive Information Sharing and Analysis Center (Auto-ISAC), um den Austausch von Cybersicherheitsinformationen in der gesamten Branche zu fördern. Das Auto-ISAC dient als zentrale Plattform für die Automobilindustrie, um gemeinsam Informationen über neue Cybersicherheitsbedrohungen zu analysieren und auszutauschen, mit dem Ziel, die Cybersicherheit vernetzter Fahrzeuge in der gesamten Branche zu stärken [152]. Es wird auch die Bedeutung klarer Verfahren zur Offenlegung von Schwachstellen hervorgehoben, die externen Forschern definierte Kanäle für die Meldung von Sicherheitsproblemen bieten. Darüber hinaus unterstützt die NHTSA die Zusammenarbeit mit Universitäten, um die Ausbildung und die Entwicklung von Fachkräften im Bereich der Cybersicherheit im Automobilbereich zu fördern. Schließlich betont der Leitfaden die Bedeutung eines Gleichgewichts zwischen starken Cybersicherheitsmaßnahmen und Wartungsfreundlichkeit, um sicherzustellen, dass die Wartung durch Dritte ohne Beeinträchtigung der Sicherheit möglich bleibt.

Tabelle 4 bietet einen Überblick über die verschiedenen Rahmenwerke.

Tabelle 4: Vergleich der Regulierungsrahmen für die Cybersicherheit von Fahrzeugen (EU, China, USA)

Aspekt	Europäische Union (UNECE R155/R156)	China (GB 44495-2024)	USA (NHTSA Best Practices)
Anwendungsbereich	Rechtsverbindlich; Fahrzeugklassen M, N, O, L6/L7, R, S, T	Rechtsverbindlich; Fahrzeugklassen M, N, O	Freiwillig, unverbindlich; alle Akteure im Bereich Fahrzeugelektronik und -software
Typgenehmigungs- und Zertifizierungsverfahren	Erfordert CSMS- und SUMS-Zertifikate; 3 Jahre Gültigkeit; strenge Zulassungsverfahren	Erfordert Dokumentation, Selbsterklärung, Vor-Ort-Inspektionen, umfangreiche Tests	Keine formelle Zertifizierung; interne Einhaltung wird empfohlen
Cybersicherheits-Managementstrukturen	Obligatorisches CSMS, gesamter Lebenszyklus; umfasst Risikoanalyse, Reaktion auf Vorfälle, forensische Tools	Obligatorisches CSMS; umfasst Schwachstellenmanagement, Lieferkettenrisiken, Echtzeit-Erkennung	Empfohlene interne Prozesse zur Gewährleistung der Cybersicherheit; Verantwortlichkeit der Führungskräfte

Sichere Software-Update-Prozesse	Obligatorisches SUMS; umfasst RXSWIN, Rollback/Fallback, OTA-Update-Schutzmaßnahmen	Sicherer Start, authentifiziertes OTA, Rollback/Fallback, Schwachstellenprüfungen	Best-Practice-OTA-Empfehlungen; Rollback und Integrität empfohlen
Umfang der Risikominderung	Anhang 5 ordnet zentrale Bedrohungen (z. B. Spoofing, Injection) den entsprechenden Abwehrmaßnahmen (z. B. M1–M13) zu.	Deckt ein breites Spektrum an Cybersicherheitsmaßnahmen ab, darunter kryptografische Schutzmaßnahmen, Netzwerksegmentierung, Zugriffskontrolle und Erkennungsfunktionen.	Deckt wichtige technische Bereiche wie Netzwerksicherheit, Zugriffskontrolle, Protokollierung und Schutz vor Risiken durch Dritte ab.
Laufende Verpflichtungen und Überwachung	Obligatorische Überwachung, Wirksamkeitsberichte, dokumentierte OTA-Aktualisierungen	Kontinuierliche Überwachung, Datenschutz, Speicherung von Daten im Inland	Empfohlene Reaktion auf Vorfälle, Audits, Dokumentation von Schwachstellen

2.1.3.3 Vergleich der Regulierungsansätze

Aufbauend auf der Analyse der einzelnen Rahmenwerke im vorigen Abschnitt vergleicht dieses Kapitel die Regulierungsansätze der Europäischen Union, Chinas und der Vereinigten Staaten in Bezug auf die Cybersicherheit von Fahrzeugen. Der Vergleich identifiziert wichtige Gemeinsamkeiten und Unterschiede in der Regulierungsstruktur, den Durchsetzungsmechanismen und den technischen Schwerpunktbereichen. Darüber hinaus werden die Auswirkungen auf Fahrzeughersteller und Zulieferer untersucht.

Gemeinsamkeiten

Rahmenwerke für die Cybersicherheit von Fahrzeugen in der Europäischen Union (UNECE R155 und R156), China (GB 44495-2024) und den Vereinigten Staaten (NHTSA Cybersecurity Best Practices) weisen eine Konvergenz ihrer grundlegenden Ziele auf. Alle drei Ansätze betonen eine risikobasierte Methodik, die sich mit der Cybersicherheit über den gesamten Lebenszyklus eines Fahrzeugs befasst. Dazu gehören Entwicklung, Produktion und Aktivitäten nach der Markteinführung. Ein gemeinsames Element ist die Förderung eines Managementsystems. Europa und China schreiben die Implementierung eines CSMS vor, während die Vereinigten Staaten interne Richtlinien empfehlen, die einer solchen Struktur ähneln. Diese Systeme sollen Risikobewertungen, Schwachstellenmanagement und kontinuierliche Überwachung umfassen. Alle drei Rahmenwerke erkennen die Bedeutung von Software-Updates an und schreiben Mechanismen zur Gewährleistung ihrer Sicherheit vor oder empfehlen diese. Das SUMS der EU, die expliziten technischen Anforderungen Chinas und die Empfehlungen der USA betonen alle die Notwendigkeit von Authentifizierungs-, Integritätsprüfungs- und Rollback-Mechanismen, insbesondere für OTA-Updates. Die Sicherheit der Lieferkette ist ein weiterer gemeinsamer Schwerpunkt. Die Vorschriften der UNECE und die Standards Chinas verlangen von den OEMs, dass sie die Cybersicherheitsabhängigkeiten zwischen Lieferanten und Subunternehmern verwalten. In ähnlicher Weise fördert die NHTSA die Teilnahme an Kooperationsplattformen wie Auto-ISAC, um den Informationsaustausch und das Bewusstsein für Bedrohungen zu verbessern. Darüber hinaus erkennen alle drei Regionen die Notwendigkeit der Erkennung und Reaktion auf Vorfälle an. Protokollierung, Intrusion Detection, forensische Fähigkeiten und Analyse nach Vorfällen werden entweder als regulatorische Anforderungen (EU, China) oder als Empfehlungen (USA) behandelt.

Unterschiede und Unstimmigkeiten

Der auffälligste Unterschied liegt in der Verbindlichkeit der Vorschriften. Während R155 und R156 sowie die chinesische Norm GB 44495-2024 rechtlich durchsetzbar sind und direkt mit der Typgenehmigung verbunden sind, sind die NHTSA-Richtlinien unverbindlich und dienen als freiwillige Empfehlungen. Dies führt zu unterschiedlichen Umsetzungsgraden in der Branche. Auch die Zertifizierungsverfahren unterscheiden sich. Die EU verlangt gültige CSMS- und SUMS-Zertifikate als Voraussetzung für die Typgenehmigung, und China schreibt ein vergleichbares Verfahren mit Dokumentation und umfangreichen Tests vor. Im Gegensatz dazu gibt es in den USA kein offizielles Zertifizierungssystem für Cybersicherheit. Die Einhaltung der Vorschriften basiert auf Selbstregulierung und interner Dokumentation. Der Anwendungsbereich variiert geringfügig. Sowohl Europa als auch China definieren bestimmte Fahrzeugkategorien, für die Cybersicherheitsmaßnahmen gelten, wobei Fahrzeuge mit ECUs und automatisierten Fahrfunktionen im Fokus stehen. Die Richtlinien der NHTSA gelten jedoch allgemeiner für alle Akteure, die an der Elektronik und Software des Fahrzeugs beteiligt sind, einschließlich Aftermarket-Produkten. In Bezug auf technische Details enthalten die R155 und die chinesische Verordnung Listen mit Bedrohungstypen und verknüpfen diese direkt mit Strategien zu deren Eindämmung. Anhang 5 der R155 enthält die Tabellen A1 und B1-B8, in denen Bedrohungen und entsprechende Schutzmaßnahmen (z. B. M1 bis M13) aufgeführt sind. China verbindet ebenfalls Bedrohungsarten mit Anforderungen und legt Fristen für die Behebung bekannter Schwachstellen fest. Das US-amerikanische Rahmenwerk bietet umfassende thematische Empfehlungen, verfügt jedoch nicht über entsprechende Zuordnungen. Im Gegensatz zu R155, das sich in erster Linie auf formelle Zertifizierungsverfahren stützt, legt Chinas GB 44495-2024 einen stärkeren Schwerpunkt auf intensive praktische Tests. Software-Update-Verfahren verdeutlichen die Unterschiede zusätzlich. Die EU schreibt die Verwendung von RXSWIN vor und erlegt strenge Dokumentations- und Update-Bedingungen auf. China schreibt sichere Boot-Mechanismen und nachvollziehbare Protokollierung vor. Der Ansatz der USA ist flexibler und erlaubt OEMs, ihre eigenen sicheren Update-Systeme zu entwickeln, solange die Dokumentation und Risikominderung gewährleistet sind.

Auswirkungen auf OEMs und Zulieferer

OEMs in Europa und China sehen sich hohen regulatorischen Anforderungen gegenüber. In Europa müssen Hersteller zertifizierte CSMS- und SUMS-Systeme einrichten und unterhalten, detaillierte technische Unterlagen einreichen und Risikominderungsmaßnahmen für die Typgenehmigung von Fahrzeugen nachweisen. China stellt ähnliche Anforderungen, darunter Vor-Ort-Inspektionen und umfassende Tests. Diese Prozesse erfordern die Koordination zwischen verschiedenen Abteilungen und erhöhte Investitionen in Ressourcen zur Einhaltung der Vorschriften. Von Zulieferern, die ECUs, Cloud-Dienste oder Softwarekomponenten anbieten, wird erwartet, dass sie die gleichen regulatorischen Anforderungen erfüllen. Dies kann vertragliche Audits und unabhängige Tests beinhalten. Wie Kölner feststellt, wirkt sich der Umsetzungsdruck auf die OEMs bereits auf strategische Entscheidungen aus, wobei einige EU-Hersteller aufgrund der hohen Kosten für die Einhaltung der Cybersicherheitsvorschriften ihre Modellpalette reduzieren. Es gibt auch konkrete Beispiele dafür, dass Hersteller als direkte Folge der neuen Cybersicherheitsvorschriften Modelle vom europäischen Markt nehmen. So kündigte Porsche an, die Produktion des Modells Macan im Frühjahr 2024 einzustellen, da die Nachrüstung der Fahrzeugplattform zur Erfüllung der R155-Anforderungen zu komplex und kostspielig wäre [153]. Auch der deutsche Hersteller VW nahm aufgrund der Verordnung Fahrzeuge vom Markt. Laut Darren Shelcuskys, Senior Consultant bei Ford, zwingen die Vorschriften die OEMs dazu, von informellen Best Practices zu

vollständig dokumentierten, überprüfbaren Cybersicherheitsprozessen überzugehen. In der Praxis hat dies zur Schaffung neuer interner Governance-Strukturen wie Cybersicherheits-Notfallteams und Vehicle Security Operations Centers (VSOC) sowie zur Einführung neuer technischer Leistungen wie Bedrohungsbewertungen, Penetrationstest-Nachweise und Compliance-Tracking-Metriken (z. B. TARA-Abschlussraten) geführt [154]. In den Vereinigten Staaten profitieren OEMs von einer größeren operativen Flexibilität. Zwar gibt es keine verbindlichen Vorschriften, doch der Marktdruck und potenzielle Haftungsrisiken fördern die Einhaltung der Best Practices der NHTSA. Im Allgemeinen wird von den Zulieferern erwartet, dass sie ihre Sorgfaltspflicht nachweisen. In allen Regionen wird Cybersicherheit zunehmend in Qualitäts- und Sicherheitsprozesse integriert. Von OEMs wird erwartet, dass sie Risiken proaktiv managen und Prozesse einrichten, die auditiert oder unabhängig überprüft werden können.

Regionale Prioritäten

Europa legt den Schwerpunkt auf die Harmonisierung der Vorschriften und formale Wege zur Einhaltung der Vorschriften. Die Integration von R155 und R156 in den Typgenehmigungsprozess gewährleistet eine einheitliche Einhaltung der Vorschriften in allen Mitgliedstaaten. China legt den Schwerpunkt auf technische Spezifität und den nationalen Datenschutz. Seine Standards schreiben strenge Testverfahren vor und verbieten die Übertragung von Fahrzeugdaten ins Ausland. Chinas Vorschriften konzentrieren sich auf strenge Fristen für die Behebung offengelegter Schwachstellen. Die Vereinigten Staaten verfolgen einen dezentralen, marktorientierten Ansatz. Der Rahmen der NHTSA fördert Innovation und Flexibilität, indem er OEMs die Möglichkeit gibt, individuelle Strategien zu verfolgen. Die Zusammenarbeit über Branchenplattformen wie Auto-ISAC und Partnerschaften mit akademischen Einrichtungen sind zentrale Bestandteile der US-Strategie. Zusammenfassend lässt sich sagen, dass alle drei Regionen zwar die Bedeutung einer umfassenden Cybersicherheit für Fahrzeuge anerkennen, sich jedoch in Bezug auf die Umsetzungsstrategie, die Durchsetzungsmechanismen und die technischen Besonderheiten unterscheiden. Diese Unterschiede haben praktische Auswirkungen auf globale OEMs und ihre Lieferketten.

2.1.3.4 Kritische Bewertung und Lücken der Vorschriften

Während im vorigen Kapitel die allgemeinen Regulierungsansätze verglichen wurden, enthält dieser Abschnitt eine kritische Bewertung der Herausforderungen und potenziellen Mängel jedes einzelnen Regelwerks. Die Analyse konzentriert sich auf die Ermittlung von Regulierungslücken, Umsetzungsschwierigkeiten und Bereichen, die einer weiteren Klärung bedürfen. Soweit verfügbar, werden öffentliche Bewertungen und Stellungnahmen von Vertretern der Industrie zur Untermauerung der Bewertung herangezogen. Wo solche Quellen nur begrenzt verfügbar sind, enthält dieser Abschnitt begründete Interpretationen, die auf der Struktur, den Durchsetzungsmechanismen und den wahrscheinlichen Umsetzungshindernissen der Regelwerke basieren.

Europäische Union: UNECE R155/R156

Die durch R155 und R156 eingeführten Regulierungsrahmen stellen einen wichtigen Schritt in Richtung einer globalen Harmonisierung der Cybersicherheitsstandards für Fahrzeuge dar. Trotz dieser bedeutenden Fortschritte bleiben die Vorschriften jedoch in mehreren Bereichen vage. Die Abstraktheit von R155/R156 wurde von Branchenexperten kritisiert, da sie nur begrenzte methodische oder operative Leitlinien bieten. Clemens Gleich [155], technischer Redakteur bei Heise, betont, dass die Anforderungen, insbesondere für das CSMS, allgemein formuliert sind und einen großen Interpretationsspielraum lassen. So definiert R155 das CSMS als einen systematischen,

risikobasierten Prozess zum Management von Cyber-Bedrohungen, überlässt die Operationalisierung jedoch weitgehend den Herstellern. Infolgedessen kann theoretisch fast jede Dokumentation so strukturiert werden, dass sie die formalen Anforderungen erfüllt, wie Gleich argumentiert. In der Praxis kann die Zertifizierung jedoch je nach der bestehenden Prozessreife innerhalb des Unternehmens immer noch mehrere Monate oder sogar über ein Jahr dauern. Gleich merkt weiter an, dass viele der erforderlichen Sicherheitsmaßnahmen (z. B. Dokumentation, Zugriffskontrolle, Reaktion auf Vorfälle) bei etablierten OEMs zwar bereits üblich sind, der zusätzliche Verwaltungsaufwand jedoch insbesondere für ältere Fahrzeugtypen beträchtlich sein kann. Darüber hinaus hängen die R155 und R156 zwar von ihrer Konzeption her von einer Harmonisierung der Cybersicherheitsstandards für Fahrzeuge in ganz Europa ab, in der Praxis hängt die Umsetzung jedoch nach wie vor stark vom jeweiligen Land ab. Jeder EU-Mitgliedstaat hat seine eigene technische Dienststelle und Zulassungsbehörde, beispielsweise den TÜV in Deutschland, die RDW in den Niederlanden oder die UTAC in Frankreich. Da die Vorschriften an vielen Stellen recht vage sind, kann die Auslegung je nach zuständiger Behörde unterschiedlich ausfallen. Infolgedessen ist der Zertifizierungsprozess in Europa nicht immer einheitlich. Dies zeigt, dass trotz der Harmonisierungsbemühungen nach wie vor große nationale Unterschiede bestehen, was die Situation für grenzüberschreitend tätige Hersteller erschwert. Außerdem erhöht dies den Zeit- und Kostenaufwand für den Prozess, insbesondere für Unternehmen, die ihre Cybersicherheits-Workflows noch nicht an diese neuen Vorschriften angepasst haben. Darüber hinaus weist Shelcuský darauf hin, dass die Dokumentation und Umsetzung der Prozesse aus UNR155 und UNR156 zeitaufwändig sein kann und möglicherweise Mitarbeiterschulungen und Änderungen der Arbeitsabläufe erforderlich macht. Trotz dieser operativen Herausforderungen wird das Kernziel von R155/R156, einen strukturierten Ansatz für Cybersicherheit zu etablieren, der den gesamten Lebenszyklus abdeckt, angesichts der Komplexität und Sicherheitsanfälligkeit vernetzter Fahrzeuge allgemein als notwendig angesehen. Obwohl R155/R156 einen nützlichen Rahmen schaffen, kann ihre Umsetzung in der Praxis ohne strengere operative Leitlinien und klarere Bewertungsmaßstäbe eine Belastung darstellen. Um die regulatorische Konsistenz in der gesamten EU zu verbessern, wäre es ratsam, zentralisierte Prüfkriterien und einheitliche Bewertungsrichtlinien festzulegen. Darüber hinaus könnte die Bereitstellung vereinfachter Compliance-Pfade für Altsysteme und konkreter Umsetzungsvorlagen, wie z. B. Prozessmodelle, die praktische Belastung für OEMs erheblich verringern. Die Bemühungen zur Operationalisierung der abstrakten Anforderungen sind bereits im Gange. Da die praktische Umsetzung oft von ergänzenden Rahmenwerken abhängt, stellt Liedtke (2024) einen strukturierten Ansatz vor, der UNECE und ISO/SAE 21434 in nachvollziehbare Prozesse übersetzt.

China: GB 44495-2024

Obwohl die chinesische Verordnung GB 44495-2024 relativ neu ist und systematische externe Bewertungen noch begrenzt sind, lassen sich aufgrund ihrer Struktur einige Herausforderungen absehen. GB 44495-2024 zeichnet sich durch ein hohes Maß an technischer Spezifität und operativen Details aus. Es bestehen jedoch weiterhin einige Einschränkungen. Die Verordnung enthält nur begrenzte methodische Leitlinien dazu, wie Risikobewertungen systematisch durchgeführt werden sollen, insbesondere innerhalb komplexer Lieferketten. Ihre starke nationale Ausrichtung, wie beispielsweise Beschränkungen für grenzüberschreitende Datenübertragungen, könnte auch die internationale Interoperabilität behindern, was für global tätige OEMs Compliance-Herausforderungen mit sich bringt. Darüber hinaus könnte die hohe regulatorische Belastung in Verbindung mit strengen Fristen für die Behebung bekannter Schwachstellen kleinere Zulieferer unter erheblichen Druck setzen. Dies könnte sich möglicherweise auf die einheitliche Umsetzung im

gesamten Automobil-Ökosystem auswirken. Insgesamt bietet GB 44495-2024 zwar klare technische Vorgaben, doch könnten die begrenzten methodischen Leitlinien und die strengen nationalen Auflagen eine globale Angleichung behindern und praktische Herausforderungen für die branchenweite Umsetzung mit sich bringen. Um die Belastungen zu verringern, könnten die chinesischen Regulierungsbehörden konkrete Vorlagen für die Umsetzung von Risikobewertungen herausgeben und unter bestimmten Sicherheitsvorkehrungen kontrollierte Ausnahmen von den grenzüberschreitenden Datenbeschränkungen zulassen. Darüber hinaus würde die Einführung gestaffelter Fristen für Abhilfemaßnahmen, die sich nach Schweregrad und Systemkritikalität richten, kleineren Zulieferern helfen, ihre Verpflichtungen besser zu erfüllen.

USA: NHTSA-Richtlinien

Aufgrund des freiwilligen und flexiblen Charakters der NHTSA-Richtlinien gibt es im Vergleich zur UN-Verordnung weniger kritische Stimmen zu diesem Standard. Allerdings kann ihr unverbindlicher Status zu uneinheitlichen Umsetzungsniveaus und Sicherheitsreife in der gesamten US-Automobilindustrie führen. Eine weitere bemerkenswerte Lücke ist das Fehlen klarer Kriterien für die Bewertung des Cybersicherheitsstatus. Obwohl die Leitlinien eine kontinuierliche Verbesserung fördern, enthalten sie keine formalen Benchmarks oder Zertifizierungsprozesse. Darüber hinaus werden in den Leitlinien zwar Risiken durch Dritte behandelt, jedoch keine konkreten Erwartungen an das Management von Lieferantenökosystemen gestellt. Zusammenfassend lässt sich sagen, dass die Flexibilität der NHTSA-Richtlinien zwar Innovation und Anpassungsfähigkeit ermöglicht, jedoch ohne verbindliche Durchsetzung und standardisierte Bewertungskriterien das Risiko einer uneinheitlichen Cybersicherheitsbereitschaft birgt. In den USA könnte ein freiwilliges Cybersicherheitslabel dazu beitragen, grundlegende Standards anzuheben und gleichzeitig den Herstellern Flexibilität zu lassen. Ergänzt durch standardisierte Bewertungsrahmen würde dies die Konsistenz verbessern und Integrationsrisiken im gesamten Fahrzeugökosystem verringern.

In Tabelle 5 sind die wichtigsten regulatorischen Lücken nach Region mit Auswirkungen und Empfehlungen aufgezeigt.

Tabelle 5: Wichtigste regulatorische Lücken nach Region mit Auswirkungen und Empfehlungen

Region	Problem/Schwäche	Auswirkungen	Empfehlung
Europäische Union	Uneinheitliche Auslegung in den Mitgliedstaaten trotz Harmonisierung durch die UN-ECE	Zertifizierungsergebnisse hängen von der nationalen Auslegung ab	Einführung EU-weiter Prüfkriterien und Bewertungsrichtlinien zur Vereinheitlichung der Zulassungsverfahren
	Vage operative Definitionen in UN-ECE R155/R156	Mangelnde Klarheit bei der Umsetzung verlangsamt die Einhaltung	Bereitstellung detaillierter Umsetzungsleitlinien, einschließlich Prozessvorlagen und Zuordnungen von Bedrohungen und Reaktionen
China	Fehlende methodische Leitlinien für Risikobewertungen	Uneinheitliche Umsetzung in der Branche und Unsicherheit bei den OEMs hinsichtlich der Umsetzung	Veröffentlichung von Vorlagen oder Rahmenwerken für die Prozessimplementierung und die Bewertung von Cybersicherheitsrisiken

	Inländische Datenbeschränkungen schränken die Interoperabilität ein	Beschränkungen des grenzüberschreitenden Datenverkehrs erschweren internationale OEM-Aktivitäten	Festlegung von Ausnahmen oder kontrollierten Verfahren für den internationalen Datenaustausch unter definierten Sicherheitsvorkehrungen
Vereinigte Staaten	Keine verbindlichen Cybersicherheitsvorschriften	Die Umsetzung variiert je nach Hersteller	Erwägung einer freiwilligen Zertifizierung (z. B. Cybersicherheitslabel) zur Förderung von Transparenz und einer grundlegenden Reife
	Fehlen formeller Bewertungskriterien	Das Fehlen einer strukturierten Konformitätsbewertung erschwert das Benchmarking	Entwicklung von Referenz-Reifegradmodellen oder Bewertungsrahmen, die an die Best Practices der NHTSA gekoppelt sind

2.1.3.5 Indirekte Einflüsse und angrenzende Vorschriften

Neben speziellen Vorschriften zur Cybersicherheit von Fahrzeugen beeinflussen eine Reihe benachbarter Rechtsrahmen zunehmend die Konstruktion und den Betrieb vernetzter Fahrzeuge. Dazu gehören digitale Gesetze, Umwelanforderungen und Datenschutzregelungen, die alle indirekte Cybersicherheitsverpflichtungen auferlegen.

Europäische Union: Horizontale digitale Vorschriften

Die Europäische Union hat horizontale Vorschriften eingeführt, die branchenübergreifend gelten, aber erhebliche Auswirkungen auf vernetzte Fahrzeuge haben. Zwei besonders relevante Beispiele sind das EU-Datengesetz und das EU-Gesetz zur Cyberresilienz (Cyber Resilience Act, CRA). Das EU-Datengesetz [156], das im Januar 2024 in Kraft getreten ist und im September 2025 anwendbar wird, legt Regeln für den fairen Zugang zu und die Nutzung von Daten fest, die von vernetzten Produkten, einschließlich Fahrzeugen, generiert werden. Er zielt darauf ab, die Nutzer zu stärken, indem er ihnen das Recht einräumt, auf die von ihren eigenen vernetzten Geräten, wie z. B. modernen Fahrzeugen, die mit IoT-Sensoren ausgestattet sind, erzeugten Daten zuzugreifen und diese weiterzugeben. Für den Automobilsektor führt der Datenakt eine Veränderung in der Datenverwaltung ein: Die Hersteller müssen sicherstellen, dass die Fahrzeugsysteme so konzipiert sind, dass sie einen sicheren und kontrollierten Datenzugriff und -austausch mit Dritten, wie z. B. unabhängigen Reparaturdienstleistern oder Flottenmanagementdiensten, unterstützen. Die Verordnung schreibt zwar keine Cybersicherheitsmaßnahmen direkt vor, ihre Bestimmungen implizieren jedoch die Notwendigkeit robuster Zugriffskontrollen, Mechanismen zur Datenintegrität und Schutz vor unbefugtem Zugriff oder Manipulation. Das Gesetz zur Cyberresilienz (Cyber Resilience Act, CRA) [157] trat Ende November 2024 in Kraft und ist eine EU-Verordnung zur Festlegung von Mindestanforderungen an die Cybersicherheit für alle Produkte mit digitalen Elementen, einschließlich Hardware und Software. Die vollständige Einhaltung wird bis Dezember 2027 verbindlich. Die CRA deckt eine breite Palette vernetzter Produkte ab und verpflichtet Hersteller, während des gesamten Lebenszyklus „Sicherheit durch Design“, den Umgang mit Schwachstellen und risikobasierte Produktbewertungen sicherzustellen. Für die Automobilindustrie bedeutet die CRA Richtlinien, die für Fahrzeugsysteme, Infotainment-Software oder nachgerüstete vernetzte Geräte gelten können, insbesondere solche, die nicht streng durch die Typgenehmigung reguliert sind. Die Hersteller müssen innerhalb von 24 bis 72 Stunden Schwachstellen melden, Software-Stücklisten (SBOMs) führen und den Zeitraum für den Cybersicherheits-Support transparent

angeben [158]. Die CRA ergänzt bestehende Vorschriften für Kraftfahrzeuge, und die Gewährleistung der Übereinstimmung mit R155, R156 und ISO 21434 trägt dazu bei, unnötige Überschneidungen bei Konformitätsbewertungen in der gesamten EU zu vermeiden.

Europäische Union: Umweltvorschriften

Die von der Europäischen Kommission im November 2022 veröffentlichte vorgeschlagene Euro-7-Verordnung ist zwar keine Cybersicherheitsvorschrift im eigentlichen Sinne, zeigt jedoch, wie eine Umweltpolitik neue technische Anforderungen einführen kann, die sich mit der Cybersicherheit überschneiden [159]. Obwohl Euro 7 in erster Linie auf die Luftqualität und die öffentliche Gesundheit abzielt, stützt sich ihre Umsetzung stark auf digitale Systeme, was sie für die Cybersicherheits-Governance im Automobilbereich relevant macht. Ein Kernelement der Verordnung ist die Anforderung einer kontinuierlichen On-Board-Überwachung (OBM) der Schadstoffwerte. Die Werte müssen von Sensoren im Fahrzeug erfasst und über die Backend-Systeme der OEMs sicher an die Aufsichtsbehörden übertragen werden. Der Europäische Automobilherstellerverband (ACEA), eine in Brüssel ansässige Branchenorganisation, die große Fahrzeughersteller in der EU vertritt, hat betont, dass solche Datenübertragungen maschinenlesbare Formate (z. B. JSON), sichere Schnittstellen und einen starken Schutz vor Manipulationen oder unbefugtem Zugriff erfordern, insbesondere bei OTA-Übertragungen [160]. In diesem Zusammenhang sind Cybersicherheitsmaßnahmen wie Verschlüsselung, Authentifizierung und sichere Protokollierung erforderlich. In Deutschland hat der Verband der Automobilindustrie (VDA), das nationale Pendant zur ACEA, im Rahmen des Konsultationsprozesses zum Euro-7-Umsetzungsgesetz eine offizielle Stellungnahme abgegeben. Der VDA argumentiert, dass die bestehende Cybersicherheitszertifizierung nach R155 als ausreichend angesehen werden sollte, um die Cybersicherheitsanforderungen von Euro 7 zu erfüllen [161]. Zusammenfassend lässt sich sagen, dass Euro 7 veranschaulicht, wie Umweltvorschriften den Umfang der digitalen Compliance-Verpflichtungen erweitern können. Branchenakteure wie ACEA und VDA beteiligen sich aktiv am Gesetzgebungsprozess, um Euro 7 an bestehende Cybersicherheitsrahmenwerke, insbesondere R155, anzupassen und so die technische Kohärenz und regulatorische Effizienz in der gesamten Branche sicherzustellen.

China: Nationales Recht

Das seit Juni 2017 geltende Cybersicherheitsgesetz der Republik China bietet einen landesweiten Rechtsrahmen für den Aufbau, den Betrieb und die Überwachung von Netzwerksystemen innerhalb Chinas (Art. 2). Es legt ein mehrstufiges Schutzsystem (MLPS) für alle Netzbetreiber fest (Art. 21) und verpflichtet diese zur Umsetzung technischer und organisatorischer Maßnahmen wie Virenschutz, Protokollierung, Datensicherung und Reaktion auf Vorfälle. Für Betreiber kritischer Informationsinfrastrukturen (CII), zu denen Sektoren wie Verkehr und öffentliche Dienste gehören (Art. 31) und die daher auch für die Automobilindustrie gelten, sind zusätzliche Verpflichtungen festgelegt. Diese Verpflichtungen umfassen Datenlokalisierung (Art. 37), jährliche Risikobewertungen (Art. 38) und Sicherheitsüberprüfungen für aus dem Ausland gelieferte Netzwerkprodukte (Art. 35) [162].

Europäische Union, China und USA: Datenschutzbestimmungen

Die Datenschutz-Grundverordnung (DSGVO) [163] ist der zentrale Rechtsrahmen der EU für den Schutz personenbezogener Daten. Sie hat direkte Auswirkungen auf vernetzte Fahrzeuge, die routinemäßig personenbezogene Daten wie Standort, Nutzungsmuster und Fahrerprofile verarbeiten. Gemäß der DSGVO muss die Datenverarbeitung rechtmäßig, transparent und auf das

erforderliche Maß beschränkt sein. Nutzer haben das Recht auf Zugang, Berichtigung und Löschung ihrer Daten, und Organisationen müssen geeignete technische und organisatorische Maßnahmen zu deren Schutz ergreifen. Für die Automobilbranche bedeutet dies eine sichere Datenspeicherung, strenge Zugriffskontrollen und Mechanismen zur Datenminimierung und -löschung. Artikel 32 verlangt ausdrücklich den Schutz vor unbefugtem Zugriff oder Verlust und steht damit im Einklang mit Cybersicherheitszielen wie Integrität, Vertraulichkeit und Verfügbarkeit. Daher unterstützt die Einhaltung von Cybersicherheitsstandards wie R155 und ISO/SAE 21434 auch die Einhaltung der DSGVO in der Praxis. In China legt das seit November 2021 geltende Gesetz zum Schutz personenbezogener Daten (Personal Information Protection Law, PIPL) [164] strenge Anforderungen für die Erhebung, Speicherung und Verarbeitung personenbezogener Daten fest. Es schreibt die ausdrückliche Zustimmung der Nutzer, Datenminimierung und Sicherheitsvorkehrungen vor, insbesondere für sensible Daten und grenzüberschreitende Datenübermittlungen. Für Automobilhersteller, die in China tätig sind, hat dies direkte Konsequenzen: Fahrzeugsysteme, die Verhaltens- oder standortbezogene Daten erfassen, müssen so konzipiert sein, dass sie den Standards des PIPL entsprechen, einschließlich der Implementierung von Zugriffskontrollen und Verschlüsselung. In ähnlicher Weise erweitert das seit Januar 2023 geltende California Privacy Rights Act (CPRA) [165] die Datenschutzrechte für Einwohner Kaliforniens und führt Verpflichtungen für Unternehmen ein, die ihre personenbezogenen Daten verarbeiten. Es verlangt angemessene Sicherheitsvorkehrungen und gewährt Verbrauchern das Recht, die Verwendung sensibler Daten wie präzise Geolokalisierung oder biometrische Identifikatoren einzuschränken. Im Automobilsektor betrifft dies vernetzte Dienste wie Telematik, Infotainment und Fahrerassistenzsysteme, die alle mit Datenschutz- und Cybersicherheitsvorkehrungen ausgestattet sein müssen, um die Einhaltung der Vorschriften zu gewährleisten.

2.1.3.6 Fazit

In diesem Abschnitt wurde die Regulierungslandschaft für Cybersicherheit im Automobilbereich untersucht, indem die in der Europäischen Union, China und den Vereinigten Staaten etablierten Rahmenwerke verglichen wurden. Die Analyse zeigt, dass alle drei Regionen die zunehmende Bedeutung der Cybersicherheit über den gesamten Lebenszyklus eines Fahrzeugs hinweg erkennen. Der Grad der rechtlichen Durchsetzbarkeit, die technischen Besonderheiten und die Umsetzungspraktiken unterscheiden sich jedoch erheblich. Die Europäische Union schreibt Cybersicherheitsanforderungen durch die UNECE-Regelungen R155 und R156 vor, die in den Typgenehmigungsprozess integriert sind. Dies gewährleistet zwar die rechtliche Durchsetzbarkeit, jedoch ergeben sich praktische Herausforderungen aufgrund vager operativer Definitionen und unterschiedlicher Auslegungen durch die nationalen Behörden. Die chinesische Norm GB 44495-2024 enthält technisch detaillierte Prüfprotokolle, jedoch keine methodischen Leitlinien für die Risikobewertung. Im Gegensatz dazu stützen sich die Vereinigten Staaten auf unverbindliche Richtlinien der NHTSA, die Flexibilität und Innovation fördern, jedoch zu einer uneinheitlichen Umsetzung und begrenzter Rechenschaftspflicht führen können. Ein regionenübergreifender Vergleich zeigt eine Konvergenz bei den wichtigsten Grundsätzen, wie z. B. der Notwendigkeit von CSMS, sicheren Software-Updates und Lieferketten, Überwachungs- und Vorfallreaktionsprozesse. Uneinheitliche Durchsetzungsmaßnahmen, Zertifizierungsmodelle und technische Erwartungen stellen jedoch weltweit tätige OEMs und Zulieferer vor Herausforderungen. Darüber hinaus beginnen benachbarte Vorschriften wie Emissionsstandards, Datenschutzgesetze und Vorschriften für digitale Produkte, die Cybersicherheitsanforderungen indirekt zu beeinflussen, was die Komplexität weiter erhöht. Um diesen Herausforderungen zu begegnen, wird eine engere Abstimmung zwischen gesetzlichen Vorgaben und technischen Standards wie ISO/SAE 21434 empfohlen.

Darüber hinaus könnten die Harmonisierung der Zertifizierungskriterien, klarere Methoden zur Risikobewertung und standardisierte Auditmechanismen eine einheitlichere Umsetzung in allen Regionen unterstützen. Auch die regulatorischen Rahmenbedingungen müssen weiterentwickelt werden, um der wachsenden Bedeutung von Integrationen durch Dritte, Software-Lieferketten und der Datenverwaltung nach der Markteinführung Rechnung zu tragen. Zusammenfassend lässt sich sagen, dass zwar erhebliche Fortschritte bei der Schaffung regulatorischer Rahmenbedingungen für die Cybersicherheit von Fahrzeugen erzielt wurden, jedoch weitere Verfeinerungen und eine internationale Angleichung erforderlich sind, um technische Konsistenz, grenzüberschreitende Kompatibilität und nachhaltige Widerstandsfähigkeit innerhalb des Automobilsektors zu gewährleisten.

2.1.4 Technologien zum Schutz der Privatsphäre für vernetzte Automobilumgebungen

Zur Definition aller privacy-relevanten Aspekte für den Automotive Use Case, war die erste Forschungsfrage, an welchen Stellen innerhalb eines Fahrzeugnetzes vertrauliche Daten anfallen und wie diese zu bewerten sind. Hierfür wurde die Seminararbeit eines Studenten mit dem Titel: „Analysis of Data Confidentiality in Smart Vehicles“ betreut. Daraus resultierte ein konzeptuelles Framework, zur Evaluation der Vertraulichkeit von Daten, die von autonomen Fahrzeugen generiert werden. Vertrauliche Daten wurden als nutzerbezogene Informationen, die von einem Fahrzeug gespeichert oder generiert werden, definiert. Als Domänen, in denen Daten verarbeitet werden können wurden Antrieb (engl. Powertrain), Fahrzeugsicherheit (engl. Vehicle Safety), Komfort (engl. Comfort), Infotainment und Telematik (engl. Telematics) betrachtet, basierend auf dem Forschungspapier von Nilsson et al. [166].

Der Antriebsstrangbereich übernimmt zentrale Funktionen im Zusammenhang mit dem Antrieb, wie beispielsweise die Steuerung von Motor und Getriebe. Er verarbeitet und speichert Daten wie die Motordrehzahl (RPM), die aktuelle Geschwindigkeit des Fahrzeugs, die Drosselklappenstellung, den Kraftstoffverbrauch und die Motortemperatur.

Die Domäne Fahrzeugsicherheit umfasst Systeme wie Bremsen und Airbags und verarbeitet sicherheitsrelevante Informationen. Dazu gehören Daten zum Auslösen der Airbags, zu plötzlichen Bremsmanövern, zur Verwendung von Sicherheitsgurten, zum Reifendruck und dazu, ob das Fahrzeug ins Schleudern geraten ist oder die Stabilität verloren hat. Diese Datenpunkte sind für die Fahrzeugsteuerung und die Unfallanalyse von entscheidender Bedeutung.

Die Komfort Domäne unterstützt Komfort-Einstellungen im Fahrzeug. Diese umfassen die Verarbeitung von Daten wie der Kabinentemperatur, der Position des Fahrersitzes, ob die Türen verriegelt oder entriegelt sind, ob Fenster oder Schiebedach geöffnet oder geschlossen sind und welche Innenleuchten eingeschaltet sind.

Zur Infotainment-Domäne gehören die Medien- und Unterhaltungssysteme des Fahrzeugs sowie dessen Verbindung zu Mobiltelefonen und anderen Geräten. Sie verarbeitet Daten wie Sprachbefehle, den Namen oder die ID des verbundenen Mobiltelefons, den Musikverlauf, die zuletzt angefahrenen Navigationsziele und die Namen der Kontakte aus dem Mobiltelefon des Fahrers oder der Fahrerin.

Die Telematik Domäne ermöglicht die Kommunikation zwischen Fahrzeug und externen Systemen. Sie erfasst GPS-Standortdaten, die Fahrthistorie, die zurückgelegte Gesamtstrecke, an

Rettungsdienste gesendete Unfallmeldungen und die ID der SIM-Karte oder des Mobilfunkmodems des Fahrzeugs.

Im ersten Schritt wurde für jede dieser Domänen untersucht, ob die Daten, die in dieser Domäne gespeichert und verarbeitet werden, eine Person oder ein bestimmtes Fahrzeug identifizieren können. Zusätzlich wurde festgehalten, ob diese Daten in Kombination mit anderen Informationen zur Identifikation einer bestimmten Person oder eines bestimmten Fahrzeugs führen können. Das Ergebnis wurde in der folgenden Tabelle 6 festgehalten:

Tabelle 6: Bewertung der Identifizierbarkeit der Datenpunkte je Domäne.

Domäne	Datenpunkte	Identifizierbarkeit (Direkt/Indirekt/Nein)
Antriebsstrang (Powertrain)	Motordrehzahl (RPM), aktuelle Fahrzeuggeschwindigkeit, Drosselklappenstellung	Indirekt: Hohe Re-Identifikationsgefahr bei Verknüpfung mit Standort/Fahrzeug-ID
	Kraftstoffverbrauch, Motortemperatur	Nein: Insgesamt weniger direktes Fahrverhalten ableitbar
Fahrzeugsicherheit (Vehicle Safety)	Auslösen der Airbags, Plötzliche Bremsmanöver, Sicherheitsgurt Verwendung, Fahrzeugschleudern/Stabilitätsverlust	Indirekt: Hohe Re-Identifikationsgefahr bei Verknüpfung mit Standort/Fahrzeug-ID
	Reifendruck	Nein: Insgesamt weniger direktes Fahrverhalten ableitbar
Komfort (Comfort)	Kabinentemperatur, Fahrersitzposition, Türen verriegelt/entriegelt, Fenster oder Schiebedach geöffnet/geschlossen, Innenleuchten an/aus	Indirekt: Re-Identifikationsgefahr bei Verknüpfung mit Standort/Fahrzeug-ID
Infotainment	Sprachbefehle, Name/ID des verbundenen Mobiltelefons	Direkte, personenbezogene Daten
	Musikhistorie, zuletzt angefahrte Navigationsziele, Kontakte aus dem Mobiltelefon	Indirekt: Hohe Re-Identifikationsgefahr bei Verknüpfung mit Standort/Fahrzeug-ID
Telematik (Telematics)	GPS-Standortdaten, Fahrtenhistorie, zurückgelegte Gesamtstrecke, gesendete Unfallmeldungen, SIM-Karten ID / Mobilfunkmodem ID des Fahrzeugs	Direkte, personenbezogene Daten

Die Analyse zeigt, dass alle Domänen in modernen Fahrzeugen vertrauliche Daten verarbeiten. Domänen wie Antriebsstrang, Fahrzeugsicherheit sowie Komfort, verarbeiten Daten, die potenziell Personen indirekt identifizieren können. Zum Beispiel können Daten aus diesen Domänen für Fahrer-Fingerprinting verwendet werden, eine Technik, die einzelne Fahrer anhand ihres Fahrverhaltens unterscheidet. Kar et al. [167] demonstrierten, dass 15 verschiedene Fahrer mit 100% Genauigkeit anhand von Daten von 15 Fahrzeugparametern identifiziert werden konnten.

Im Gegensatz dazu enthalten Domänen wie dem Infotainment und der Telematik sogar Daten, die eine Person direkt identifizieren können, wie z. B. Sprachaufnahmen, GPS-Standort Daten oder die Fahrtenhistorie. Die Datenpunkte Motortemperatur, Kraftstoffverbrauch und Reifendruck werden nicht als vertraulich angesehen, weil sie rein technische Werte sind, die den Systemstatus widerspiegeln und weder vom Fahrer beeinflusst noch personalisiert werden können. Die Analyse

bestätigt, dass umfassende Schutzmaßnahmen für die Datenvertraulichkeit domänenübergreifend notwendig sind, wobei ein besonderes Augenmerk auf Systeme gelegt werden sollte, die direkt identifizierbare personenbezogene Daten verarbeiten. Allerdings müssen, bevor spezifische Schutzmaßnahmen ausgewählt werden, die Risikoniveaus der verschiedenen vertraulichen Datenpunkte im nächsten Schritt des Frameworks bewertet werden. Dafür wurde eine Vertraulichkeits-Scoring Matrix definiert, die in Tabelle 7 beschrieben ist:

Tabelle 7: Vertraulichkeits-Scoring Matrix.

Faktor	Niedriges Risiko (0 Punkte)	Mittleres Risiko (1 Punkt)	Hohes Risiko (2 Punkte)
Identifizierbarkeit	Insgesamt weniger direktes Fahrverhalten ableitbar	Hohe Re-Identifikationsgefahr bei Verknüpfung mit anderen Daten	Direkte, personenbezogene Daten
Schadenshöhe bei Datenleak	Keine Auswirkung	Geringe Auswirkung	Hohe Auswirkung
Spezielle DSGVO Kategorie	Nicht sensitiv	Möglicherweise sensitiv, oder unklar	Sensitive Daten
Datenverbreitung	Innerhalb des Fahrzeugs	Eingeschränktes Teilen mit vertrauenswürdigen Drittparteien	Extern geteilt, oder im Cloud/Backend gespeichert

Die Bewertung der Identifizierbarkeit ist bereits in Tabelle 6 vorgenommen worden. Alle Daten, die dabei als direkt oder nicht direkt identifizierbar zugeordnet werden, werden anschließend der Vertraulichkeits-Scoring Matrix zugeordnet. Das Ergebnis wird in der nachfolgenden Tabelle 8 festgehalten:

Tabelle 8: Risikobewertung der Datenpunkte.

Domäne	Datenpunkte	Faktor	Risikobewertung	Gesamtbewertung
Antriebsstrang (Powertrain)	Motordrehzahl (RPM), aktuelle Fahrzeuggeschwindigkeit, Drosselklappenstellung	Identifizierbarkeit	1	2
		Schadenshöhe bei Datenleak	0	
		Spezielle DSGVO Kategorie	0	
		Datenverbreitung	1	
Fahrzeugsicherheit (Vehicle Safety)	Auslösen der Airbags, Plötzliche Bremsmanöver, Sicherheitsgurt Verwendung, Fahrzeugschleudern/Stabilitätsverlust	Identifizierbarkeit	1	2
		Schadenshöhe bei Datenleak	1	
		Spezielle DSGVO Kategorie	0	
		Datenverbreitung	0	
Komfort (Comfort)	Kabinentemperatur, Fahrersitzposition, Türen verriegelt/entriegelt, Fenster oder Schiebedach geöffnet/geschlossen, Innenleuchten an/aus	Identifizierbarkeit	1	2
		Schadenshöhe bei Datenleak	1	
		Spezielle DSGVO Kategorie	0	
		Datenverbreitung	0	

Infotainment	Sprachbefehle, Name/ID des verbundenen Mobiltelefons	Identifizierbarkeit	2	7
		Schadenshöhe bei Datenleak	2	
		Spezielle DSGVO Kategorie	1	
		Datenverbreitung	2	
	Musikhistorie, zuletzt angefahrene Navigationsziele, Kontakte aus dem Mobiltelefon	Identifizierbarkeit	1	6
		Schadenshöhe bei Datenleak	2	
		Spezielle DSGVO Kategorie	1	
		Datenverbreitung	2	
Telematik (Telematics)	GPS-Standortdaten, Fahrtenhistorie, zurückgelegte Gesamtstrecke, gesendete Unfallmeldungen, SIM-Karten ID / Mobilfunkmodem ID des Fahrzeugs	Identifizierbarkeit	2	6
		Schadenshöhe bei Datenleak	1	
		Spezielle DSGVO Kategorie	1	
		Datenverbreitung	2	

Die Ergebnisse aus Tabelle 8 zeigen deutliche Unterschiede im Vertraulichkeitsrisiko über die Domänen hinweg. Während Powertrain, Fahrzeugsicherheit, sowie Komfort aufgrund begrenzter Identifizierbarkeit, geringem potenziellen Schaden und dem Fehlen sensibler Kategorien ein geringes Risiko tragen (Risikowertung: 2), weisen andere Domänen größere Kritikalität auf.

Beispielsweise umfassen Infotainment-Daten (Gesamt-Risiko-Wert: 7) direkte Identifikatoren wie Sprachbefehle und Telefon-IDs. Bei einem Leak könnten diese Informationen sensible Nutzungspräferenzen oder Kontaktpersonen offenlegen, was zu Reputationsschäden oder gezieltem Betrug führen könnte. Die Daten werden oft an externe Server übertragen, was das Risiko einer Offenlegung erhöht. In einigen Fällen verarbeiten Infotainment-Systeme gemäß DSGVO besondere Kategorien personenbezogener Daten, wie religiöse Lieder, politische Podcast-Abonnements oder aufgezeichnete Sprachbefehle, die biometrische Merkmale oder gesundheitsbezogene Informationen offenbaren (z. B. Erinnerungen an Medikamente über den Sprachassistenten). Diese Kombination rechtfertigt hohe Werte für Identifizierbarkeit (2), potenziellen Schaden (2) und Datenverbreitung (2), sowie einen mittleren Wert für besondere Kategorien von Daten (1). Telemetriedaten rangieren ebenfalls im hochkritischen Bereich (Gesamt-Risikowert: 6) aufgrund von Datenpunkten wie den GPS-Standortdaten und der Fahrtenhistorie, die als besondere Kategorien personenbezogener Daten nach DSGVO gelten können. Sie werden zudem tendenziell extern übertragen, was das Expositionsrisiko erhöht.

Diese Analyse hebt den Bedarf an strengeren Schutzmaßnahmen hervor, insbesondere in Infotainment- und Telematik-Systemen, während gleichzeitig angemessene Schutzmaßnahmen für andere Domänen beibehalten werden sollten. Wir werden uns in unserem Use Case daher auf Daten dieser beiden Domänen beschränken.

2.1.4.1 Use Case 3: Sichere Netzwerkkommunikation Autonomer Fahrzeuge

Es gibt verschiedene Fahrzeugnetzwerke, wie beispielsweise „Vehicular Cloud Networks“ (VCNs), auch V2C-Netzwerke genannt, und „Vehicle to Everything“ (V2X)-Netzwerke und „In-Vehicular Networks“ (IVNs). In unserem Paper haben wir uns auf die letzte Netzwerkart konzentriert. Unsere vorherige, systematische Analyse hat ergeben, dass vor allem Daten aus dem Infotainment und

Telematik Bereich besonders kritisch bzw. risikoreich in ihrer Gesamtbewertung sind. Daher wollen wir uns in unserem Use Case auf diese Daten fokussieren, genauer: Sprachbefehle, Name/ID des verbundenen Mobiltelefons, Musikhistorie, zuletzt angefahrte Navigationsziele, Kontakte aus dem Mobiltelefon, GPS-Standortdaten, Fahrtenhistorie, zurückgelegte Gesamtstrecke, gesendete Unfallmeldungen, SIM-Karten ID / Mobilfunkmodem ID des Fahrzeugs.

Zum besseren Verständnis werden Sprachbefehle beispielhaft durchexerziert. Sprachbefehle, die von Sprachassistenten im Auto aufgezeichnet und verarbeitet werden, bieten den Nutzern und Nutzerinnen Automatisierungen von Aktionen. Meistens wird die Aufzeichnung durch ein Aktivierungswort oder durch einen Knopfdruck eingeleitet. Das Mikrofon des Assistenten nimmt den Sprachbefehl auf und sendet ihn an eine vertrauenswürdige Drittpartei, wie einen Cloud-Server, der die Daten analysiert und eine Antwort kreiert, die dem Nutzenden zurückgegeben wird [168].

Daten können extern und intern von Angreifern abgehört und manipuliert werden. Dazu gehören Kreditkarten- und Kontonummern, IBAN, Sicherheitscodes oder Online-Banking-Passwörter, die laut diktiert werden, oder im Hintergrund zu hören sind. Angreifer können auf diese bei unsicherer Speicherung zugreifen oder beim Abhören direkt für ihren Betrug nutzen. Zudem ist oft nicht eindeutig wie lange und vor allem in welchem Umfang die Daten z. B. in der Cloud gespeichert werden und verstärkt wird die Problematik, wenn Sprachassistenten dauerhaft mit dem Internet verbunden sind [169]. Weitere Beispiele sind Befehle wie „navigiere nach Hause“, „ins Büro“ oder „zur Schule der Kinder“, die konkrete, sensible Orte offenlegen, mit dem Fahrer oder der Fahrerin verknüpft werden können und bei wiederholten Kommandos Rückschlüsse auf genaue Routinen- und Bewegungsprofile zulassen.

Für den Sprachassistenten gibt es mehrere Datenflüsse: vom Mikrofon über interne Bussysteme zum Infotainment-Steuergerät, optional weiter über die Mobilfunkverbindung zu Cloud-Diensten, und dann zurück zu Fahrzeugfunktionen wie Navi, Klima oder Telefonie. Für unseren Use Case der sicheren Netzwerkkommunikation innerhalb von autonomen Fahrzeugen, betrachten wir nur die IVN-Datenflüsse. Potenzielle Angriffsvektoren entstehen daher hauptsächlich durch unsichere Clients, oder semi-vertrauenswürdigen Personen, die das Fahrzeug ebenso verwenden.

2.1.4.2 Zuordnung von PETs auf vertrauliche Daten

In unserem Paper wurden PETs systematisch beschrieben, sodass jeweils die Definition, Funktionalität, Privacy Komponente, Vor- und Nachteile, sowie die Reife innerhalb unserer Use Cases klar verdeutlicht werden. Die PETs wurden nach dem OECD-Whitepaper [170] folgendermaßen geclustert:

- Tools zur Datenverschleierung
 - Anonymisierung/Pseudonymisierung
 - Synthetische Daten
 - Differential Privacy (DP)
 - Zero-Knowledge-Proofs (ZKP)
- Tools zur verschlüsselten Datenverarbeitung
 - Homomorphe Verschlüsselung – Homomorphic Encryption (HE)
 - Sichere Mehrparteienberechnung – Secure Multiparty Computation (SMPC)
 - Vertrauenswürdige Ausführungsumgebungen – Trusted Execution Environments (TEE)
- Föderierte und verteilte Analytik

- Förderiertes Lernen – Federated Learning (FL)
- Verteilte Analytik – Distributed Analytics
- Tools zur Datenverantwortlichkeit
 - Verantwortliche Systeme - Accountable systems
 - Schwellwert Teilung von Geheimnissen - Threshold secret sharing
 - Personenbezogene Datenspeicher / Systeme zur Verwaltung personenbezogener Daten

Als Privacy Engineering Frameworks wurden die Taxonomie von Heurix et al. [11] und das erweiterte LINDDUN Framework von Kunz et al. [12] aufgeführt und auf unsere drei Use Cases angewendet. Unser Ziel war es herauszufinden, ob diese Frameworks geeignet sind, um PETs für die sichere kollaborative Maschinen Werkzeug Daten Nutzung, sowie für IoT Geräte in Privatsphäre schützenden Smart Buildings und für die sichere Netzwerkkommunikation innerhalb von autonomen Fahrzeugen, abzuleiten.

Nach der Taxonomie von Heurix et al., werden die Privatsphäre-Dimensionen folgendermaßen definiert:

- **Szenario:** Die Dimension „Szenario“ definiert den primären nicht-vertrauenswürdigen Akteur und potenziellen Angreifer in einem Vorgang zum Austausch vertraulicher Informationen.
- **Aspekt:** Die Dimension „Aspekt“ definiert, welcher Datenschutzaspekt durch die PET behandelt wird.
- **Ziel:** Die Dimension „Ziel“ definiert das Ziel oder die Mittel der PET zum Schutz der Privatsphäre.
- **Grundlage:** Die Dimension „Grundlage“ definiert das zugrunde liegende Sicherheitsmodell und die Stärke der PETs.
- **Daten:** Die Dimension „Daten“ definiert die Art der Daten, die von der PET behandelt werden.
- **Vertrauenswürdige Drittpartei:** Die Dimension „Vertrauenswürdige Drittpartei“ definiert die Notwendigkeit einer vertrauenswürdigen dritten Partei und deren Beteiligung an einer PET.
- **Umkehrbarkeit:** Und schließlich definiert die Dimension „Umkehrbarkeit“, ob und unter welchen Umständen ein PET-Vorgang umkehrbar ist.

Wir haben den für ATLAS-L4 relevanten Use Case aus 2.1.4.1 auf das Privacy Framework von Heurix et al. in der folgenden Tabelle 9 angewendet.

Tabelle 9: Privacy Framework nach Taxonomie von Heurix et al.

Anforderungen	Use Case 3 (ATLAS-L4)
Szenario	Nicht-vertrauenswürdiger Client (z. B. Leihwagen, Familie), Nicht-vertrauenswürdiger Server (z. B. Cloud-Dienste, die Sprachbefehle speichern) und Extern (Remote Zugriff auf geteilte Daten)
Aspekt	Inhalte (z. B. Geistiges Eigentum des OEM, Kontakte, Audiodaten) und Nutzerverhalten (z. B. Fahrverhalten, Fahrtenhistorie)
Ziel	Schutz der Vertraulichkeit (z. B. Geistiges Eigentum des OEM, sensible Daten aus dem Infotainment und der Telematik Domäne), Ununterscheidbarkeit bei Kommunikation mit externen Entitäten

Grundlage	Computational und symmetrische Kryptografie (ähnlich wie MACsec, SecOC, Speicherverschlüsselung)
Daten	Gespeichert (IP, Datenbank im Infotainment) Übertragen (zwischen ECUs), Verarbeitet (z. B. Sensible Datenverarbeitung im Infotainment)
Vertrauenswürdige Drittpartei	Keine vertrauenswürdige Drittpartei innerhalb von Fahrzeugnetzen
Umkehrbarkeit	Keine Kooperation erforderlich, Vollständige Umkehrbarkeit bei symmetrischer Verschlüsselung

Als Szenario für den primären, nicht-vertrauenswürdigen Akteur sehen wir den nicht-vertrauenswürdigen Client, zu dem semi-vertrauenswürdige Personen zählen, die Zugriff auf das IVN erhalten. Dazu gehören Arbeitskolleginnen, – Kollegen, und Familienmitglieder, die dasselbe Fahrzeug fahren. Oder nicht-vertrauenswürdige Personen im Leihwagen Szenario, welche vor- oder nachher einen Zugriff auf dieselben Steuergeräte (ECUs) haben. Wie bereits im Use Case erwähnt wurde, stellen nicht-vertrauenswürdige Server, wie Cloud-Dienste, oder Mobilgeräte, die die Sprachbefehle verarbeiten auch ein erhebliches Risiko dar. Zudem sehen wir potenzielle Externe Angreifer, die auf remote geteilte Inhalte zugreifen können, wie z. B. Navigationszielen.

Für das Kriterium Aspekt haben wir die Identität der Person, die das Fahrzeug fährt, als Sekundärziel eingeschätzt. Das eine Person, ein Auto fährt ist erstmal nicht schützenswert. Die Identität wird besonders in den Use Cases außerhalb des Fahrzeugs relevant beim Teilen von Daten mit anderen Entitäten. Innerhalb des Fahrzeugs sind vor allem Inhalte, die im Fahrzeug übertragen und gespeichert werden, wie zum Beispiel Kontaktdaten aus dem Smartphone und Audioaufnahmen relevant. Zu den Inhalten gehören auch das geistige Eigentum des OEM. Zusätzlich ist das Fahrverhalten zum Beispiel für Versicherungsfirmen interessant, oder die Fahrtenhistorie für Familienangehörige.

Das Ziel für PETs innerhalb von Fahrzeugen sollte daher vor allem der Schutz der Vertraulichkeit sein für das geistige Eigentum des OEM, und sensible Daten, die im Infotainment und Telematik Bereich geteilt werden. Außerhalb des Fahrzeugs wäre bei der Kommunikation von sensiblen Fahrverhaltensdaten an eine externe Identität das Ziel der Ununterscheidbarkeit bedeutend.

Im Automotive Sektor ist die Verbreitung symmetrischer Verschlüsselung (z. B. MACsec, SecOC und Speicherverschlüsselung) weit bekannt und standardisiert z. B. nach AUTOSAR. Daher bieten sich PETs an, die ebenso symmetrische Verschlüsselungsprimitive verwenden. Perfekte Informationstheoretische Verschlüsselungen sind, wie in den meisten Use Cases, eher hinderlich, daher ist das Sicherheitsmodell "Computational", welches eine angemessene Sicherheitsstufe darstellt.

Im Fahrzeug müssen alle drei Daten Dimensionen geschützt werden. Gespeicherte Daten zum Beispiel in den Datenbanken des Infotainments und auch geistigen Eigentums; Übertragene Daten zwischen zwei Steuergeräten, die sensible Informationen enthalten; und Verarbeitete Daten, die zum Beispiel aus der Verarbeitung sensibler Daten im Infotainment Bereich resultieren.

Für den Use Case des Schutzes der Datenströme innerhalb von Fahrzeugnetzwerken, ist keine Vertrauenswürdige Drittpartei relevant.

Für die letzte Anforderung, Umkehrbarkeit, sehen wir keine Notwendigkeit, dass die Partei, die verschlüsselt zum Entschlüsseln mit einbezogen werden soll, daher ist keine Kooperation

erforderlich. In einigen Bereichen muss jedoch gewährleistet werden, dass zum Beispiel bei dem Einsatz symmetrischer Verschlüsselungsverfahren, dieses vollständig von der empfangenden Partei wieder entschlüsselt werden kann.

Die Anwendung des Privacy-Frameworks von Heurix et al. auf unseren Use Case 2.1.4.1, hat dazu beigetragen Anforderungen an die Privacy Enhancing Technologies zu stellen, die innerhalb eines Fahrzeugnetzwerks eingesetzt werden können. Das Herzstück des Frameworks ist eine Tabelle, die PETs zu den Anforderungen zuordnet. Diese ist allerdings nicht vollständig, da wichtige PETs, wie z. B. Homomorphic Encryption, oder Trusted Execution Environments fehlen und zudem enthält sie fast ausschließlich alte Publikationen. Zudem lässt sich für einen so breiten Use Case schwer bestimmen welche PETs für einen vollumfänglichen Schutz sorgen würden. Allerdings kann festgehalten werden, dass Secure Multi Party Computation (SMPC) (z. B. n-Server PIR, 1/2 OT, 1-n OT) eine potenziell passende Technologie wäre für viele der gestellten Anforderungen, wie dem Vertraulichkeitsschutz der übertragenen Inhalte und Ununterscheidbarkeit von übertragenen Fahrverhaltensdaten. Für Gespeicherte Daten fehlen die Alternativen zu der Disc Encryption, um diese auf den Use Case anzuwenden. Dasselbe gilt für die Übertragung der Daten innerhalb des Fahrzeugs. Hier wurden von dem Framework keine ausreichenden Vorschläge geliefert.

2.1.4.3 Zusammenfassung

Unsere erste Forschungsfrage lautete: Welche Arten von Daten werden von intelligenten Fahrzeugen verarbeitet, die als vertraulich betrachtet werden sollten? Um diese Frage zu beantworten, klassifizierten wir im ersten Schritt unseres Frameworks typischer In-vehicle-Daten aus den verschiedenen Domänen danach, ob sie eine direkte oder indirekte Zuordnung zu Personen ermöglichen. Die Analyse zeigte, dass Daten aus den Domänen Infotainment und Telematik-Domänen direkte persönliche Informationen offenlegen können, aber auch indirekte. Im Gegensatz dazu enthalten Daten aus Domänen wie Antriebsstrang oder Fahrzeugsicherheit in der Regel nur indirekt zuordbare persönliche Informationen. Wenn diese über einen längeren Zeitverlauf beobachtet werden können, oder mit anderen Datenquellen (wie der Fahrzeugs-ID oder den Standortdaten) verknüpft werden können, können ihre Datenpunkte identifizierbar werden. Aus diesem Grund sollten sie ebenfalls als vertraulich behandelt werden.

Die zweite Forschungsfrage lautete: Wie kann die Vertraulichkeit von In-vehicle-Daten mithilfe strukturierter Kriterien bewertet werden? Diese Frage wird im zweiten Schritt des Frameworks adressiert, die vier Risikofaktoren nutzt, um die Risikohöhe und Kritikalität jeder Datengruppe zu bewerten. Die Ergebnisse zeigen klare Unterschiede über ECU-Domänen hinweg. Daten aus den Domänen Antriebsstrang, Fahrzeugsicherheit sowie Komfort erhielten aufgrund begrenzter Identifizierbarkeit und geringer Sensitivität einen niedrigen Gesamt-Risikowert von 2. Im Gegensatz dazu schnitten Daten aus Infotainment- (Gesamt-Risikowert: 7) und Telematik (Gesamt-Risikowert: 6) -Domänen deutlich höher ab, da sie oft persönliche Identifikatoren, Verhaltensmuster und besondere Kategorien von Daten gemäß GDPR enthalten.

Anschließend wurde der Use Case festgesetzt, in dem mit kritischen Daten aus dem Infotainment- und Telematikbereich von In-Vehicular Networks (IVNs) geschützt werden sollen. Das kritischste Beispiel, Sprachbefehle, wurde intensiv ausgeführt.

In unserer letzten Forschungsfrage haben wir untersucht, ob die genannten Frameworks geeignet sind, um PETs für die sichere kollaborative Maschinen Werkzeug Daten Nutzung, sowie für IoT Geräte in Privatsphäre schützenden Smart Buildings und für die sichere Netzwerkkommunikation innerhalb von autonomen Fahrzeugen, abzuleiten. Am Beispiel des Frameworks von Heurix et al.

auf unseren automotive Use Case, wurde demonstriert, dass es zwar möglich ist, Anforderungen abzuleiten, diese jedoch sehr generisch sind und schwer zuzuordnen zu den dort aufgeführten PETs, da diese teilweise veraltet und unvollständig sind. Jedoch ließ sich SMPC als potentiell passende Möglichkeit für die Kommunikation mit anderen Entitäten ableiten, da damit viele unserer identifizierten Anforderungen abgedeckt werden konnten.

Durch die Anwendung weiterer Privacy Frameworks und ganzheitliche Betrachtung weiterer Literatur könnten der Einsatz von PETs in den erwähnten Use Cases in Future Work noch weiter eingeschränkt werden. Unser Privacy Framework zur Identifikation besonders kritischer Daten in den unterschiedlichen Fahrzeug-Domänen bietet eine ausschließlich statische Sicht auf Vertraulichkeitsrisiken. Aktuelle Arbeiten von Grimm et al. [171] deuten darauf hin, dass Vertraulichkeitsrisiken in Fahrzeugen nicht feststehen, sondern sich je nach Fahrkontext, Nutzeraktivität und Umweltfaktoren ändern können. Zukünftige Forschung könnte das Framework dynamischer und kontextbewusster gestalten. Weitere mögliche Erweiterungen umfassen die Validierung des Scoring-Systems mit realen Daten, die Einbindung von Branchenexperten bei der Verfeinerung der Risikofaktoren und die Erweiterung des Modells, um Verfügbarkeits- und Integritätsrisiken zusätzlich zur Vertraulichkeit zu berücksichtigen. Insgesamt bietet diese Arbeit einen strukturierten Weg zur Bewertung von Vertraulichkeitsrisiken in vernetzten Fahrzeugen und dient als Grundlage für zukünftige Forschung und Entwicklung in diesem Bereich.

2.1.5 Einschätzung zu den Auswirkungen des EU AI Act auf ATLAS-L4

Im Rahmen dieses Arbeitsschritts wurde eine Analyse der aktuellen maschinellen Lernverfahren und infrastrukturellen Voraussetzungen für das automatisierte Fahren auf Level 4 durchgeführt. Dabei lag der Fokus darauf, wie die neuen Regularien des EU AI Act den Einsatz dieser Technologien beeinflussen und welche Anpassungen möglicherweise erforderlich sind, um eine rechtskonforme Umsetzung sicherzustellen. Insbesondere wurden die Anforderungen an Risikomanagement, Datenverwaltung, Protokollierung, Transparenz und Sicherheit untersucht, da diese essenzielle Aspekte darstellen, um hochautomatisierte Fahrzeugsystemen nach dem EU AI Act konform zu betreiben.

Ein zentraler Bestandteil der Analyse war die Identifikation der spezifischen Artikel des EU AI Act, die für das ATLAS-L4-Projekt von Relevanz sind. Dazu gehörte beispielsweise die Einordnung von Level-4-Fahrfunktionen als Hochrisiko-KI-System, wodurch besondere Anforderungen an die technische Robustheit und die Nachvollziehbarkeit der Entscheidungsprozesse gestellt werden. Zudem wurde überprüft, inwiefern bestehende Sicherheits- und Datenschutzmaßnahmen des Projekts den regulatorischen Anforderungen entsprechen oder ob zusätzliche Maßnahmen erforderlich sind.

Basierend auf den gewonnenen Erkenntnissen wurden abschließend konkrete Handlungsempfehlungen formuliert, um eine EU AI Act-konforme Umsetzung zu gewährleisten. Dazu zählen unter anderem mögliche Anpassungen der Trainings- und Evaluationsverfahren der zugrunde liegenden ML-Modelle sowie ergänzende Dokumentations- und Testverfahren, um die geforderte Transparenz und Nachvollziehbarkeit sicherzustellen.

2.1.5.1 Klassifizierung der Systeme

Die im Lkw eingesetzten KI-Systeme sind gemäß Artikel 6 Absatz 1 des EU AI Act als Hochrisiko-Systeme einzustufen. Der EU AI Act definiert Sicherheitskomponenten, die unter eine in Anhang I genannte Verordnung fallen und einer Konformitätsbewertung durch Dritte unterliegen, als

Hochrisiko-Systeme. Dies trifft insbesondere auf automatisierte und vollautomatisierte Fahrzeuge zu, die in der in Anhang I aufgeführten Verordnung zur Typenzulassung [67] geregelt sind. Besonders hervorzuheben ist Artikel 11 dieser Verordnung, der spezifische Anforderungen an automatisierte und vollautomatisierte Fahrzeuge festlegt. Diese Anforderungen bestätigen die Einstufung der KI-Systeme im Lkw als sicherheitskritisch und damit als Hochrisiko. Das Control Center wird hier als Teil des KI-Systems der nach L4 autonom fahrenden Lkw verstanden, da es für Aufgaben wie Überwachung und Teleoperation, menschliches Eingreifen ermöglicht und somit relevant für aus dem EU AI Act resultierenden Pflichten ist. Insgesamt ergibt sich aus der Hochrisiko-Einstufung sowohl der Fahrzeug- als auch der Control Centers-KI-Systeme eine Reihe von Pflichten, welche durch den EU AI Act definiert werden. Im folgenden Abschnitt werden wir diese näher erörtern.

2.1.5.2 Resultierende Pflichten

Die Hochrisiko-Einstufung der im Fahrzeug und im Control Center eingesetzten KI-Systeme führt zu spezifischen Anforderungen an das System sowie zu Verpflichtungen für dessen Anbieter und Betreiber, wie sie im EU AI Act festgelegt sind. Wir betrachten hier die folgenden, welche nach unserer Einschätzung besonders relevant für ATLAS-L4 sind:

- die Einführung und Umsetzung eines Risikomanagementsystems (Artikel 9),
- Praktiken zur Daten- und Datenverwaltungsstrategie (Artikel 10),
- automatische Aufzeichnung und Protokollierung mit definierten Mindestaufbewahrungszeiten (Artikel 12, 19, 26),
- Transparenz- und Interpretierbarkeitsanforderungen (Artikel 14),
- Mindeststandards für Genauigkeit, Robustheit und Cybersicherheit (Artikel 15).

Im Folgenden werden wir diese besonders relevanten Artikel des EU AI Act zusammenfassen, wobei wir uns auf die Anforderungen an Hochrisiko-KI Systeme konzentrieren. Dies bildet die Grundlage, um im folgenden Abschnitt eine Einschätzung abgeben zu können, welche Auswirkungen der EU AI Act für das Projekt in Bezug auf die Lkw- und Control Centers-Komponenten haben können.

Risiko Management. Aufgrund des risikobasierten Ansatzes des EU AI Act nimmt das Risikomanagement der Hochrisiko-KI Systeme im EU AI Act eine zentrale Rolle ein. Auf Basis von Artikel 9¹⁴ muss für jedes Hochrisiko-KI-System ein **Risiko-Management System** erstellt und durch den gesamten Lebenszyklus hinweg gewartet und regelmäßig aktualisiert werden. Hierdurch sollen Risiken identifiziert und analysiert werden, wie sie aus dem KI-System für die Gesundheit, Sicherheit oder Grundrechte von Menschen entstehen können. Dies findet einerseits im Rahmen der Ordnungsgemäßen Nutzung des KI-Systems, sowie von absehbarem Missbrauch statt. Weiter soll das Risikomanagement System die Möglichkeit geben, weitere Risiken aufgrund der im Post-Market Monitoring (Artikel 72, hier nicht weiter betrachtet) anfallenden Daten zu Evaluieren. Aufgrund der Analysierten Risiken werden im Anschluss angemessene Methoden eingeführt werden, um diese zu mittigeren. Im Rahmen des Risikomanagements müssen Hochrisiko-KI-Systeme während ihrer gesamten Lebensdauer sowohl unter Labor- als auch Realbedingungen getestet werden, um die angemessenen Maßnahmen bestimmen. Dafür sollen a priori geeignete Test-Metriken definiert werden, welche zur Evaluation des Risikomanagement Systems dienen sollen. Für

¹⁴ <https://artificialintelligenceact.eu/article/9/>

Projekte, für welche bereits ein Risiko-Management nach anderer Gesetzgebung gefordert ist, kann hier geforderte Risiko-Management mit diesem kombiniert werden.

Daten Management. Artikel 10¹⁵ besagt, dass Hochrisiko-KI-Systeme mit hochwertigen Datensätzen für das Training, Validierung und Testen entwickelt werden müssen. Hierbei sollten diese möglichst repräsentativ, fehlerfrei und vollständig sein. Dafür sollen angemessene **Daten-Management-Praktiken** eingeführt werden, welche Daten auch auf mögliche Verzerrungen (Bias) untersuchen, um Sicherheitsrisiken oder Diskriminierung zu verhindern. Für die Verwendung personenbezogener in Trainingsdatensätzen bestehen zudem erhöhte Auflagen, wie es auch schon nach DSGVO der Fall ist.

Protokollierung. In Artikel 12¹⁶ wird explizit eine **automatisierte Protokollführung** von implementierten KI-Systemen gefordert. Dies bedeutet für selbstfahrende Lkws eine Aufzeichnung der gesamten Lebensdauer, um potenziell im Nachhinein Risikosituationen besser aufarbeiten zu können (Paragraf 2). Artikel 19¹⁷ weist darauf hin, dass alle nach Artikel 12(1) genannten Protokolle mindestens für 6 Monate aufbewahrt werden müssen. Artikel 26¹⁸ fordert darüber hinaus, dass Betreiber Hochrisiko-KI-Systeme kontinuierlich überwachen und bei identifizierten Risiken unverzüglich Anbieter und Behörden informieren. Zudem sind sie verpflichtet, sicherzustellen, dass Eingabedaten relevant sind, und Mitarbeiter vor der Nutzung entsprechend zu schulen.

Transparenz und Menschliche Aufsicht. Artikel 13¹⁹ legt Bestimmungen bezüglich Transparenz und Interpretierbarkeit für Hochrisiko-KI-Systeme fest. Diese können zu einem großen Teil durch eine zur Verfügung gestellte Anleitung umgesetzt werden, die unter anderem Angaben zu Metriken wie Robustheit und Security des Systems enthält. Des Weiteren sollen Informationen bzgl. Erzeugung des ML Modells sowie Input- und Outputdaten gegeben werden.

Artikel 14²⁰ ergänzt diese Anforderungen explizit um die Möglichkeiten zur Menschliche Aufsicht. Er besagt, dass Hochrisiko-KI-Systeme so gestaltet sein müssen, dass Menschen sie effektiv überwachen können mit dem Ziel, Risiken für Gesundheit, Sicherheit oder Grundrechte, die durch die Nutzung dieser Systeme entstehen könnten, zu verhindern oder zu minimieren. Die Überwachungsmaßnahmen sollten an die Risiken und den Nutzungskontext des KI-Systems angepasst sein. Diese Maßnahmen können entweder vom Anbieter in das System integriert oder vom Nutzer umgesetzt werden. Das KI-System sollte so bereitgestellt werden, dass die Überwachenden dessen Fähigkeiten und Grenzen verstehen, Probleme erkennen und beheben, und jederzeit in das System eingreifen können.

Genauigkeit, Sicherheit, Robustheit. In Artikel 15²¹ ist festgehalten das Hochrisiko-KI-Systeme konsistent über ihre Lebenszeit akkurat, robust und sicher laufen. Hierfür wird momentan an relevanten Metriken gearbeitet, mit denen dies gemessen werden kann. Die Anforderungen an Sicherheit gegenüber Einfluss durch Dritte bedeuten nach unserem Verständnis im Kontext von Machine Learning, dass Gegenmaßnahmen zu Angriffen wie Data bzw. Modell Poisoning oder Adversarial Examples getroffen werden müssen.

¹⁵ <https://artificialintelligenceact.eu/article/10/>

¹⁶ <https://artificialintelligenceact.eu/article/12/>

¹⁷ <https://artificialintelligenceact.eu/article/19/>

¹⁸ <https://artificialintelligenceact.eu/article/26/>

¹⁹ <https://artificialintelligenceact.eu/article/13/>

²⁰ <https://artificialintelligenceact.eu/article/14/>

²¹ <https://artificialintelligenceact.eu/article/15/>

Zusammengefasst ist für eine dem EU AI Act konforme Implementation der ATLAS-L4 Systeme somit sicherzustellen, dass entsprechende Risikomanagementsysteme, Datenverwaltung, Protokollierung und Transparenz gegeben sind. Hier gilt es diese Maßnahmen auch für die Endnutzer verständlich zu kommunizieren und diese in ihrer Nutzung zu schulen. Wir diskutieren im nächsten Abschnitt, inwiefern dies auf Grundlage der uns zugänglichen Dokumente schon erfüllt ist, und empfehlen gegebenenfalls weitere mögliche Maßnahmen.

2.1.5.3 Handlungsempfehlungen für eine EU AI Act-konforme Umsetzung

Risiko Management. Durch das Fraunhofer AISEC wurden Risikoanalysen für das Automated Driving System des Lkw sowie das Control Center erstellt, wobei die analysierten Bedrohungen vom STRIDE Modell abgeleitet wurden. Die Analyse geschieht somit aus einer Security-Perspektive, die beleuchteten Schadensfälle behandeln jedoch auch Safety, Privatsphäre und finanzielle sowie operative Schäden. Die vorliegenden Risikoanalysen decken größtenteils die Anforderungen des EU AI Act abdecken, wobei jedoch nach unserer Einschätzung genauer auf KI-Komponenten des Automated Driving Systems eingegangen werden sollte. So werden Risiken wie gezielte Angriffe auf KI-Systeme (wie adversarial attacks) oder Probleme, wie sie sich aus mangelnder Robustheit des Systems gegenüber Eingabedaten oder mangelnder Fairness des Trainingsdatensatzes ergeben, nach unserem Verständnis nicht ausreichend behandelt. Diese Angriffe sollten bei künftigen Risikoanalysen, die für einen konkreteren und fortgeschritteneren Stand eines autonomen Lkw erstellt werden, zusätzlich berücksichtigt werden.

Der EU AI Act ist bereits am 1. August 2024 in Kraft getreten, ab Februar 2025 werden die ersten Bestimmungen für Unternehmen verpflichten - die Regulierung von "Hochrisiko-KI" soll voraussichtlich im Sommer 2026 folgen. Da das Risikomanagement ein zentrales Element des EU AI Act ist, scheint essenziell bereits jetzt mit den Vorbereitungen für die Compliance zu beginnen, um eine reibungslose Umsetzung der Vorgaben sicherzustellen.

Daten-Management. Praktiken für das Management von Trainingsdaten ergeben sich aus best-practices und der Forschung zu Machine Learning, welche im ATLAS-L4-Projekt zur Anwendung kommen können. So bestehen Methoden, die Fairness eines Datensatzes und im Modell bestehender Bias zu messen. Nach EU AI Act ist der Schutz von personenbezogenen Daten ebenso relevant. Durch Effekte wie Memoisation können sich diese in trainierten KI-Modellen wiederfinden und unter anderem Risiken für Robustheit, Bias und Privatsphäre darstellen. Hier können Methoden wie Differential Privacy Abhilfe schaffen, welche während des Trainings der ML Modelle eingesetzt werden. Zudem bestehen Methoden, um Bias oder Privatsphärerisiken von bestehenden Modellen zu untersuchen.

Protokollierung. Wir sehen die Anforderungen an die Protokollierung durch die Datenspeicherung im Lkw sowie im zu Teil im Control Center zum großen Teil erfüllt. Es sollte darauf geachtet werden, dass sich das Verhalten der im Automated Driving System verwendeten Modelle bzgl. Ein- und Ausgabe aus den Protokolldaten rekonstruieren lässt. Zudem muss der Zeitraum von 6 Monaten zur Speicherung aller Protokolldaten eingehalten werden. Es erfordert jedoch der Überprüfung, inwiefern möglicherweise aufgezeichnete sensible Daten wie menschliche Gesichter oder Nummernschilder Privatsphärerisiken mit sich bringen. Dies gilt sowohl für die in den Lkw sowie auch in der Datenbank im Control Center gesammelten Protokolldaten. Das Erkennen und Entfernen von personenbezogenen Daten kann hier eine Möglichkeit darstellen, um diesen Risiken entgegenzuwirken.

Transparenz und Menschliche Aufsicht. Mit einem Handbuch, basierend auf der laufend im Projekt zu erstellenden Dokumentation können große Teile der Anforderungen abgedeckt werden, welche der EU AI Act mit Artikel 13 an die Transparenz von Hochrisiko-KI-Systemen stellt. Nach unserem Verständnis sollen die Möglichkeiten zur Menschlichen Aufsicht und Kontrolle, wie sie nach Artikel 14 des EU AI Act gefordert sind, im Projekt nach Ablauf der Erprobungsphasen durch das Control Center umgesetzt werden. Die geplante Überwachung und die Möglichkeit zur Teleoperation scheinen sinnvoll. Wir empfehlen zusätzlich Modellerweiterungen, welche die Entscheidungen der KI-Systeme verständlich für die Aufsichtsperson kommuniziert. Explainable AI, ein sehr aktives Forschungsfeld, beinhaltet viele mögliche Techniken, in denen unterschiedlichste Netzwerkstrukturen so erweitert werden, dass deren Entscheidungen nachvollziehbar demonstriert und visualisiert werden können.

Genauigkeit, Sicherheit, Robustheit. Bei der Entwicklung des Automated Driving Systems, insbesondere beim Testen der ML Modelle, sollte ein Augenmerk auf Genauigkeit und Robustheit gegenüber erwartetem und unerwartetem Input gelegt werden. Hierdurch besteht die, dass sich aussagefähige Angaben zur Genauigkeit und Robustheit des KI-Systems bereits aus dem Entwicklungsprozess ergeben. Diese können anschließend durch Testfahrten überprüft werden, in welchem das System potenziell in neue (Gefahren-) Szenarien (out-of-distribution) gebracht wird, um zu analysieren, zu welche Entscheidungen dies führt und wie es zu dem Entscheidungsprozess gekommen ist (Explainable AI). Die Sicherheit des KI-Systems kann durch gezielte Maßnahmen gegen Angriffe auf KI erhöht werden. Hier kann zum Beispiel Adversarial Training gegen die Bedrohung durch Adversarial Attacks zum Einsatz kommen, wobei zu jeder Zeit die Möglichkeit von adaptiven Angriffen im Auge behalten werden muss.

2.1.5.4 Zusammenfassung der Bewertungen des EU AI Act bezüglich Innovation und Schutz der Privatsphäre

In folgendem Abschnitt fassen wir Meinungen und Kritik am EU AI Act bezüglich Innovationsförderung und Privatsphäre zusammen.

Während Konsens herrscht über die Werte, welche der EU AI Act versucht bei Implementation von KI-Produkten zu versichern, gibt es vermehrt Kritik an der konkreten Umsetzung. Sogar der Chefautor Gabriele Mazzini bemerkt, dass “die Messlatte für die Regulierung vielleicht zu hochgelegt worden ist, und somit Unternehmen in Europa nicht genug Rechtssicherheit gibt”. In der Tat sind viele Unternehmen unsicher, ob sie vom EU AI Act betroffen sind oder nicht. Diese Unsicherheit verbunden mit potenziell sehr hohen Compliance/Straf-Kosten könnte die Innovationskraft und Produktivität europäischer Unternehmen beeinträchtigen, während internationale Konkurrenz Vorteile behält. Die Einhaltung der Anforderungen für ein Hochrisiko-KI-Produkt kann ein mittelständisches Unternehmen mit 50 Mitarbeitern zwischen 159.000 und 319.000 Euro kosten. Verstöße werden mit Strafen von bis zu 35 Millionen Euro oder sieben Prozent des globalen Umsatzes geahndet. Zudem herrsche Unsicherheit, dass die Liste der Hochrisikoanwendungen erweitert wird.

Ebenfalls häufige Kritik bezieht sich auf die Kategorisierung in unterschiedliche Risikostufen und die davon abhängige und oft sehr unterschiedlichen Anforderungen. Hier wird oft auf andere Länder wie die USA, Großbritannien und Japan verwiesen, welche flexiblere Regulierungs-Ansätze verfolgen, in welchen bestehende Gesetze für die Regulierung von KI ausgeweitet werden. Kritiker schlagen vor, sich bei der Regulierung auf Ergebnisse und Verbote zu konzentrieren, anstatt zu versuchen, zulässige KI-Anwendungen zu definieren. Durch den Versuch, risikoreiche

Anwendungen starr zu definieren, besteht die Gefahr, dass das EU-KI-Gesetz veraltet oder unwirksam wird, wenn sich KI weiterentwickelt.

Eine weitere Kritik an der Zukunftsfähigkeit des EU AI Act verweist auf die Pflicht zu menschlicher Aufsicht. Während diese Forderung sehr nachvollziehbar ist, insbesondere um KI-Entscheidungen im Nachhinein zur Rechenschaft zu ziehen, wird sie vermutlich an ihre Grenzen stoßen, sobald die KI den Menschen bei der Entscheidungsfindung übertrifft.

Der KI-Bundesverband, ein Zusammenschluss aus über 400 deutschen KI-Unternehmen und Expert:innen, geht in seiner Kritik so weit, dass er als Auswirkung des EU AI Act in seiner aktuellen Form einen signifikanten Wettbewerbsnachteil gegenüber den USA und China zuschreibt. Der Verband fordert den Ausschluss von General Purpose AI (GPAI) und Large Language Models (LLMs) aus der pauschalen Einstufung als Hochrisiko-KI, die Überprüfung der aktuellen Anforderungen zur Klassifizierung von Hochrisiko-KI-Systemen, Maßnahmen zum Schutz und zur Förderung europäischer Investitionen in LLMs und multimodaler KI-Systeme und die Klarstellung unklarer oder fehlender Definitionen, um Rechtsunsicherheit zu vermeiden.

Hinsichtlich des Schutzes der Privatsphäre gibt der EU AI Act in seiner Implementation einige mögliche Angriffspunkten. Die Forderung nach Protokollierung und Datenspeicherung für 6 Monate nach Artikel 19 muss angemessen umgesetzt werden, damit die Privatsphäre der Trainingsdaten des Modells sowie die Inferenzdaten, im Falle von ATLAS-L4 die Daten des fahrenden Lkw, gut vor möglichen Angriffen geschützt werden. Hier empfehlen sich wie oben schon genannt Methoden der Datenverschlüsselung sowie Differential Privacy beim Training der Modelle.

Zusammengefasst wird dem EU AI Act die richtige Absicht zugeschrieben, jedoch in seiner Umsetzung Kritik bezüglich Auswirkung auf Innovation und Privatsphäre ausgesprochen. Welche Auswirkungen der EU AI Act auf das europäische KI-Ökosystem haben wird, wird sich sehr bald herausstellen, da erste Regelungen schon im Februar 2025 in Kraft treten werden.

2.1.6 Sicherheit vernetzter Fahrzeugtechnologien im Nutzfahrzeugsektor

2.1.6.1 V2V/V2X

Aktuelle Lösungen für Sicherheit in V2X

Kryptografische Sicherheit im V2X-Bereich ist aus mehreren Gründen unerlässlich. Zunächst gewährleistet sie den Datenschutz, indem sichergestellt wird, dass persönliche Informationen der Nutzer geschützt sind und nicht unbefugt abgerufen werden können. Darüber hinaus spielen die Authentifizierung und Integrität der übertragenen Nachrichten eine wichtige Rolle, um sicherzustellen, dass die kommunizierenden Fahrzeuge und andere Entitäten authentisch sind und nicht manipuliert werden können. Ein weiterer wichtiger Aspekt ist der Schutz vor Cyberangriffen, wie z. B. Spoofing oder Denial-of-Service Attacken, die die Sicherheit und den Betrieb des Verkehrssystems gefährden könnten. Letztlich trägt die kryptographische Sicherheit dazu bei, Vertrauen in V2X-Technologien zu fördern, was entscheidend für deren Akzeptanz und Einsatz ist.

Um V2X-Kommunikation kryptografisch abzusichern, ist der gängige Ansatz die Verwendung asymmetrischer Kryptographie unter Verwendung einer Public Key Infrastructure (PKI) zur Verwaltung von Credentials. Eine PKI ermöglicht den sicheren Austausch von Nachrichten über das verwendete Netzwerk. Jedes Fahrzeug erhält ein asymmetrisches Schlüsselpaar und ein Zertifikat. Das Zertifikat enthält den öffentlichen Schlüssel mit V2X-spezifischen Attributen wie einer ID und

ist von der Certificate Authority (CA) signiert – auf diese Weise werden Fahrzeuge als gültige V2X-Teilnehmer registriert.

Im Folgenden werden aktuelle Sicherheitslösungen im V2X Bereich beschreiben. Dabei liegt der Fokus auf dem IEEE Standard 1609, der momentan am meisten verbreitet und in Verwendung ist [81]. Der IEEE Standard 1609.2 [79] beschreibt mit Wireless Access in Vehicular Environments (WAVE) ein Kommunikationsprotokollstack, der für den Einsatz in Fahrzeugen optimiert ist. Dabei werden neben dem üblichen Protokollstack für Daten eine Reihe von Sicherheitsdiensten definiert, den sogenannten WAVE Security Services, vergleiche Abbildung 17.

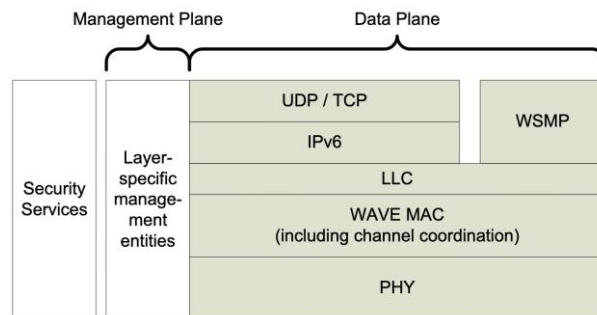


Abbildung 17: Darstellung des WAVE Referenzmodells mit den Security Services, die sich über den gesamten Stack erstrecken. Quelle: [79].

Die WAVE Security Services können in zwei Dienste eingeteilt werden, die WAVE Internal Security Services und die WAVE Higher Layer Security Services. Die WAVE Internal Security Services umfassen zwei Hauptdienste: den Secure Data Service (SDS) und das Sicherheitsmanagement. Der SDS transformiert unsichere Protokoll Daten-Einheiten (PDUs) in Sicherheitsdienst-Protokoll Daten-Einheiten (SPDUs), die zwischen kommunizierenden Entitäten übertragen werden. Entitäten, die den SDS verwenden, werden als Secure Data Exchange Entities (SDEEs) bezeichnet. Das Sicherheitsmanagement umfasst die Verwaltung von Informationen über Zertifikate, um die Sicherheitsprozesse zu unterstützen. Die WAVE Higher Layer Security Services umfassen Zertifikatsmanagementaufgaben auf einer übergeordneten Ebene. Dazu gehören die Validierung von Zertifikatswiderrufslisten (Certificate Revocation Lists, CRLs) und die peer-to-peer Zertifikatsverteilung (P2PCD).

Um eine gesicherte Kommunikation durch die WAVE Security Services zu realisieren, empfiehlt der IEEE Standard die Verwendung der folgenden kryptografischen Komponenten als Grundlage:

- für digitale Signaturen den Elliptic Curve Digital Signature Standard (ECDSA),
- für asymmetrische Verschlüsselung das Elliptic Curve Integrated Encryption Scheme (ECIES),
- für symmetrische authentifizierte Verschlüsselung den Advanced Encryption Standard im CCM-Modus (AES-CCM).

Im Folgenden wird kurz auf die Verwendung der einzelnen kryptografischen Primitive eingegangen.

ECDSA wird hauptsächlich für die Signierung von SPDUs verwendet. ECDSA bietet Authentifizierung, Integrität und Nicht-Abstreitbarkeit, indem es sicherstellt, dass die signierten Daten von einem legitimen Sender stammen und nicht nach der Signierung verändert wurden. Der Standard definiert spezifische elliptische Kurven, die für ECDSA verwendet werden können, wie NIST P-256 und NIST P-384, sowie die entsprechenden Hash-Algorithmen (SHA-256 und SHA-384).

Um symmetrische Schlüssel auszutauschen, wird in IEEE 1609.2 das hybride Verfahren ECIES eingesetzt. ECIES ist ein Verfahren, das elliptische Kurven nutzt, um einen symmetrischen Schlüssel für die Verschlüsselung von Daten zu generieren und sicher zu übertragen. Dabei wird ein gemeinsames Geheimnis aus den öffentlichen Schlüsseln generiert, aus welchem dann ein gemeinsamer symmetrischer Schlüssel erzeugt wird, der zur weiteren Datenverschlüsselung verwendet wird. Im Kontext von V2X wird ECIES ausschließlich zur Übertragung von symmetrischen Schlüsseln verwendet und nicht direkt für die Verschlüsselung von anderen Daten. Der Standard unterstützt zwei elliptische Kurven, NIST P-256 und brainpoolP256r1, die für die ECIES-Verschlüsselung verwendet werden. Während des Verschlüsselungsprozesses wird ein geheimer Wert abgeleitet, der aus dem elliptischen Kurven-Diffie-Hellman-Protokoll stammt. Der symmetrische Schlüssel wird dann unter Verwendung einer Stream-Cipher parametrisiert durch eine spezifische Hashfunktion verschlüsselt. Als asymmetrische Verschlüsselung wird auch zusätzlich noch der chinesische Standard SM2, definiert in GB/T 32918.4-2016 und GB/T 32918.5-2017, unterstützt.

Für die symmetrische Verschlüsselung von Daten wird der Advanced Encryption Standard (AES) mit 128-bit Schlüsseln (AES-128) im Counter Mode mit Cipher Block Chaining Message Authentication Code (CCM) verwendet (AES-128-CCM). Dieser Modus kombiniert die Verschlüsselung mit einer Nachrichtenauthentifizierung, um die Integrität und Authentizität der Daten sicherzustellen. Es wird außerdem der chinesische Standard für symmetrische Verschlüsselung unterstützt, SM4 (GB/T 32918.4-2016).

PQ-Crypto in V2X

Wie im vorherigen Absatz beschrieben wurde, verwenden V2X Protokolle kryptografische Algorithmen, um vielfältige Sicherheitsziele im Automotive-Bereich zu erreichen. Aber vor allem die Sicherheit asymmetrischer Verfahren, die auf den Problemen des Faktorisierens und des Lösen des diskreten Logarithmus beruhen, sind durch den Einsatz zukünftiger Quantencomputer gefährdet. Hier setzt die sogenannte Post-Quanten-Kryptografie (PQC) an, bei der kryptografische Primitive entwickelt werden, die Schutz gegen zukünftige Quantencomputerangriffe bieten. Die heutigen Standards im V2X-Bereich sind noch nicht auf den Einsatz von PQC-Algorithmen vorbereitet. Im Folgenden werden aktuelle Bemühungen vorgestellt, die bereits jetzt den Einsatz von PQC im V2X-Bereich untersuchen.

PQC-Implementierungen auf dem AURIX-Mikrocontroller

Der AURIX-Mikrocontroller ist eine Familie von Hochleistungs-Mikrocontrollern, die von der Infineon Technologies entwickelt wurde. Diese Mikrocontroller sind speziell für sicherheitskritische Anwendungen in der Automobil- und Industrieelektronik konzipiert. Sie bieten mehrere Kerne, integrierte Sicherheitsfunktionen, Echtzeitverarbeitung und hohe Rechenleistung, um komplexe Steuerungs- und Regelungsaufgaben zu bewältigen. AURIX-Mikrocontroller unterstützen auch Funktionen wie Fahrzeugkommunikation, Motorsteuerung und Fahrerassistenzsysteme. Sie erreichen zudem das höchste Sicherheitsniveau (ASIL-D) und erlauben die Einhaltung der Norm ISO26262.

In [172] stellen Fritzmann et al. die erste Implementierung des Post-Quantum-Protokolls NewHope auf einem AURIX-Mikrocontroller vor. Als Ausgangspunkt für die Implementierung haben die Autoren die optimierte Referenzimplementierung der bei der NIST eingereichten NewHope-Version verwendet. Konkret haben diese NewHope im CPA-Modus mit der stärksten Sicherheitsstufe (NewHope1024CPA) ausgewählt. Die Autoren haben NewHope auf dem AURIX

Mikrocontroller durch mehrere Optimierungstechniken verbessert. Hier sind die wichtigsten Ansätze:

- **Datenverlagerung:** Häufig genutzte Variablen und Datenstrukturen wurden in schnelleren Speicher (Data Scratchpad RAM, DSPR) verlagert, um die Zugriffszeiten zu minimieren.
- **Inline-Assembly:** Durch Verwendung von Inline-Assembly konnten kritische Operationen auf der Assemblerebene optimiert werden, was die Effizienz steigerte.
- **Schleifenentfaltung:** Die Entfaltung von Schleifen reduzierte die Anzahl der Iterationen und verbesserte die Ausführungsgeschwindigkeit.
- **Schnellere arithmetische Operationen:** Die Autoren ersetzten komplexe arithmetische Berechnungen durch schnellere Alternativen, wie das Verschieben von Bits anstelle von Multiplikation oder Division.
- **Profiling:** Der Einsatz von Profiling-Tools wie dem TASKING Embedded Profiler half dabei, Engpässe im Code zu identifizieren und gezielte Verbesserungen vorzunehmen.

Die folgende Tabelle 10 zeigt einen Vergleich der Taktzyklusanzahl der Referenzimplementierung von NewHope1024CPA auf dem AURIX-Mikrocontroller und dem Cortex M4, sowie der durch die Autoren optimierte NewHope1024CPA-Implementierung auf dem AURIX-Mikrocontroller [172].

Insgesamt konnten die Autoren die Ausführungsgeschwindigkeit der NewHope-Implementierung um etwa 10,2% steigern. Im Vergleich zu den für den Cortex M4 angegebenen Zyklen bedeutet dies sogar eine Gesamtverbesserung von etwa 219%.

Wie Hermelink et al. [173] erläutern, ist es im Automobilbereich für konkrete Anwendungsfälle nicht ausreichend, lediglich ein gemeinsames Geheimnis für die symmetrische Verschlüsselung festzulegen, insbesondere bei Fernverbindungen für Diagnosedienste.

Tabelle 10: Taktzyklusanzahl von NewHope1024 im CPA-Modus auf AURIX und Cortex M4 [172].

Implementierung	Schlüssel-Generierung	Verkapselung/Verschlüsselung	Entkapselung/Entschlüsselung	Insgesamt
Cortex M4	2669559	3910871	163887	6744317
AURIX ref.	1249939	1819215	326294	3395448
AURIX opt.	1126265	1641684	315780	3083720

In vielen Fällen ist vorwärts gerichtete Geheimhaltung sowie eine gegenseitige Authentifizierung erforderlich, was in der Regel den Einsatz von Langzeitzertifikaten bedeutet. Daher ist es entscheidend, die Integration von NIST PQC-Primitiven in Protokolle und reale Systeme zu analysieren und die Eignung potenzieller zukünftiger Algorithmen zu prüfen. Aus diesem Grund haben Hermelink et al. in ihrer Arbeit [173] ein umfängliches authenticated key exchange (AKE) auf Basis von NewHope betrachtet. Im Allgemeinen basieren klassische AKE Protokolle auf einem Diffie-Hellman-Schlüsselaustausch, der durch eine Signatur und einen symmetrischen message authentication code (MAC) authentifiziert wird.

Wie in [173] beschrieben, ergeben sich mit der Notwendigkeit, zu Post-Quantum-AKE zu migrieren, zahlreiche Herausforderungen: Beispielsweise sind die Größen der öffentlichen Schlüssel und Signaturen, deutlich größer als bei RSA oder ECC, was zu erhöhten Latenzzeiten und Speicheranforderungen führen kann. Zudem scheinen Post-Quantum-Signaturen gegenwärtig komplexer in der Konstruktion und weniger effizient zu sein als PKEs oder KEMs. Aus diesem Grund

stellt ein vielversprechender Ansatz für einen effizienten AKE das von Guilhem et al. [174] vorgeschlagene Protokoll dar, das gezielt auf Signierungen im Protokoll verzichtet. Dieses Protokoll ermöglicht einen authentifizierten Schlüsselaustausch zwischen Geräten, indem es ein IND-CPA-gesichertes Schlüsselaustauschprotokoll, ein IND-CCA-gesichertes Verschlüsselungsprotokoll für private Schlüssel, eine symmetrische Chiffre sowie eine Hash-Funktion zur Nachrichtenauthentifizierung nutzt. Die Abbildung 18 zeigt übersichtlich die wesentlichen Protokollschritte gemäß Guilhem et al. [174].

Party U (identified by id_U)	Party V (identified by id_V)
<i>Step 1: Key Generation U</i>	
$(sk_{U,kem}, pk_{U,kem}) \leftarrow \text{KeyGenKEM}$	
$m_1 = pk_{u,kem}$	
$m_1 \leftarrow \text{Enc}_{pk_{V,pke}}(id_U m_1)$	$\xrightarrow{m_1}$ <i>Step 2: Response V</i>
	$(id_U, m_1) \leftarrow \text{Dec}_{sk_{V,pke}}(m_1)$
	$(m_2, k_V) \leftarrow \text{Encaps}_{pk_U}(m_1)$
<i>Step 3: Response U</i>	$\xleftarrow{m_2}$ $m_2 \leftarrow \text{Enc}_{pk_{U,pke}}(m_1 m_2)$
$m'_1 m_2 \leftarrow \text{Dec}_{sk_{U,pke}}(m_2)$	
If $m_1 \neq m'_1$ abort	
$k_U \leftarrow \text{Decaps}_{sk_{U,kem}}(m_2)$	
$k_{U,1} \leftarrow H_1(k_U)$	
$m_3 \leftarrow \text{Mac}_{k_{U,1}}(id_U id_V)$	$\xrightarrow{m_3}$ <i>Step 4: Final V</i>
$k_{U,final} \leftarrow H_2(k_U id_U id_V)$	$k_{V,1} \leftarrow H_1(k_V)$
	If $\text{Mac}_{k_{V,1}}(id_U id_V) \neq m_3$ abort
	$k_{V,final} \leftarrow H_2(k_V id_U id_V)$

Abbildung 18: Authenticated key exchange [174, 173].

Wie in [173] beschrieben, besitzen die beiden Parteien, U und V , langfristige Schlüsselpaare, bezeichnet als $(pk_{U,pke}, sk_{U,pke})$, und $(pk_{V,pke}, sk_{V,pke})$. Diese Schlüssel müssen auf andere Weise authentifiziert werden. Zudem sind Hash-Funktionen H_1 und H_2 sowie ein Authentifizierungsalgorithmus für Nachrichten (MAC) beteiligt. KeyGenKEM wird als nicht vorhersagbar und CPA-sicher angenommen. U beginnt den Austausch, indem es ein neues Schlüsselpaar $(sk_{U,kem}, pk_{U,kem})$ mit KeyGenKEM generiert. Danach verschlüsselt U die Konkatenation $id_U || pk_{U,kem}$ mit $pk_{V,pke}$ und sendet den resultierenden Geheimtext an V . V entschlüsselt die Nachricht mit $sk_{V,pke}$ und erhält $pk_{U,kem}$ und id_U . Anschließend verwendet V die Kapselungsmethode der KEM mit $pk_{U,kem}$, um ein gemeinsames Geheimnis k_V und eine Nachricht m_2 zu erzeugen. V verschlüsselt nun $m_2 || pk_{U,kem}$ mittels $pk_{U,pke}$ und sendet den resultierenden Geheimtext an U . U entschlüsselt den erhaltenen

Geheimtext mit $sk_{U,pke}$ und erhält $m'_1 || m_2$. Nun überprüft U ob m'_1 mit $pk_{U,kem}$ übereinstimmt. Ist dies der Fall, kann U das gemeinsame Geheimnis k_U aus m_2 entkapseln. U erstellt daraufhin mit $H_1(k_U)$ einen MAC über die Identifizierer $id_U || id_V$, sendet diesen an V und berechnet das finale gemeinsame Geheimnis als $H_2(k_U || id_U || id_V)$. V überprüft schlussendlich den erhaltenen MAC und kann im Erfolgsfall das gemeinsame geheimnis analog als $H_2(k_V || id_U || id_V)$ berechnen.

Zusammenfassend beinhalten die ersten beiden Nachrichten des Protokolls die Authentifizierung von V gegenüber U , während die zweite und dritte Nachricht U gegenüber V authentifizieren. U kennt mit hoher Wahrscheinlichkeit k_U und damit sk_U , wenn es den finalen MAC bereitstellt und der Vergleich erfolgreich ist. Um die langfristigen geheimen Schlüssel in mehreren Durchläufen zu schützen, muss das PKE gegen CCA-Angriffe gesichert sein. Für das KEM genügt CPA-Sicherheit, da in jedem Durchlauf ein neues Schlüsselpaar generiert wird.

Auf dieser Grundlage schlagen die Autoren in [173] vor, das Protokoll 3 mit NewHope1024CPA-KEM [175] für den ephemeren Schlüsselaustausch, NewHope-1024-CCA-KEM für die verschlüsselte Authentifizierung, AES256-GCM zur Datenverschlüsselung und SHA3 als MAC zu instanziiieren. Zum Schutz der PKI verwenden sie außerdem XMSS-SHA2-10256 [176] Signaturen.

In einer weiteren Arbeit [177] erweitern die Autoren Fritzmann et al. ihre vorherige Untersuchung von NewHope auf dem AURIX-Mikrocontroller [172] unter anderem um die Gitter-basierten Verfahren CRYSTAL-KYBER, Saber und NTRU. Hierbei wurde die Performanz für verschiedene Sicherheitsniveaus der NIST bewertet. Die Tabelle 11 zeigt ihre Ergebnisse [177].

Es zeigt sich, dass die CRYSTALS-KYBER-Implementierungen, insbesondere Kyber512 mit dem geringsten Sicherheitsniveau, mit einer Gesamtanzahl von 2454381 Taktzyklen relativ schnell sind und damit potenziell für V2V-Anwendungen geeignet sein könnten. Die schnelleren Verarbeitungszeiten sind besonders wichtig, da V2V-Kommunikation oft in Echtzeit erfolgen muss, um Sicherheit und Effizienz im Straßenverkehr zu gewährleisten.

Im Vergleich dazu haben die NTRU-Implementierungen, wie ntruhs2048509 mit 98614885 Taktzyklen, eine signifikant höhere Ausführungszeit. Diese langen Verarbeitungszeiten lassen NTRU weniger geeignet in einer V2V-Umgebung erscheinen.

Insgesamt deuten die Ergebnisse darauf hin, dass CRYSTALS-KYBER und möglicherweise auch Saber geeignete Optionen für V2V-Kommunikationssysteme darstellen, während die NTRU-Algorithmen aufgrund ihrer höheren Latenz möglicherweise weniger geeignet sind.

Tabelle 11: Taktzyklusanzahl von den gitterbasierten Verfahren CRYSTALS-KYBER, Saber und NTRU im CCA-Modus auf AURIX [177].

Implementierung	Schlüssel-Generierung	Verkapselung/Ver-schlüsselung	Entkapselung/Ent-schlüsselung	Insgesamt
Kyber-512	684696	846402	923283	2454381
Kyber-768	992324	1203042	1176436	3371802
Kyber-1024	1612002	1786338	1712 873	4601382
Lightsaber	889026	1162042	1336895	3387963
Saber	1736518	2168152	2449162	6353832
Firesaber	2867689	3450745	3847442	10165876
ntruhs2048509	86905630	3700492	8008 63	98614885
ntruhs2048677	153245662	6084278	14065691	173395631
ntruhs4096821	224988347	8566935	20598483	254153765

2.1.6.2 In-Vehicle Netzwerke

Sicherheit von In-Vehicle Netzwerken

Hu und Luo [178] beschreiben, dass mit der Entwicklung vernetzter Fahrzeuge die Anzahl externer Schnittstellen, die in Fahrzeuge integriert sind, erheblich zugenommen hat. Diese Schnittstellen eröffnen gleichzeitig neue Angriffsflächen für Cyberkriminelle. Ein bekanntes Beispiel ist der erfolgreiche Angriff auf einen Jeep Cherokee im Jahr 2015, der die Verwundbarkeit moderner Fahrzeuge eindrucksvoll demonstrierte. Diese Angriffe können sowohl die kritischen Sicherheitsdaten eines Fahrzeugs als auch Geschäftsgeheimnisse der Hersteller, Komfortsysteme und sicherheitsrelevante Signale betreffen.

In-vehicle Netzwerke, die ursprünglich isoliert und ohne Berücksichtigung von Sicherheitsmechanismen entwickelt wurden, verbinden heutzutage verschiedene elektronische Steuergeräte, Sensoren und Gateways. Diese Netzwerke sind in der Lage, große Mengen an sensiblen Daten zu übertragen, was neue Herausforderungen im Bereich der Cybersicherheit aufwirft. Die zentralen Probleme umfassen das Fehlen von Authentifizierungsmechanismen, die Möglichkeit des Abhörens, da die Nachrichten als Broadcast gesendet werden, das Fehlen von Zeitstempeln zur Gewährleistung der Nachrichtenfrische und Schwachstellen im Schiedsprozess für Nachrichten, die zu Denial-of-Service-Angriffen führen können.

Um die genannten Sicherheitsanforderungen zu adressieren, wurden verschiedene Ansätze für kryptografische Lösungen entwickelt, die die Integrität, Authentizität und Vertraulichkeit der Daten innerhalb von Fahrzeugen gewährleisten sollen.

Nachrichtenauthentifizierung

Message Authentication Codes: MACs werden eingesetzt, um die Integrität und Authentizität von Nachrichten sicherzustellen. Sie sind besonders geeignet für Netzwerke wie den CAN-Bus, wo die Datenfelder begrenzt sind. MACs können durch symmetrische Algorithmen wie AES berechnet werden, was die Rechenzeit minimiert. Der Einsatz von HMACs (Hash-basierte MACs) ist weit verbreitet, da sie eine effiziente Authentifizierung bieten. Die Herausforderung besteht darin, die zusätzliche Latenz und die erhöhte Buslast durch die Berechnung und Übertragung von MACs zu berücksichtigen.

Digitale Signaturen: Diese bieten eine robuste Authentifizierung und Nichtabstreitbarkeit, sind jedoch aufgrund ihrer Länge besser für Netzwerke mit größeren Datenfeldern wie FlexRay oder Ethernet geeignet. Digitale Signaturen sind besonders nützlich bei Over-the-Air (OTA) Software-Updates, um die Integrität und Authentizität der übertragenen Software sicherzustellen.

Datenverschlüsselung

Symmetrische Algorithmen: AES ist ein weit verbreiteter Algorithmus zur Verschlüsselung von Daten, um die Vertraulichkeit zu sichern. In Fahrzeugnetzwerken wird oft die Hardwareunterstützung genutzt, um die Berechnungszeit zu minimieren und den Echtzeitanforderungen gerecht zu werden.

Leichtgewichtige Algorithmen: Aufgrund der eingeschränkten Ressourcen in eingebetteten Systemen sind leichtgewichtige Algorithmen wie PRESENT ideal, da sie weniger Rechenleistung benötigen und dennoch wirksamen Schutz bieten.

Frische von Nachrichten

Zeitstempel und Zähler: Um Replay-Angriffe zu verhindern, können Nachrichten mit Zeitstempeln oder Zählern versehen werden. Diese gewährleisten, dass nur aktuelle Nachrichten akzeptiert werden. Ein synchronisierter Zähler oder ein Pseudo-Zufallswert kann zur Validierung der Nachrichtenfrische eingesetzt werden.

Schlüsselmanagement

Ein effektives Schlüsselmanagement ist entscheidend für die Sicherheit von In-Vehicle Netzwerken. Schlüssel sollten sicher gespeichert und regelmäßig aktualisiert werden. Ein Key Distribution Center (KDC) kann für die sichere Verteilung von Sitzungsschlüsseln eingesetzt werden, um Kommunikationsgruppen zu sichern. Eine häufig verwendete Methode ist die Nutzung eines speziellen Schlüsselmasters als KDC, der die Verteilung und Aktualisierung der Schlüssel koordiniert.

PQC für In-Vehicle Netzwerke

Die Weiterentwicklung kryptografischer Lösungen in Fahrzeugnetzwerken wird von der Integration funktionaler Sicherheit und Cybersicherheit geprägt sein. Die Harmonisierung von Sicherheitsentwicklungsprozessen und die kontinuierliche Durchführung von Bedrohungsanalysen sind notwendig, um die Sicherheit von Fahrzeugnetzwerken weiter zu verbessern. Die Anpassung an neue Bedrohungsszenarien und die Entwicklung neuer Standards und Protokolle werden entscheidend sein, um den wachsenden Herausforderungen in der vernetzten Fahrzeugwelt gerecht zu werden. Quantencomputer stellen eine unmittelbar bevorstehende potenzielle Bedrohung für die derzeitigen kryptografischen Verfahren dar, da sie in der Lage sein könnten, viele der aktuell verwendeten Verschlüsselungsalgorithmen zu brechen. Dies unterstreicht die Notwendigkeit der Erforschung von Post-Quanten-Kryptografie, um sicherzustellen, dass die Integrität und Vertraulichkeit von In-Vehicle Netzwerken auch in Zukunft gewahrt bleibt.

Ravi et al. [179] demonstrieren, wie PQC für die sichere Kommunikation in Fahrzeugnetzwerken eingesetzt werden kann. Sie betonen die Bedeutung der Sicherheitsauthentifizierung in Echtzeitnetzwerken von Automobilen, da diese Netzwerke sicherheitskritische Daten austauschen.

In ihrem Paper stellen sie die Implementierung des LASAN M-Protokolls vor, das auf post-quantum kryptografischen Algorithmen basiert, um die Authentifizierung in Fahrzeugnetzwerken zu sichern. LASAN M ist eine Weiterentwicklung des LASAN-Protokolls, das speziell für die Authentifizierung und Autorisierung von Electronic Control Units entwickelt wurde, ohne auf vorab geteilte Schlüssel zu setzen. Stattdessen nutzt es öffentliche Schlüssel, um eine sichere Authentifizierung zu gewährleisten. Im Mittelpunkt stehen die Algorithmen Kyber für den Schlüsselaustausch und Dilithium für digitale Signaturen, die auf Gitter-basierten mathematischen Problemen beruhen und Teil der CRYSTALS Suite sind.

Die Implementierung von LASAN M erfolgte auf einem praktischen Automobil-Testbed mit ECUs, die auf TMS570LS3157 Mikrocontrollern basieren. Die Studie bewertet die Leistung von PQC in Bezug auf Rechenkomplexität und Kommunikationsanforderungen im Vergleich zu traditionellen Public-Key-Kryptographiesystemen. Die Ergebnisse zeigen, dass das post-quantum Protokoll eine höhere Kommunikationsbandbreite benötigt und langsamer als seine traditionellen Gegenstücke ist. Dennoch bietet es zukunftsichere Sicherheitsvorteile, indem es widerstandsfähig gegenüber Quantenangriffen ist.

Letztlich unterstreicht das Paper die Notwendigkeit, PQC in Fahrzeugnetzwerke zu integrieren, um zukünftige Bedrohungen durch Quantencomputer zu adressieren und die langfristige Sicherheit der In-Vehicle-Kommunikation zu gewährleisten. Die beschriebenen Ergebnisse bieten wertvolle Einblicke in die praktische Anwendbarkeit von PQC in sicherheitskritischen Fahrzeugumgebungen und liefern ein vielversprechendes Modell für künftige Sicherheitslösungen in der Automobilindustrie.

Campos et al. [180] untersuchen ebenfalls die Auswirkungen von Quantencomputern auf die Sicherheit elektronischer Steuergeräte in Fahrzeugen und die Eignung von PQC als Gegenmaßnahme.

In ihrem Paper analysieren sie verschiedene PQC-Algorithmen und deren Anwendbarkeit in sicherheitskritischen Anwendungsfällen der Automobilindustrie, insbesondere für sichere Software-Updates von ECUs. Die Autoren argumentieren, dass die Bedrohung durch Quantencomputer bereits heute ernst genommen werden muss, da Fahrzeuge lange Produktlebenszyklen haben und die Sicherheit über die gesamte Lebensdauer gewährleistet sein muss. Sie betonen die Bedeutung der Krypto-Agilität, also die Fähigkeit, kryptografische Algorithmen bei Bedarf nahtlos auszutauschen, was eine große Herausforderung für ressourceneffiziente eingebettete Systeme darstellt.

Das Paper zeigt, dass vielversprechende PQC-Kandidaten nicht nur Vorteile hinsichtlich der Sicherheit gegen zukünftige Bedrohungen durch Quantencomputer bieten, sondern auch bestehende kryptografische Algorithmen in einigen Fällen übertreffen können. Besonders hervorgehoben werden Lattice-basierte Algorithmen wie Dilithium, die eine gute Balance zwischen Rechenleistung und Schlüsselgrößen bieten und daher als geeignete Kandidaten für den Einsatz in der Automobilindustrie angesehen werden. Die Autoren führen eine Bedrohungsanalyse und Risikobewertung durch, die aufzeigt, dass insbesondere das sichere Software-Update der ECUs das höchste Risikopotenzial aufweist, wenn klassische kryptografische Algorithmen durch Quantencomputer kompromittiert werden könnten.

In [181] untersuchen Bos et al. die Implementierung des post-quanten-sicheren Signaturverfahrens CRYSTALS-Dilithium zur Absicherung von OTA-Updates in der Automobilindustrie.

In ihrem Paper fokussieren sie sich auf die Integration von CRYSTALS-Dilithium, einem der Gewinner des NIST-Wettbewerbs, in die AUTOSAR Adaptive Platform, wobei sie die NXP S32G Fahrzeugnetzwerkprozessoren verwenden. Der Hauptfokus liegt auf der Bewertung der Leistung von Dilithium sowohl auf dem Arm Cortex-A53 Mikroprozessor als auch auf dem Arm Cortex-M7 Mikrocontroller, der die Hardware Security Engine (HSE) umfasst. Die Autoren stellen fest, dass die PQC-Implementierung nur geringe Auswirkungen auf den OTA-Update-Prozess hat und die Implementierung von Dilithium die Sicherheit gegenüber physikalischen Angriffen verbessert, indem sie die Integrität und Authentizität von Update-Paketen sicherstellt.

Im Paper wird eine Verifikationszeit von 0,5 ms auf dem Host-Prozessor und 11,1 ms auf der HSE angegeben. Obwohl die Verifikation auf dem Host-Prozessor schneller ist, bietet die HSE erweiterte Sicherheitsmerkmale wie Schutz gegen Seitenkanal- und Fehlerangriffe, was sie zur bevorzugten Wahl für sicherheitskritische Anwendungen macht.

Die Autoren heben hervor, dass der Wechsel zu post-quanten-sicheren Algorithmen wie Dilithium zwar eine geringe Leistungseinbuße verursacht, diese im Vergleich zu den Sicherheitsvorteilen jedoch vernachlässigbar ist. Das Paper unterstreicht, dass künftige

Prozessor-Generationen, die Hardware-Beschleunigung für SHA-3 bieten, die Performance-Differenz weiter verringern werden. In der Zwischenzeit überwiegen die Sicherheitsvorteile der HSE die geringfügig höhere Verifikationszeit, was Dilithium zu einer vielversprechenden Option für die Sicherung von OTA-Updates in der Automobilindustrie macht.

2.1.7 Testen von Resilienzeigenschaften in Ethernet-Netzwerken

Dieses Vorhaben entwickelt ein durchgängig automatisiertes, intent-basiertes Testverfahren zur Validierung und Quantifizierung von Resilienzeigenschaften in produktionsnahen Ethernet-/TSN-Netzen. Wissenschaftlich wird Resilienz klar als Fähigkeit beschrieben, dass ein System nach einem Fehlerzustand innerhalb einer messbaren Wiederanlauf- bzw. Rekonvergenzzeit in den voll funktionsfähigen Zustand zurückkehrt. Methodisch wird dies technologieunabhängig durch gezielte, reproduzierbare Fehlerinduktion auf Ebene der Sicherungsschicht und durch eine Messkette validiert, die Verlust, Duplikation, Reordering und Verzögerung eines Testflusses erfasst. Technisch führt die Arbeit mit VLAN-based Source Routing (VBSR) ein quellgesteuertes Weiterleitungskonzept ein, das die realistische, minimal-invasive Einspeisung und Rückführung von Testverkehr in laufenden Netzen erlaubt, ohne Endgeräte zu verändern. Ergänzt wird dies durch eine modulare, Intent-basierte Testarchitektur, die Topologie und Flüsse automatisch erfasst (LLDP/NETCONF), Testfälle aus Intent-Beschreibungen ableitet und die Tests vollständig automatisiert ausführt, bewertet und das Netz danach ephemeral in den Ursprungszustand zurückführt.

Mit der aktuellen Testmethodik werden drei unterschiedliche Resilienzklassen getestet. Als Erstes wird die Konnektivität als Basisfall der Resilienz getestet. Die Fehlerinduzierung kann dann systematisch auf jede aktive Schnittstelle des Netzwerkes, bekannt durch die Network Discovery Phase, angewandt werden. Zusätzlich zur Konnektivität erlaubt dies das Testen von 1:1- und 1+1-Protection-Switching-Mechanismen wie Multiple Spanning Tree Protocol (MSTP) und Frame Replication and Elimination for Reliability (FRER). Hierbei können unterschiedliche Messgrößen zum Einsatz kommen, welche durch einen allgemeinen Messdatenerhebungsmechanismus umgesetzt werden. Dieser Messdatenansatz basiert auf dem Einfügen von Informationen zur Identifikation und Zeitmessung in die Nutzdaten der Netzwerkpakete direkt. Zu den erfassbaren Messgrößen gehören Erreichbarkeit, Paketverlust, Duplikate, Paketvertauschungen oder die Konvergenzzeit nach Induzierung des Fehlerfalls.

Die Arbeit präzisiert Resilienz auf der Sicherungsschicht als empirisch erfassbare und vergleichbare Kenngröße, die die Zeitspanne zwischen Fehlerinjektion und Netzrekonvergenz misst. Dadurch wird Resilienz von einer allgemeinen Eigenschaft zu einer objektiv überprüfbaren, testbaren Größe. Daraus folgt eine klare Einordnung relevanter Resilienzklassen für Ethernet-/TSN-Umgebungen: Konnektivität als die Erreichbarkeit zwischen Endpunkten, 1:1-Schutzmechanismen mit rekonvergenzbasierter Umschaltung (z. B. STP/RSTP/MSTP oder funktional vergleichbare Verfahren) sowie 1+1-Schutzmechanismen mit parallelen, disjunkten Pfaden (z. B. FRER im TSN-Kontext). Für diese Klassen werden technologieunabhängige Testziele, Fehlerstimuli und Auswertungskriterien benannt. Ein Algorithmus zur 1-Link-Failure-Prüfung liefert eine verallgemeinerbare Methodik, die systematisch für jeden potenziellen Link innerhalb des Netzwerkes Fehler induziert, die Reaktion des Netzes misst und pro Fehlerort ein Testergebnis mit Zeitbezug erzeugt. Dadurch entsteht eine belastbare, empirische Basis zur Quantifizierung von Resilienz unabhängig von den eingesetzten Schutzmechanismen. Im Kontext des Stands der Technik verknüpft die Arbeit theoretische Modelle zur Resilienzanalyse (z. B. probabilistische Unverfügbarkeitsmodelle) mit praktischer Validierung im laufenden Netzbetrieb. Sie schließt damit eine Lücke zwischen

analytischer Abstraktion und betrieblicher Realität, in der Fehlkonfigurationen, Implementierungsdetails oder gerätespezifische Eigenheiten häufig erst unter realen Bedingungen evident werden.

Zentrales technisches Ergebnis ist die Konzeption eines automatisierten, modularen Testsystems (Resilience Testing System (RTS)), das intent-basiert arbeitet und die folgenden Kernfähigkeiten integriert. Eine prozessorientierte Sicht auf die einzelnen Phasen des Systems wird in Abbildung 19 gezeigt.

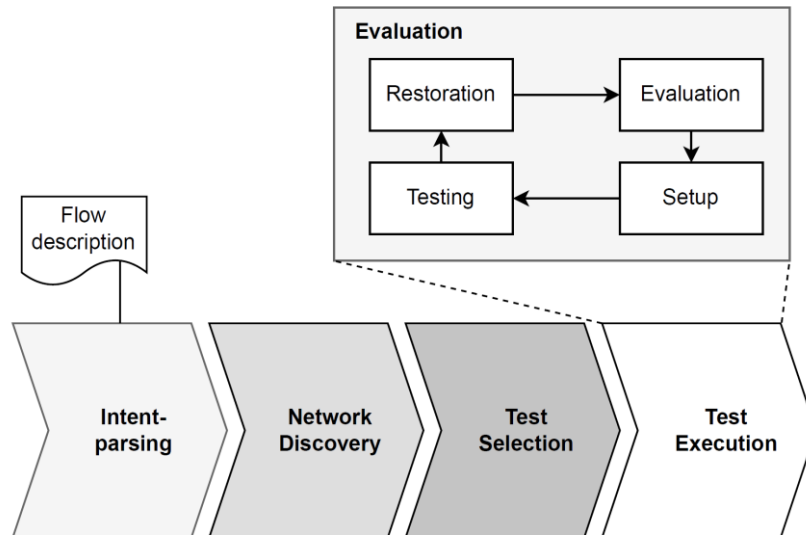


Abbildung 19: Prozessorientierte Sicht auf das modulare Testsystem von der Beschreibung von Datenflüssen bis zur Testausführung.

Erstens ermöglicht VBSR die explizite, quellseitige Pfadsteuerung über einem VLAN-Stack, der in drei logisch getrennte Sub-Pfade gegliedert ist: ein Einrichtungs-Pfad vom Testsystem zur Testquelle (Bridge nahe dem Sender), ein Test-Pfad unverändert mit derselben Konfiguration und Flusseigenschaften wie die produktiven Datenströme, und ein Ergebnis-Pfad von der Testsammelstelle (Bridge nahe dem Empfänger) zurück zum Testsystem. Das Entfernen oder Überschreiben eines VLAN-Headers an definierten Punkten erlaubt die schrittweise Weiterleitung entlang dieser Sub-Pfade, analog zum Label-Stacking in MPLS. Dies wird durch dezentrale Konfiguration des VBSR mittels NETCONF oder SNMP erreicht. Diese Konstruktion bewirkt, dass die Testpakete identisch mit den Produktionsflüssen behandelt werden (gleiche Forwarding- und QoS-Entscheidungen), ohne dass andere Endgeräte oder produktive Applikationen beeinflusst werden müssen.

Zweitens setzt die Architektur klar definierte Designprinzipien um: Realismus der Testflüsse, vollständige Automatisierung von Einrichtung, Test und Wiederherstellung, intent-basierte Parametrisierung statt manueller Konfiguration, Minimalinvasivität und Flüchtigkeit aller Teständerungen sowie Modularität zur späteren Erweiterung (weitere Protokolle, zusätzliche Fehlerszenarien, zusätzliche Metriken).

Drittens werden mit einem mehrstufigen Testprozess alle Schritte automatisiert ausgeführt: Das Intent-Parsing extrahiert aus einer Intent-Spezifikation (hier NEMO) die relevanten Flüsse und deren Anforderungen (z. B. Bandbreite, Verzögerungsbudget, Redundanzbedarf sowie MAC-/IP-/VLAN-/Prioritätsprofile). Die Network Discovery rekonstruiert per LLDP-Lesezugriff (über

NETCONF) die Topologie mittels Breitensuche und erzeugt daraus ein Graphenmodell des Netzes. Abbildung 20 zeigt den Ablauf der Entdeckung der Topologie im Netzwerk.

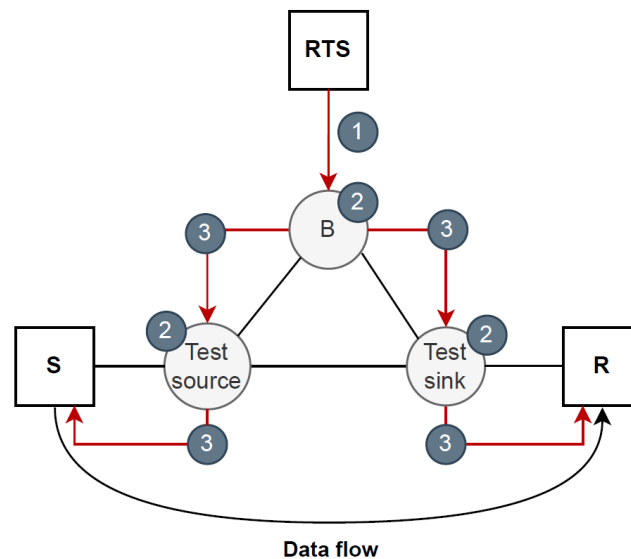


Abbildung 20: Entdeckung der Netzwerktopologie mithilfe von LLDP über NETCONF. In Schritt 1 entdeckt das RTS den ersten angeschlossenen Netzwerkknoten. Schritt 2 zeigt das Auslesen von LLDP-Informationen und Schritt 3 das Entdecken von weiteren Netzwerkknoten. Das Verfahren wird iterativ wiederholt, bis keine neuen Knoten mehr entdeckt werden.

Darauf aufbauend leitet die Test Selection die geeigneten Tests und ihre Parameter je Fluss ab (z. B. Test zur Konnektivitätsprüfung und 1-Link-Failure-Test für 1:1- und 1+1-Protection-Switching-Mechanismen) und berechnet die für VBSR nötigen Sub-Pfade einschließlich VLAN-Nutzung und Konfigurationsanpassungen. Die Test Execution steuert schließlich den gesamten Ablauf von Setup, Testing, Evaluation und Restoration. Für die Fehlerinduktion wird gezielt die VLAN-ID des geprüften Flusses an einem Port entfernt, statt ganze Ports zu deaktivieren. Das reduziert Topologie spezifische Seiteneffekte und vermeidet störende globale Konvergenzreaktionen, wie sie bei Port-Disable auftreten könnten. Die Wiederherstellung geschieht deterministisch und vollständig automatisch, indem alle temporären Konfigurationen in derselben Reihenfolge entfernt werden, in der sie gesetzt wurden. Viertens umfasst die Arbeit eine auswertungssichere Messkette: Die generierten Testframes tragen eindeutige Identifikatoren, sodass Paketverlust, Duplikate und Reordering zuverlässig erkannt werden können; Latenzen können ermittelt und mit den Intent-Anforderungen abgeglichen werden. Für empirisch schwierige Fälle (z. B. Paketverlust im Netz) definiert die Methodik klare Timeout-Regeln, um unbestimmte Situationen in nachvollziehbare Testergebnisse zu überführen. Die Ergebnisse werden pro Fluss, Fehlerort und getesteter Klasse persistiert.

Die Bewertung richtet sich konsistent nach den abgeleiteten Resilienzklassen. Für Connectivity ist primär die Ende-zu-Ende-Erreichbarkeit unter typischen Bedingungen ausschlaggebend. Als Messgröße dient, ob gesendete Pakete durch das Netzwerk übertragen werden können. Für 1:1-Schutzmechanismen steht die Rekonvergenzzeit nach Fehlerinduktion im Vordergrund. Kurzzeitige Unterbrechungen sind erwartbar, müssen aber definierte Zeit- und Verlustbudgets einhalten. Für 1+1-Schutzmechanismen ist das Ziel eine durchgängige Zustellung bei Linkausfall mit korrekter Duplikatelimination; relevante Größen sind Duplikatrate, Verlust und Verzug von Paketen, idealerweise bei vernachlässigbarer bis keiner Ausfallrate. Das Vorhaben stellt ein

technologieunabhängiges Vorgehen zur 1-Link-Failure-Prüfung vor, das über alle relevanten Ports iteriert, je Fehlerpunkt die VID-Entfernung ausführt, Pakete aussendet und die Reaktion bis zur Wiederherstellung oder bis zum Timeout misst. Die 1-Link-Failure-Prüfung wird in Abbildung 21 gezeigt. Dadurch lassen sich kritische Links je Fluss identifizieren und Resilienzkennzahlen den jeweiligen Schutzmechanismen (Connectivity, 1:1, 1+1) zuordnen. Die Methodik ist explizit erweiterbar, etwa um 2-Link-Failures oder Knotenausfälle zu modellieren, wodurch sich komplexere Resilienzklassen und Fehlermodelle abdecken lassen.

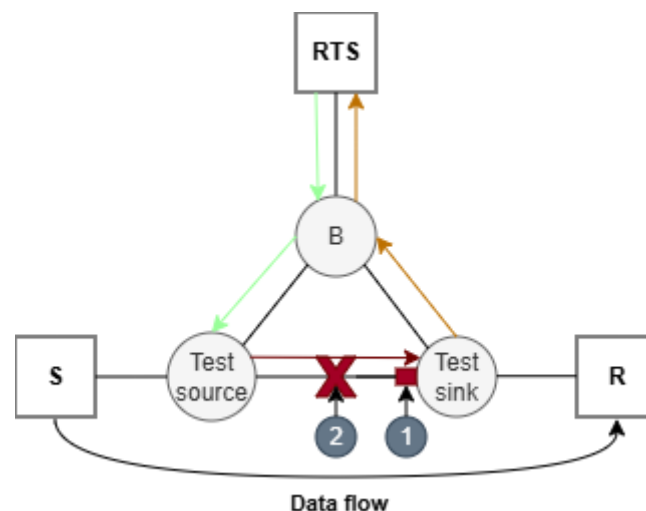


Abbildung 21: Beispielhafter Ablauf des technologieunabhängigen Tests für 1-Link-Failures. Die verschiedenen Farben zeigen das Einschleusen des Datenverkehrs von RTS zur Test Source, das produktive Verhalten von Test Source zur Test Sink und das Extrahieren der Testdaten von Test Sink zu RTS mittels VBSR. Zur Fehlerinduzierung wird in Schritt 1 die entsprechende VLAN-ID entfernt, wodurch es in Schritt 2 zu einem Ausfall der Verbindung kommt.

Im Vergleich zu verwandten Arbeiten, die häufig simulations- oder laborzentriert sind, adressiert die vorliegende Methodik reale, heterogene Betriebsumgebungen. Der Ansatz ist mit gängigen Management- und Kontrollschnittstellen (LLDP/NETCONF) kompatibel, arbeitet minimalinvasiv an produktiven Netzen und vermeidet die Notwendigkeit, Endgeräte zu modifizieren oder produktive Applikationen zu stören. Spezifisch für TSN-Netze integriert die Methode VBSR, um VLAN-Header gezielt zu überschreiben, sodass auch TSN-spezifische Protokolle getestet werden können. Damit wird eine Brücke zwischen TSN-spezifischen Redundanzmechanismen und generischen Layer-2-Testverfahren geschlagen. Gleichzeitig bleibt die Architektur modular und offen für weitere TSN-Bausteine oder alternative Schutzverfahren.

Die Methode setzt eine VLAN-basierte Segmentierung sowie die Verfügbarkeit von LLDP-Informationen und NETCONF bzw. SNMP-gestützte Gerätekonfiguration voraus. VBSR erfordert eine disziplinierte VLAN-Nutzung, bei der bestimmte VLAN-IDs eindeutig bestimmten Sub-Pfaden zugeordnet sind. Dies bedeutet, dass das Verfahren freie VLAN-IDs zur logischen Segmentierung von produktivem Datenverkehr und Test-Datenverkehr benötigt. VLAN-Header-Entfernung bzw. -Überschreibung muss an den vorgesehenen Knoten verfügbar sein. Unter diesen Bedingungen lässt sich das Verfahren in verschiedenartigen industriellen Topologien anwenden. Die vorgestellte Fehlerinduktion über VID-Entfernung minimiert Nebeneffekte gegenüber einer groben Port-Deaktivierung. Wenn benötigt, kann der Ansatz jedoch auf andere Mechanismen zur Fehlerinduzierung erweitert werden (z. B. Deaktivierung von Ports, Knotenabschaltung, Per-Stream Filtering and Policing (PSFP)), sofern Sicherheits- und Betriebsrichtlinien dies zulassen. Für weitergehende

Analysen (z. B. 2-Link- oder Node-Failures) ist das Verfahren konzeptionell vorbereitet; es erfordert primär eine passende Erweiterung des Testplaners und der Bewertungslogik.

2.1.8 Sicherheitsanforderungen von Industrial Ethernet Protokollen

2.1.8.1 Kurzfassung

In unserer Forschung untersuchen wir die Sicherheitsherausforderungen, denen Industrial-Ethernet-Protokolle (IE) in modernen, intelligenten Fertigungsumgebungen gegenüberstehen. Wir zeigen einige der Schwachstellen auf, die in weit verbreiteten IE-Protokollen vorhanden sind und Risiken für miteinander verbundene industrielle Systeme darstellen können, insbesondere in kleinen und mittleren Unternehmen. Anhand einer Fallstudie zum IE-Protokoll EtherNet/IP zeigen wir, wie die Informationssicherheit in der Betriebstechnik (OT) durch die Verwendung von Nachrichtenauthentifizierungscodes (MAC) zur Gewährleistung der Integrität und Authentizität in industriellen Netzwerken verbessert werden kann. Unsere Studie bewertet die Auswirkungen dieser kryptografischen Kontrollen auf die Kommunikationsleistung und zeigt, dass kryptografische Operationen durchgeführt werden können, ohne die Echtzeitanforderungen wesentlich zu beeinträchtigen. Unsere Ergebnisse bieten Einblicke und praktische Lösungen für die Sicherung eingebetteter industrieller Systeme und kann als Anhaltspunkt für OT-Ingenieure dienen.

2.1.8.2 Sicherheitsbewertung

Laut [14] tragen die folgenden Industrial-Ethernet-Protokolle derzeit zum höchsten Marktanteil innerhalb aller industriellen Netzwerkprotokolle bei: Profinet hat einen Marktanteil von 23 %, EtherNet/IP von 21 % und EtherCAT von 16 %. Das nächste Protokoll ist Modbus/TCP mit einem Marktanteil von 4 %, was auf eine große Lücke zwischen den drei führenden Protokollen und den anderen Marktteilnehmern hindeutet. Aus diesem Grund kann ein pragmatischer Ansatz verfolgt werden, um die Industrial-Ethernet-Protokolle mit dem höchsten Marktanteil auszuwählen, da diese derzeit am relevantesten zu sein scheinen, und die anderen Protokolle außer Acht zu lassen. Dadurch werden zwar einige Netzwerkarchitekturen aus der nachfolgenden Analyse ausgeschlossen, aber dennoch wird ein Großteil der verwendeten Protokolle abgedeckt, in unserem Fall 60 % des Marktanteils. Aus diesem Grund werden wir uns im Folgenden weiterhin mit Profinet, EtherNet/IP und EtherCAT befassen.

Profinet (Process Field Network) ist ein offener Industrial-Ethernet-Standard [15]. Er nutzt TCP/IP- und IT-Standards, ist echtzeitfähig und ermöglicht die Integration von Feldbussystemen. Profinet hat ein modulares Konzept und ermöglicht es seinen Anwendern, verschiedene Funktionskonfigurationen auszuwählen. Seit 2023 enthält Profinet eine Sicherheitsspezifikation mit dem Titel „PROFINET Security Class 1 Guideline“, die einige Sicherheitsfunktionen in die Profinet-Spezifikation einführt. Weitere Erweiterungen, beispielsweise zur Nachrichtenauthentifizierung und Kommunikationsverschlüsselung, sind für zukünftige Versionen geplant.

EtherNet/IP (Ethernet Industrial Protocol) ist ein offenes Kommunikationsprotokoll für Industrial Ethernet. Es wird für industrielle Automatisierungsanwendungen verwendet und ermöglicht die Echtzeitsteuerung und den Datenaustausch zwischen Geräten in einem Ethernet-Netzwerk. Seine Architektur basiert auf Standard-Ethernet und TCP/IP. EtherNet/IP basiert auf dem Common Industrial Protocol (CIP) für die Gerätekommunikation, einem Kommunikationsprotokoll, das in der industriellen Automatisierung zur Entwicklung von Anwendungen verwendet wird. CIP definiert eine gemeinsame Anwendungsschicht für industrielle Geräte, auf der Anwendungen aufgebaut und zwischen heterogenen Fertigungsanlagen verteilt werden können. CIP enthält eine

Empfehlung zur Sicherheit in CIP in Bezug auf die Ziele des Informationssicherheitsschutzes hinsichtlich Integrität, Authentizität und Autorisierung.

EtherCAT (Ethernet for Control Automation) ist ein weiteres Industrial-Ethernet-Protokoll. Es ist für Echtzeit-Steuerungsanwendungen konzipiert und nutzt Standard-Ethernet-Hardware. Darüber hinaus arbeitet es über einen dedizierten EtherCAT-Master, der einen kontinuierlichen Datenrahmen sendet, der von den EtherCAT-Slaves on-the-fly verarbeitet wird. Der Schwerpunkt liegt dabei vor allem auf einer schnellen Kommunikation mit kurzen Zykluszeiten und geringem Kommunikationsjitter. EtherCAT ist direkt in Standard-Ethernet-Frames eingebettet. Unser Fokus liegt auf der Nutzung von Industrial Ethernet in größeren Produktionsumgebungen, die vernetzte Kommunikation nutzen. Aus diesem Grund führen wir eine Diskussion, die sich auf die TCP/IP-Protokollsuite und ihre Anwendungen in der vernetzten Fertigung konzentriert [182]. Daher setzen wir unsere Sicherheitsdiskussionen im nächsten Abschnitt mit den Protokollen Profinet und EtherNet/IP fort. Dies ermöglicht die Untersuchung bestimmter Angriffsvektoren, wie sie im nächsten Abschnitt behandelt werden.

Im Folgenden werden die erforderlichen Sicherheitseigenschaften für die Kommunikation in industriellen Netzwerken erörtert. Dazu stellen wir zunächst eine Referenzarchitektur für ein typisches industrielles Netzwerk vor, bevor wir mit der Erörterung der damit verbundenen Schutzziele und der sich daraus ergebenden Konsequenzen fortfahren. Ein modernes industrielles Netzwerk besteht aus mehreren miteinander verbundenen Geräten wie Werkzeugmaschinen und Feldgeräten [183]. Abbildung 22 zeigt ein solches industrielles Netzwerk in einer abstrahierten Darstellung. Das Netzwerk besteht aus mehreren OT-Netzwerkgeräten (rechteckige Formen), die miteinander kommunizieren. Zu diesem Zweck befindet sich eine Reihe von OT-Netzwerk-Switches (kreisförmige Formen) innerhalb des Netzwerks, um die Kommunikation zwischen den OT-Geräten zu ermöglichen. Die Switches können beispielsweise dazu verwendet werden, die Kommunikation zwischen verschiedenen Werkzeugmaschinen oder Fertigungszellen innerhalb einer Produktionsstätte zu leiten. Innerhalb eines solchen Netzwerks können mehrere Angreifer anwesend sein, die verschiedene Arten von Angriffen durchführen [184]. Wie von [96] hervorgehoben, kann sich ein Angreifer beispielsweise als Man-in-the-Middle positionieren, um die Kommunikation abzuhören oder Nachrichten zu manipulieren. Wir gehen von einem Angreifer mit diesen Fähigkeiten aus, da er Zugriff auf das OT-Netz hat einigermaßen mit OT-Protokollen und OT-Netzwerkkonfigurationen vertraut ist.

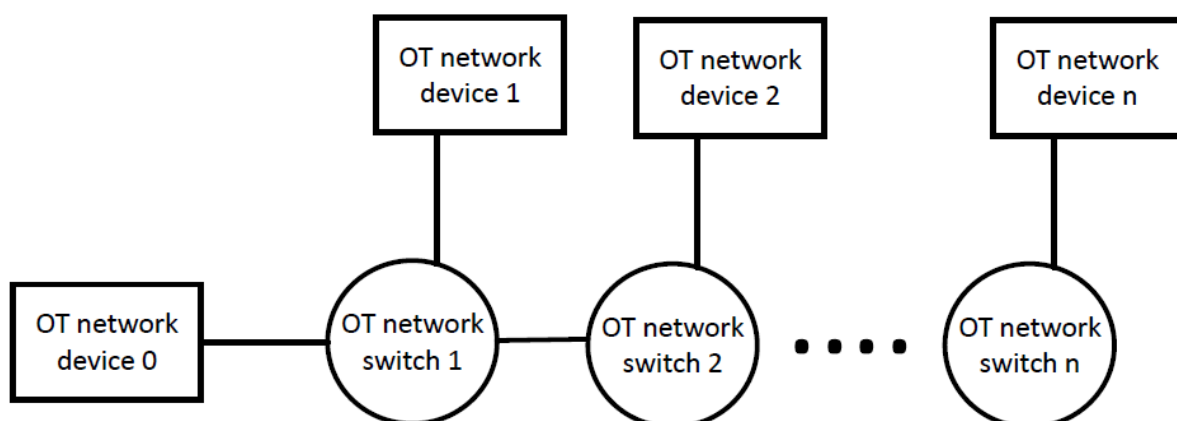


Abbildung 22: Referenzarchitektur für OT-Netzwerke.

Die Informationssicherheit selbst befasst sich mit ihren drei Hauptschutzzielen, nämlich Vertraulichkeit, Integrität/Authentizität und Verfügbarkeit [185]. In unserem Zielbereich OT wird die Verfügbarkeit oft als das wichtigste Schutzziel angesehen [186]. Dies trifft aus Sicht der OT-Betreiber zu und gilt auch für einige Angriffe auf OT-Systeme, die in der Praxis durchgeführt werden [21]. Wie jedoch mehrere reale Cybervorfälle in jüngster Zeit gezeigt haben, wird die Verfügbarkeit oft durch eine anfängliche Beeinträchtigung des Schutzziels Integrität (in Verbindung mit Authentizität) gefährdet [187]. Beispielsweise können kompromittierte Anmeldedaten zu einem unbefugten Zugriff auf ein System führen, was in Kombination mit nicht authentifiziertem Netzwerkverkehr zu Beeinträchtigungen und schweren Schäden an OT-Geräten führen kann.

Um eine systematische Analyse der möglichen Angriffsvektoren und deren Auswirkungen zu ermöglichen, ist ein strukturierter Ansatz zur Risikobewertung von Vorteil [2]. Dieser kann die oben diskutierten Angreifer-Modelle umfassen und enthält zusätzliche Komponenten für die Durchführung eines strukturierten Risikoanalyseprozesses [188]. Dazu gehören unter anderem Bedrohungsmodelle und Kriterien zur Folgenabschätzung für den Zielbereich. Beispiele für relevante Bedrohungskategorien, die die Sicherheit unserer in Abbildung 22 dargestellten Referenzarchitektur beeinträchtigen können, sind Nachrichtenfälschung, Manipulation von Nachrichten oder Denial-of-Service (DoS).

DoS steht in direktem Zusammenhang mit dem Schutzziel der Verfügbarkeit, während Spoofing und Manipulation mit Integrität und Authentizität zusammenhängen. Mehrere Angriffe in der Praxis sind möglich, weil die Authentizität und Integrität der Kommunikation innerhalb eines OT-Netzwerks und der damit verbundenen Netzwerke, wie z. B. der Büro-IT oder dem Internet, nicht gewährleistet sind. Daher können die Integrität von Nachrichten und die Authentizität der Kommunikation einen direkten Einfluss auf die Verfügbarkeit von OT-Geräten und der gesamten Produktionsanlage haben. Um diesem Problem zu begegnen, müssen geeignete Sicherheitskontrollen und Gegenmaßnahmen vorhanden sein, mit denen der Empfänger einer Nachricht die Identität des Absenders überprüfen kann.

2.1.8.3 Fallstudie zur Authentifizierung von Nachrichten

In diesem Abschnitt folgen wir unseren oben genannten Sicherheitsüberlegungen, um eine Fallstudie zu einer relevanten Informationssicherheitskontrolle im Bereich der OT-Sicherheit durchzuführen. Die Fallstudie wird unter Berücksichtigung der Anforderungen an (harte) Echtzeitanforderungen durchgeführt, die innerhalb einer industriellen Ethernet-Kommunikationsarchitektur auftreten können.

Die Integrität von Nachrichten und die Authentizität von Absendern sind relevante Schutzziele, da sie unter anderem Angriffe auf die Verfügbarkeit von Produktionsanlagen ermöglichen. Kryptografische Hash-Funktionen werden verwendet, um die Integrität und Authentizität von Nachrichten zu schützen. Eine Hash-Funktion H ist eine Anwendung der symmetrischen Kryptografie und erfordert daher einen symmetrischen geheimen Schlüssel k . Funktionen vom Typ H sind nicht-injektive Funktionen und werden jeweils auf eine Nachricht m angewendet, d. h. $H(m, k)$. Das Ergebnis $H(m, k) = h$ ist der Hashwert für die Eingabenachricht m unter dem symmetrischen Schlüssel k . Da H eine sogenannte Einwegfunktion ist, folgt daraus, dass h effizient berechnet werden kann, während die Umkehrung, d. h. die Berechnung von $H^{-1}(h) = M$, ist nicht möglich. Darüber hinaus ist eine Hash-Funktion H kollisionsresistent in dem Sinne, dass es nicht möglich ist, auf effiziente Weise eine andere Nachricht l zu identifizieren, für die $H(l) = H(m) = h$ gilt.

Hash-Funktionen mit diesen Eigenschaften ermöglichen es dem Empfänger einer Nachricht zu überprüfen, ob der Inhalt der Nachricht verändert, d. h. manipuliert wurde. Damit der Empfänger der Nachricht diese Überprüfung der empfangenen Nachricht durchführen kann, wird h an m angehängt und beides wird an den Empfänger gesendet. Der Empfänger muss ebenfalls im Besitz von k sein und kann dann $H(m, k)$ selbst berechnen und seinen Wert mit dem angehängten Wert von h vergleichen. Sind beide Werte identisch, kann der Empfänger sicher sein, dass die Nachricht nicht manipuliert wurde und somit zuverlässig ist. Da der Absender im Besitz desselben symmetrischen Schlüssels wie der Empfänger sein muss, damit dieses Verfahren funktioniert, kann der Empfänger davon ausgehen, dass die Nachricht von der Stelle gesendet wurde, die angibt, die Nachricht gesendet zu haben. Dies basiert auf der Annahme, dass k geheim bleibt. Eine Hash-Funktion H mit diesen Eigenschaften wird als Nachrichtenauthentifizierungscode (MAC) bezeichnet.

Eine kryptografische Verschlüsselung, die zur Berechnung von MACs verwendet wird, muss zwei Anforderungen erfüllen: konstante Rechenzeit und kryptografische Sicherheit. Die erste Anforderung ist für die Echtzeitkommunikation notwendig. Konstante Rechenzeiten für kryptografische Operationen wie MACs (für Nachrichten mit einer bestimmten Nachrichtengröße) sind notwendig, um die oberen Zeitgrenzen für das Senden/Empfangen von Nachrichtenrahmen abzuschätzen.

Die zweite Anforderung ergibt sich implizit aus unserer Einführung in das Thema oben. Es gibt verschiedene MAC-Verfahren, die derzeit noch als sicher gelten [189]. Dazu gehören häufig verwendete Verfahren wie cipher-based MAC (CMAC), Galois MAC (GMAC) und hash-based MAC (HMAC). Wie frühere Arbeiten gezeigt haben, sind HMACs in der Regel die leistungsfähigsten der kryptografisch sicheren MACs [190]. Aus diesem Grund konzentrieren wir unsere Evaluationsbemühungen auf HMAC-Verfahren und deren Einsatz in Echtzeitumgebungen unter Verwendung von Industrial Ethernet.

2.1.8.4 Bewertung

In diesem Abschnitt diskutieren wir die Ergebnisse, die wir bei der Anwendung von HMAC auf ein industrielles Ethernet-Protokoll erzielt haben. Für den Rahmen dieser Bewertung haben wir uns für das industrielle Ethernet-Protokoll EtherNet/IP entschieden. Studien zu den Auswirkungen kryptografischer Primitive auf das Kommunikationsverhalten von industriellem Ethernet existieren für Powerlink [15], scheinen jedoch für EtherNet/IP zu fehlen (vgl. auch Abschnitt 2). EtherNet/IP bietet die Implementierung einiger Sicherheitsfunktionen, jedoch bleibt der Einfluss anderer Sicherheitskontrollen auf die Implementierung von EtherNet/IP unklar. Darüber hinaus unterstützt EtherNet/IP die TCP/IP-Protokollsuite, die es ermöglicht, die relevante Klasse von Netzwerkangriffen in OT-Umgebungen zu untersuchen (vgl. Abschnitt 3). Wir gehen von einem Angreifer aus, der im OT-System präsent ist und über gewisse Kenntnisse der OT-spezifischen Netzwerkkommunikation verfügt. Beachten Sie, dass ein Mangel an Sicherheitskontrollen es Angreifern mit begrenzten Hintergrundkenntnissen ermöglichen kann, innerhalb des unzureichend gesicherten Netzwerks wirkungsvolle Angriffe durchzuführen für die Implementierung unserer Simulationsumgebung.

Darüber hinaus gehen wir davon aus, dass die für die Berechnung der MACs erforderlichen kryptografischen Operationen andere Prozesse, die auf den OT-Netzwerkgeräten ausgeführt werden, nicht beeinträchtigen, wie in Abbildung 22 dargestellt. Diese Annahme ist plausibel, da die konstante Kommunikationszeit für die HMAC-Verschlüsselung vom Echtzeitbetriebssystem

entsprechend geplant werden kann [15]. Darüber hinaus gehen wir davon aus, dass das simulierte OT-Netzwerk einem gewissen Maß an Jitter oder zufälligem Rauschen unterliegt, das innerhalb des Netzwerks auftreten kann. Diese Annahme soll die zunehmend vernetzten Verarbeitungslandschaften modellieren, in denen es mit höherer Wahrscheinlichkeit als in isolierten Umgebungen zu zeitlichen Kommunikationsstörungen kommen kann. Unser simuliertes OT-Netzwerk besteht aus einer variablen Anzahl von Geräten, die miteinander kommunizieren. Das bedeutet insbesondere, dass mehrere OT-Netzwerk-Switches innerhalb des Netzwerks vorhanden sind.

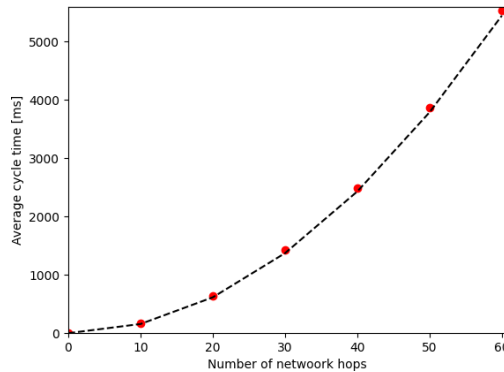


Abbildung 23: Ergebnisse für 100-Megabit/s-Netzwerke.

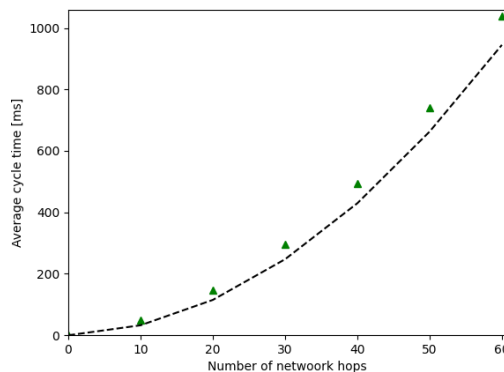


Abbildung 24: Ergebnisse für 1-Gigabit/s-Netzwerke.

Die Nachricht und der angehängte HMAC werden zwischen zwei einzelnen OT-Netzwerkgeräten entlang des Netzwerks gesendet. Der Weg, den die Nachricht zurücklegt, umfasst somit mehrere OT-Netzwerk-Switches oder Hops.

$$t_{\text{delay}} = (t_{\text{cycle}} + t_{\text{jitter}}) * n_{\text{nodes}} \quad (1)$$

$$t_{\text{cycle}} = t_{\text{min}} + 2 * t_{\text{crypto}} \quad (2)$$

Dies wird durch Gleichung 2 zusammengefasst. Hier wird t_{delay} anhand der individuellen Zykluszeit für jede Nachricht berechnet.

Die Gesamtzykluszeit ist das Produkt der OT-Netzwerk-Switches, über die die Nachricht übertragen wird, t_n Knoten, bis sie den vorgesehenen Nachrichtenempfänger, ein anderes OT-Netzwerkgerät, als Endpunkt erreicht. Die in Gleichung 1 verwendete Zykluszeit t_{cycle} wird gemäß Gleichung 2 berechnet. Sie setzt sich zusammen aus der minimalen Zykluszeit t_{min} und der Zeit, die für die Berechnung des HMAC benötigt wird, t_{crypto} . Da der Absender den entsprechenden HMAC berechnen muss und der Absender nach dem Empfang der Nachricht denselben HMAC

berechnen muss, um die beiden Werte zu vergleichen, wird t_{crypto} mit dem Faktor zwei multipliziert. Gleichung 1 basiert auf den von [191] berichteten Ergebnissen, während t_{min} der von [192] berichtete Wert ist. Schließlich basiert t_{crypto} auf den von uns in früheren Arbeiten [15] gemessenen Werten.

Die Simulation der Netzwerkkommunikation wird durchgeführt innerhalb von zwei verschiedenen Arten von EtherNet/IP-Netzwerken: 100-Megabit/s- und 1-Gigabit/s-Netzwerken. Dies ermöglicht einen Vergleich zwischen verschiedenen Kommunikationsarchitekturen, die in OT-Netzwerken verwendet werden. Wir haben die Kommunikation zwischen den OT-Netzwerkgeräten mit dem kryptografischen Overhead weiter auf verschiedenen Netzwerktopologien mit einer steigenden Anzahl von OT-Netzwerk-Switches simuliert. Die Ergebnisse für das 100-Megabit/s-Netzwerk sind in Abbildung 23 dargestellt. Es zeigt die Anzahl der Netzwerk-Hops und die durchschnittliche Zykluszeit in Millisekunden, die innerhalb solcher Topologien auftreten. Hier wird die prognostizierte durchschnittliche Zykluszeit für die Standardkommunikation, d. h. den Datenverkehr ohne kryptografische Operationen, durch eine gepunktete schwarze Linie dargestellt. Die roten Kreise zeigen die Ergebnisse unserer Simulation für die Netzwerktopologien mit jeweils 10, 20, 30, 40, 50 und 60 OT-Netzwerk-Switches. Dasselbe ist in Abbildung 24 für ein 1-Gigabit/s-Netzwerk dargestellt. Hier werden die Simulationsergebnisse durch grüne Rechtecke dargestellt. Wie aus beiden Abbildungen ersichtlich ist, hat die Berechnung des HMAC einen Einfluss auf die Zykluszeiten, die in allen Simulationen erhöht sind. Dies ist zu erwarten, da die Berechnung eines HMAC eine zusätzliche Operation ist, die von allen anderen von den Netzwerkteilnehmern durchgeführten Operationen entkoppelt ist und somit zur Gesamtzeit für den Austausch von Nachrichten beiträgt. Die durchschnittliche Verzögerung zwischen der Kommunikation mit und ohne kryptografische Operationen beträgt 47,60 ms für das 100-Megabit/s-Netzwerk. Für das 1-Gigabit/s-Netzwerk wird dieselbe Verzögerung mit einem Durchschnittswert von 47,50 ms berechnet.

2.1.8.5 Diskussion

Die Ergebnisse unserer Simulation zeigen, dass HMAC einen messbaren Overhead für die Kommunikation innerhalb eines Industrial-Ethernet-Netzwerks mit EtherNet/IP verursacht. Der Overhead ist in Netzwerken mit einer Kommunikationsgeschwindigkeit von 100 Megabit/s und 1 Gigabit/s zu beobachten und untereinander vergleichbar. Der Overhead kann durch unsere Simulation innerhalb bestimmter Grenzen geschätzt werden, die von Echtzeitarchitekten berücksichtigt werden können. Die Gesamtzykluszeit erhöht sich mit der Größe des Netzwerks. Dieser Anstieg scheint einem exponentiellen Wachstum bei steigender Anzahl von OT-Netzwerk-Switches zu folgen. Das bedeutet, dass HMACs für sehr große Kommunikationsnetzwerke möglicherweise nicht mehr realisierbar sind. Ob ein Netzwerk mit mehr als 60 OT-Netzwerk-Switches in der Praxis realisierbar bleibt, ist jedoch umstritten.

Durch HMACs geschützte Kommunikation kann eine erhöhte Sicherheitsgarantie für die Kommunikation innerhalb des Netzwerks bieten. Sie ermöglichen zwar die Überprüfung der Nachrichtenintegrität und der Authentizität des Absenders, es ist jedoch zu beachten, dass HMACs und MACs im Allgemeinen keinen Vertraulichkeitsschutz für die über das Netzwerk gesendeten Nachrichten bieten. Ein Angreifer innerhalb des Netzwerks kann weiterhin die Kommunikation abhören und daraus wichtige Informationen gewinnen. Um die Vertraulichkeit der Kommunikation zu schützen, müssen innerhalb des Netzwerks weitere kryptografische Maßnahmen durchgeführt werden, z. B. durch die Einführung einer symmetrischen Verkehrsverschlüsselung über AES. Dies kann zu neuen Obergrenzen für den gesamten Kommunikationsaufwand führen.

Die für den HMAC in unserer Simulation verwendete Verschlüsselung, d. h. SHA-256, gilt derzeit als sicher [189]. Dies wird sich jedoch wahrscheinlich irgendwann in der Zukunft ändern, und ihre Verwendung wird bei der Entwicklung künftiger IT- (und damit auch OT-)Netzwerke nicht mehr empfohlen werden. Da OT-Netzwerkgeräte über einen längeren Zeitraum betrieben werden, müssen Entwickler von OT-Systemen die Grundlagen für eine sichere Entwicklung eingebetteter OT-Geräte berücksichtigen. Dazu gehört unter anderem die Notwendigkeit einer kryptografischen Agilität. Damit ist die Fähigkeit von Geräten gemeint, ihre kryptografischen Verschlüsselungen zu einem späteren Zeitpunkt durch sicherere Verschlüsselungen zu ersetzen. Insbesondere im Hinblick auf Quantencomputer scheint die Einbeziehung der Möglichkeit eines Verschlüsselungswechsels auch für den Bereich der OT-Sicherheit relevant zu sein.

2.1.8.6 Fazit

Wir haben gezeigt, wie aktuelle IE-Protokolle mit Sicherheitskontrollen verbessert werden können. Dazu haben wir eine kurze Marktstudie durchgeführt und relevante IE-Protokolle identifiziert. Wir haben den Sicherheitsstatus dieser Protokolle diskutiert. Auf Grundlage dieser Untersuchung haben wir potenzielle Sicherheitskontrollen identifiziert, die die Gesamtsicherheit des Ethernet/IP-Protokolls verbessern können. Insbesondere haben wir die Auswirkungen der authentifizierten Kommunikation mit HMAC untersucht. Wir haben Simulationen durchgeführt, in denen wir die Leistung von ungeschütztem Datenverkehr mit der von Datenverkehr verglichen haben, bei dem zusätzlich zum regulären Datenverkehr-Overhead kryptografische Operationen durchgeführt werden. Unsere Ergebnisse zeigen, dass für Netzwerke normaler Größe ein HMAC-geschütztes Kommunikationsschema eine sinnvolle Ergänzung des Kommunikationsstacks darstellt.

2.1.9 Group Key Agreement – GRACYBUS

Systemmodell. Wir betrachten ein broadcast-orientiertes Bussystem mit half-duplex Betrieb und begrenzter Nutzlast, typisch für moderne Cyber-Physische Systeme, wie Automotive- oder industrielle Busumgebungen (z. B. CAN, PROFIBUS, Automotive/Industrial Ethernet). Ein entsprechendes einfaches Bussystem ist in Abbildung 25 dargestellt.

Unsere Annahmen zum Systemmodell sind:

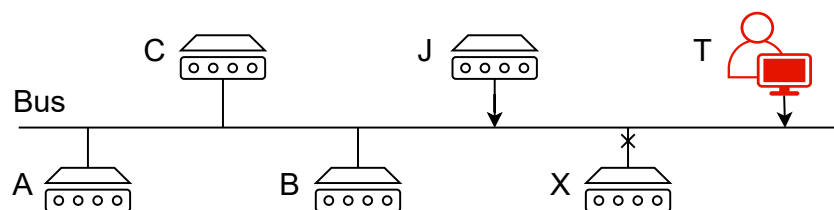


Abbildung 25: Systemmodell - Bussystem mit den angeschlossenen Geräten A, B und C. Gerät J tritt dem Bus bei. Gerät X verlässt den Bus abrupt. Der Angreifer T hat physischen Zugriff auf den Bus.

Angreifermodell. Ein starker Dolev-Yao-Angreifer mit physischem Buszugriff kann Nachrichten lesen, injizieren, modifizieren, wiederholen, verwerfen und umordnen, bis hin zur Bus-Partitionierung. Kryptografische Algorithmen werden jedoch als sicher angenommen. Verfügbarkeit kann so nicht garantiert werden, Zielgrößen sind daher Authentizität und Integrität (und bei Bedarf Vertraulichkeit) über einen gruppenweit geteilten Schlüssel.

Anforderungen. Die Anforderungen werden aus den skizzierten Betriebsrealitäten von CPS-Bussen gemäß Systemmodell und dem Dolev-Yao-Angreifermodell abgeleitet. In CPS steht Verfügbarkeit zwar häufig an erster Stelle (Schutzziele in der Priorität „AIC“ statt „CIA“), sie lässt sich auf

Bussen jedoch nicht rein kryptografisch erzwingen (z. B. bei Bus-Partitionierung). Daher fokussiert das GKA auf Integrität und Authentizität. Vertraulichkeit ist mit einem durch ein GKA-Protokoll ausgehandelten Shared Secret optional darstellbar, aber in vielen Broadcast-Szenarien aufgrund der Kurzlebigkeit der übertragenen Daten zweitrangig.

Daraus folgen zentrale Prinzipien: Nur authentifizierte Teilnehmer dürfen Protokollnachrichten erzeugen; das Protokoll muss vollständig verteilt und im Normalbetrieb unabhängig von externen Diensten funktionieren (keine Single Points of Failure). Um heterogene Busumgebungen zu adressieren, darf es nicht von link-spezifischen Ordnungs-/Adressmerkmalen abhängen und benötigt lediglich ausreichende Nutzlast. Da Mitgliedschaften zur Laufzeit schwanken (Power-Cycling, Hot-Swap, Ausfälle), sind dynamische Joins/Leaves sowie die Entfernung inaktiver Knoten ohne Kommunikationsunterbrechung nötig. Für Gruppen mit potenziell >100 Knoten sind Zustand, Rechen- und Nachrichtenaufwand zu skalieren.

Gegen einen Dolev-Yao-Gegner wird Robustheit gegen Lauschen, Injection, Modifikation, Replay und Drop gefordert; Verfügbarkeit bleibt außerhalb der Zielgröße des GKA. Angesichts langer Gerätelebenszyklen sind Post-Compromise Security (Heilung nach temporärer Kompromittierung) und Forward Secrecy (Schutz vergangener Kommunikation) notwendig. Zusätzlich braucht es kryptografische Agilität (inkl. PQC-Fähigkeit) und strikte Ressourcenschonung (CPU, Speicher, Bandbreite). Für reale Betriebsabläufe ist schließlich die sichere Unterstützung von Gruppen-Split/Merge als Erweiterung der Dynamik wünschenswert.

Die Anforderungen sind in Tabelle 12 dargestellt.

Tabelle 12: Protokollanforderungen für ein ideales sicheres GKA auf CPS-Bussen.

R#	Name	Erklärung
R01	Authentizität	Nur authentifizierte Teilnehmer können gültige Protokollnachrichten senden.
R02	Vollständig verteilt	Jeder Knoten kann alle Protokolloperationen ausführen.
R03	Unabhängig	Funktioniert im Normalbetrieb ohne externe Dienste.
R04	Bus-agnostisch	Unabhängig von sonstigen Protokollinformationen (z. B. keine MAC-Adressen für Ordnung/Reihenfolge notwendig).
R05	Dynamisch	Knoten können zur Laufzeit beitreten und verlassen. Inaktive Knoten werden nach einer gewissen Zeit entfernt, ohne den normalen Protokollablauf zu stören.
R06	Skalierbar	Effizient für größere Gruppen. Moderne CPS können über 100 Geräte umfassen.
R07	Dolev-Yao-Angreifer	Robust gegenüber Dolev-Yao-Angreifern.
R08	Post-Compromise Security (PCS)	Eine Kompromittierung eines Knotens „heilt“ nach einer gewissen Zeit.
R09	Forward Secrecy (FS)	Vergangene Kommunikation bleibt bei späterer Kompromittierung trotzdem sicher.
R10	Kryptografische Agilität	Aktualisierung von Kryptoprimitiven ermöglicht Reaktion auf Schwachstellen und unterstützt Post-Quantum-Kryptografie (PQC).

R11	Ressourcenschonung	Minimaler Overhead bei Rechenleistung, Speicher und Bandbreite, passend für ressourcenarme Umgebungen.
R12	Merge und Split	Aufbauend auf der Dynamik (R06) sollen Gruppen sich in Untergruppen aufteilen und mit ihnen zusammenführen können.

Rückverweis auf Analyse zum Stand der Forschung. Die Analyse möglicher Kandidaten zur Erfüllung der Protokollanforderungen wurde bereits in Abschnitt 1.4.9 erläutert. Dabei wurde TreeKEM als bestmöglicher Startpunkt identifiziert. Jedoch bietet TreeKEM in der Originalform keine Authentizitätsgarantien (diese sind an den zentralen MLS Authentication Service ausgelagert) und funktioniert nur mit einem zentralen und jederzeit erreichbaren Dienst, dem Delivery Service. Deshalb ist eine Anpassung erforderlich.

Grundlegende Gruppenoperationen. Im Folgenden werden vier grundlegende Gruppenoperationen verwendet. CREATE erstellt eine neue Gruppe und initialisiert die gemeinsame Schlüssel- bzw. Sicherheitsstruktur. JOIN fügt ein Mitglied hinzu und löst eine Rekonfiguration aus, damit alle aktuellen Teilnehmer aktualisierte Schlüssel erhalten. UPDATE rotiert die Schlüssel des initiierenden Mitglieds, und LEAVE entfernt ein Mitglied (freiwillig oder erzwungen) und erneuert die Gruppenschlüssel, damit der Ausgetretene keinen Zugriff mehr hat.

TreeKEM. Der Tree Key Encapsulation Mechanism [107] (deutsch etwa: baumstrukturierter Schlüssel-Einkapselungs-Mechanismus) organisiert Kommunikationsgruppen als linksbalaancierte binäre Bäume von Subgruppen. Die Blätter des Baumes sind Geräte, also einzelne Gruppenmitglieder. Jeder Knoten repräsentiert eine Subgruppe und besitzt ein Schlüsselpaar (privat/öffentlich). Interne Knotengeheimnisse werden durch Hashen des Geheimnisses eines Kindes abgeleitet, typischerweise des zuletzt geänderten. Dadurch sind interne Schlüssel nicht beitragsbasiert. Ein Kind bestimmt den neuen Knotenwert. Der Gruppennachrichtenschlüssel am Wurzelknoten wird aus einer Kette von Wurzelschlüsseln mittels einer Key-Derivation-Funktion abgeleitet.

Beim CREATE werden frische Blattschlüssel für alle Mitglieder generiert und die nötigen Knoten- und Co-Path-Schlüssel verteilt. Der Co-Path ist für ein Blatt (ein Mitglied) die Menge der Geschwisterknoten entlang seines Pfads zur Wurzel. Die Sende-Komplexität beim Erstellen ist $O(n)$. Empfänger leisten eine Entschlüsselung und $O(\log n)$ Hashes.

Beim UPDATE erzeugt ein Mitglied einen frischen Blattschlüssel und hasht ihn entlang seines Pfads bis zur Wurzel. Für jeden Knoten auf dem Co-Path werden die neuen Elternschlüssel an die jeweilige Subgruppe verschlüsselt übermittelt. Empfänger entschlüsseln genau einmal (für den niedrigsten gemeinsamen Vorfahren) und hashen bis zur Wurzel weiter.

Beim JOIN erhält das neue Gerät wie beim Update frische Schlüssel entlang seines Pfads; bestehende Mitglieder bekommen die entsprechenden Knotenupdates. Beim REMOVE werden neue Schlüssel entlang des Pfads des zu entfernenden Geräts generiert, jedoch nicht an dieses ausgeliefert.

UPDATE/JOIN/LEAVE haben die Sende-Komplexität $O(\log n)$. Empfänger führen eine Entschlüsselung plus $O(\log n)$ Hashes aus. TreeKEM erlaubt außerdem das effiziente Senden an Teilmengen, indem an die Knoten verschlüsselt wird, die die Co-Path-Zerlegung der Zielmenge abdeckt. Gleichzeitige Updates lassen sich oft lokal zusammenführen, z. B. durch eine feste Reihenfolge der Teilbäume.

Protokoll Design. Wir nennen das durch uns konstruierte Protokoll **GRACYBUS**, für *GRoup key Agreement on Cyber-phYsical system BUSES*. Es ist ein vollständig verteiltes, authentifiziertes Group-Key-Agreement für Broadcast-/Half-Duplex-Busse und baut auf TreeKEM auf, jedoch ohne die zentralen Dienste mit denen MLS TreeKEM verwendet bzw. erweitert (kein Authentication Service oder Delivery Service). Die Kernbausteine ergeben sich wie folgt:

- Der Schlüsselbaum wird aus TreeKEM übernommen: Binäre Baumstruktur - ein Gerät auf dem Bus entspricht einem Blatt. Jeder Knoten hält private Schlüssel auf seinem Pfad und öffentliche Schlüssel des Co-Path. Zusätzlich werden alle aktiven Blätter-Public-Keys redundant gespeichert.
- Der Epochen und Schlüsselplan wird aus TreeKEM übernommen: Jede Gruppenoperation (UPDATE, JOIN, LEAVE) erzeugt eine neue Epoche. Der Verkehrsschlüssel wird per Key-Derivation-Funktion aus dem aktuellen Root-Secret und dem vorherigen Epoch-Key abgeleitet et alte Schlüssel werden gelöscht.
- Die Operationen JOIN/UPDATE/LEAVE werden grundsätzlich unverändert übernommen. Modifikationen und Ergänzungen sind:
 - JOIN: Dem signierten Handshake zwischen Joiner und Sponsor kann über die gemeinsame PKI vertraut werden. Der Sponsor fügt den Joiner als neues Blatt ein, aktualisiert die Secrets, informiert die Gruppe (abgesichert via MAC) und liefert dem Joiner den neuen Epoch-Key verschlüsselt. Der Joiner erhält zudem alle Leaf-Public-Keys.
 - LEAVE: Von einem anderen Mitglied initiiert werden neue Secrets auf dem Pfad des Leavers angelegt und abgesichert durch Verschlüsselung an die anderen Empfänger verteilt. Der Leaver kann Folgenachrichten nicht mehr entschlüsseln. Unangekündigte Leaves werden über Update-Fenster erkannt und verarbeitet.
- Um die Konsistenz Schlüsselbaums zu wahren, muss die Annahme eines total geordneten, zuverlässigen Broadcast auf Bus-Ebene getroffen werden, bzw. dieser durch eine weitere Protokollschicht ermöglicht werden.

Evaluation. Dieser Abschnitt bewertet GRACYBUS unter den in unserem System- und Angreifermodell skizzierten Busrestriktionen entlang der Protokollanforderungen R01–R12. Wir betrachten dazu den rechnerischen und nachrichtenbezogenen Aufwand der Gruppenoperationen auf Basis der Baumhöhe, den Speicherbedarf pro Teilnehmer, die Sicherheitsziele gegen einen Dolev–Yao-Gegner, die Erfüllung von Forward Secrecy und Post-Compromise Security über den Epochen-Schlüsselplan sowie die kryptografische Agilität und PQC-Bereitschaft. Abschließend diskutieren wir Grenzen und Optimierungspotenzial. Die folgenden Punkte fassen die Ergebnisse kompakt zusammen.

- Komplexität: Der Rechen- und Nachrichtenaufwand pro Gruppenoperation skaliert mit der Baumhöhe $O(\log n)$. JOIN Request und Challenge sind konstant. JOIN-Success, UPDATE und LEAVE skalieren.
- Speicheraufwand: Private Schlüssel $O(\log n)$, öffentliche Schlüssel $O(n)$ (gewollte Redundanz), sowie ein aktueller Epoch-Key.
- Sicherheit: Signaturen sichern Beitritte ab, Verschlüsselung schützt Geheimnisse und MACs gewährleisten Konsistenz der Gruppen-Updates. Gegen einen Dolev–Yao-Angreifer werden Authentizität und Integrität erreicht. Verfügbarkeit bleibt bei Bus-Partitionierung außerhalb der Garantien.

- FS/PCS: Die Key Derivation Funktion mit flüchtigen Secrets und Löschung alter Schlüssel bietet Forward Secrecy. Post-Compromise Security wird nach begrenzter Kompromittierung erreicht, sobald ein UPDATE erfolgreich durchläuft.
- Kryptografische Agilität und PQC: Die Referenz-Implementierung nutzt u. a. bereits AES-256, HKDF, HMAC-SHA-512, ECDSA/Dilithium (hybrid) und Kyber (PQC-KEM).
- Grenzen und Ausblick: Merge/Split von Gruppen sind als Erweiterungen potenziell möglich, jedoch noch nicht umgesetzt. Es besteht außerdem Potenzial für Batching/Parallelisierung und verbesserte Trunkierung/Rebalancing.

Fazit. GRACYBUS zeigt, dass ein effizienter, verteilter GKA-Mechanismus ohne zentrale Infrastruktur auf ressourcenbeschränkten, Broadcast-orientierten CPS-Bussen (z. B. CAN FD, Automotive Ethernet) praktikabel ist und die geforderten Sicherheits- und Effizienzmerkmale zu großen Teilen (bis auf R07 und R12) erfüllen kann.

2.1.10 Relevanz des OWASP MASVS für die Automobilindustrie

Im weiteren Verlauf werden zunächst die Zielsetzung und Struktur des OWASP MASVS erläutert, bevor dessen Relevanz für die Automobilindustrie anhand technischer, organisatorischer und datenschutzbezogener Aspekte betrachtet wird. Anschließend werden Herausforderungen und Grenzen bei der Anwendung des Standards diskutiert, ehe die wesentlichen Erkenntnisse in einem abschließenden Fazit zusammengefasst werden.

2.1.10.1 Zielsetzung und Struktur des OWASP MASVS

Der OWASP MASVS definiert ein plattformübergreifendes Anforderungsprofil zur Bewertung der Sicherheit mobiler Anwendungen. Er dient gleichermaßen als Leitfaden für Design- und Entwicklungsprozesse wie auch als Grundlage für Sicherheitsüberprüfungen und Audits. Die modulare Struktur des Standards umfasst mehrere zentrale Themenbereiche, die den wesentlichen Angriffsflächen mobiler Applikationen entsprechen:

- **Sichere Datenspeicherung (MASVS-STORAGE):** Vorgaben zur geschützten Ablage sensibler Daten auf dem Endgerät mittels sicherer Plattformmechanismen.
- **Kryptographie (MASVS-CRYPTO):** Spezifikation angemessener kryptographischer Verfahren und sicherer Schlüsselnutzung.
- **Authentifizierung und Autorisierung (MASVS-AUTH):** Anforderungen an robuste Identitäts- und Berechtigungskonzepte.
- **Netzwerkcommunication (MASVS-NETWORK):** Absicherung der Datenübertragung zwischen App, Backend und ggf. Fahrzeug.
- **Platformsicherheit (MASVS-PLATFORM):** Schutz vor unsicherer Interaktion mit Systemdiensten und anderen Anwendungen.
- **Codequalität und Konfigurationssicherheit (MASVS-CODE):** Richtlinien für sichere Softwareentwicklung und Build-Konfigurationen.
- **Resilienz gegenüber Manipulation (MASVS-RESILIENCE):** Maßnahmen zur Erschwerung von Reverse Engineering, Debugging und App-Tampering.
- **Datenschutz (MASVS-PRIVACY):** Anforderungen zur datenschutzkonformen Verarbeitung personenbezogener Daten.

Diese klare Strukturierung erlaubt eine zielgerichtete Ableitung technischer Kontrollen und Prüfziele, die anwendungsunabhängig und reproduzierbar sind. Der MASVS kann in Softwareentwicklungsprozessen, Lieferantenmanagement und Sicherheitszertifizierungen gleichermaßen eingesetzt werden und ergänzt damit bestehende Standards um eine spezialisierte Sicht auf mobile Applikationen.

2.1.10.2 Relevanz des MASVS im automobilen Kontext

Erweiterung sicherheitskritischer Funktionen in mobilen Anwendungen: Mobile Anwendungen bilden zunehmend die operative Schnittstelle zu Fahrzeugfunktionen. In vielen Fällen werden sicherheitsrelevante Interaktionen, etwa Remote-Funktionen oder der Zugriff auf Telemetriedaten, über Smartphones abgewickelt. Studien zeigen, dass gerade im Bereich der Elektromobilität mobile Apps häufig Schwachstellen aufweisen, die Angriffe auf Fahrzeuge oder Nutzerdaten ermöglichen könnten [193].

Der MASVS stellt für diese Problemfelder konkrete Anforderungen bereit, etwa zu sicherer Speicherung von Token, Absicherung kryptographischer Schlüssel oder Schutz der App-Integrität. Damit trägt der Standard wesentlich zur Minderung von Risiken bei, die aus der wachsenden sicherheitsrelevanten Rolle mobiler Anwendungen entstehen.

Beitrag zu einem ganzheitlichen Cybersecurity-Ansatz: Die Automobilindustrie ist durch hochgradig vernetzte Ökosysteme geprägt, in denen Fahrzeugsysteme, mobile Applikationen und Cloud-Infrastrukturen eng miteinander interagieren. Branchenanalysen betonen, dass Cybersecurity heute nicht mehr isoliert betrachtet werden kann, sondern domänenübergreifend gedacht werden muss [22].

Der MASVS liefert hierfür einen spezifischen Baustein: Während andere Standards die Fahrzeugarchitektur, Embedded-Systeme oder Backend-IT adressieren, fokussiert MASVS auf mobile Schnittstellen. Dadurch ergänzt er bestehende normative Anforderungen um eine Ebene, die bislang oft unterrepräsentiert war, jedoch in modernen Mobilitätsdiensten von hoher sicherheitstechnischer Bedeutung ist.

Datenschutz und Nutzervertrauen: Durch mobile Anwendungen werden umfangreiche personenbezogene Daten erhoben und verarbeitet, insbesondere Standortdaten und Nutzungsprofile.

MASVS-PRIVACY adressiert genau diese Anforderungen und liefert konkrete Vorgaben zu Datenminimierung, sicherer Speicherung, transparente Einwilligung und sicherem Logging. Dadurch eignet sich der Standard, sowohl regulatorische Vorgaben zu erfüllen als auch langfristiges Vertrauen in digitale Fahrzeugdienste zu stärken.

Standardisierung und Governance entlang von Lieferketten: Mobile Anwendungen werden im Automotive-Bereich häufig durch spezialisierte Softwaredienstleister entwickelt [193]. Ein standardisierter, nachvollziehbarer Anforderungskatalog wie MASVS ermöglicht es, Sicherheitsanforderungen frühzeitig im Beschaffungsprozess zu definieren, die Vergleichbarkeit externer Entwicklungsergebnisse zu verbessern und die Sicherheit auf Organisationsebene zu harmonisieren. Für komplexe Lieferketten in der Automobilindustrie ist dies ein entscheidender Vorteil.

2.1.10.3 Herausforderungen und Abgrenzungen

Obwohl der MASVS eine umfassende Grundlage für die Absicherung mobiler Applikationen bietet, verbleibt die Absicherung der restlichen Fahrzeuginfrastruktur, einschließlich In-Vehicle-

Kommunikation, sicherheitskritischer Echtzeitsysteme oder Steuergeräte, außerhalb seines Scopes. Daher ist der MASVS als Baustein eines mehrschichtigen Sicherheitskonzeptes zu betrachten.

Zudem erfordert seine Anwendung eine geeignete Bedrohungsanalyse, um festzulegen, welche Anforderungen im jeweiligen Anwendungskontext notwendig sind. Je nach Applikation können unterschiedliche Schutzprofile erforderlich sein, was eine projektspezifische Abwägung verlangt. Auch organisatorische Voraussetzungen wie entsprechende Entwicklungsprozesse, kontinuierliche Sicherheitsprüfungen und qualifiziertes Personal sind unabdingbare Faktoren für die erfolgreiche Umsetzung.

2.1.10.4 Fazit

Die Rolle mobiler Anwendungen im automobilen Umfeld hat sich in den letzten Jahren fundamental gewandelt. Als integraler Bestandteil moderner Fahrzeug-Ökosysteme sind sie sowohl funktional als auch sicherheitstechnisch von zentraler Bedeutung.

Der OWASP MASVS bietet einen klar strukturierten, allgemein anerkannten und anwendungsorientierten Rahmen, um diese Anwendungen systematisch abzusichern. Durch die Kombination aus technischen Mindestanforderungen, Prüfkatalogen und modularen Schutzprofilen leistet der Standard einen wesentlichen Beitrag zur Erhöhung des Sicherheitsniveaus vernetzter Fahrzeuge.

Er stellt damit einen wichtigen Baustein dar, um die ganzheitliche Cybersecurity moderner Mobilitätslösungen sicherzustellen und sowohl technische Risiken als auch Datenschutzerfordernisse verlässlich zu adressieren.

2.1.11 Sicherheit von Ortungsdiensten

Für die Untersuchung der Vertrauenswürdigkeit mobiler Standortdienste wurde ein modulares Testbed aufgebaut, das sowohl GNSS-Spoofing als auch die Emulation eigener Mobilfunkzellen umfasst. Ein softwaredefinierter Sender (SDR) erzeugte GPS-L1-Signale in kontrollierter Laborumgebung; parallel betrieben wir eigene GPRS- und LTE-Zellen auf SDR-Hardware. Diese Infrastruktur erlaubte, die Reaktion realer Endgeräte auf manipulierte Standortquellen systematisch zu analysieren und zugleich die dabei entstehenden Protokollflüsse auf der Control- und User-Plane mitzuschneiden. Zur Verkehrsanalyse setzten wir Wireshark auf den Hosts, sowie auf Android-Geräten PCAPdroid ein. Wo möglich, wurden TLS-Verbindungen mittels systemseitig vertrauten Zertifikaten und selektiv blockiertem QUIC abgefangen. Dies ermöglichte Detailanalysen insbesondere für PSDS- und SUPL-Verkehr. Ein zentrales praktisches Ergebnis ist dabei zugleich eine methodische Erkenntnis: Basisband-vermittelte Verbindungen umgehen teils die OS-Netzwerk-Stacks, sodass reine On-Device-Captures (ohne Root/Trust-Injection) den Standortverkehr nicht vollständig abdecken.

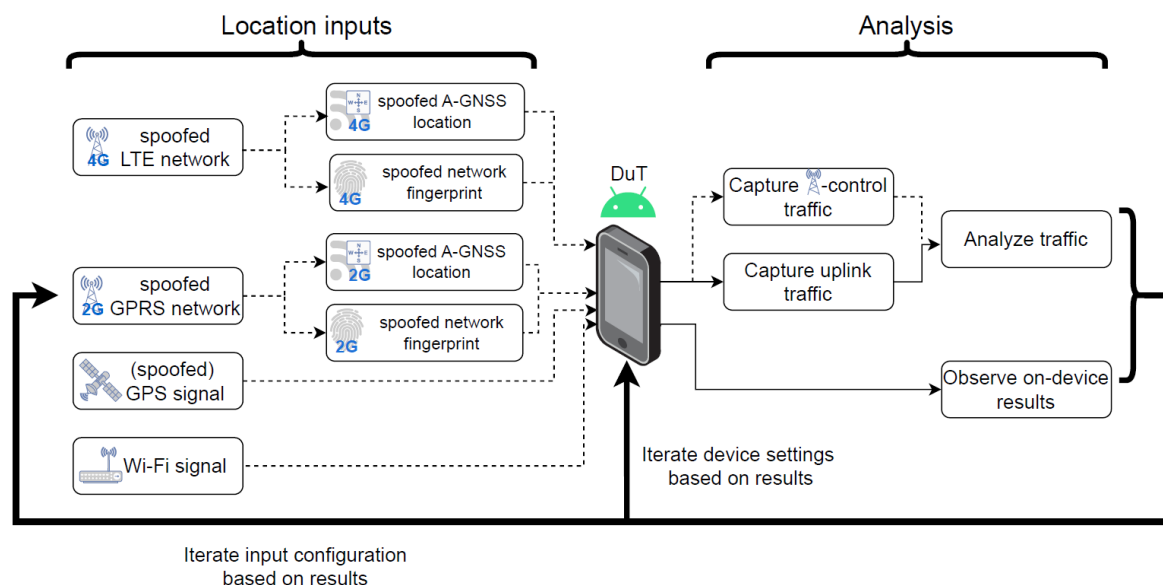


Abbildung 26: Konzept des Test-Frameworks.

Die Analyse der A-GNSS-Unterstützung zeigte über Gerätekategorien hinweg ein konsistentes Muster bei PSDS, jedoch mit herstellerspezifischen Ausprägungen. Geräte luden regelmäßig Vorhersage- und Bahndaten über dedizierte Server (u. a. agnss.goog, xtracloud.net, ssiloc.com, vereinzelt gllto.glpals.com). Die Verbindungen waren überwiegend mit TLS ≥ 1.2 abgesichert. Im entschlüsselten Datenpfad fanden wir bei aktuellen Geräten keine personenbezogenen Nutzlasten jenseits generischer Header und der unvermeidlichen IP-Metadaten; bei Altgeräten traten hingegen gelegentlich schwächere Cipher und TLS-1.0-Kompatibilität auf.

Device	Chipset	User Data	Encryption	Weak ciphers	TLS 1.0	PSDS Server
Pixel 4a	Qualcomm	?	✓	✓	✓	path1.xtracloud.net
Pixel 6a	Google	✗	✓	✓	✓	agnss.goog
Galaxy S24	Samsung	✗	✓	✓	✗	1.ssiloc.com
Galaxy Tab S8	Qualcomm	?	✓	✓	✗	qcc.qualcomm.com (?) or path2.xtracloud.net
G2	Qualcomm	✗	✗	✓	✓	xtrapath5.izacloud.net or xtrapath6.izacloud.net
Mi 9T Pro	Qualcomm	?	?	✓	✓	path2.xtracloud.net or path3.xtracloud.net
P20	HiSilicon	✗	✗	✓	✗	gllto.glpals.com
Venue 8 Pro	Intel	?	✓	✓	✗	inference.location.live.net
iPhone XR	Apple	?	✓	✓	✓	gs-loc.apple.com

Abbildung 27: Beobachteter PSDS-Server für verschiedene Geräte. ? kennzeichnet Geräteeigenschaften, die wir nicht testen konnten.

Deutlicher als bei PSDS traten bei SUPL sicherheits- und datenschutzrelevante Befunde zutage. Android-Geräte kontaktierten in der Voreinstellung bei Standortanforderungen regelmäßig `supl.google.com` (Port 7275/TLS) und übermittelten im `mSUPLSTART` die eindeutige IMSI, MCC/MNC sowie Zellen-Metadaten (z. B. ECI/TAC/PCI/EARFCN, RSRP/RSRQ/TA). Diese Praxis ist carrierseitig vorkonfiguriert und ohne Root-Zugriff nicht nutzerseitig änderbar. Im WLAN-only-Betrieb wurden teils Dummydaten für Zellinfos gesendet. Tablets nutzten SUPL in unseren Stichproben seltener oder nicht. Insgesamt bestätigt die Protokollanalyse, dass Google bzw. Carrier aus SUPL-Verbindungen regelmäßig eine trackbare Kennung plus grobe Standortinformation erhalten, während PSDS überwiegend unkritische Hilfsdaten bereitstellt.

Device	Chipset	SUPL Wi-Fi	SUPL GPRS	PCAPdroid
Pixel 4a	Qualcomm	✗	✓	✗
Pixel 6a	Google	✓	✓	✓
Galaxy S24	Samsung	✗	✓	✓
Galaxy S22	Samsung	✗	✓	✓
Galaxy Tab S8	Qualcomm	✗	N/A	✗
G2	Qualcomm	✗	?	?
Mi 9T Pro	Qualcomm	?	?	✗
P20	HiSilicon	✓	✓	✓
Venue 8 Pro	Intel	✗	N/A	N/A
iPhone XR	Apple	✗	?	N/A

Abbildung 28: Liste der für SUPL getesteten Mobilgeräte. Die Tests mit ? wurden aufgrund der fehlenden erforderlichen Laborausstattung nicht durchgeführt.

Auf der Control-Plane (RRLP in GSM, LPP in LTE/5G) ließ sich in unserem Setup trotz gezielter Suche kein positionsbezogener Signalisierungsverkehr beobachten. Angesichts funktionierender U-Plane-Unterstützung (SUPL) und der moderneren Gerätestacks ist plausibel, dass C-Plane-basierte Ortungsprozeduren in den von uns untersuchten Konfigurationen nicht genutzt wurden oder unsere Open-Source-Netzkerne die relevanten Pfade nicht abdecken. Für die Bewertung der realweltlichen Relevanz dieser Verfahren bleibt dies eine Einschränkung und zugleich ein Hinweis auf die derzeitige Dominanz der U-Plane-Assistenz im Android-Ökosystem.

Method	Root	Mobile Traffic	Full U-Plane Traffic	C-Plane Traffic	Speed	Encryption Breaking Inbuilt	Ease of Use
PCAPdroid (root)	✓	✓	✗	✗	✓	✓	High
PCAPdroid (VPN)	✗	✓	✗	✗	✓	Partial	Very High
Wi-Fi Hotspot	✗	✗	✓	✗	✓	✗	Medium
Custom GPRS Network	✗	✓	✓	✓	✗	✗	Low
Custom LTE Network	✗	✓	✓	✓	✓	✗	Very Low

Abbildung 29: Vergleich von Methoden zur Erfassung des Datenverkehrs für Android.

Im Kern unseres Versuchsdesigns stand die empirische Eingrenzung der Priorisierungs- und Fusionslogik des Fused Location Provider (FLP). Dazu wurden Geräte kontrolliert unterschiedlichen, teils widersprüchlichen Quellen ausgesetzt (WLAN-Fingerprints, Mobilfunk-Fingerprints, GNSS-Spoofing). Der FLP zeigte dabei ein stabiles, einfache Regeln widerspiegelndes Verhalten: Sobald ein GNSS-Fix vorliegt, dominiert GNSS systematisch gegenüber Netzwerkquellen. Ein bestehender GNSS-Fix wird nach Sichtverlust über mehrere Minuten gehalten; eine räumliche Plausibilisierung gegenüber zeitnah verfügbaren Netzwerk-Positionen, z. B. Sprünge über hunderte Kilometer, war in unseren Tests nicht erkennbar. Liegt kein GNSS vor, pendelt der FLP zwischen Mobilfunk- und WLAN-basierter Standort, wobei in erster Linie die Aktualität der Messung zu zählen scheint; eine feste Präferenz zwischen Mobilfunk und WLAN konnten wir nicht feststellen. Dieses Verhalten replizierten wir geräte- und appübergreifend, u. a. Google Maps, GnsLogger, eigene Test-App.

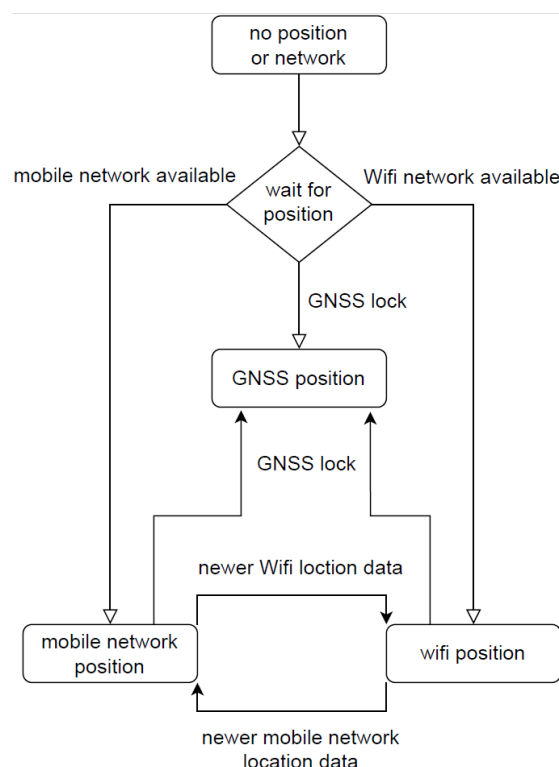


Abbildung 30: Unsere Vermutung für den Algorithmus zur Ableitung des Standorts für Google FLP.

Die praktischen Spoofing-Ergebnisse unterstreichen diese Prioritätenordnung. GNSS-Spoofing (GPS L1) führte in der Laborsituation zuverlässig zu falschen Fixes bei Smartphones und einer Dual-GNSS-Fitnessuhr: eine falsch ausgestrahlte GNSS-Zeit wurde nicht zur Systemzeit erhoben, hinderte die Positionsannahme aber nicht. Bei konkurrierender echter Satellitensicht bevorzugten Endgeräte im Freifeld i. d. R. die legitimen Signale (Signalqualität, Mehrkonstellation/Mehrfrequenz), hielten jedoch einmal etablierte Spoofing-Fixes weiter. Netzwerkbasierter Manipulation über Mobilfunk-Fingerprinting gelang durch Betrieb einer Rogue-Zelle mit konfigurierten Kennungen (MCC/MNC/LAC/ECI/PCI/TAC): Sobald das Endgerät unsere Zelle nutzte, sprang die Netzwerk-Position unverzüglich an den Zielort. Praktisch erwies sich LTE aufgrund der notwendigen (Test-)SIM-Authentisierung als aufwendigerer Angriffsweg; GPRS ist einfacher aufzusetzen, aber instabiler und mit deutlichen Latenz-/Durchsatzproblemen behaftet. „Mock-Location“-Apps

lieferten erwartungsgemäß markierte Messwerte (API-Flag) und sind für sicherheitskritische Szenarien ungeeignet.

Methodische und technische Limitationen unserer Ergebnisse sind zu beachten. Die Experimente fanden nur im Labor statt. GNSS-Spoofing beschränkte sich auf GPS L1, reale Mischbedingungen mit starker Mehrkonstellations-Sicht wurden nur begrenzt untersucht. C-Plane-Ortung konnten wir nicht feststellen. Ob dies an der fehlenden Nutzung durch die Geräte oder an den Grenzen der Open-Source-Komponenten lag, bleibt offen. Schließlich zeigten sich geräte- und chipsetabhängige Unterschiede (z. B. SUPL-Nutzung bei Tablets, PSDS-Serverwahl), die eine nur eine beschränkte Generalisierung nahelegen. Insgesamt liefern die Befunde jedoch ein konsistentes, über mehrere Geräte hinweg repliziertes Bild der FLP-Logik, der A-GNSS-Nutzung unter Android und der praktischen Wirksamkeit von GNSS- und Netzwerk-Spoofing im untersuchten Rahmen.

2.1.12 Bereichsübergreifendes Security-Risikomanagement in der Automobilindustrie: Anforderungen und aktuelle Praktiken

2.1.12.1 Kurzfassung

Die Zusammenarbeit zwischen verschiedenen Bereichen der Automobilindustrie, darunter Fahrzeugentwicklung, Produktion und Backend-Services, erschwert das Risikomanagement im Bereich Cybersicherheit. Zwar bieten Standards wie ISO/SAE 21434, die ISO/IEC 27000-Familie und die IEC 62443-Reihe jeweils domänenspezifische Leitlinien, doch eine gezielte Überprüfung zeigt, dass sie kein vollständig integriertes, bereichsübergreifendes Rahmenwerk bieten. Vielmehr enthalten sie verstreute Leitlinien zu Themen wie Kommunikationskanälen, externen Abhängigkeiten und abgestimmten Risikokriterien, wobei es den Organisationen überlassen bleibt, diese Elemente zu vereinheitlichen.

Um zu untersuchen, wie sich diese Lücke in der Praxis manifestiert, wurden halbstrukturierte Interviews mit sechs Automobilherstellern durchgeführt, um reale Herausforderungen und Strategien für das abteilungsübergreifende Cybersicherheitsrisikomanagement zu erfassen. Die Ergebnisse zeigen unterschiedliche Risikobewertungsmethoden, uneinheitliche Terminologie und fragmentierte Kommunikationskanäle zwischen diesen Abteilungen, die eine ganzheitliche Sicherheitsstrategie behindern. Umgekehrt unterstreichen die Ergebnisse die Vorteile koordinierter Strategien, wie z. B. verbesserte Risikotransparenz, effizientere Ressourcenzuweisung und stärkere Einhaltung gesetzlicher Vorschriften.

Auf der Grundlage der Standardanalyse und der Interviewergebnisse plädiert dieser Artikel für einen einheitlichen Rahmen, der Prozesse, Tools und Sprache in allen Automobilabteilungen harmonisiert und die Hersteller letztendlich zu einer übergreifenden, robusteren Cybersicherheitsstrategie führt.

2.1.12.2 Cybersicherheitsstandards mit Relevanz für Cybersicherheitsrisikomanagement in der Automobilindustrie

Um Cybersicherheitsrisiken über mehrere Unternehmensbereiche hinweg erfolgreich zu managen, müssen sowohl die domänenspezifischen Standards für Automobil-E/E-Systeme als auch die für Informations- und Betriebstechnologien geltenden Standards verstanden werden. In diesem Abschnitt werden drei wichtige Normenreihen vorgestellt: ISO/SAE 21434, die ISO/IEC 27000-Familie und die IEC 62443-Reihe. Dabei werden ihre bereichsübergreifenden Anforderungen und/oder Empfehlungen für das organisatorische und Cybersicherheits-Risikomanagement

hervorgehoben. Der Abschnitt schließt mit einer Zusammenfassung der bereichsübergreifenden Leitlinien der Normen.

ISO/SAE 21434

Die Norm ISO/SAE 21434 [27] wurde 2021 veröffentlicht. Sie dient Organisationen als Leitfaden für die Einbeziehung der Cybersicherheit in die Konstruktion von Serienfahrzeugen durch die Implementierung eines Cybersicherheits-Managementsystems (CSMS), die Definition von Cybersicherheitsrichtlinien und -prozessen, das Management von Cybersicherheitsrisiken und die Förderung einer Cybersicherheitskultur. Systeme außerhalb des Fahrzeugs, wie Backend-Server oder Produktionssysteme, fallen nicht in den Geltungsbereich der Norm. Die UN-Regelung Nr. 155 [41] enthält gesetzliche Anforderungen für die Zulassung von Fahrzeugen in Bezug auf Cybersicherheit und ist mit ISO/SAE 21434 verknüpft. Konkret verweist der Auslegungsleitfaden [194] zur UN-Regelung Nr. 155 auf ISO/SAE 21434 als besonders hilfreich für die Umsetzung ihrer Anforderungen.

Bereichsübergreifende Aspekte des organisatorischen Cybersicherheitsmanagement

ISO/SAE 21434 weist in Abschnitt 5 darauf hin, dass die Cybersicherheitsrichtlinie Verknüpfungen zu den Zielen und anderen Richtlinien der Organisation enthalten kann, wodurch implizit die Kohärenz zwischen verschiedenen Bereichen ermöglicht wird. Die Norm verlangt die Identifizierung von Disziplinen im Zusammenhang mit Cybersicherheit, wie z. B. IT-Sicherheit, und die Einrichtung von Kommunikationskanälen zwischen ihnen, um Cybersicherheit in bestehende Prozesse zu integrieren und den Informationsaustausch zu koordinieren. Darüber hinaus wird darauf hingewiesen, dass die Koordination den Austausch von Prozessen, Strategien und Tools zwischen den Disziplinen umfassen kann, und es werden Beispiele für den Austausch von Bedrohungsszenarien, Gefahreninformationen oder Cybersicherheitszielen genannt. ISO/SAE 21434 verlangt von Organisationen außerdem, dass sie sicherstellen, dass das Cybersicherheitspersonal über die erforderlichen Kompetenzen und das notwendige Bewusstsein verfügt, einschließlich der Kenntnisse über verwandte Disziplinen. Außerdem schreibt sie die Aufrechterhaltung eines Qualitätsmanagementsystems zur Unterstützung der Cybersicherheitsentwicklung vor, wobei der Schwerpunkt auf Aspekten wie dem Änderungsmanagement liegt. Die Norm nennt als Beispiel die Überprüfung von Änderungen in Produktionsprozessen, um die Einführung neuer Schwachstellen zu verhindern. Darüber hinaus empfiehlt sie die Einrichtung eines Cybersicherheitsmanagementsystems speziell für Produktionsprozesse und die Verwaltung von Arbeitsergebnissen in Übereinstimmung mit einem Informationssicherheitsmanagementsystem (ISMS).

Bereichsübergreifende Aspekte des Cybersicherheitsrisikomanagements

ISO/SAE 21434 verlangt in den Abschnitten 9 und 15 eine detaillierte Beschreibung der für die Cybersicherheit relevanten Betriebsumgebung, einschließlich aller Annahmen über externe Abhängigkeiten wie Backend-Systeme, auf die das Fahrzeug angewiesen ist, um die Identifizierung und Analyse relevanter Bedrohungsszenarien und Angriffspfade zu unterstützen, die mehrere Bereiche betreffen können. Wenn Entscheidungen zur Risikobehandlung aufgrund bestimmter Annahmen, möglicherweise in Bezug auf andere Bereiche, die Weitergabe oder Beibehaltung des Risikos beinhalten, verlangt die Norm die Angabe entsprechender Cybersicherheitsanforderungen. ISO/SAE 21434 verlangt darüber hinaus die Definition von Cybersicherheitsanforderungen für das Produkt und seine Betriebsumgebung, wobei zu beachten ist, dass die Anforderungen an die Betriebsumgebung außerhalb des Produkts realisiert werden, aber in den

Cybersicherheitsvalidierungsprozess einbezogen werden. Darüber hinaus schreibt die Norm vor, dass sicherheitsrelevante Auswirkungsbewertungen aus der funktionalen Sicherheitsnorm ISO 26262-3:2018 [195] abgeleitet werden müssen, sodass Organisationen Bewertungen, die für funktionale Sicherheitszwecke durchgeführt wurden, für die Cybersicherheit nutzen können.

ISO/IEC 27000 Familie

Die ISO/IEC 27000 ISMS-Familie [28] umfasst etwa 100 Normen, die von Übersichten und Vokabular bis hin zu Leitlinien für bestimmte Anwendungsbereiche reichen, wobei die erste im Jahr 2000 veröffentlicht wurde. Sie ermöglicht es Organisationen, einen Rahmen für das Management der Sicherheit ihrer Informationsressourcen zu entwickeln und umzusetzen, indem sie einen Risikomanagementprozess anwenden und ein ISMS einrichten, implementieren, aufrechterhalten und verbessern. Die Anforderungen der ISO/IEC 27001 [49] sollen für alle Organisationen gelten, unabhängig von ihrer Art, Größe oder Beschaffenheit.

Bereichsübergreifende Aspekte des Cybersicherheitsmanagements in Organisationen

ISO/IEC 27001 in den Abschnitten 4 und 7 verlangt von Organisationen, interne Fragen zu klären, die für ihr

ISO/IEC 27003 [50] empfiehlt dabei, bestehende Governance- und Organisationsstrukturen zu berücksichtigen, und schlägt vor, dass Organisationen das ISMS an anderen bestehenden Managementsystemen ausrichten und gemeinsame Funktionen wie Managementbewertung und Audits kombinieren können. Bei der Festlegung des Geltungsbereichs des ISMS betont ISO/IEC 27003, dass genaue Kenntnisse über Grenzen und Abhängigkeiten zu anderen Teilen der Organisation von entscheidender Bedeutung sind, da spätere Änderungen zu erheblichem Mehraufwand und zusätzlichen Kosten führen können. ISO/IEC 27001 verlangt von Organisationen außerdem, den Bedarf an interner Kommunikation im Zusammenhang mit dem ISMS zu ermitteln, wobei ISO/IEC 27003 empfiehlt, Pläne und Ergebnisse des Risikomanagements, Ziele der Informationssicherheit und Vorfälle nach Bedarf an interessierte Parteien zu kommunizieren, was die bereichsübergreifende Sensibilisierung und Zusammenarbeit erleichtern kann.

Bereichsübergreifende Aspekte des Cybersicherheitsrisikomanagements

ISO/IEC 27003 empfiehlt in Abschnitt 8, dass Organisationen Informationssicherheitsrisikobewertungen durchführen, wenn wesentliche Änderungen am Kontext des ISMS auftreten. Dies könnte so interpretiert werden, dass auch Änderungen an Bordsystemen im Geltungsbereich des CSMS, die sich auf Außensysteme im Geltungsbereich des ISMS auswirken, darunter fallen. ISO/IEC 27005 [48] empfiehlt in den Abschnitten 6 und 8, dass die Kriterien für die Risikoakzeptanz mit den allgemeinen Kriterien für die Risikoakzeptanz der Organisation übereinstimmen sollten, was auf die Notwendigkeit einer bereichsübergreifenden Abstimmung hinweist. Außerdem wird empfohlen, die Kriterien für die Risikobewertung in der gesamten Organisation zu standardisieren, um die Kommunikation, den Vergleich und die Aggregation von Risiken, die mit mehreren Geschäftsbereichen verbunden sind, zu erleichtern. Die Norm schlägt vor, dass die Folgenkriterien auf eine gemeinsame Skala bezogen werden sollten, um eine Aggregation der Risiken über verschiedene Bereiche hinweg zu ermöglichen und einen genauen Vergleich der Folgenstufen zu gewährleisten. Darüber hinaus empfiehlt ISO/IEC 27005, den Ansatz und die Methoden des Informationssicherheits-Risikomanagements an denen auszurichten, die für das Management anderer Risiken innerhalb der Organisation verwendet werden. Bei der Auswahl von Optionen zur Risikobehandlung schlägt die Norm vor, dass die Risikoteilung eine Aufteilung der

Verantwortlichkeiten zwischen internen Parteien und die Delegierung der Umsetzung von Schutzmaßnahmen an eine andere Einheit umfassen kann. Sie weist auch darauf hin, dass Organisationen berücksichtigen sollten, wie Risiken von den betroffenen Parteien wahrgenommen werden, und geeignete Wege zur Kommunikation von Risiken an diese Parteien festlegen sollten.

IEC 62443 Reihe

Die IEC 62443-Reihe [29] umfasst etwa zehn Normen und technische Berichte, von denen der erste 2007 veröffentlicht wurde. Sie befasst sich mit der Informationssicherheit von industriellen Automatisierungs- und Steuerungssystemen (IACS) und deren Integration in Unternehmensnetzwerke. Einige Normen der Reihe richten sich an Anlagenbesitzer, Systemintegratoren und Produktlieferanten von IACS, während andere sich auf eine bestimmte Gruppe konzentrieren. IEC 62443-2-1 [51] enthält Anforderungen an ein IACS-Sicherheitsprogramm (SP) für IACS-Anlagenbesitzer, das laut Norm häufig durch die Koordination und Integration mit dem ISMS der Organisation verbessert wird. IEC 62443-3-2 [47] definiert technische Maßnahmen, die einer Organisation als Leitfaden für das Risikomanagement von IACS dienen.

Bereichsübergreifende Aspekte des organisatorischen Cybersicherheitsmanagements

IEC 62443-2-1 in den Abschnitten 4 und 6 betont, dass ein IACS-SP das ISMS der Organisation ergänzen sollte, um eine koordinierte Betriebs- und Informationssicherheit zu erreichen. Die Norm weist darauf hin, dass die Abstimmung verbessert werden kann, indem Sicherheitsziele harmonisiert, Gemeinsamkeiten und Unterschiede formell dokumentiert und das SP in Übereinstimmung mit anderen Sicherheitsspezifikationen umgesetzt werden. Sie verlangt, dass ein Anlagenbesitzer, der über ein ISMS verfügt, das IACS SP damit abstimmen muss, was die Zusammenarbeit zwischen Sicherheitsadministratoren, die Verwaltung gemeinsamer Schnittstellen und die Behebung potenzieller Konflikte in Richtlinien und Praktiken umfasst. Darüber hinaus unterstreicht IEC 62443-2-1 Anhang B die Bedeutung der Integration des Geschäftsrisikomanagements in der gesamten Organisation und plädiert für einen nahtlosen und umfassenden Risikomanagementprozess, der die kontinuierliche Verbesserung risikobezogener Aktivitäten und eine effektive Kommunikation zwischen allen Beteiligten fördert.

Bereichsübergreifende Aspekte des Cybersicherheitsrisikomanagements

IEC 62443-3-2 in Abschnitt 4 verlangt von Organisationen, alle Zugangspunkte von Geschäftssystemen zum betrachteten System (SUC) zu identifizieren und sie in vom IACS getrennte Zonen zu gruppieren. Die Norm empfiehlt, Ergebnisse aus funktionalen Sicherheitsbewertungen einzubeziehen, um die schlimmsten Auswirkungen zu identifizieren, analog zu ISO/SAE 21434. Darüber hinaus schlägt die Norm vor, bestehende Risikobewertungen aus Bereichen wie der IT-Sicherheit zu überprüfen, um die Folgen und Auswirkungen besser bestimmen zu können.

Zusammenfassung der bereichsübergreifenden Leitlinien

Obwohl jede Norm in erster Linie einen bestimmten Bereich abdeckt, enthält jede auch Bestimmungen, die die Notwendigkeit einer bereichsübergreifenden Koordination hervorheben. ISO/SAE 21434 beispielsweise verlangt Kommunikationskanäle mit anderen Disziplinen, wenn externe Abhängigkeiten auftreten, legt Anforderungen an die Cybersicherheit fest und empfiehlt den Austausch von Prozessen, Tools, Bedrohungsszenarien oder Cybersicherheitszielen. Die Normenreihe ISO/IEC 27000 befürwortet hingegen ein breit angelegtes ISMS, das die Kriterien für die Risikoakzeptanz und die Definitionen der Grenzen über verschiedene Organisationsbereiche hinweg

vereinheitlicht. IEC 62443 verlangt in ähnlicher Weise die Abstimmung eines IACS SP mit dem ISMS der Organisation, und Anhang B von IEC 62443-2-1 unterstreicht die Bedeutung eines unternehmensweiten Risikomanagements und einer kontinuierlichen Zusammenarbeit.

Keine dieser Normen legt jedoch für sich genommen vollständig fest, wie das Cybersicherheitsrisikomanagement über alle Automobilbereiche hinweg vereinheitlicht werden kann. Ihre jeweiligen Anforderungen und Empfehlungen liefern die Bausteine, indem sie beispielsweise Kommunikationskanäle vorschreiben, Annahmen und externe Abhängigkeiten beschreiben oder die Angleichung von Risikokriterien befürworten, überlassen es jedoch den Organisationen, diese Elemente in eine kohärente Strategie zu integrieren. Das Ergebnis ist ein Flickenteppich aus bereichsübergreifenden Prozessen, die jeweils durch die jeweiligen Standards und die bestehenden Strukturen der Organisation geprägt sind. Im folgenden Abschnitt wird anhand von Experteninterviews untersucht, ob und wie Automobilhersteller diese Herausforderung derzeit in der Praxis angehen.

2.1.12.3 Experteninterviews zu bereichsübergreifendem Cybersicherheitsrisikomanagement

In diesem Abschnitt werden die Ergebnisse der halbstrukturierten Experteninterviews vorgestellt. Der erste Unterabschnitt umreißt die Ziele und Forschungsfragen der Studie, der zweite Unterabschnitt beschreibt die Methode und der dritte Unterabschnitt enthält die detaillierten Ergebnisse. Eine kurze Zusammenfassung im vierten Unterabschnitt schließt den Abschnitt ab, indem die Ergebnisse mit den angegebenen Zielen verknüpft werden.

Ziele und Forschungsfragen

Das Ziel der Studie war vielschichtig. Ein Ziel bestand darin, Informationen über den aktuellen Stand des bereichsübergreifenden Cybersicherheitsrisikomanagements in der Automobilindustrie zu sammeln und zu untersuchen, wie verschiedene Bereiche Cybersicherheitsrisiken identifizieren, bewerten und verwalten. Es war wichtig, festzustellen, inwieweit eine bereichsübergreifende Zusammenarbeit stattfindet und welche Strategien, Methoden und Instrumente eingesetzt werden. Von Interesse waren auch die bestehenden Herausforderungen und die Frage, ob es Gemeinsamkeiten oder Unterschiede in der Terminologie, den Prozessen und der Umsetzung von Vorschriften und Standards gibt.

Ein weiteres Ziel war es, Möglichkeiten und Maßnahmen zur Verbesserung der Koordination und Abstimmung zwischen den Bereichen zu identifizieren, um ein effektives bereichsübergreifendes Cybersicherheits-Risikomanagement zu etablieren. Es sollte untersucht werden, wie Risiken aus verschiedenen Bereichen verglichen werden können und ob ein Bedarf an verbesserten bereichsübergreifenden Strukturen besteht. Dazu wurden die Perspektiven der Befragten hinsichtlich der für die erfolgreiche Umsetzung eines solchen Managements erforderlichen Ressourcen sowie die Voraussetzungen und Einschränkungen beim Austausch von Risikodaten bewertet. Von weiterem Interesse war die Frage, wie Vorschriften und Standards durch ein bereichsübergreifendes Risikomanagement besser erfüllt werden können und welche Auswirkungen eine verbesserte Zusammenarbeit auf die Cybersicherheit und die Risikolandschaft des Unternehmens haben könnte.

Darüber hinaus zielte die Studie darauf ab, Empfehlungen und Best Practices zu entwickeln, die in die Gestaltung eines bereichsübergreifenden Cybersicherheits-Risikomanagements einfließen könnten. Es war wichtig zu erfahren, welche Maßnahmen die Befragten für sinnvoll halten, um die Wirksamkeit eines solchen Managements zu bewerten, und wie die Integration in bestehende Unternehmensprozesse erfolgen kann. Schließlich sollte das Potenzial untersucht werden, das sich

aus einer verbesserten Zusammenarbeit und Koordination zwischen den Bereichen ergeben könnte.

Auf der Grundlage dieser Ziele befasst sich die Studie mit den folgenden Forschungsfragen (RQs):

- RQ1 Status quo: Wie sieht die derzeitige Praxis des bereichsübergreifenden Cybersicherheitsrisikomanagements bei Automobilherstellern aus?
- RQ2 Machbarkeit und Anforderungen: Welche Organisationsstrukturen, Ressourcen und Voraussetzungen sind erforderlich, um ein effektives bereichsübergreifendes Cybersicherheits-Risikomanagement zu etablieren?
- RQ3 Chancen und Risiken: Welche Vorteile erwarten Praktiker von einem bereichsübergreifenden Ansatz und welche Herausforderungen oder Bedenken könnten dessen Einführung behindern?

Die Antworten auf diese Forschungsfragen werden im vierten Unterabschnitt zusammengefasst und in der Schlussfolgerung erneut aufgegriffen.

Methode

Es wurde ein qualitativer Forschungsansatz gewählt, der den Richtlinien von Edgar und Manz [196] zur Durchführung deskriptiver Studien folgt. Es wurden halbstrukturierte Interviews gewählt, da diese vordefinierte Fragen ermöglichen und gleichzeitig Flexibilität bieten, um auf der Grundlage der Erfahrungen der Teilnehmer neue Themen zu erforschen. Dieser Ansatz eignet sich gut für die Cybersicherheitsforschung, wo direkte Messungen komplex sind und Expertenwissen entscheidend ist, um vielschichtige Herausforderungen wie das bereichsübergreifende Cybersicherheits-Risikomanagement zu verstehen.

Stichprobe und Teilnehmer

Die Experten wurden anhand einer gezielten Stichprobe ausgewählt, um verschiedene Funktionen und Verantwortungsbereiche innerhalb der Automobilindustrie abzudecken. Sechs Fachleute aus sechs verschiedenen OEMs nahmen teil, die jeweils über fundierte bis Expertenkenntnisse im Bereich Cybersicherheitsrisikomanagement verfügten. Ihre Hintergründe umfassten Fahrzeug-Cybersicherheitsarchitektur, Unternehmens-IT-Sicherheit, Automobilproduktion und Beratungsfunktionen, wodurch eine Vielzahl von Perspektiven zur bereichsübergreifenden Koordination gewährleistet war. Die sechs ausführlichen Interviews reichten aus, um eine thematische Sättigung zu erreichen, wie sie in explorativen Studien üblich ist [197].

Durchführung der Interviews

Es wurde ein Interviewleitfaden entwickelt und intern sowie von einem Branchenexperten begutachtet, um Relevanz und Klarheit sicherzustellen. Die Interviews wurden zwischen Juli und Oktober 2024 durchgeführt. Vor Beginn der Interviews wurde die Zustimmung der Teilnehmer eingeholt und diese über den Zweck der Studie, die freiwillige Teilnahme und die Anonymität informiert. Jedes Interview dauerte zwischen 60 und 120 Minuten, wurde auf Deutsch geführt und unter Einhaltung der Europäischen Datenschutz-Grundverordnung (DSGVO) über Microsoft Teams aufgezeichnet. Die Interviews wurden transkribiert und die Transkripte durch Entfernen von Namen und persönlichen oder Unternehmensinformationen anonymisiert. Die in den Fragebogen eingebetteten Transkripte wurden den Teilnehmern zur Anpassung und Bestätigung zugesandt und erst nach Bestätigung analysiert. Die endgültige Bestätigung der Transkripte ging im Februar 2025 ein.

Die Teilnehmer wurden um ihre Zustimmung gebeten, ihre vollständig ausgefüllten Fragebögen, die den Interviewleitfaden und die anonymisierten Transkripte enthalten, öffentlich zugänglich zu machen. Das zur Veröffentlichung freigegebene Material wird für wissenschaftliche und pädagogische Zwecke zur Verfügung gestellt²², um die Transparenz und Reproduzierbarkeit der Ergebnisse zu gewährleisten. Die anonymisierten Transkripte wurden für Berichts- und Dokumentationszwecke mit DeepL Pro Advanced aus dem Deutschen ins Englische übersetzt, und alle Übersetzungen wurden anschließend auf Genauigkeit und Konsistenz überprüft.

Datenanalyse

Alle sechs Transkripte bildeten den Datensatz, der einer induktiven Kodierung auf der Grundlage etablierter Verfahren für qualitative Forschung unterzogen wurde [198, 199]. Die Codes wurden den wiederkehrenden Ideen, Praktiken und Anliegen der Experten zugeordnet. Obwohl die Häufigkeiten in Tabellen und Abbildungen angegeben sind, dienen diese eher als Indikator für die Häufigkeit eines Themas und nicht als definitive Messgröße für dessen Bedeutung. Nach der Kodierung wurden die Ergebnisse unter thematischen Überschriften kategorisiert, die die Ziele der Studie widerspiegeln, nämlich den Status quo, die Machbarkeit und die Anforderungen zu erfassen, und Chancen und Risiken. Eine schnelle Überprüfung der Antworten im Vergleich zu den Rollen der Teilnehmer ergab keine systematischen Unterschiede, sodass alle Ergebnisse in zusammengefasster Form dargestellt werden.

Ergebnisse

Status Quo

Die Interviews ergaben ein vielfältiges Bild des bereichsübergreifenden Cybersicherheitsrisikomanagements. Vier Experten bestätigten, dass sie über eine spezielle Strategie verfügen, während zwei keine Kenntnis davon hatten oder sich unsicher waren. Obwohl bestehende Strategien oft auf spezifischen Managementsystemen basieren, ist die Koordination zwischen den Bereichen nach wie vor unzureichend. Einige Experten heben zentrale Funktionen oder Ausschüsse als entscheidend für eine effektive Zusammenarbeit hervor, während andere auf Kommunikationslücken und eine isolierte Risikobehandlung hinweisen. Ein vollständig etabliertes bereichsübergreifendes Rahmenwerk scheint in der Automobilindustrie daher selten zu sein.

Innerhalb der einzelnen Bereichen findet oft ein einheitliches Risikomanagement statt, aber die Praktiken bleiben heterogen und weitgehend unabhängig voneinander. Unterschiedliche Prozesse und Methoden behindern die Zusammenarbeit und Kommunikation. Mehrere Experten erkennen bestehende Abhängigkeiten und plädieren für eine stärkere Koordination. Um die Konsistenz und Vergleichbarkeit zu verbessern, wird eine einheitliche Risikomatrix vorgeschlagen.

Experten bestätigen, dass zwischen den Bereichen ein gewisser Austausch stattfindet, jedoch in unterschiedlichem Umfang und mit unterschiedlichen Strukturen. Obwohl formelle Prozesse bis zu einem gewissen Grad vorhanden sind, führen inkonsistente Kommunikation und unvollständige Übertragung von Claims zu Lücken im Risikomanagement. Mehrere Kanäle und teilweise implementierte Prozesse erschweren eine effektive Zusammenarbeit zwischen den Bereichen zusätzlich.

²² <https://dx.doi.org/10.24406/fordatis/399>

Die Interviews zeigen auch, dass die Bereichen unterschiedliche Cybersicherheitstools und Risikobewertungsmethoden verwenden, was den Informationsaustausch erschwert. Zwar überschneiden sich einige Vorlagen oder Prozesse, doch gibt es keine zentralisierte Datenverarbeitung oder standardisierte Tools, was nach Ansicht der Experten die Effizienz einschränkt und die Verwendung einheitlicher Lösungen empfiehlt.

In Bezug auf Vorschriften und Standards spielen die UN-Vorschrift Nr. 155 und ISO/SAE 21434 eine zentrale Rolle, wobei einige Experten auch auf die ISO/IEC 27000-Familie für IT-Kontexte verweisen. Einige wenige heben widersprüchliche Anforderungen aufgrund regionaler Unterschiede hervor, während andere keine Konflikte sehen, da sie sich auf Standards innerhalb ihres Bereichs konzentrieren. Insgesamt sehen sich Unternehmen verschiedenen regulatorischen Beschränkungen gegenüber, was die Harmonisierung und Umsetzung mehrerer Standards erschwert.

Schließlich gibt es keine einheitliche bereichsübergreifende Terminologie für das Cybersicherheits-Risikomanagement, was zu Kommunikationsproblemen führt. Obwohl die Bereiche möglicherweise ein einheitliches internes Vokabular verwenden, weichen diese aufgrund unterschiedlicher Prioritäten und Referenzen oft voneinander ab. Einige Experten berichten von einem grundlegenden gemeinsamen Verständnis, aber uneinheitliche Terminologie erschwert nach wie vor die Zusammenarbeit. Die meisten halten es für unerlässlich, Begriffe zu standardisieren, um die Effektivität des bereichsübergreifenden Cybersicherheits-Risikomanagements zu erhöhen. Tabelle 13 zeigt die induktiven Codes. Der Gesprächskontext, aus dem jeder Code abgeleitet wurde, ist in den anonymisierten Transkripten zu finden (siehe Fußnote²²).

Tabelle 13: Themen und induktive Codes mit Häufigkeiten für den Status quo

Thema	Induktive Codes [Häufigkeit]
Vorhandensein von Strategien	Vorhandensein einer bereichsübergreifenden Strategie zum Management von Cybersicherheitsrisiken [4] Einsatz spezifischer Managementsysteme (z. B. CSMS, ISMS) [2] Koordination und Schnittstellen zwischen Systemen/Bereichen [2] Unklarheit oder mangelnde Kenntnisse über eine bereichsübergreifende Strategie [2] Strategien existieren, sind jedoch nicht vollständig etabliert oder dokumentiert [2] Risiken werden in einzelnen Bereichen separat behandelt [3] Allgemeines Risikomanagement ohne besonderen Fokus auf Cybersicherheit [2] Verbesserungsbedarf bei der bereichsübergreifenden Zusammenarbeit [2]
Einheitlichkeit und gegenseitige Abhängigkeit der Praktiken	Homogenität innerhalb der Bereiche [5] Heterogenität zwischen Bereichen/Managementsystemen [4] Unabhängigkeit zwischen Bereichen [3] Abhängigkeiten zwischen Bereichen/Managementsystemen [2] Verwendung derselben Methoden/Prozesse (z. B. Risikomatrix) [2]
Bereichsübergreifen der Austausch und	Austausch zwischen den Bereichen besteht [6] Formelle Prozesse oder Strukturen bestehen [3] Herausforderungen bei der direkten Kommunikation zwischen Bereichen [2] Probleme oder Herausforderungen bei der Kommunikation oder bei Prozessen [2] Prozesse sind nicht vollständig implementiert oder es gibt Verbesserungspotenzial [2]

Zusammenarbeit	Forderungen werden nicht korrekt übertragen oder das Backend wird nicht informiert [3]
Verwendete Methoden und Tools	Unterschiedliche Tools/Methoden in den Bereichen [4] Verwendung von Excel-basierten Tools für das Risikomanagement [2] Ähnliche oder identische Vorlagen/Prozesse zwischen den Bereichen [3] Unterschiedliche Methoden zur Risikobewertung (qualitativ vs. quantitativ) [2]
Vorschriften und Normen	Verwendung der UN-Vorschrift Nr. 155 [5] Verwendung von ISO/SAE 21434 [6] Verwendung der ISO 27000-Familie [3] Verwendung anderer regulatorischer Anforderungen weltweit [4] Es bestehen widersprüchliche/kontradiktorische Anforderungen [2] Keine widersprüchlichen Anforderungen bekannt [3]
Es gibt eine einheitliche Terminologie	Es gibt keine bereichsübergreifende einheitliche Terminologie [4] Es besteht ein gemeinsames Verständnis, aber die Terminologie unterscheidet sich [2] Einheitliche Terminologie innerhalb bestimmter Managementsysteme/Funktionen [2] Verschiedene Bereiche verwenden aufgrund ihres Schwerpunkts unterschiedliche Terminologien [2]

Machbarkeit und Anforderungen

Experten betonen, dass die gemeinsame Nutzung von Risiken und Schwachstellen zwischen den Bereichen die Transparenz erhöht und ein effektiveres Risikomanagement ermöglicht. Ein gemeinsames Verständnis der technischen Probleme und der Zuständigkeitsbereiche anderer Bereiche fördert die bereichsübergreifende Zusammenarbeit und verhindert Missverständnisse. Der Austausch bewährter Verfahren wird als wertvolle Möglichkeit angesehen, voneinander zu lernen und effiziente Ansätze zu entwickeln.

Risikodaten sollten mit anderen Bereichen geteilt werden, wenn sie für diese relevant sind und sie direkt betreffen. Für vertrauliche oder sensible Informationen gelten Einschränkungen, wobei ein Rechte- und Rollenkonzept den Zugriff regelt. Während die meisten beim Austausch sensibler Daten vorsichtig sind, befürwortet ein Experte einen uneingeschränkten internen Austausch.

Die Meinungen darüber, ob Risiken in verschiedenen Bereichen direkt verglichen werden können, gehen auseinander. Einige bestehen auf einheitlichen Tools, gemeinsamen Prozessen und einer gemeinsamen Terminologie, während andere auf erhebliche kontextspezifische Einschränkungen hinweisen. Die Angleichung der Auswirkungskriterien kann sowohl vorteilhaft als auch problematisch sein, da sie eine Vergleichbarkeit ermöglicht, wenn die Bereiche eng miteinander verbunden sind, andernfalls jedoch weniger.

Experten betonen auch, dass eine erfolgreiche bereichsübergreifende Cybersicherheit angemessene Budgets für qualifiziertes Personal und Technologie sowie die Unterstützung durch die oberste Führungsebene erfordert. Funktionsübergreifende Spezialisten helfen dabei, Domänen zu überbrücken, und standardisierte Prozesse sowie klar definierte Verantwortlichkeiten steigern die Effizienz und Effektivität.

Die meisten Befragten halten die Integration des Cybersicherheitsrisikomanagements in Geschäftsprozesse für notwendig und wünschenswert. Einige sehen jedoch regulatorische

Anforderungen als treibende Kraft, während andere kulturelle Barrieren oder widersprüchliche Ziele anführen, die die Einführung behindern könnten.

Um die Koordination zu verbessern, empfehlen Experten die Einführung zentraler Funktionen, die Bildung bereichsübergreifender Teams oder Gemeinschaften und die Benennung von Mediatoren zur Erleichterung der Kommunikation. Die Standardisierung von Methoden, Tools und Prozessen wird als unerlässlich angesehen; Schulungsprogramme und ein größeres Bewusstsein werden ebenfalls als Schlüssel zur Förderung einer gemeinsamen Cybersicherheitskultur angesehen.

Zur Bewertung der Wirksamkeit schlagen Experten vor, die Risikominderung im Zeitverlauf zu messen, einschließlich der Vorfalldaten und Reaktionszeiten, Audits zur Überprüfung der Compliance und zur Ermittlung von Verbesserungsmöglichkeiten durchzuführen und KPIs oder IT-Tools zur Verfolgung von Risiken und Maßnahmen zu implementieren. Die Definition übergeordneter Kennzahlen bleibt jedoch eine Herausforderung.

Die Befragten weisen darauf hin, dass eine bessere bereichsübergreifende Zusammenarbeit die Einhaltung gesetzlicher Vorschriften durch Transparenz und eine einheitliche Auslegung der Anforderungen verbessert. Die Kenntnis aller relevanten Vorschriften ermöglicht eine ganzheitlichere Sichtweise und hilft dabei, Überschneidungen oder Unstimmigkeiten zu erkennen. Die Zusammenarbeit rationalisiert ebenfalls die Prozesse, indem sie Missverständnisse reduziert und die Effizienz verbessert.

Externe Partner können durch einen Ausgleich zwischen Wissensaustausch und Vertraulichkeit effektiv einbezogen werden. Experten raten dazu, Sicherheitsanforderungen frühzeitig in Verträgen festzulegen und Lieferanten aktiv in Vorfälle einzubeziehen, um die Reaktion und Zusammenarbeit zu stärken. Technologische Schnittstellen mit kontrolliertem Zugriff können einen sicheren Austausch erleichtern.

Die rollenbasierte Zugriffskontrolle wird als unerlässlich angesehen, um sensible Daten auf autorisierte Personen zu beschränken. Technische Schutzmaßnahmen, z. B. Authentifizierung und Autorisierung, bieten zusätzlichen Schutz vor unbefugtem Zugriff. Tabelle 14 enthält Einzelheiten zu diesen Codes.

Tabelle 14: Themen und induktive Codes mit Häufigkeiten für Anforderungen und Machbarkeit

Thema	Induktive Codes [Häufigkeit]
Gemeinsame Informationen und deren Nutzen	Austausch von Risiken und Schwachstellen zwischen Bereichen [4] Verständnis technischer Objekte und ihrer Beschreibung [1] Verständnis der Verantwortlichkeiten und Probleme anderer Bereiche [1] Bewährte Verfahren und Erfahrungen [1]
Bedingungen für den Austausch von Risikodaten	Risikodaten werden geteilt, wenn sie für andere Bereiche relevant sind [4] Einschränkungen für vertrauliche oder sensible Informationen [3] Befürwortung eines uneingeschränkten Austauschs von Risikodaten innerhalb des Unternehmens [1]
Methoden zum Vergleich	Bedeutung standardisierter Tools zur Gewährleistung der Vergleichbarkeit [3] Herausforderungen beim Vergleich von Risiken aufgrund unterschiedlicher Kontexte [3] Notwendigkeit einer standardisierten Terminologie oder einer gemeinsamen Sprache [2] Harmonisierung der Auswirkungskriterien ist vorteilhaft [2]

Risiken zwischen Bereichen	Harmonisierung der Auswirkungskriterien ist schwierig oder nicht sinnvoll [2] Verwendung standardisierter Risikomatrizen und Risikomanagement-Rahmenwerke [2] Vergleichbarkeit ist nur innerhalb eng verwandter Bereiche möglich [2]
Erforderliche Ressourcen	Notwendigkeit klarer Zuständigkeiten/Mandate/Rollen [2] Notwendigkeit eines Budgets für Personal/Ressourcen [4] Notwendigkeit von Tools/technologischen Investitionen (z. B. einheitliche Tools) [3] Notwendigkeit von Experten, die bereichsübergreifend arbeiten können [3] Notwendigkeit der Unterstützung durch die oberste Führungsebene [2] Notwendigkeit standardisierter Prozesse und Methoden [2]
Integration in bestehende Prozesse	Integration ist notwendig und sollte stattfinden [4] Integration ist möglich, erfordert jedoch ausreichenden Druck oder Treiber [1] Integration ist möglich, wird jedoch durch kulturelle Konflikte oder Zielkonflikte behindert [1]
Maßnahmen zur Verbesserung der der Koordination	Einführung zentraler Rollen/Verantwortlichkeiten zur Verbesserung der Koordination [3] Einrichtung bereichsübergreifender Ausschüsse zur Förderung des Austauschs [3] Einsatz bereichsübergreifender Mediatoren zur Verbesserung der Kommunikation [2] Schulungen und Sensibilisierungsmaßnahmen zur Förderung einer Cybersicherheitskultur [1] Standardisierte Prozesse, Methoden und Tools [1]
Bewertung der Wirksamkeit	Messung der Risikominderung im Zeitverlauf als Wirksamkeitsindikator [2] Audits zur Bewertung der Wirksamkeit und Einhaltung von Prozessen [2] Verwendung von KPIs zum Vergleich vor und nach der Implementierung [2]
Einhaltung von Vorschriften und Standards	Bedeutung von Transparenz und Austausch zwischen den Bereichen, um Vorschriften/Normen besser zu erfüllen [2] Koordinierte Auslegung und Umsetzung von Vorschriften und Standards [3] Bereichsübergreifendes Risikomanagement führt zu mehr Transparenz und besserer Übersicht über Vorschriften/Risiken [2] Bereichsübergreifendes Risikomanagement erleichtert die Einhaltung von Vorschriften/Standards [1] Einsatz von Automatisierung und KI zur Einhaltung von Vorschriften und Standards [1]
Einbeziehung externer Parteien	Notwendigkeit, den technischen Austausch mit Vertraulichkeit/IP-Schutz in Einklang zu bringen [2] Festlegung von Sicherheitsanforderungen für Lieferanten in Verträgen [2] Lieferanten in die Bearbeitung von Vorfällen und die Zusammenarbeit einbeziehen [2] Einbeziehung von Lieferanten über geeignete Schnittstellen/Systeme mit rollenbasiertem Zugriff [2]
Datenschutz und Sicherheitsaspekte	Implementierung eines rollenbasierten Zugriffskontrollsystems [4] Beschränkung des Zugriffs auf sensible Risikodaten zwischen Bereichen und auf autorisierte Personen [4] Einsatz technischer Schutzmaßnahmen, z. B. Authentifizierung, Autorisierung, Sicherheitsprinzipien [3]

Chancen und Risiken

Experten sehen Vorteile wie ein verbessertes Risikomanagement, Kosteneinsparungen und schnellere Reaktionen durch bereichsübergreifende Cybersicherheit. Ein ganzheitlicher Risikoüberblick unterstützt fundierte Entscheidungen, während die Koordinierung von Maßnahmen über Bereichen hinweg die Ressourcennutzung optimiert und Strategien vereinheitlicht. Der Zugriff auf zentralisierte Tools erleichtert die Zusammenarbeit und die Umsetzung von Schutzmaßnahmen.

Die Experten betonen, dass der Austausch von Methoden, Tools und Prozessen zwischen den Bereichen die Effizienz und das gegenseitige Verständnis fördert, obwohl eine direkte Übernahme möglicherweise eine Anpassung an die Bedürfnisse der einzelnen Bereiche erfordert.

Bei der Einführung eines bereichsübergreifenden Risikomanagements sehen die Experten Risiken wie Informationslecks, Missverständnisse, hohe Bürokratie und Verlust der Autonomie. Um diese zu minimieren, empfehlen sie klare Zugriffsrechte, Datenschutzmaßnahmen und kontextbezogene Risikodaten. Die Vereinfachung von Prozessen und die aktive Einbindung der Mitarbeiter werden als wesentlich angesehen, um Widerstände zu überwinden. Darüber hinaus sollten technische Sicherheitsmaßnahmen und die Unterstützung durch die Unternehmensleitung sichergestellt werden.

Die Experten betonen, dass eine verbesserte bereichsübergreifende Zusammenarbeit und ein ganzheitlicher Überblick über die Risikolandschaft zu erheblichen Kosteneinsparungen führen, die Cybersicherheit des Unternehmens verbessern und bessere Entscheidungsgrundlagen schaffen. Wirtschaftliche Vorteile ergeben sich aus effizienteren Prozessen, der Vermeidung von Doppelarbeit und einer optimalen Ressourcenzuweisung. Eine umfassende Risikobetrachtung ermöglicht fundierte Entscheidungen und reduziert das Gesamtrisiko. Die Transparenz wird erhöht, Redundanzen können beseitigt und Lücken identifiziert werden, wodurch die Wirksamkeit der Schutzmaßnahmen erhöht wird. Tabelle 15 listet die relevanten Codes auf.

Tabelle 15: Themen und induktive Codes mit Häufigkeiten für Chancen und Risiken

Thema	Induktive Codes [Häufigkeit]
Vorteile für das Unternehmen und einzelne Geschäftsbereiche	Besseres Risikomanagement / ganzheitliche Betrachtung von Risiken [3] Kosteneinsparungen durch effizientere Ressourcenzuweisung [5] Verbesserte Kommunikation und gegenseitiges Verständnis zwischen den Bereichen [1] Verbesserte Risikominimierung / schnellere Reaktion auf Risiken [3] Vereinfachte Entscheidungsfindung durch eine einheitliche Strategie [3] Zugang zu zentral bereitgestellten Ressourcen und Tools / einheitliche Tools [2]
Von anderen Bereichen lernen	Der Austausch von Methoden, Werkzeugen und Prozessen kann von Vorteil sein [5] Der Erfahrungsaustausch durch Zusammenarbeit verbessert die Zusammenarbeit zwischen den Bereichen [4] Notwendigkeit der Anpassung; nicht alles ist direkt übertragbar [2]
Mögliche Risiken oder Bedenken	Informationslecks an unbefugte Dritte [4] Missverständnisse aufgrund falsch interpretierter Risikodaten aus anderen Bereichen [2] Hohe Komplexität und Bürokratie bei der Einführung [2]

	Verlust der Autonomie in den einzelnen Bereichen [1]
	Widerstand gegen Veränderungen und Silo-Denken [2]
	Verlust des Überblicks über relevante Risiken bei zu vielen Informationen [1]
Auswirkungen auf die allgemeine Cybersicherheit	Wirtschaftliche Vorteile durch Kosteneinsparungen oder besseres Risikomanagement [4]
	Ganzheitlicher Überblick verbessert die Entscheidungsfindung und verdeutlicht das Gesamtrisiko [5]

Direkte Anfragen

Zusätzlich zu den offenen Diskussionen beantworteten die Teilnehmer direkte Anfragen und konnten weitere Informationen in ihre Antworten einfließen lassen. Abbildung 31 zeigt, wie oft Experten Informationen einbeziehen und wie gut sie über Vorschriften aus anderen Bereichen informiert sind. Die Antworten reichten von häufigem, relevanzbasiertem Austausch bis hin zu seltenen Interaktionen. Ein Experte stellte fest, dass Backend- und Produktionsannahmen konsequent einbezogen werden, was die wiederkehrende Zusammenarbeit unterstreicht. Auch das Bewusstsein für die Cybersicherheitsstandards und -vorschriften anderer Bereiche variiert. Einige Experten berichten von guten bereichsübergreifenden Kenntnissen, andere geben zu, sich auf ihren spezifischen Bereich zu konzentrieren. Unterdessen gehen die Meinungen darüber auseinander, ob die aktuellen Vorschriften widersprüchlich oder konsistent sind, wobei Faktoren wie regionale Unterschiede und sich weiterentwickelnde Regelwerke die Meinungen prägen.

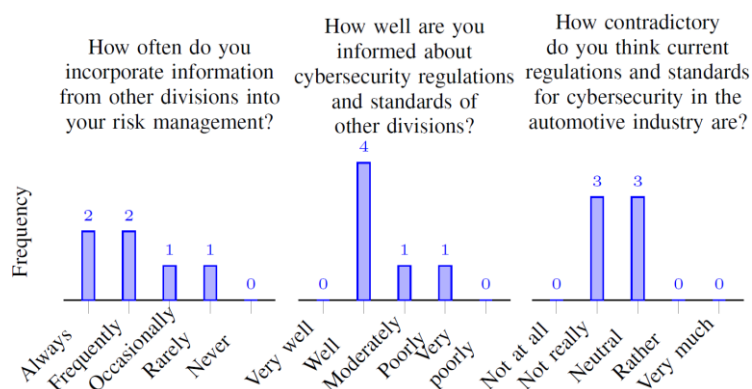


Abbildung 31: Einbeziehung von Informationen und Kenntnis der Vorschriften in den verschiedenen Bereichen

Abbildung 32 zeigt, wie Experten die Vorteile und Herausforderungen der bereichsübergreifenden Cybersicherheit bewerten. Viele sehen starke oder sehr starke Auswirkungen, insbesondere bei der bereichsübergreifenden Bewertung von Vorfällen und der effizienten Bearbeitung von Vorfällen. Die meisten Experten bewerteten den Nutzen eines bereichsübergreifenden Cybersicherheits-Risikomanagements für die Verbesserung der Cybersicherheit als hoch bis sehr hoch. Einige betonten die Verbesserung der Sicherheitskultur und die Fähigkeit, über Silos hinweg zu arbeiten. Ein anderer Experte erkannte dessen Bedeutung an, wies jedoch darauf hin, dass die Unternehmenskultur eine wichtige Rolle spielt. Die meisten sind sich einig, dass die Integration von Daten aus verschiedenen Quellen technisch schwierig ist und einheitliche Metriken oder eine höhere Abstraktionsebene erfordert.

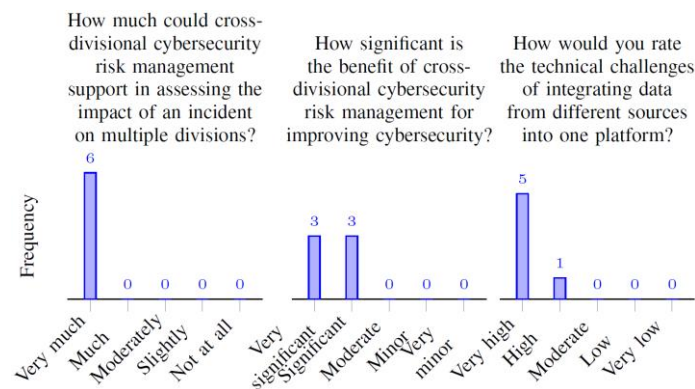


Abbildung 32: Wahrgenommene Vorteile und Herausforderungen

Schließlich zeigt Abbildung 33, dass weitgehend Einigkeit darüber besteht, dass eine einheitliche Terminologie und Datennormalisierung von großer Bedeutung sind. Ein Experte betonte, dass ein gemeinsames Verständnis für fundierte Entscheidungen von entscheidender Bedeutung ist. Die Normalisierung von Risikodaten wurde als unerlässlich angesehen, insbesondere für automatisierte Bewertungen und Auditberichte, wobei einige Experten darauf hinwiesen, dass dies ein robustes Risikomanagement unterstützt. Die meisten Befragten halten den Austausch von Best Practices zwischen den Bereichen für ebenso wichtig für Effizienzsteigerungen und bessere Risikostrategien, obwohl einer darauf hinwies, dass nicht alle Maßnahmen direkt übertragbar sind. Dennoch sind die grundlegenden Erkenntnisse und Einsichten nach wie vor von unschätzbarem Wert für die Verbesserung der allgemeinen Cybersicherheitslage eines Unternehmens.

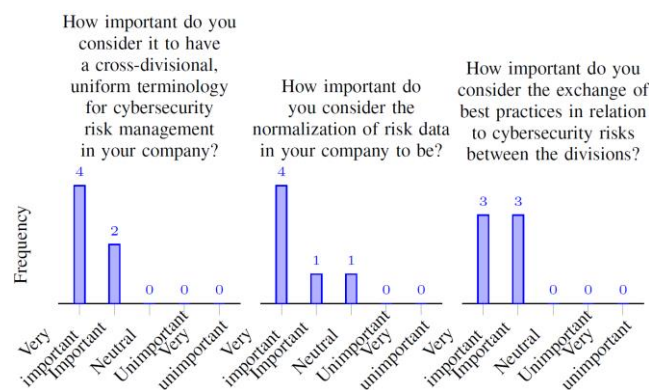


Abbildung 33: Bedeutung einer einheitlichen Terminologie und Datenstandardisierung

Zusammenfassung

Die Ergebnisse der Befragung bestätigen den dringenden Bedarf an einer stärker integrierten, bereichsübergreifenden Cybersicherheit. Sie liefern auch direkte Antworten auf die im ersten Unterabschnitt aufgeführten Forschungsfragen:

RQ1 (Status quo). Die meisten OEMs verfügen nur über fragmentarische, bereichsspezifische Strategien; Methoden, Tools und Terminologie sind nach wie vor heterogen und die Koordinationskanäle sind schwach.

RQ2 (Machbarkeit und Anforderungen). Praktiker halten Führungsaufträge, gemeinsame Tools, rollenbasierten Zugriff, bereichsübergreifende Funktionsspezialisten und harmonisierte Prozesse für den Erfolg unerlässlich.

RQ3 (Chancen und Risiken). Zu den erwarteten Vorteilen zählen ein ganzheitlicher Risikoüberblick, eine schnellere Bearbeitung von Vorfällen, Kosteneinsparungen und eine einfachere Einhaltung von Vorschriften, denen jedoch Bedenken hinsichtlich Informationslecks, Bürokratie und Verlust der Bereichsautonomie gegenüberstehen.

Diese Erkenntnisse bilden die Grundlage für die Empfehlungen und Schlussfolgerungen, die im nächsten Abschnitt erörtert werden.

2.1.12.4 Fazit

Diese Studie bietet einen detaillierten Einblick in das bereichsübergreifende Cybersicherheits-Risikomanagement in der Automobilindustrie und zeigt, wie Standards wie ISO/SAE 21434, die ISO/IEC 27000-Familie und die IEC 62443-Reihe in erster Linie domänenspezifische Probleme behandeln, jedoch nicht vollständig vorschreiben, wie diese Bemühungen bereichsübergreifend koordiniert werden sollen. Wie aus Experteninterviews hervorgeht, wenden Unternehmen verschiedene bereichsübergreifende Praktiken an, werden jedoch durch uneinheitliche Terminologie, fragmentierte Risikobewertungsmethoden und begrenzte Kommunikationskanäle behindert. Diese Ergebnisse lassen sich auch direkt auf die im ersten Unterabschnitt gestellten Forschungsfragen übertragen: RQ1 – Der aktuelle Zustand ist fragmentiert; RQ2 – Eine effektive Integration hängt von der Unterstützung durch die Führungskräfte, gemeinsamen Tools, einer klaren Governance und einem rollenbasierten Datenzugriff ab; RQ3 – Praktiker erwarten eine ganzheitliche Risikobetrachtung, eine schnellere Bearbeitung von Vorfällen, Kosteneinsparungen und eine bessere Compliance, die jedoch durch Bedenken hinsichtlich Informationslecks und zusätzlicher Bürokratie gedämpft werden.

Durch die gemeinsame Betrachtung dieser Standards und der Erkenntnisse aus der Praxis wird deutlich, dass ein integrierter Ansatz mit standardisierten Tools, Prozessen und Begrifflichkeiten die Zusammenarbeit, die Risikotransparenz und die Einhaltung gesetzlicher Vorschriften erheblich verbessern könnte. Die Angleichung domänenspezifischer Richtlinien unter einem gemeinsamen Rahmenwerk kann operative Ineffizienzen reduzieren, die Ziele der einzelnen Bereiche vereinheitlichen und die Cybersicherheit insgesamt verbessern. Zukünftige Forschungsarbeiten sollten sich auf die Entwicklung kohärenter Strategien konzentrieren, die relevante Leitlinien aus allen drei Standards berücksichtigen und gleichzeitig organisatorische Strukturen und kulturelle Faktoren einbeziehen. Weitere Studien könnten auch untersuchen, wie die Unterstützung durch das Top-Management und strukturierte Governance-Mechanismen die Einführung und Aufrechterhaltung eines robusten bereichsübergreifenden Cybersicherheits-Risikomanagements in der Automobilbranche erleichtern und gewährleisten können.

Organisationen müssen angesichts sich ständig weiterentwickelnder Cyber-Bedrohungen agil bleiben.

2.1.12.5 Usability

In diesem Unterkapitel werden aufbauend auf den Experteninterviews Anforderungen und Empfehlungen beschrieben, die sich speziell für die nutzendenfreundliche Gestaltung eines bereichsübergreifenden Risikomanagement-Werkzeugs ergeben. Im Fokus steht dabei ein SharePoint-basiertes System, die Prinzipien sind jedoch allgemeiner auf andere Werkzeuge übertragbar.

Ein zentraler Aspekt betrifft die **Kommunikation**. Das Werkzeug sollte klare Kommunikationsstrukturen und -kanäle unterstützen, um die Entstehung von „Silos“ zu vermeiden und gezielten Informationsaustausch genau dort zu ermöglichen, wo er zielführend ist. Analog zu Nielsens

Heuristik #8 („Aesthetic and Minimalist Design“) sollte unnötige Information vermieden werden, da sie Wichtiges überdecken kann; das System sollte daher helfen, relevante Informationen zu filtern und kontextbezogen darzustellen. Wo immer möglich sollte der Austausch von Informationen automatisiert auf Basis festgelegter Prozesse oder Bedingungen erfolgen (z. B. automatische Benachrichtigung anderer Bereiche bei Änderungen an bestimmten Risiken oder Controls). Wichtig ist zudem, bereichsübergreifende Kommunikationskanäle explizit für Risiken zu unterstützen – sowohl, weil gleiche Risiken in unterschiedlichen Bereichen auftreten können, als auch, weil Abhängigkeiten zwischen Bereichen bestehen. Das Werkzeug sollte die Zuweisung von Verantwortlichkeiten über Bereichsgrenzen hinweg ermöglichen und sichtbar machen. Für eine gemeinsame Sprache ist entscheidend, dass klar wird, worüber gesprochen wird (technischer Gegenstand) und wie dieser beschrieben wird: dieselben Objekte werden in verschiedenen Bereichen aus unterschiedlichen Blickwinkeln betrachtet, dem die Struktur und Terminologie des Systems gerecht werden muss (siehe hierzu auch die Anforderungen an die Dokumentation). Darüber hinaus sind Schutz- und Steuerungsmöglichkeiten für den Informationsaustausch notwendig, etwa zur Kontrolle, welche Informationen an Dritte (Partner, Zulieferer) weitergegeben werden und wie interne Interessenkonflikte (konkurrierende Bereiche) adressiert werden. Das System sollte Nutzende dabei unterstützen, zwischen dem Schutz sensibler Informationen und dem Nutzen des Informationsaustauschs abwägen zu können. Nicht zuletzt sollte ein Erfahrungsaustausch über Risiken, Maßnahmen und gelernte Lektionen aktiv gefördert werden, etwa durch gemeinsame Arbeitsräume oder Kommentarfunktionen auf Artefakt-Ebene.

Ein zweiter Themenkomplex betrifft die **Übertragbarkeit** von Inhalten. Grundsätzlich sollte das Werkzeug die Übertragbarkeit von Dokumentationen zwischen Bereichen ermöglichen, ohne eine vollständige Vereinheitlichung zu erzwingen. Übertragbarkeit ist damit ein Angebot, keine Pflicht. Konkret sollte das System erlauben, Risiken mitsamt ihrer Dokumentation, geplanten Methoden und Bewertungen in andere Bereiche zu übertragen – inklusive der Möglichkeit einer Art „Vererbung“, wenn Schäden an einem System unmittelbar Schäden an anderen Systemen nach sich ziehen oder wenn die Sicherheit eines Systems von anderen Komponenten abhängt. Analog dazu sollte das Werkzeug die Übertragung von Maßnahmen, Methoden (z. B. für Steuerung und Überwachung), Prozessen und formalisierten Praktiken unterstützen, etwa indem etablierte Controls oder Workflows als Vorlage in anderen Bereichen wiederverwendet werden können. Ebenso sollte es möglich sein, Werkzeuge (z. B. Bewertungsverfahren, Scoring-Schemata) oder deren Ergebnisse so abzubilden, dass sie in anderen Bereichen übernommen oder referenziert werden können, ohne bestehende bereichsspezifische Werkzeuge zu verdrängen.

Eng damit verknüpft ist die **Flexibilität** des Systems. Ein bereichsübergreifendes Risikomanagement-Werkzeug muss hinreichend flexibel gestaltet sein, um unterschiedlichen Organisationsformen und Domänenlogiken gerecht zu werden. Es sollte zulassen, dass verschiedene Bereiche unterschiedliche Methoden für die Behandlung gleicher Risiken einsetzen – etwa unterschiedliche Impact-Kriterien, Schadensstufen oder Bewertungsverfahren – und trotzdem eine übergreifend einheitliche Erfassung und gegebenenfalls das Teilen von Informationen ermöglichen. Verantwortlichkeiten sollten klar getrennt werden können; Kopplungen zwischen Bereichen sind dort zu ermöglichen, wo sie sinnvoll sind, sollten sich aber feingranular steuern lassen, um unnötige Abhängigkeiten zu vermeiden. Die bereichsübergreifende Risikosteuerung sollte durch das Werkzeug unterstützt, aber nicht erzwungen werden: Bereiche müssen ihre eigenen Prozesse weiterführen können, während sie dort „andocken“, wo gemeinsame Risiken oder Abhängigkeiten bestehen. Technisch sollte das System Schnittstellen bieten, um proprietäre Tools und Lösungen für das Risikomanagement einzubinden, statt ein exklusives Monolith-Werkzeug zu erzwingen. Wo

unterschiedliche technische, organisatorische oder rechtliche Anforderungen bestehen, muss das Werkzeug die Möglichkeit bieten, verschiedene Varianten von Maßnahmen zum gleichen Risiko abzubilden (z. B. unterschiedliche Controls pro Markt oder Domäne), um alle Anforderungen gleichzeitig abzudecken.

Als Querschnittsfunktion spielt die **Dokumentation** eine wesentliche Rolle für die Usability. Das System sollte eine klare, konsistente Dokumentation unterstützen, die auch bereichsübergreifend verständlich ist – inklusive solcher Inhalte, die im eigenen Bereich vermeintlich „selbsterklärend“ sind. Gleichzeitig ist ein kontrollierter bereichsübergreifender Zugriff auf relevante Dokumente zu ermöglichen. Verantwortlichkeiten sollten auf verschiedenen Ebenen nachvollziehbar dokumentiert werden: von einzelnen Risiken und Maßnahmen (z. B. „Risk Owner“, „Control Owner“) bis hin zu Letztentscheidungen auf Management-Ebene. Ebenso wichtig ist die Dokumentation von Abhängigkeiten – etwa zwischen Information Security und Cyber Security, zwischen vorgelagerten Prozessschritten oder zwischen Produkt-, Backend- und Produktionsrisiken. Terminologien müssen eindeutig und verständlich definiert sein; bei Unterschieden zwischen Bereichen sollte das Werkzeug ermöglichen, Begriffe zu verknüpfen und Unterschiede klar darzustellen (z. B. durch Synonym-Beziehungen oder Mapping-Tabellen). Automatisierte Unterstützung, etwa durch ein generiertes Glossar oder die kontextabhängige Anzeige des im jeweiligen Bereich üblichen Begriffs, kann das Verständnis zusätzlich erleichtern. Darüber hinaus sollten Kommunikationswege, Schnittstellen und einschlägige Standards sowie Regulierungen dokumentiert werden – idealerweise mit einer Darstellung ihrer Bedeutung für den eigenen Bereich und Hinweisen, wo bereichsübergreifender Austausch sinnvoll oder erforderlich ist.

Für das Verständnis komplexer Zusammenhänge ist schließlich die **Darstellung** entscheidend. Wo immer möglich sollte das Werkzeug eine klare visuelle Darstellung, etwa in Form von Diagrammen oder Übersichten, unterstützen. Dazu gehören die Visualisierung von Abhängigkeiten (z. B. zwischen Komponenten, Risiken und Maßnahmen), Schnittstellen (z. B. zwischen CSMS, ISMS und IACS-SP), Kommunikationswegen und weiteren Zusammenhängen, die für die bereichsübergreifende Steuerung relevant sind. Je nach Zielgruppe kann es sinnvoll sein, zwischen einer eher technischen Ebene (System- und Datenflüsse, Schnittstellen) und einer konzeptionellen Ebene (Risikokategorien, Verantwortlichkeiten, Prozesse) zu differenzieren und entsprechende Sichten anzubieten, um sowohl Fachexperten als auch Management-Rollen abzuholen.

Ergänzend dazu haben sich mehrere **sonstige Anforderungen** herauskristallisiert, die für die Usability eines bereichsübergreifenden Risikomanagement-Werkzeugs wesentlich sind. Viele Interviewpartner befürworten eine zentrale, in der Regel bereichsunabhängige Instanz mit bereichsübergreifendem Zugriff, die einen Gesamtüberblick über Risiken erhält, Risiken aus verschiedenen Bereichen gegenüberstellen kann und bereichsübergreifende Verantwortlichkeiten wahrnimmt. Ein solches „zentrales Cockpit“ sollte das Treffen relevanter Entscheidungen für mehrere Bereiche unterstützen, ohne die Autonomie der Fachbereiche unnötig einzuschränken. Darüber hinaus sollte das Werkzeug die Messung von Erfolgen des Risikomanagements und der bereichsübergreifenden Kommunikation unterstützen (z. B. durch Kennzahlen, Dashboards), um eine kontinuierliche Verbesserung zu ermöglichen. Es sollte helfen, Mehrwerte zu identifizieren, die sich aus einer bereichsübergreifenden Homogenität ergeben (z. B. Effizienzgewinne, schnellere Reaktionen, bessere Compliance). Wo Komponenten voneinander abhängen, sollte ein bereichsübergreifendes Tracking von Risiken möglich sein – etwa indem Risiken entlang der Abhängigkeitskette verfolgt und konsistent in allen betroffenen Bereichen sichtbar gehalten werden.

Insgesamt zeigen diese Anforderungen, dass Usability im Kontext eines bereichsübergreifenden Security-Management-Werkzeugs weit über „Oberflächenkomfort“ hinausgeht: Das System muss Kommunikations-, Organisations- und Dokumentationsbedarfe aus mehreren Domänen zugleich adressieren, ohne diese zu überfrachten. Die hier beschriebenen Empfehlungen geben einen Rahmen vor, an dem sich eine Weiterentwicklung des prototypischen SharePoint-Werkzeugs nach ATLAS-L4 orientieren kann.

2.1.13 Prototypisches Werkzeug für ein bereichsübergreifendes Security-Management

2.1.13.1 Kurzfassung

Im Arbeitsschritt „Prototypisches Werkzeug für ein bereichsübergreifendes Security-Management“ wurde ein SharePoint-basierter Prototyp entwickelt, der die im Projekt eingesetzte MoRA-Methode, bereichsübergreifende Rollen und normbasierte Compliance-Anforderungen in einem gemeinsamen Workspace zusammenführt. Kern des Werkzeugs ist eine SharePoint-Site, auf der die wichtigsten MoRA-Artefakte (Dokumentation der TOEs, Funktionen, Daten, Komponenten, Verbindungen, Datenflüsse, Schadensszenarien, Schutzziele, Bedrohungen, Maßnahmen, Annahmen und Risiken) als miteinander verknüpfte Listen abgebildet werden.

Ein Power-Automate-Flow importiert regelmäßig neue oder geänderte MoRA-Excel-Dateien in diese Listenstruktur und aktualisiert dabei TOE-spezifische Einträge (z. B. Funktionen, Daten, Technologien, Komponenten, Datenflüsse, Threats, Controls, Risks). Auf dieser Datenbasis wurden SharePoint-Seiten aufgebaut, die einerseits eine TOE-Sicht auf Architektur und Risikoanalysen („Risk Assessments“) und andererseits personalisierte Übersichten („My Risks“) für Risk Owner bereitstellen. Ein weiterer Flow sorgt dafür, dass die in den Risiken hinterlegten Risk Owner automatisch als Berechtigte auf den jeweiligen Einträgen gesetzt werden.

Parallel dazu wurden die im Projekt analysierten Compliance-Anforderungen aus ISO/SAE 21434, ISO/IEC 27001, IEC 62443 und UN R155 in einer eigenen Liste „Compliance Requirements“ modelliert und mit TOE-spezifischen Erfüllungsständen verknüpft. Über die Seiten „Compliance Overview“ und „My Compliance“ können Security- und Process-Owner für einen ausgewählten TOE den Status relevanter Anforderungen einsehen und pflegen.

Der Prototyp erfüllt damit drei zentrale Funktionen:

- er macht MoRA-basierte Risikoanalysen über TOEs hinweg strukturiert vergleichbar,
- er unterstützt die Zuweisung und Nachverfolgung von Verantwortung über das Active Directory und
- er verbindet technische Risikoanalysen mit normativen Compliance-Anforderungen in einem bereichsübergreifenden Werkzeug.

2.1.13.2 Konzept und Architektur

Konzeptionell basiert das prototypische Werkzeug auf einem gemeinsamen Metamodell, das sowohl die MoRA-Methode (Abschnitt 2.1.1) als auch die bereichsübergreifenden Anforderungen aus den Normen ISO/SAE 21434, ISO/IEC-27000-Familie und IEC-62443 (Abschnitt 2.1.2) sowie die Ergebnisse der Experteninterviews (Abschnitt 2.1.12) berücksichtigt.

Im Zentrum steht die Liste **Documentation**, in der für jedes betrachtete System („Target of Evaluation“, TOE) ein Eintrag mit Titel, Kurzbeschreibung, beteiligten Analysten und Ansprechpersonen

gepflegt wird. Alle weiteren fachlichen Listen enthalten ein Lookup-Feld TOE Name, das auf die Dokumentationsliste verweist. Dadurch können sämtliche Funktionen, Daten, Komponenten, Datenflüsse, Schadensszenarien, Schutzziele, Bedrohungen, Maßnahmen und Risiken eindeutig einem oder mehreren TOEs zugeordnet werden.

Die MoRA-spezifischen Artefakte werden jeweils in eigenen Listen abgebildet, u. a.:

- **Functions, Data, Components, Connections** und **Data flows** zur Modellierung der Systemarchitektur,
- **Damage Scenarios, Security Goals, Threats, Controls, Assumptions** und **Risks** zur Abbildung der Risikoanalyse,
- Hilfslisten wie **Impact Rating, Risk Factors, Attack Feasibility Rating, Risk Values, Security Goal Classess** und **Technology Catalog** zur parametrisierten Bewertung.

Zwischen diesen Listen bestehen Referenzbeziehungen analog zum MoRA-Metamodell (z. B. Threats → Security Goals, Controls → Threats, Risks → Threats/Controls/Assumptions). Auf diese Weise kann die aus dem Excel-Werkzeug bekannte Struktur in SharePoint reproduziert und für mehrere TOEs gemeinsam genutzt werden.

Für die Abbildung regulatorischer Anforderungen wurde eine eigenständige Liste **Compliance Requirements** aufgebaut. Jeder Eintrag repräsentiert eine konkrete Forderung, z. B. aus ISO/SAE 21434 (RequirementID, Titel, Standard, Clause, wörtliche Beschreibung) und ist einer Division (Vehicle/product, Backend/IT, Production/OT, Cross-division) sowie einem globalen Process Owner zugeordnet. Weitere Felder wie Compliance Status („Not assessed“, „In progress“, „Fulfilled“, „Not applicable“) und Responsible (Personen oder Rollen im AD) ermöglichen eine Einschätzung, ob und durch wen die Anforderung in der Organisation adressiert wird.

TOE-spezifische Erfüllungsstände werden in einer separaten Liste **TOE Compliance** modelliert. Dort verweisen Einträge jeweils auf genau einen Requirement-Eintrag und einen TOE, enthalten einen TOE-bezogenen Compliance Status, eine verantwortliche Person (Responsible) sowie Freitext zu Evidenzen und Review-Zeitpunkten. Damit wird abgebildet, dass z. B. die Anforderung RQ-09-03 („Perform TARA based on item definition“) zwar einmal im Katalog existiert, aber für TOE A von Person X und für TOE B von Person Y erfüllt werden muss.

Diese Architektur erlaubt es,

- MoRA-basierte Risikoanalysen mit normativen Anforderungen zu verknüpfen,
- bereichsübergreifende Verantwortlichkeiten transparent zu machen und
- für jeden TOE sowohl die Risikolage als auch den Compliance-Status konsistent abzubilden.

2.1.13.3 Umsetzung in SharePoint und Power Automate

Die konzeptionelle Architektur wurde auf einer SharePoint-Online-Site umgesetzt, die im Projekt als Workspace für das „Cross-Divisional Cybersecurity Management“ genutzt wurde. Die wichtigsten technischen Bausteine sind:

Automatisierte Übernahme von MoRA-Risikobewertungen

Für die Bibliothek **MoRA Files** wurde ein Power-Automate-Flow „Import MoRA Files“ entwickelt (vgl. Abbildung 34). Der Flow läuft täglich an und verarbeitet alle Excel-Dateien,

deren TransferStatus auf „New“ steht. Für jede Datei wird der Status zunächst auf „In Progress“ gesetzt und anschließend über die Excel-Online-Schnittstelle tabellenweise ausgelesen:

- die Tabelle „Documentation“ wird genutzt, um für das in der Datei betrachtete System einen Eintrag in der Liste **Documentation** anzulegen oder zu aktualisieren (inkl. Analysten, Kontaktpersonen und Management Summary),
- weitere Tabellen (u. a. „Functions“, „Data“, „Technologies“, „Components“, „Connections“, „Data flows“, „Damage Scenarios“, „Security Goals“, „Threats“, „Controls“, „Risks“) werden zeilenweise in die entsprechenden SharePoint-Listen übertragen,
- pro Tabellenzeile wird geprüft, ob für den aktuellen TOE bereits ein Eintrag mit gleichem Namen existiert; falls ja, wird dieser aktualisiert, andernfalls wird ein neuer Listeneintrag erzeugt,
- die Beziehung zum TOE wird über das Lookup-Feld TOE Name hergestellt; in einigen Listen (z. B. „Technologies“, „Components“, „Connections“) können Einträge mehreren TOEs zugeordnet werden.

Am Ende des Importprozesses wird TransferStatus auf „Completed“ gesetzt; ein „Do until“-Abschnitt stellt sicher, dass temporäre Fehlzustände beim Aktualisieren der Datei abgefangen werden. Durch diese Automatisierung werden MoRA-Risikobewertungen aus Excel in eine versionierbare, durchsuchbare und zwischen TOEs vergleichbare SharePoint-Struktur überführt.

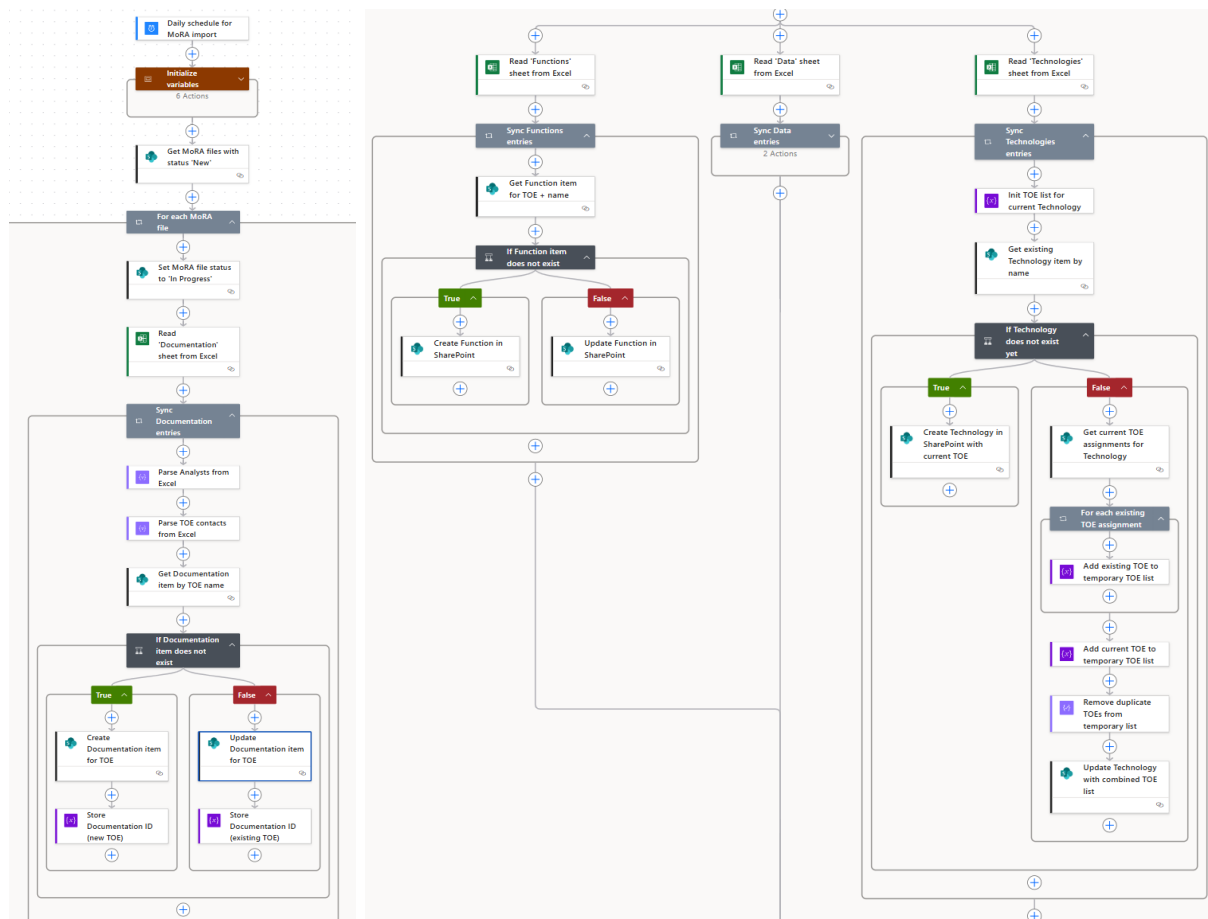


Abbildung 34: Auszug des Power-Automate-Flows „Import MoRA Files“ zur automatisierten Übernahme der MoRA-Risikobewertungen aus Excel in die SharePoint-Listen des prototypischen bereichsübergreifenden Security-Management-Werkzeugs.

Risikodashboards und persönliche Übersichten

Auf Basis der Listen wurden mehrere Site Pages erstellt, die unterschiedliche Sichten auf die Daten erlauben:

- Die Seite „**Risk Assessments**“ (vgl. Abbildung 35) dient als zentrales Dashboard für MoRA-Analysen. Oben befindet sich ein Banner, darunter eine kurze Schritt-für-Schritt-Anleitung. Im ersten List-Webpart wird die Liste **Documentation** angezeigt. In weiteren List-Webparts werden die Listen **Functions, Data, Components, Data flows, Damage Scenarios, Security Goals, Threats, Controls** und **Risks** eingebunden. Über die dynamische Webpart-Verknüpfung wird jeweils der ausgewählte TOE aus der Dokumentationsliste als Filter (TOE Name) auf alle anderen Webparts angewandt. Nutzerinnen und Nutzer können so ein System auswählen und sehen unmittelbar die dazugehörige Architektur- und Risikolandschaft.
- Die Seite „**My Risks**“ stellt eine personalisierte Sicht bereit. Sie enthält ein Banner, einen kurzen Erklärungstext und ein List-Webpart für die Liste **Risks**, das eine Ansicht verwendet, die nur Einträge anzeigt, bei denen das Personenfeld RiskOwner die aktuell angemeldete Person enthält.

Zur Unterstützung der Verantwortlichkeitszuweisung wurde ein weiterer Flow „Enforce Risk Permissions (by RiskOwner)“ erstellt. Er wird bei jeder Anlage oder Änderung eines Risiko-Eintrags ausgelöst, setzt zunächst die Berechtigungsvererbung am Listenelement zurück, bricht diese dann mit Kopie der Listrechte und vergibt anschließend für jede in RiskOwner hinterlegte Person explizit Zugriffsrechte auf das Element. Damit wird sichergestellt, dass Risk Owner nicht nur inhaltlich, sondern auch über die technische Berechtigung mit „ihren“ Risiken verknüpft sind.

Risk Assessments
Wagner, Patrick

Select a TOE in the Documentation list below, then review the other filtered lists (Risks, Controls, Functions, Data flows, etc.) for that TOE.

Documentation [See all](#)

[+ Add new item](#) [Edit](#) [Edit in grid view](#) [Share](#) [Copy link](#) [Delete](#) 1 selected [Dashboard - TOE selector](#)

Title	High-level description of the TOE	Analysts	Contact for the TOE
Automated Driving System (ATLAS-L4)	The Automated Driving System (ADS) consists of seven main components: Perception, Prediction, Planning and Control are the control loop that enables environment awareness and autonomous driving. In addition, System Management monitors the health of ADS-relevant components and initiates Minimum Risk Manoeuvres (MRM) when necessary. Furthermore, Mission Control establishes communication with the external Control Center. Finally, an onboardHMI displays information to a test driver or dispatcher. In general, the communication flow to perform the Dynamic Driving Task (DDT) is as follows: Sensors, Base Vehicle Monitoring, and Control Center transmit information about the environment and the vehicle to the control loop. The control loop processes the information and sends control commands to Actuators.	Wagner, Patrick	
Control Center (ATLAS-L4)	Provides an interface to remotely assist and monitor driverless trucks.	Wagner, Patrick	

Functions > Automated Driving System (ATLAS-L4) [See all](#)

[+ Add new item](#) [Edit in grid view](#) [Share](#) [Copy link](#) [Export to Excel](#) [Dashboard - Functions*](#)

FunctionID	Title	Description	Sub-Functions	Comment
F1	Data collection	Sensors, Control Center, and Base Vehicle Monitoring transmit vehicle and environment data to Perception. Furthermore, the Control Center can request further environment data from the vehicle.		
F2	Object and Event Detection and Response	The ADS core components interact with each other in		

Abbildung 35: SharePoint-Seite „Risk Assessments“ des prototypischen Werkzeugs mit TOE-Auswahl (oben) und den automatisch aus den MoRA-Dateien befüllten Listen zum Systemmodell und den Risikoartefakten (unten).

Compliance-Übersichten

Für das Compliance-Thema wurden zwei zusätzliche Seiten aufgebaut:

- Die Seite **„Compliance Overview“** entspricht konzeptionell der Risk-Assessments-Ansicht, fokussiert aber auf Normanforderungen. Oben wird die Liste **Documentation** eingeblendet. Darunter zeigt ein List-Webpart die Liste **TOE Compliance** mit Filter auf den ausgewählten TOE. In der Ansicht werden neben Compliance Status, Responsible, Last Reviewed und Next Review auch Lookup-Felder aus **Compliance Requirements** (z. B. RequirementID, Standard, Clause, Description, Division) angezeigt. Damit erhalten Security- und Process-Owner eine vollständige Übersicht, welche Anforderungen aus UN R155, ISO/SAE 21434, ISO/IEC 27001 und IEC 62443 für einen TOE relevant sind, wie deren Bearbeitungsstand ist und wer dafür verantwortlich ist.
- Die Seite **„My Compliance“** zeigt analog zur Seite „My Risks“ eine persönliche Sicht auf TOE-bezogene Compliance-Einträge, indem sie **TOE Compliance** auf Responsible = [Me] filtert.

Einordnung und Ausblick

Der entwickelte Prototyp zeigt, dass sich ein bereichsübergreifendes Security-Management-Werkzeug auf Basis vorhandener Standardplattformen realisieren lässt. Durch die Überführung der MoRA-Excel-Analysen in eine zentrale SharePoint-Struktur werden Security-Risiken und Maßnahmen für ADS und Control Center vergleichbar, durchsuchbar und langfristig nachverfolgbar. Die dynamischen „Risk Assessments“-Sichten und personalisierten „My Risks“-Ansichten

adressieren unmittelbar die in den Experteninterviews identifizierten Bedarfe nach Transparenz, klaren Verantwortlichkeiten und bereichsübergreifender Kommunikation (Abschnitt 2.1.12).

Die Abbildung der Compliance-Anforderungen und TOE-spezifischen Erfüllungsstände ermöglicht es, die in Abschnitt 2.1.2 und 2.1.3 analysierten Normen und Regulierungen nicht nur textlich, sondern als strukturiertes Artefakt im selben Workspace zu führen. Damit kann für jeden TOE nachvollzogen werden, welche Anforderungen gelten, wie deren Status ist und wie sie mit konkreten Risikoanalysen und Maßnahmen verknüpft sind.

Usability-Aspekte wurden sowohl in der Seiten- und Listenstruktur als auch in einem begleitenden Usability-Leitfaden berücksichtigt (vgl. Abschnitt 2.1.12.5). Dazu gehören u. a. klare, aufgabenorientierte Seiten („Risk Assessments“, „My Risks“, „Compliance Overview“, „My Compliance“), reduzierte und kontextbezogene Informationsdarstellung, die Nutzung bekannter Interaktionsmuster in SharePoint sowie der Einsatz von AD-basierten Personenfeldern zur Zuweisung von Verantwortung.

Der Prototyp ist bewusst als initiales Werkzeug zu verstehen. Er bildet eine belastbare Grundlage, auf der nach Projektende weitere Funktionen aufbauen können, etwa

- ein domänenübergreifendes Cockpit mit konsolidierten Kennzahlen (z. B. offene hohe Risiken pro Domain, Erfüllungsgrad von Normanforderungen pro TOE),
- erweiterte Workflows (z. B. Freigabeprozesse für Risiken und Maßnahmen, Erinnerungen an fällige Reviews),
- zusätzliche Sichten für spezifische Zielgruppen (z. B. Management-Dashboards, OT-spezifische Risikoberichte) sowie
- eine tiefere Integration mit bestehenden CSMS-, ISMS- und IACS-Security-Programmen.

Insgesamt leistet der Arbeitsschritt damit einen konkreten Beitrag zur Operationalisierung der in ATLAS-L4 entwickelten Konzepte für bereichsübergreifendes Security-Risikomanagement und zeigt exemplarisch, wie diese mittels eines prototypischen Werkzeugs in die Praxis überführt werden können.

2.1.13.4 Umsetzung weiterer Anforderungen aus Standards, Interviews und Usability-Analyse

Die in den Kapiteln 2.1.2, 2.1.3, 2.1.12 und 1.4.11.2 herausgearbeiteten Anforderungen an ein bereichsübergreifendes Security-Risikomanagement werden im prototypischen Werkzeug gezielt aufgegriffen und funktional unterstützt.

Domänenübergreifende Sichtbarkeit von Risiken

Aus den Normen (insb. ISO/SAE 21434, ISO/IEC 27005, IEC 62443-3-2; vgl. 2.1.2) und den Experteninterviews (2.1.12) ergibt sich die Forderung, Risiken entlang der Bereiche Fahrzeug/CSMS, Backend/ISMS und Produktion/IACS strukturiert vergleichen zu können. Im Prototyp wird dies wie folgt umgesetzt:

- In der Liste **Risks** wurde das Choice-Feld Domain eingeführt (Werte u. a. Vehicle/product, Backend/IT, Production/OT, Cross-division).
Damit lässt sich jedes Risiko einem organisatorischen Bereich zuordnen.
- In der Liste **Compliance Requirements** existiert mit Division ein analoger Domänen-Indikator für Normanforderungen.

- Auf Basis dieser Felder wurde eine zusätzliche Seite „**Cross-Domain Risks**“ aufgebaut:
 - List-Webpart **Risks** mit Ansicht „Cross-Domain Overview“,
 - Gruppierung und Filter nach Domain, TOE Name, optional Risiko-Schwere,
 - Nutzung der AD-Felder RiskOwner und Domain, um Verantwortlichkeiten pro Domäne sichtbar zu machen.
- Damit wird die in 2.1.12 geforderte **bereichsübergreifende Transparenz** erreicht: zentrale Stellen können Risiken domänenübergreifend sichten; einzelne Bereiche können ihre eigenen Risiken nach Domain filtern und in Kontext zu anderen Bereichen setzen.

Harmonisierung und Vergleichbarkeit von Risikokriterien

Die in ISO/IEC 27005, ISO/SAE 21434 und IEC 62443 formulierte Forderung nach harmonisierten Risikokriterien steht in der Praxis vor der Herausforderung, dass verschiedene Organisationseinheiten unterschiedliche Methoden und Werkzeuge einsetzen. In manchen Bereichen kommen TARA- bzw. MoRA-basierte Ansätze mit Impact- und Attack-Feasibility-Bewertung zum Einsatz, in anderen Bereichen werden etablierte IT-Risikowerkzeuge mit eigenen Impact-Kategorien, Risikomatrizen und Kennzahlen verwendet, und in der Produktions-IT können wiederum andere Bewertungsmodelle genutzt werden. Das prototypische Werkzeug wurde so konzipiert, dass es beide Situationen unterstützt: eine vollständige Harmonisierung auf Basis von MoRA, aber auch die kontrollierte Koexistenz verschiedener Bewertungsmodelle mit anschließender Zusammenführung der Ergebnisse.

Wenn mehrere Bereiche MoRA als gemeinsames Bewertungsmodell nutzen, entsteht die Harmonisierung im Wesentlichen durch das Modell selbst. In diesem Fall verwenden alle Beteiligten dieselben Impact-Kategorien, dieselben Faktoren für die Angriffsbewertung und eine einheitliche Risikoskala. Im Prototyp werden diese Skalen zentral über die Hilfslisten (u. a. Impact Rating, Risk Factors, Attack Feasibility Rating, Risk Values) abgebildet. Die MoRA-Import-Workflows übernehmen die Bewertungen verschiedener Risikoanalysen in diese einheitliche Struktur. Risiken aus unterschiedlichen Systemen und Bereichen, die auf MoRA basieren, sind damit ohne weitere Transformation direkt vergleichbar; insbesondere lassen sich Risikowerte und zugrunde liegende Impact-/Feasibility-Einschätzungen in gemeinsamen Sichten auswerten.

Gleichzeitig ist es weder realistisch noch sinnvoll, alle Domänen kurzfristig auf ein einziges Bewertungsmodell zu verpflichten. Daher unterstützt der Prototyp auch Szenarien, in denen verschiedene Bereiche ihre etablierten Risiko-Tools weiter nutzen, die Ergebnisse aber im SharePoint-Werkzeug konsolidiert werden. Dazu werden die originalen Risikobewertungen aus den jeweiligen Werkzeugen über zusätzliche Importpfade in den Workspace übertragen und dort mit ihren ursprünglichen Kennzahlen gespeichert, beispielsweise mit IT-spezifischen Impact-Stufen und Risikoscores oder mit OT-spezifischen Risk Levels. Die Semantik der jeweiligen Methode bleibt erhalten und ist für Fachspezialisten vollständig sichtbar.

Um dennoch eine organisationsweite Vergleichbarkeit herzustellen, werden die Beziehungen zwischen den unterschiedlichen Skalen in Form von Konfigurationen abgebildet. Mögliche Abbildungen sind etwa Zuordnungen zwischen MoRA-Impact-Stufen und IT-Impact-Kategorien oder zwischen IT-Risikowerten und einer kanonischen numerischen Skala. Auf dieser Basis leiten Power-Automate-Flows für jeden Risikoeintrag zusätzliche standardisierte Kennzahlen ab, etwa ein StandardizedImpact, eine StandardizedLikelihood und einen StandardizedRiskValue. Welche Mapping-Regel angewendet wird, hängt von der Herkunft des Risikos (z. B. MoRA-Analyse,

IT-Risikotool, OT-Bewertung) ab; die Mapping-Tabellen sind so ausgestaltet, dass sie angepasst werden können, wenn sich Bewertungsgrundlagen in einem der beteiligten Bereiche weiterentwickeln.

Die grundlegende Annahme dabei ist, dass identische standardisierte Risikowerte eine vergleichbare Schutzbedarfs-Semantik haben sollen, unabhängig davon, aus welchem Ursprungsmodell sie abgeleitet wurden. Der Prototyp macht diese Annahmen explizit und überprüfbar, indem er Risiken aus unterschiedlichen Domänen in gemeinsamen Übersichten zusammenführt. Verantwortliche können so prüfen, ob beispielsweise ein Risiko mit standardisiertem Wert 4 im Fahrzeugumfeld und ein Risiko mit demselben Wert in einer Backend-Komponente tatsächlich zu ähnlich gewichteten Maßnahmen und Restrisiken führen, und die Mappings bei Bedarf nachschärfen. In bereichsübergreifenden Sichten werden primär die standardisierten Kennzahlen verwendet, sodass sich Fragen nach der Anzahl und Verteilung hoher Risiken pro Domäne und System beantworten lassen. In den Detailansichten bleiben die ursprünglichen, domänenspezifischen Bewertungen sichtbar, sodass die jeweiligen Fachabteilungen weiterhin in „ihren“ Modellen arbeiten können, während das prototypische Werkzeug eine gemeinsame Auswertungs- und Steuerungsebene bereitstellt.

Zentrales bereichsübergreifendes Cockpit und Rollenmodell

Die in den Normen und in den Experteninterviews identifizierte Anforderung, ein zentrales bereichsübergreifendes Gremium mit Gesamtüberblick über Risiken und Compliance-Status zu unterstützen, wird im Prototyp durch eine Kombination von Sichten und Rollenimplementierung adressiert.

Aus fachlicher Sicht bildet die SharePoint-Site ein zentrales „Cockpit“, in dem unterschiedliche Perspektiven auf dieselbe Datenbasis verfügbar sind. Die Seite „Risk Assessments“ stellt eine TOE-bezogene Sicht bereit: Für ein ausgewähltes System werden alle relevanten MoRA-Artefakte (Funktionen, Daten, Komponenten, Datenflüsse, Schadensszenarien, Schutzziele, Bedrohungen, Maßnahmen, Risiken) angezeigt, einschließlich der aus MoRA abgeleiteten bzw. aus anderen Tools übernommenen Impact- und Risikoindikatoren. Ergänzend dazu bietet die Seite „Cross-Domain Risks“ eine aggregierte Sicht über alle Domänen hinweg. Durch die Nutzung der Felder „Domain“ und der standardisierten Risikoindikatoren können Risiken aus Fahrzeug-, Backend- und Produktionsumfeldern in einer gemeinsamen Übersicht betrachtet, gefiltert und gruppiert werden.

Auf der Compliance-Seite wird das Bild vervollständigt: „Compliance Overview“ verknüpft pro TOE die im Katalog hinterlegten Normanforderungen mit den TOE-spezifischen Erfüllungsständen aus „TOE Compliance“ und macht damit sichtbar, welche Anforderungen aus ISO/SAE 21434, ISO/IEC 27001, IEC 62443 und UN R155 für ein System gelten, wie deren Status ist und welche Personen verantwortlich sind.

Rollen und Verantwortlichkeiten werden konsequent über Active-Directory-basierte Personenfelder abgebildet. Risiko-Einträge enthalten einen Risk Owner, Compliance-Einträge einen Responsible sowie einen globalen Process Owner pro Requirement. Die personalisierten Seiten „My Risks“ und „My Compliance“ nutzen diese Felder, um jeweils nur die Einträge anzuzeigen, für die die angemeldete Person verantwortlich ist. Ein Power-Automate-Flow setzt Berechtigungen auf Risiko-Einträgen so, dass die eingetragenen Risk Owner automatisch Zugriffsrechte erhalten; analog kann dieses Prinzip auf Compliance-Einträge übertragen werden.

In der Kombination ermöglicht das Werkzeug einerseits zentrale bereichsübergreifende Sichten für Governance-Gremien und andererseits rollenbezogene, aufgabenorientierte Sichten für einzelne Verantwortliche. Damit wird die in den Anforderungen beschriebene Trennung zwischen Gesamtsteuerung und operativer Bearbeitung technisch abgebildet, ohne unterschiedliche Domänen in eine einzige Sicht „zu zwingen“.

Abbildung von Normanforderungen und Claims über unterschiedliche Managementsysteme hinweg

Ein weiterer zentraler Anspruch aus den analysierten Normen und Regulierungen ist die Nachvollziehbarkeit zwischen regulatorischen Anforderungen, organisatorischer Verantwortung und den konkreten Ergebnissen der Risikoanalysen und Maßnahmenumsetzungen – unabhängig davon, ob diese im Rahmen eines Fahrzeug-CSMS, eines Informationssicherheits-Managementsystems oder eines Produktions-Security-Programms entstehen.

Der Prototyp adressiert dies durch eine klare Trennung zwischen einem globalen Anforderungskatalog und TOE-spezifischen Erfüllungsständen. In der Liste „Compliance Requirements“ werden einzelne Forderungen aus den relevanten Standards als eigenständige Objekte geführt. Für jede Anforderung werden u. a. Standard, Clause, wörtliche Beschreibung, primär betroffene Division sowie ein globaler Process Owner hinterlegt. Damit existiert eine zentrale, normübergreifende Referenz, in der Anforderungen unabhängig von konkreten Projekten oder Systemen verwaltet werden.

Die Liste „TOE Compliance“ bildet dann die Brücke zu konkreten Systemen: Jeder Eintrag verbindet genau einen Katalogeintrag aus „Compliance Requirements“ mit einem TOE aus der Dokumentationsliste. Dazu kommen ein TOE-spezifischer Compliance-Status, eine verantwortliche Person und ein Feld für Evidenzen und Kommentare. In diesen Evidenzfeldern können Verweise auf MoRA-Risiken und -Maßnahmen, auf Ergebnisse anderer Risikowerkzeuge oder auf Auditberichte und Policies hinterlegt werden. Auf diese Weise lässt sich etwa darstellen, dass eine bestimmte Anforderung zur Durchführung einer TARA, zur Behandlung von Schwachstellen oder zur Etablierung von Monitoringprozessen durch eine Kombination aus TARA-Ergebnissen, Maßnahmen in spezifischen Bereichen und organisatorischen Regelwerken erfüllt wird.

Akzeptanz- und Claim-Entscheidungen, wie sie insbesondere in ISO/SAE 21434 vorgesehen sind (z. B. Risikoteilung oder bewusste Beibehaltung eines Restrisikos unter bestimmten Annahmen), können im Prototyp sowohl in den Risikoobjekten selbst (z. B. über zusätzliche Felder für Treatment-Entscheidung und Begründung) als auch in den zugehörigen TOE-Compliance-Einträgen dokumentiert werden. Damit ist nachvollziehbar, welche Normforderungen mit welchem Restrisiko erfüllt werden und auf welchen Annahmen oder Claims diese Entscheidungen beruhen.

In den Compliance-Sichten des Werkzeugs ergibt sich somit eine durchgängige Kette: von der abstrakten Normanforderung über verantwortliche Rollen und TOE-spezifische Erfüllungsstände bis hin zu den konkreten Risiko- und Maßnahmenartefakten aus unterschiedlichen Domänen. Diese Traceability ermöglicht es, bei Änderungen in Regulierungen oder im Risikobild gezielt zu erkennen, welche Systeme, Verantwortlichen und Arbeitsergebnisse betroffen sind.

Einbindung externer Partner und Lieferanten

Ein Teil der in den Normen und Regulierungen adressierten Risiken und Anforderungen entsteht an Schnittstellen zu externen Partnern, etwa zu Zulieferern sicherheitskritischer Komponenten, Betreibern von Backend-Diensten oder Betreibern von Produktionsanlagen. Der Prototyp

unterstützt diese Perspektive, indem er supplier-bezogene Risiken und Compliance-Einträge explizit abbildet, ohne dass externe Parteien zwingend direkten Zugriff auf den Workspace erhalten müssen. In der Liste „Documentation“ können TOEs auch externe Systeme oder Dienste repräsentieren (z. B. ein von einem Dienstleister betriebenes Backend-System); in „Compliance Requirements“ und „TOE Compliance“ lassen sich Anforderungen, die sich auf Supplier-Management, verteilte Entwicklung oder Risk-Sharing mit Dritten beziehen, gezielt markieren. Über das Feld „Responsible“ werden dabei interne Rollen hinterlegt, die für die Steuerung und Überwachung der jeweiligen externen Partner verantwortlich sind. In den Evidenz-Feldern können vertragliche Sicherheitsanforderungen, Auditberichte oder vom Lieferanten bereitgestellte Nachweise referenziert werden. Supplier-bezogene Risiken können wie andere Risiken einem oder mehreren TOEs zugeordnet und in den bereichsübergreifenden Sichten (z. B. „Cross-Domain Risks“) ausgewertet werden. Damit bildet das Werkzeug auch die in den Standards geforderten Lieferanten- und Risk-Sharing-Aspekte ab und macht sichtbar, welche externen Parteien für welche Teile der Gesamtrisikolage und Normerfüllung mitverantwortlich sind.

Umsetzung der Usability-Anforderungen

Die in den Kapiteln 1.4.11.2 und 2.1.12.5 zusammengefassten Usability-Heuristiken und Gestaltungsprinzipien wurden bei Konzeption und Umsetzung des Prototyps systematisch berücksichtigt. Ziel war es, ein Werkzeug zu schaffen, das trotz komplexer fachlicher Inhalte von den verschiedenen Rollen im Security-Management ohne hohe Einstiegshürden genutzt werden kann.

Ein zentrales Prinzip betrifft die Sichtbarkeit des Systemzustands und der Aktivitäten. Statusinformationen wie „Compliance Status“, „Domain“, die Zuordnung zu Divisionen sowie optional der Lebenszyklusstatus der Risiken werden in den Listen nicht nur als Text, sondern mittels JSON-basierter Formatierungen als farbige Markierungen dargestellt. Dies erleichtert es, auf einen Blick offene, in Bearbeitung befindliche oder erfüllte Anforderungen und Risiken zu erkennen. Ergänzend sorgt die Kombination aus Standardfeldern (z. B. „Modified“, „Version“) und Freitext-Evidenzfeldern dafür, dass Änderungen und Entscheidungen an zentralen Artefakten nachvollziehbar bleiben und die im Literaturteil geforderte „History of Actions and Changes“ vorhanden ist.

Ein weiteres Prinzip ist die flexible Repräsentation von Informationen für unterschiedliche Nutzergruppen. Statt alle Inhalte in einer einzigen, sehr dichten Ansicht darzustellen, bietet der Prototyp mehrere Seiten mit klar zugeschnittenen Aufgaben: „Risk Assessments“ für die TOE-bezogene Analyse, „Cross-Domain Risks“ für den bereichsübergreifenden Überblick, „My Risks“ und „My Compliance“ für die persönliche Aufgabensteuerung sowie „Compliance Overview“ für den Abgleich von Normanforderungen und Erfüllungsständen. Innerhalb dieser Seiten können Listen über Filter, Gruppierungen und Sortierungen an individuelle Bedürfnisse angepasst werden, ohne dass dadurch die zugrunde liegende Datenstruktur verändert wird.

Die Unterstützung von Rollen und Arbeitsteilung wird durchgängig über Personenfelder und Berechtigungskonzepte realisiert. Risk Owner, verantwortliche Personen für Normanforderungen und globale Process Owner werden direkt im Tool hinterlegt und über personalisierte Ansichten in den Vordergrund gerückt. Durch die Verbindung mit dem Active Directory können diese Rollen mit den realen Organisationsstrukturen abgeglichen und bei Rollenwechseln aktualisiert werden. Dies entspricht den in den Heuristiken geforderten Mechanismen zur Abbildung von Rollen, Verantwortlichkeiten und arbeitsteilten Prozessen.

Schließlich wurden auch Aspekte der Hilfestellung und Terminologie adressiert. Die Benennung von Listen und Feldern folgt weitgehend der in den Normen und in der MoRA-Methode etablierten

Terminologie, sodass sich Fachanwenderinnen und -anwender aus verschiedenen Bereichen schneller zurechtfinden. Kurze Einführungstexte auf den Seiten erklären die jeweils vorgesehenen Schritte (z. B. Auswahl eines TOEs, anschließende Überprüfung von Risiken oder Compliance-Einträgen), ohne die Nutzenden mit umfassenden Handbüchern zu konfrontieren.

2.1.14 Entwicklung öffentlich verfügbarer Testtools für Fahrzeugdiagnose

gallia ist ein erweiterbares Framework für Penetrationstests mit Fokus auf den Automotive-Bereich, welches von Fraunhofer AISEC in vorangegangenen Projekten entwickelt und als Open Source veröffentlicht wurde. Der Anwendungsbereich der Toolchain umfasst die Durchführung von Penetrationstests von einem einzelnen Steuergerät bis hin zu ganzen Fahrzeugen. Der Fokus liegt dabei auf der UDS-Schnittstelle, ist aber nicht darauf beschränkt. gallia kann dabei dank seiner Vielzahl an mitgelieferten Tools direkt zum Testen eingesetzt werden, etwa, um über die Diagnoseschnittstelle Steuergeräte im Fahrzeug zu identifizieren oder deren Funktionen zu enumerieren. Dabei werden Testabläufe und -ergebnisse automatisch und umfassend dokumentiert.

Im Folgenden wird beispielhaft dargestellt, wie mithilfe von gallia zunächst verfügbare Sessions und dann darauf aufbauend verfügbare Services eines Steuergeräts enumeriert werden können. Die Abläufe sind in Abbildung 36 schematisch dargestellt. gallia verwendet zur Vereinfachung der Programmaufrufe optional Konfigurationsdateien. Der Übersichtlichkeit halber wird hier angenommen, dass eine entsprechende Datei mit bereits vorausgefüllten Verbindungsparametern zur ECU existiert.

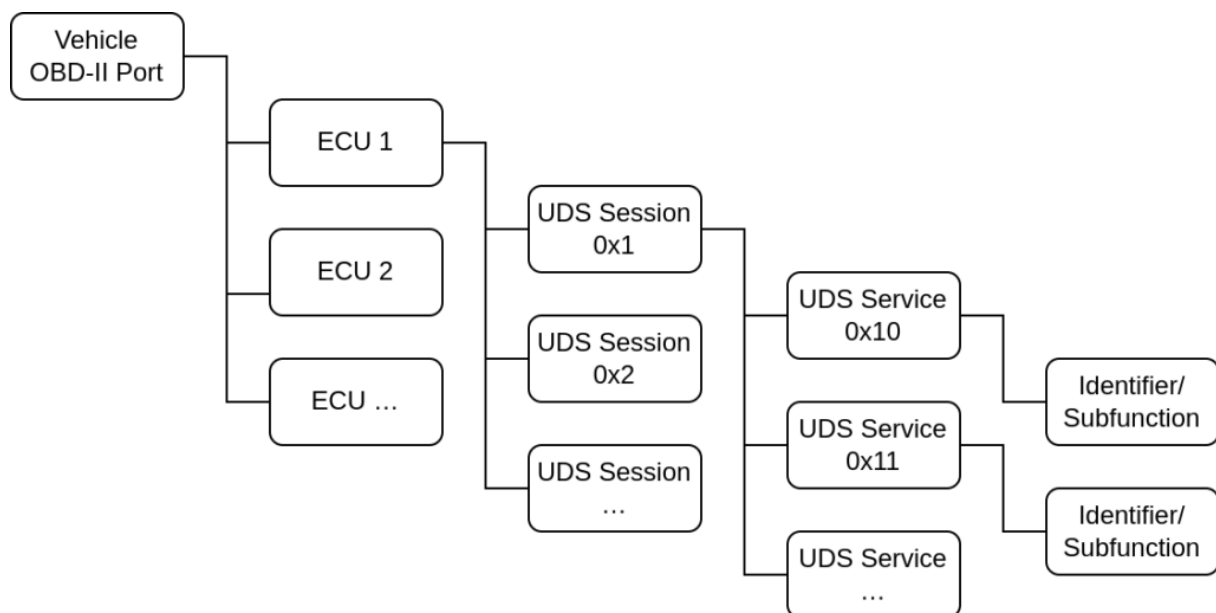


Abbildung 36: Die Tools in gallia können verwendet werden, um ECUs und deren Funktionalitäten zu scannen.

Zunächst wird ein Session Scan durchgeführt, welcher auch Diagnosesessions finden kann, welche nicht aus der Standardsession, sondern nur innerhalb spezieller Sessions zugänglich sind:

```
$ gallia scan uds sessions
```

Die folgenden Ergebnisse zeigen für die hier getestete ECU etwa, dass die Sessions 1, 2, 3, 0x46 und 0x4b verfügbar sind, die Session 2 aber nur aus der Session 0x46 heraus erreichbar ist:

Scan finished; Found the following sessions:

* Session 0x01

via stack: defaultSession

via stack: defaultSession->0x03

via stack: defaultSession->0x46

via stack: defaultSession->0x4b

via stack: defaultSession->0x46->0x02

* Session 0x02

via stack: defaultSession->0x46

* Session 0x03

via stack: defaultSession

* Session 0x46

via stack: defaultSession

* Session 0x4b

via stack: defaultSession

Mit diesen Ergebnissen kann daraufhin ein Scan gestartet werden, welcher die in den jeweiligen Sessions verfügbaren UDS Services, also die eigentlichen Funktionen, enumeriert:

```
$ gallia scan uds services --sessions 1 2 3 0x46 0x4b
```

Bei Verwendung der Datenbank zum Logging werden die im Session Scan bereits gefundenen notwendigen Transitionen automatisch berücksichtigt. Im Folgenden ist ein Ausschnitt des Scan-Ergebnisses für die Sessions 1 und 2 zu sehen:

findings in session 0x01:

[0x10] DiagnosticSessionControl: subFunctionNotSupported

[0x14] ClearDiagnosticInformation: ClearDiagnosticInformationResponse()

[0x19] ReadDTCInformation: subFunctionNotSupported

[0x22] ReadDataByIdentifier: requestOutOfRange

[0x37] RequestTransferExit: generalReject

[0x85] ControlDTCSetting: subFunctionNotSupported

findings in session 0x02:

[0x10] DiagnosticSessionControl: subFunctionNotSupported

[0x14] ClearDiagnosticInformation: ClearDiagnosticInformationResponse()

[0x19] ReadDTCInformation: subFunctionNotSupported

[0x22] ReadDataByIdentifier: requestOutOfRange

[0x29] Authentication: incorrectMessageLengthOrInvalidFormat

Basierend auf den hiermit gewonnen Informationen über den unterstützten Funktionsumfang, kann mit weiteren Tools das Verhalten der identifizierten Services weiter untersucht werden. Etwa können für die Sessions 1 und 2 Daten über den dort verfügbaren ReadDataByIdentifier Service aufgelistet werden:

```
$ gallia scan uds identifiers --sessions 1 2
```

Die Testdurchläufe und -ergebnisse können sowohl dateibasiert oder auch strukturiert in einer Datenbank gespeichert und entsprechend ausgewertet werden. Die mitgelieferten Logviewer erlauben dabei ein fokussiertes Abrufen relevanter Informationen innerhalb einzelner Tests, während die Datenbank umfangreiche Auswertungen auch über mehrere Tests hinweg erlaubt.

Neben einem großen Satz an bestehenden Tools bietet gallia aber durch seine quelloffene Implementierung in Python auch die Möglichkeit bestehende Tests zu erweitern oder, etwa mithilfe der Plugin-Schnittstelle, neue Testskripte in das Tool zu integrieren. Dazu stellt gallia umfangreiche Implementierungen von Transport- und Applikationsprotokollen im Bereich der automobilen Diagnose zur Verfügung und bietet über abstrakte Schnittstellen eine einfache Möglichkeit eigene Testprogramme zu erstellen oder herstellerspezifische Kommunikationsabläufe auch für bestehende Tests zu integrieren. Ein Überblick über die Architektur von gallia ist in Abbildung 37 gegeben.

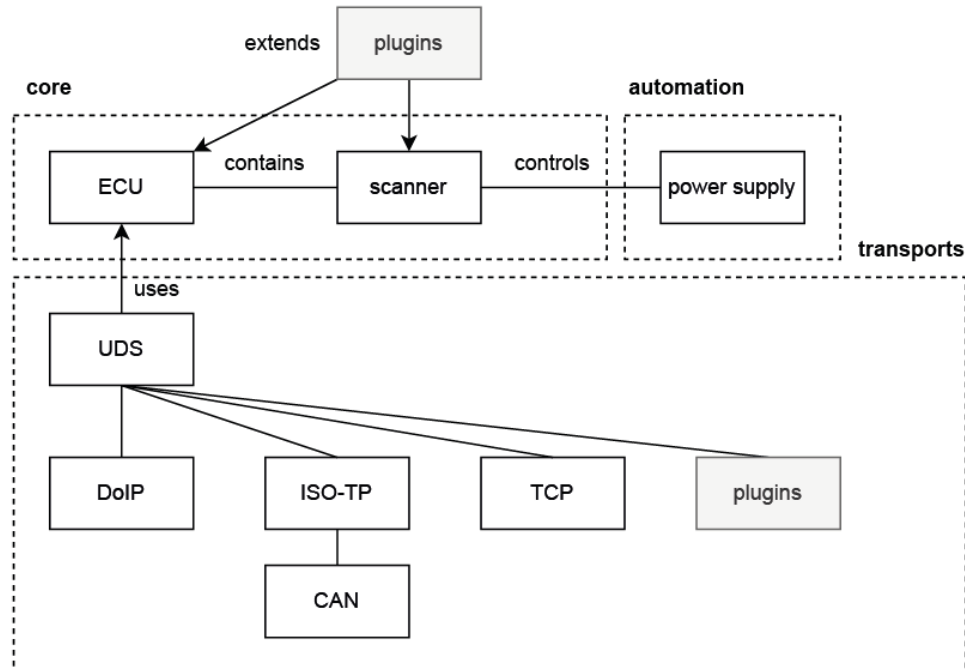


Abbildung 37: Überblick über die Software-Architektur von gallia

Im Rahmen des Projekts wurden diese Schnittstellen nochmals verbessert. Durch umfangreiche Anpassungen im Quelltext²³ können Testskripte typischer direkt im Programmcode aufgerufen werden, wodurch Automatisierungen deutlich vereinfacht werden. Durch die Änderungen wird zugleich auch die Codequalität verbessert, da Aufrufparameter nun von statischen Typprüfern erfasst werden können und die Eingaben während der Laufzeit einfacher validiert werden können. Zudem wurden auch die Tests an der Software selbst überarbeitet und erweitert, etwa mithilfe einer virtuellen ECU²⁴, welche wahlweise zufällige Konfigurationen annehmen oder aber basierend auf vorangegangenen Testresultaten das Verhalten von realen Steuergeräten emulieren kann. Mit diesen Verbesserungen konnten einerseits bestehende Fehler im Quelltext identifiziert und behoben werden, sie dienen darüber hinaus aber auch dazu, nachhaltig eine hohe Qualität aufrechtzuerhalten. Zusätzlich erlauben diese Änderungen, Testdurchläufe einfacher reproduzieren zu können. Hierzu wurde ein Tool hinzugefügt, welches basierend auf den automatisch geloggtten Informationen, Tests mit denselben Parametern erneut ausführen kann.

gallia wurde jedoch nicht nur im Hinblick auf Codequalität und Reproduzierbarkeit verbessert, sondern auch funktional deutlich erweitert. Eine wesentliche Erweiterung betrifft die umfangreiche Überarbeitung der Implementierung des für moderne Fahrzeuge relevanten Transportprotokolls Diagnostic communication over Internet Protocol (DoIP) [200], sowie darauf aufbauend die Implementierung eines automatisierten Tools zum Finden von Gateways und Steuergeräten über DoIP²⁵. Im Folgenden ist ein Auszug aus den Scan-Ergebnissen eines DoIP-Scans am OBD Port eines Fahrzeugs zu sehen:

```
Enumerating all TargetAddresses from 0x0 to 0xffff
HEUREKA: target address 0x100a is valid!
It cannot get nicer: 0x100a responded: TesterPresentResponse()
HEUREKA: target address 0x100b is valid!
HEUREKA: target address 0x100c is valid!
It cannot get nicer: 0x100c responded: TesterPresentResponse()
```

Dabei ist zu sehen, dass zu den Endpunkten 0x100a und 0x100c eine positive Antwort eines Steuergeräts empfangen wurde, während 0x100b zwar eine seitens des Gateways valide Adresse darstellt, jedoch keine Verbindung mit einem Steuergerät über diese Adresse möglich ist. Der Scanner erzeugt vollständige Verbindungsparameter, welche wiederum für weitergehende Scans, wie zuvor beschrieben, verwendet werden können.

Darüber hinaus wurde gallia auch um die Unterstützung für das häufig im Antriebsstrang eingesetzte Protokoll Flexray [201] erweitert²⁶. Dabei wurde auch die Unterstützung von Windows als weiteres Betriebssystem neben Linux implementiert. Nicht zuletzt konnte auch die UDS Implementierung erweitert werden, etwa um eine im WWH-OBd für Nutzfahrzeuge vorgeschriebene Möglichkeit zum Auslesen von Fehlercodes (DTCs)²⁷.

²³ <https://github.com/Fraunhofer-AISEC/gallia/pull/493>

²⁴ <https://github.com/Fraunhofer-AISEC/gallia/pull/82>

²⁵ <https://github.com/Fraunhofer-AISEC/gallia/pull/430>

²⁶ <https://github.com/Fraunhofer-AISEC/gallia/pull/555>

²⁷ <https://github.com/Fraunhofer-AISEC/gallia/pull/695>

2.1.15 Entwicklung eines Testsystems für Ladekommunikation in E-Fahrzeugen

Im Projekt wurde eine Testsuite entwickelt, welche sicherheitsrelevante Überprüfungen der fahrzeugseitigen Ladeschnittstelle automatisiert durchführen kann. Um trotz der Vielzahl an Anwendungsprotokollen eine effiziente Entwicklung zu ermöglichen, wurde auf quelloffene Implementierungen der standardisierten Protokolle zurückgegriffen. Im Wesentlichen wurden dabei die in Python entwickelten Umsetzungen pylac [202] und iso15118 verwendet. pylac ist dabei für die Verbindung von Fahrzeug und Ladestellen auf den untersten Protokollschichten mithilfe des Signal Level Attenuation Characterization (SLAC) Protokolls zuständig, während iso15118 die weiterführende IPv6 basierte Kommunikation, insbesondere die Anwendungsprotokolle nach DIN SPEC 70121 und ISO 15118 realisiert.

Basierend auf diesen Implementierungen, wurden mehrere Testskripte entwickelt, welche potentielle Angriffsvektoren der fahrzeugseitigen Ladeschnittstelle überprüfen. Darunter befinden sich Tests zum Scannen der unterstützten Applikationsprotokolle und der unterstützten TLS Varianten und Chiffren, als auch ein Skript, welches prüft ob über die Ladeschnittstelle Endpunkte der Fahrzeugdiagnose exponiert sind. Weiterhin wurde basierend auf dem öffentlichen Werkzeug nmap ein vollautomatischer Scanner entwickelt, welcher die Schnittstelle auf offene Ports überprüft und dabei, falls notwendig, selbständig neue Verbindungen aufbauen und damit Tests über mehrere Ladesessions hinweg, durchführen kann. Dies ist insbesondere von Vorteil, falls es bei Testsetups, welche, etwa aus Sicherheitsgründen, keinen Ladestrom bereitstellen, zu fahrzeugseitigen Abbrüchen der Kommunikation kommt. Weiterhin wurden Skripte entwickelt, welche auf die Low-Level Kommunikation bzw. die dort eingesetzten Komponenten abzielen, etwa ein Programm, welches überprüft, ob für die verwendeten Chips Default Zugriffsschlüssel verwendet werden. Zudem wurden Skripte entwickelt, welche das Testen mit externen Tools vereinfachen, etwa indem das Fahrzeug im SECC Discovery Protokoll zum externen Testtool umgeleitet werden kann.

Hardwareseitig wurde im Projekt zudem eine EVSE-seitige Steuer- und Signalisierungsplatine entwickelt, welche die Initialisierung der High Level Kommunikation (HLC) nach ISO 15118 auf Basis der Low-Level Signale gemäß IEC 61851-1/IEC 62196 zuverlässig abbildet. Ziel war es, die digitalen Kommunikationsbedingungen des Control Pilot (CP) und Proximity Pilot (PP) herzustellen und mit einer modularen Hardwareplattform für Labor- und Entwicklungszwecke bereitzustellen.

Für die CP/PP Signalisierung muss nach IEC 61851-1 folgende Beschaltung vorliegen, um den Wechsel in die HLC zu erlauben:

- CP: Ein 1 kHz PWM Signal mit einem High Level von $U_a = 9\text{ V}$ und einem Tastverhältnis zwischen 3 % und 7 % (Default 5 %) und einem Low-Pegel von -12 V , signalisiert nach IEC 61851-1 die Bereitschaft zur digitalen Kommunikation. Der Low Pegel liegt normgerecht bei -12 V . Damit werden die HLC Initialisierungsbedingungen gemäß IEC 61851 1 erfüllt; die Stromfreigabe wird nicht über das Tastverhältnis codiert, sondern explizit als „digitale Kommunikation aktiv“ signalisiert.

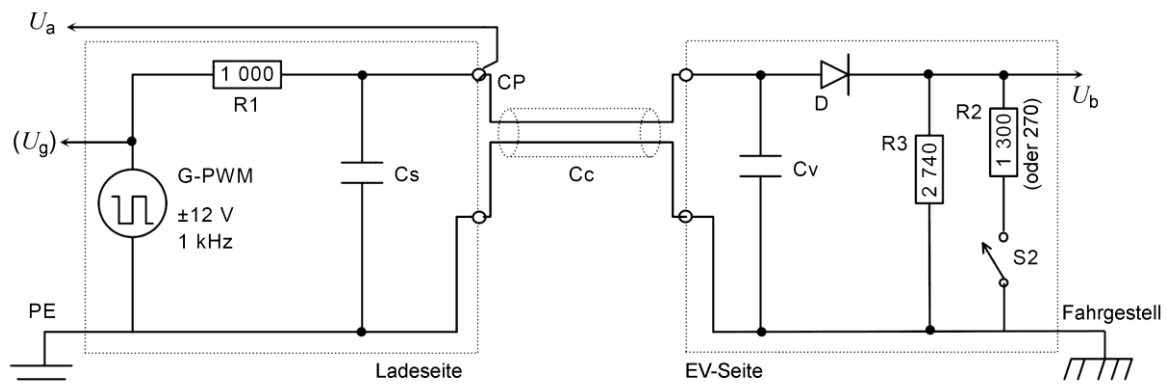


Abbildung 38: Control Pilot Schaltkreis nach IEC 61851-1 [34].

- PP: Signalisiert, ob EV und EVSE verbunden sind, und definiert die maximale Stromstärke des Ladekabels.

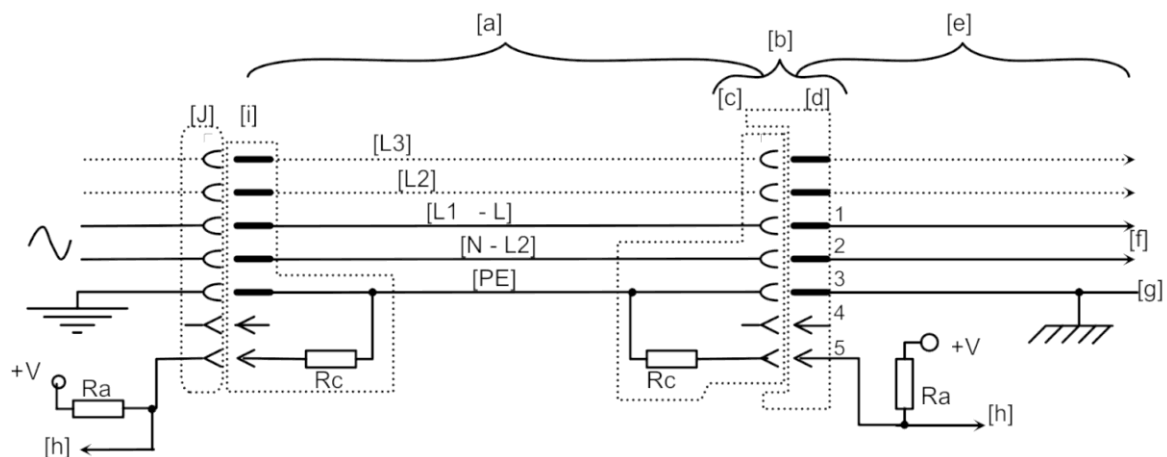


Abbildung 39: Proximity Pilot Schaltkreis nach IEC 61851-1 [34].

Um diese Anforderungen zu erfüllen haben wir folgendes Elektronik- und Softwarekonzept im Projekt entwickelt:

- **Steuerung:** Ein Raspberry Pi Pico übernimmt die PWM Erzeugung und eine zustandsbasierte Steuer-Logik, die sowohl über die serielle Schnittstelle wie auch über Taster und Status LEDs kontrolliert werden kann. Der Pico steuert Relais, mit denen CP/PP gezielt geöffnet werden können, um digitales „Abstecken“ zu erlauben.
- **Split Rail Versorgung:** Aus der 5 V Versorgung wird eine symmetrische ± 12 V Schiene erzeugt. Das Netzteil ist für die CP Treiberstufe ausgelegt und so gefiltert, dass saubere Flanken und ein stabiler -12 V Low Pegel gewährleistet sind.
- **Pegelanpassung/CP Treiber:** Eine Transistor Treiberstufe wandelt das 3.3 V PWM Signal des Pico auf die ± 12 V Schiene. Auf der positiven Halbwelle ist der 1 k Ω Serienwiderstand in den CP Pfad geschaltet, wie in IEC 61851 1 gefordert.
- **Über einen DIP Schalter wird der PP Widerstand gewählt und damit die zulässige Stromstärke des angeschlossenen Kabels gemäß IEC 62196 2 codiert. Die Auslegung deckt die gängigen Kennwerte ab.**

- Schutz- und Trennmaßnahmen: Die CP/PP/PE Anschlüsse sind mit Überspannungs- und Überstromschutz versehen. Die Relais schaffen eine elektrisch robuste Trennmöglichkeit. Eine BNC-Buchse erlaubt außerdem die Verifikation und Messung der CP Signale.

Für die Platine wurde, wie in Abbildung 40 dargestellt, ein Schaltplan und PCB designed und mittels einer Platinenfräse prototypisch umgesetzt.

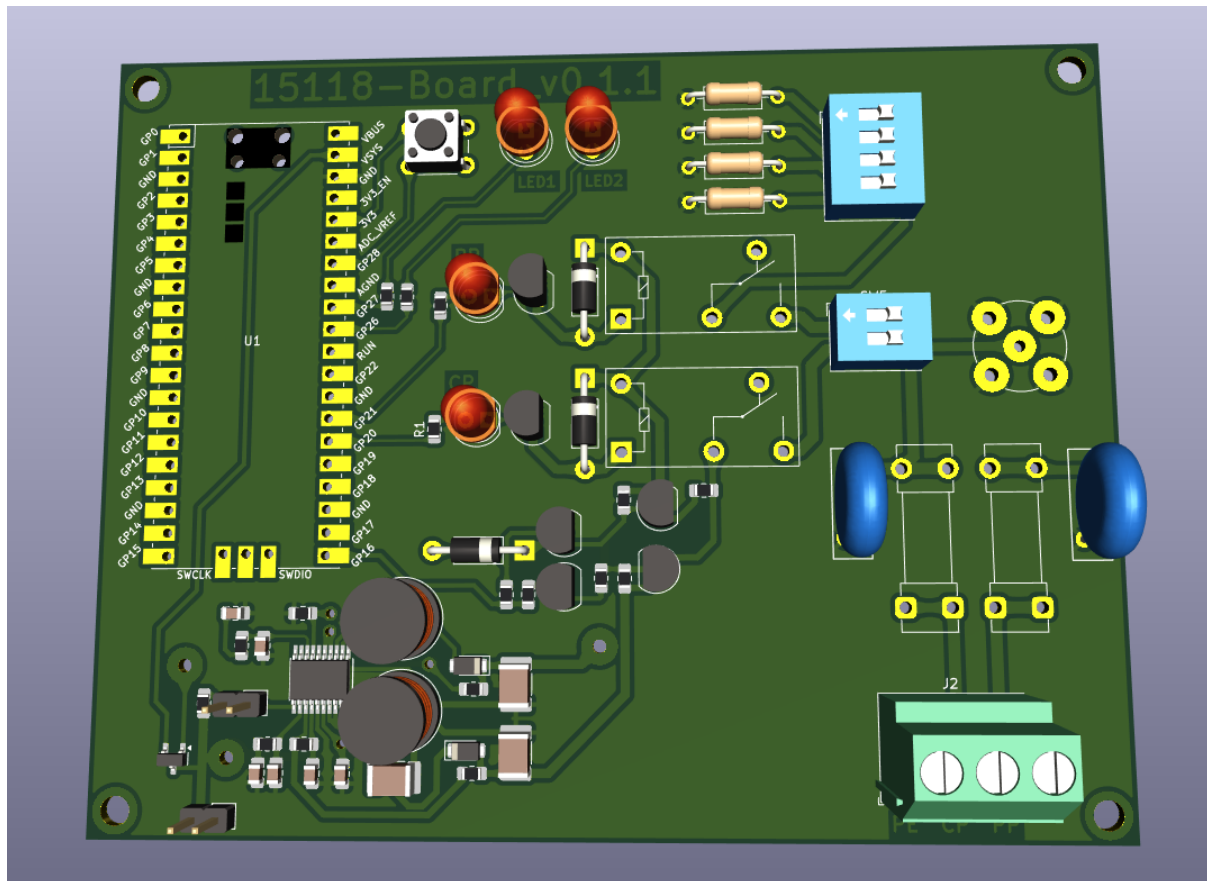


Abbildung 40: Render der designedn Platine in KiCad

Zur Ansteuerung der Platine wurde eine eigene Schnittstelle in Python implementiert, welche es erlaubt, deren Zustände programmatisch über einen angeschlossenen Rechner zu steuern. Dabei kann insbesondere durch das Öffnen der Schaltkreise ein Verbindungsabbruch erzeugt werden, und mittels erneutem Schließen des Schaltkreises eine neue Kommunikation aufgebaut werden.

Abbildung 41 zeigt schematisch den Aufbau des Testsystems mit den im Projekt entwickelten Komponenten, sowie die Schnittstelle zum Fahrzeug.

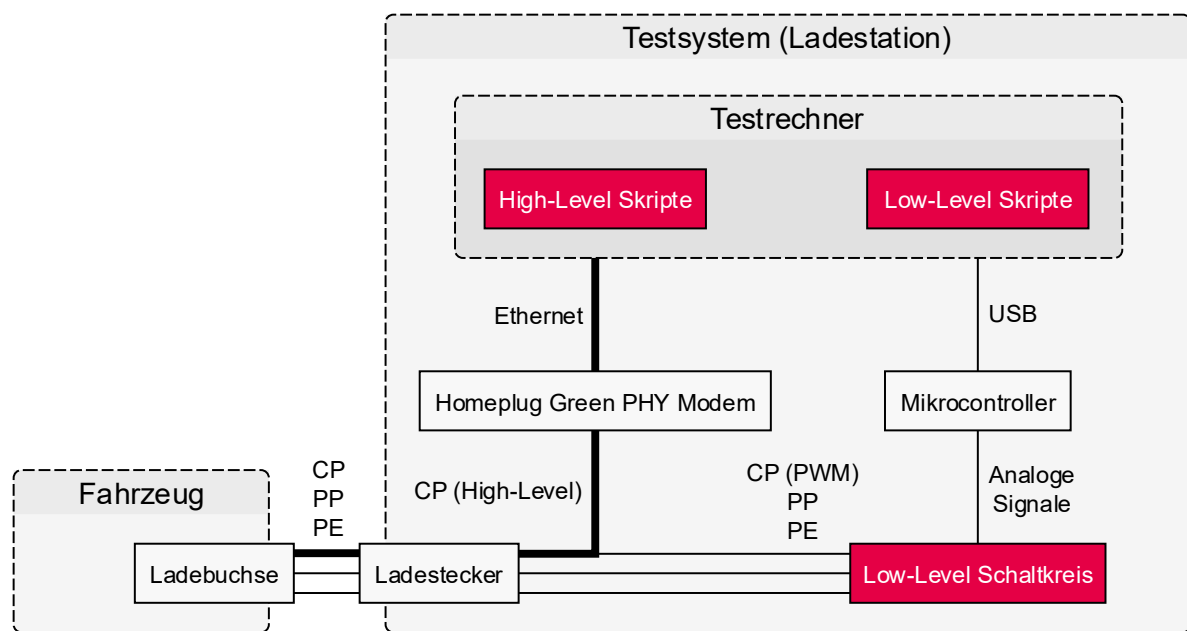


Abbildung 41: Aufbau des Testsystems. Im Projekt entwickelte oder erweiterte Komponenten sind rot eingefärbt.

Die Funktionalität der Testsuite und des Hardwareaufbaus, sowie dessen Möglichkeit zum programmatischen Simulieren eines Aus- und Einsteckens konnte an mehreren isolierten Laboraufbauten, als auch an vollständigen Serienfahrzeugen, nachgewiesen werden.

2.1.16 Entwicklung eines Test-Frameworks für V2X

Im Projekt wurde ein durchgängiges, modular aufgebautes Testframework für C-ITS/V2X realisiert, das den gesamten Software-Stack von der physikalischen Übertragung bis zur Anwendungsebene abdeckt. Die Durchführung erfolgte im Rahmen eines studentischen Praktikums, das auf einen bereits am Fraunhofer AISEC entwickelten, erste Prototypen aufbauen konnte. Kern ist eine Python-basierte modulare Architektur mit Komponenten wie Sender, Logger und Health-Monitoring. Das Framework kann über eine CLI für reproduzierbare, automatisierte Tests angesprochen werden. Auf Protokollebene wurden Scapy-Erweiterungen für GeoNetworking (Basic/Common) und BTP B implementiert und mit den Sicherheitsfunktionen nach IEEE 1609.2 verknüpft. Signaturen, Zeitstempel und abhängige Felder werden beim Erstellen einer Nachricht automatisch konsistent erzeugt. Für die Zertifikatsverwaltung wurde die Microsec-Pilot-PKI (Level 0) integriert und Certificate Enrollment und Authorization Tickets (inkl. CAM/DENM Permissions) wurde automatisiert. Zugang zur PKI erfolgte auf Basis unserer bereits bestehenden C2CCC Mitgliedschaft.

Für die physikalische Ebene wurden zwei Sendewege etabliert: ein Raspberry Pi 5 Setup mit Atheros Chips (AR9280/AR9462/AR9580) und ein GNU Radio / SDR Pfad mit einstellbaren PHY Parametern und Software Loopback für hostbasierte Tests. Für das Raspberry Pi Setup mussten entsprechende Patches, wie für den ath9k Treiber, durchgeführt werden.

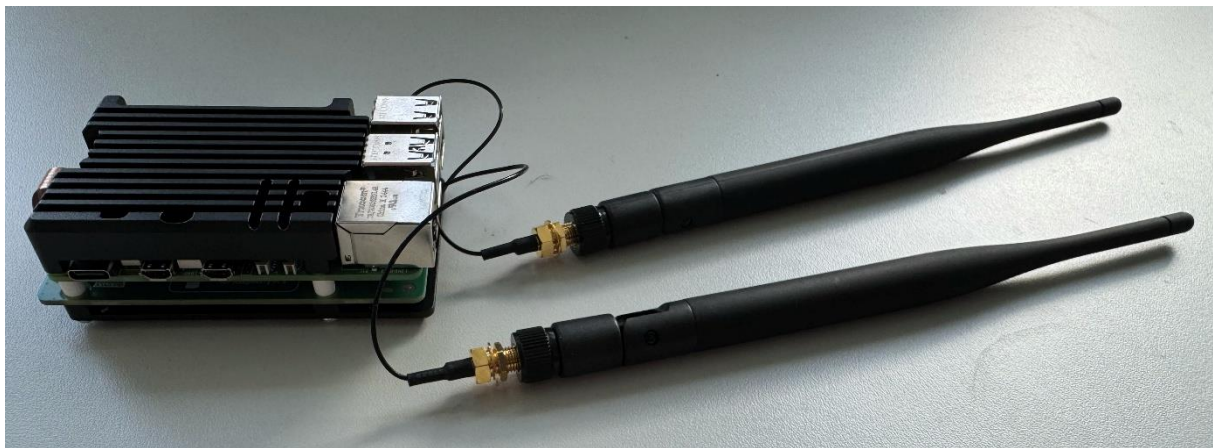


Abbildung 42: Raspberry Pi Setup mit einem Atheros miniPCIe-HAT und zwei Antennen.

Die Pentest-Funktionalität umfasst eine mehrstufige Fuzzing Suite:

- (1) ein ASN.1 Fuzzer, der gezielt Kodierkontrollbytes in CAM/DENM mutiert und anschließend neu signiert
- (2) einen strukturierten Fuzzer, der C-ITS schemakonform vollständige ASN.1 Strukturen generiert und signiert
- (3) einen Radamsa basierten Byte Level Fuzzer der schnelles und einfaches Fuzzing der gesamten Nachricht ermöglicht

Ein Health-Checker überwacht den CAM Heartbeat des Zielsystems, pausiert bei Ausfällen, identifiziert Ziele robust über MAC und führt gezieltes Replay der letzten Nachrichten durch, um den Auslöser zu isolieren.

Für Analysen zur Verwundbarkeit gegen Nachrichten spoofing wurden verschiedene Szenarien implementiert, die verschiedene gültige CAM und DENM Nachrichten verschicken. Dazu können sowohl einzelne Nachrichten gespoofed werden wie auch ein ganzes Szenario dargestellt werden. Dazu wurde das Emergency vehicle approaching (EVA) C-ITS Szenario ausgewählt, in dem sich ein Einsatzfahrzeug nähert. Dazu werden zeitsynchronisierte CAM / DENM Nachrichten entlang GeoJSON Trajektorien mit realistischer Dynamik erzeugt. Eine dynamische Karte, die die empfangenen Nachrichten darstellt und die Tests visualisiert, rundet den Betrieb ab.

Das Test-Framework wurde unter Laborbedingungen an einem Serienfahrzeug praxisnah evaluiert.

2.1.17 Modul-Baukasten Woodpecker zur statischen Code Analyse

Woodpecker kombiniert die Ausführung verschiedener Open-Source-SAST-Tools (z. B. cppcheck, Clang Static Analyzer, FB Infer) und wendet Best-Practice-Konfigurationen an. Als einheitliche Datenbasis dient die LLVM Compilation Database (compile_commands.json). Die Ergebnisse werden im standardisierten SARIF-Format gespeichert. Für Visualisierung, Filterung und Unterstützung des Review-Prozesses steht ein VS-Code-Plugin (SARIF Editor) bereit. Zusätzlich bietet Woodpecker Utility-Funktionen zum Erstellen und Filtern von Compilation-Datenbanken. Durch die modulare Architektur lassen sich weitere SAST-Tools einfach integrieren. Woodpecker und alle unterstützten SAST-Tools werden als Ready-to-Run-Docker-Image ausgeliefert.

Viele in der Automobilindustrie genutzte Entwicklungsumgebungen sind proprietär und nicht frei zugänglich. Für Forschung und Evaluierung fehlen dadurch realitätsnahe, frei verfügbare Referenzprojekte. Das erschwert reproduzierbare Tests und belastbare Vergleiche zwischen Werkzeugen.

Hinzu kommen Unterschiede zwischen Windows- und Linux-Systemen, die sich direkt auf die statische Analyse auswirken. Unter Windows werden andere Zeilenendungen verwendet als unter Linux, zudem treten Unterschiede bei der Textkodierung (z. B. Latin vs. UTF-8) auf. Einige Analysewerkzeuge können damit nicht umgehen, oder müssen entsprechend konfiguriert werden.

Auch die Dateisysteme verhalten sich unterschiedlich: Windows ist in der Regel nicht case-sensitiv, Linux schon. In der Praxis kann die Groß- und Kleinschreibung von Header-Dateinamen in Quelltexten von der Variante im Dateisystem abweichen. Während Builds unter Windows dadurch nicht beeinträchtigt werden, schlagen sie unter Linux fehl, weil Header nicht gefunden werden.

Schließlich unterscheiden sich die in proprietären Umgebungen eingesetzten Compiler und deren Optionen häufig von den in offenen Linux-Umgebungen üblichen Werkzeugen und von den Erwartungen der Analyse-Tools. Das führt zu abweichenden Build-Prozessen und erschwert eine einheitliche Integration der statischen Analyse.

Umsetzungen im Berichtszeitraum von ATLAS-L4:

- Anpassungen an die Automotive-Domäne, inkl. Unterstützung domänenspezifischer CWE-Kategorien.
- Unterstützung von Windows als Plattform:
 - Optimierte Ausführung unter WSL.
 - Verbesserungen am SARIF-Editor-VS-Code-Plugin für Windows (z. B. Umgang mit Windows-Dateipfaden).
 - Umgang mit Windows/Unix-Zeilenenden.
 - Umgang mit inkonsistentem Path-Casing (Windows nicht case-sensitive, Linux schon).
- Optimierung anhand domänenspezifischer Open-Source-Projekte wie mbedTLS und COVESA vsomeip.

Beispiel Security Code Review: COVESA vsomeip

1. Zugang zum Source Code

Der Quellcode ist als Open Source auf GitHub verfügbar und wird lokal heruntergeladen und entpackt.

```
$ wget https://github.com/COVESA/vsomeip/archive/refs/tags/3.5.11.tar.gz -O vsomeip-3.5.11.tar.gz
$ tar xf vsomeip-3.5.11.tar.gz
$ cd vsomeip-3.5.11/
```

2. Buildumgebung einrichten und Compilation Database erstellen

Mit CMake wird ein Build-Verzeichnis angelegt und die LLVM Compilation Database (compile_commands.json) erzeugt.

```
$ mkdir build  
$ cd build  
$ cmake -DCMAKE_EXPORT_COMPILE_COMMANDS=1 ..
```

3. Sicherstellen, dass das Projekt kompiliert; Abhängigkeiten bereitstellen

Woodpecker unterstützt beim Kompilieren auf Basis der Compilation Database und prüft, ob alle Dateien erfolgreich gebaut werden können.

```
$ woodpecker compile_commands run compile_commands.json  
[...]  
All 145 file(s) compiled successfully
```

4. Analyse mit Woodpecker anhand der Compilation Database

Die konfigurierten SAST-Tools werden parallel ausgeführt, die Findings im SARIF-Format gesammelt.

```
$ woodpecker -j8 analyze -p vsomeip compile_commands.json
```

5. SAST-Ergebnisse in VS Code mit dem SARIF-Editor filtern und sortieren

Vorab werden große SARIF-Dateien nach Relevanz (z. B. Warning/Error) gefiltert, anschließend im VS-Code-Plugin interaktiv geprüft.

```
$ woodpecker sarif filter --level warning --level error vsomeip_2025_12_03-07_09_03.sarif -o  
vsomeip_2025_12_03-07_09_03_filter.sarif  
Filter based on level: ('warning', 'error')
```

6. Review der SAST-Ergebnisse

Die Tool-Ergebnisse werden systematisch manuell klassifiziert (True Positive vs. False Positive). Abbildung 43 zeigt die gefilterte Liste an Ergebnissen, die eine hohe Wahrscheinlichkeit haben, ein True Positive zu sein. Zwei Findings sollen hier exemplarisch dargestellt werden.

Level Select 4 ▾

Kind Select 6 ▾

Rank

70.0

100.0

Driver Name Select 6 ▾

Message

Enter pattern here

Uri

Enter pattern here

Level	Kind	Rank	Message	Uri	Line
>			CWE-119 (Improper Restriction of Operations within the Bounds of a Memory Buffer)	51	
>			CWE-190 (Integer Overflow or Wraparound)	28	
>			CWE-398 (7PK - Code Quality)	146	
>			CWE-401 (Missing Release of Memory after Effective Lifetime)	2	
✓			CWE-404 (Improper Resource Shutdown or Release)	1	
	Open	70	File descriptor dynamically all...	utility.cpp	167
>			CWE-457 (Use of Uninitialized Variable)	12	
>			CWE-628 (Function Call with Incorrectly Specified Arguments)	2	
✓			CWE-682 (Incorrect Calculation)	8	
	Open	80	Found function call inside size...	register_events_command.cpp	18
	Open	80	Found function call inside size...	register_events_command.cpp	18
	Open	80	Found function call inside size...	register_events_command.cpp	20
	Open	80	Found function call inside size...	register_events_command.cpp	20
	Open	80	Found function call inside size...	register_events_command.cpp	19
	Open	80	Found function call inside size...	register_events_command.cpp	21
	Open	80	Found function call inside size...	register_events_command.cpp	19

Abbildung 43: Gefilterte Liste an Findings.

Das Finding in Abbildung 44 hat sich als False Positive herausgestellt, da sizeof Expressions zulässt und entsprechend der Funktion Return-Type verwendet wird. Dies scheint auch die Absicht des Entwicklers gewesen zu sein.

```
// implementation/protocol/src/register_events_command.cpp:18
bool register_events_command::add_registration(const register_event& _register_event) {
    size_t its_size(size_ + COMMAND_HEADER_SIZE + sizeof(_register_event.get_service()) + sizeof(_register_event.get_instance())
        + sizeof(_register_event.get_event()) + sizeof(_register_event.get_event_type()) + sizeof(_register_event.is_provided())
        + sizeof(_register_event.get_reliability()) + sizeof(_register_event.is_cyclic())
```

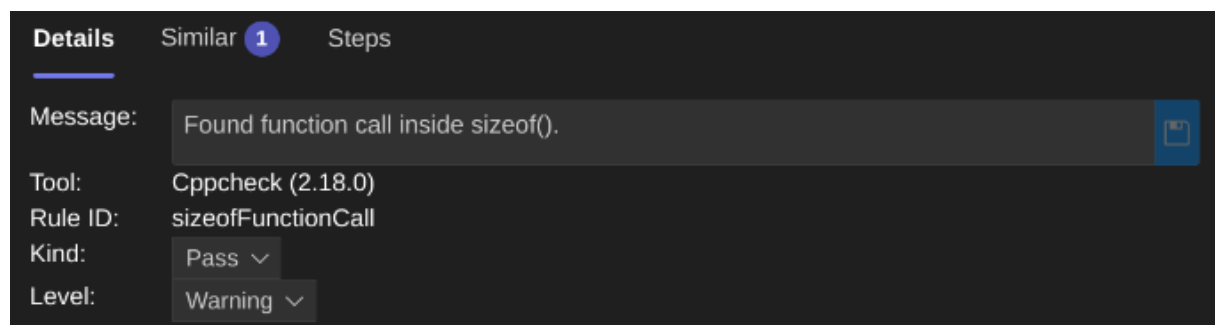
Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung eingetragener Verein; Ausführende Stelle:
Fraunhofer-Institut für Angewandte und Integrierte Sicherheit AISEC

```
+ sizeof(_register_event.get_num_eventgroups()) + (_register_event.get_num_event-
groups() * sizeof(eventgroup_t));

// check size
if (its_size > std::numeric_limits<command_size_t>::max())
    return false;

// set size
size_ = static_cast<command_size_t>(its_size - COMMAND_HEADER_SIZE);
registrations_.push_back(_register_event);

return true;
}
```

A screenshot of the Cppcheck IDE showing a 'Details' panel for a finding. The panel has tabs for 'Details', 'Similar' (with a count of 1), and 'Steps'. The 'Details' tab is active, showing a message: 'Found function call inside sizeof()'. Below the message, it lists the tool as 'Cppcheck (2.18.0)', the rule ID as 'sizeofFunctionCall', the kind as 'Pass' (with a dropdown arrow), and the level as 'Warning' (with a dropdown arrow).

Details Similar **1** Steps

Message: Found function call inside sizeof().

Tool: Cppcheck (2.18.0)

Rule ID: sizeofFunctionCall

Kind: Pass ▾

Level: Warning ▾

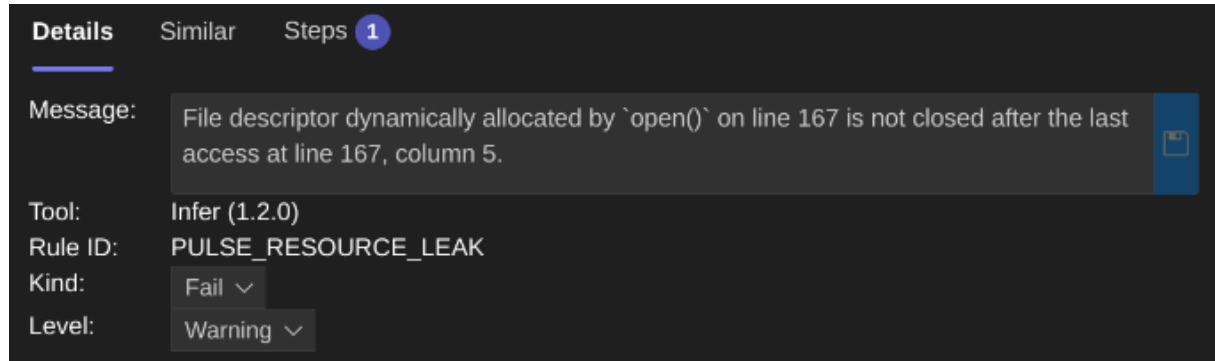
Abbildung 44: False positive Finding (Kind: Pass).

Das Finding in Abbildung 45 bedarf einer genaueren Analyse durch den Entwickler, da ein Resource Leak nicht ausgeschlossen werden kann. Das Finding wird entsprechend markiert, um später in den Code Audit Bericht aufgenommen zu werden.

```
// implementation/utility/src/utility.cpp:176
r.first->second.lock_fd_ = open(its_lockfile.c_str(), O_WRONLY | O_CREAT, S_IWUSR |
S_IWGRP);
if (-1 != r.first->second.lock_fd_) {
    its_lock_data.l_pid = getpid();
    its_lock_ctrl = fcntl(r.first->second.lock_fd_, F_SETLK, &its_lock_data);
} else {
    VSOMEIP_ERROR << __func__ << ": Could not open " << its_lockfile << ": errno " << errno;
}
```



```
return (its_lock_ctrl != -1);
```



Details Similar Steps **1**

Message: File descriptor dynamically allocated by `open()` on line 167 is not closed after the last access at line 167, column 5.

Tool: Infer (1.2.0)

Rule ID: PULSE_RESOURCE_LEAK

Kind: Fail

Level: Warning

Abbildung 45: True positive Finding (Kind: Fail).

7. True-Positive-Findings als Markdown-Report exportieren

Relevante Ergebnisse werden mit Woodpecker als Markdown zusammengefasst.

```
$ woodpecker sarif report vsomeip_2025_12_03-07_09_03_filter.sarif -o report.md
```

Der Bericht wird mit den Informationen aus der SARIF Datei befüllt und muss anschließend ergänzt werden.

```
# Entry-01
## Rating
Info/Low/Medium/High
## Short Abstract
CWE-682
## Location
vsomeip-3.5.11/implementation/protocol/src/register\_events\_command.cpp:18
## Description
Found function call inside sizeof().
## Code Snippet
```c++

 size_t its_size(size_ + COMMAND_HEADER_SIZE + sizeof(_register_event.get_service()) + sizeof(_register_event.get_instance())
 + sizeof(_register_event.get_event()) + sizeof(_register_event.get_event_type()) + sizeof(_register_event.is_provided())
 ...

Recommendation
```

|      |
|------|
| TODO |
|------|

**Beitrag zum Gesamtprojekt ATLAS-L4.** Im Berichtszeitraum von ATLAS-L4 wurden domänenspezifische Anpassungen für die Automotive-Domäne umgesetzt. Dazu gehören die Unterstützung domänenspezifischer CWE-Kategorien, sichergestellt durch Analysen von Referenzprojekten wie mbedTLS und COVESA vsomeip sowie durch Erfahrungswerte aus einschlägigen Projekten. Der SARIF Editor für VS Code wurde für Windows-Systeme optimiert, unter anderem im Hinblick auf den Umgang mit Windows-Dateipfaden. Darüber hinaus wurde die Unterstützung von Windows als Plattform erweitert: Woodpecker ist für die Ausführung unter WSL optimiert und adressiert Unterschiede bei Windows/Unix-Line-Endings sowie inkonsistentem Path-Casing (Windows ist nicht case-sensitive, Linux schon). Hierzu wurde ein Pre-Processing-Modul zur Homogenisierung des Codes implementiert. Eine Evaluation auf frei verfügbaren Daten ist aufgrund der stark abgeschotteten Domäne, proprietärer Tools und fehlender realitätsnaher Open-Source-Projekte schwierig; die Evaluierung erfolgte daher in der Praxis in einschlägigen Projekten. Ergänzend wurde Woodpecker anhand domänenspezifischer Open-Source-Projekte wie mbedTLS und COVESA vsomeip optimiert. Diese Maßnahmen erhöhen die Nutzbarkeit und Zuverlässigkeit der statischen Code-Analyse in typischen Automotive-Entwicklungsumgebungen.

## 2.1.18 Security-Risikoanalyse eines automatisierten Fahrsystems

### 2.1.18.1 Kurzfassung

Neue Gesetze und Technologien, aber auch anhaltende Probleme wie der Mangel an Lkw-Fahrern haben zu Fortschritten im Bereich des autonomen Fahrens und damit zu neuen Cyberrisiken geführt. Wir präsentieren die Ergebnisse unserer Cybersicherheits-Risikoanalyse für ein von einem Control Center überwachtes automatisiertes Fahrsystem (ADS) der Stufe 4, dessen Systemmodell wir anhand von Experteninterviews mit einem globalen Lkw-Hersteller erstellt haben.

Beispiele für Schadensszenarien mit hoher Auswirkungsbewertung sind die Offenlegung von Videodaten, der Verlust der ADS-Funktion während der Fahrt, gefährliche Fahrmanöver und die Aktivierung außerhalb des Betriebsbereichs. Wir haben über 200 Bedrohungsszenarien identifiziert, die sich aus einer Kombination von Hauptangriffsschritten, die bestimmte Teile des Objekts bedrohen, und Vorbereitungsschritten, die bestimmen, wie auf diese Teile zugegriffen wird und durch welche Art von Angreifer, zusammensetzen. Ohne Berücksichtigung von Kontrollmaßnahmen führt die Realisierung dieser Bedrohungsszenarien zu 65 erheblichen Risiken.

Wir schlagen vor, die Bedrohungsszenarien einerseits durch Anforderungen hinsichtlich Implementierungsrelevanter Aspekte und des Angreifer-Modells und andererseits durch Sicherheitsmaßnahmen wie die Erkennung von Systemausfällen und Schutzmaßnahmen wie die authentische Übertragung von Daten zu behandeln.

Abschließend führen wir die Grundsätze auf, die wir aus unserer Analyse abgeleitet haben und die auf andere Cybersicherheitsrisikoanalysen von automatisierten Fahrsystemen angewendet werden können.

### 2.1.18.2 Methode

Wir haben uns für MoRA als Methode entschieden, da sie wissenschaftlich fundiert ist, der Norm ISO/SAE 21434 entspricht und in der Automobilindustrie bereits etabliert ist [1]. Abbildung 46 zeigt die wichtigsten Aktivitäten.

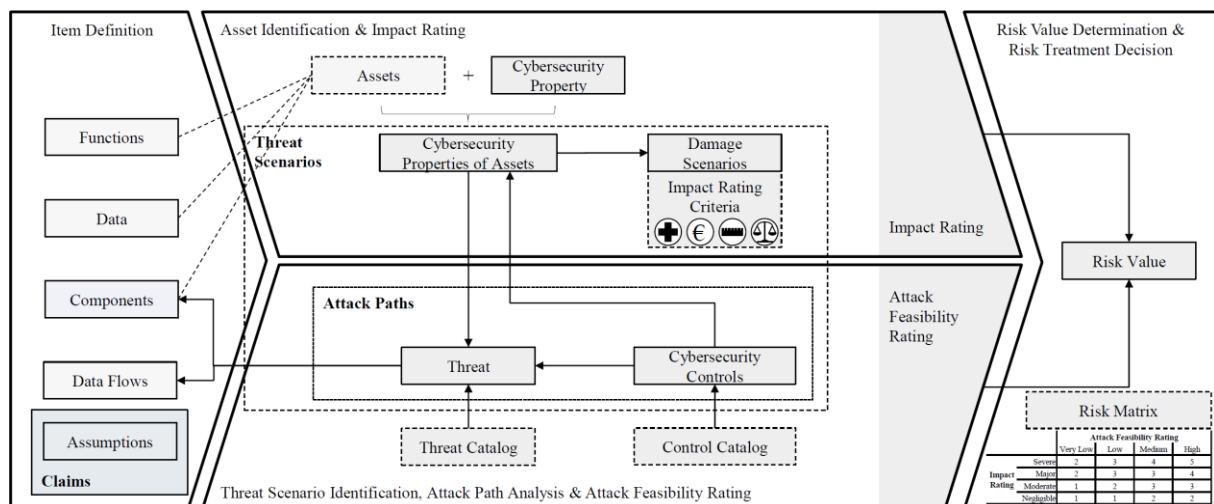


Abbildung 46: Hauptaktivitäten von MoRA, entnommen aus [1] mit Anpassungen an die Terminologie von ISO/SAE 21434. Die Risikomatrix für unsere CRA ist in der unteren rechten Ecke dargestellt.

Bei der Definition der Elemente wird das zu bewertende Ziel (Target of Evaluation, TOE) in seine Funktionen, Daten, Komponenten und Datenflüsse unterteilt. Darüber hinaus werden Annahmen zum Umfang und zum Angreifer-Modell als Anforderungen definiert. Bei der Identifizierung der Vermögenswerte und der Bewertung der Auswirkungen werden Schadensszenarien in den Kategorien Sicherheit, Finanzen, Betrieb und Datenschutz identifiziert. Diese treten ein, wenn ein Angreifer die Vermögenswerte in Bezug auf ihre Sicherheitseigenschaften Vertraulichkeit, Verfügbarkeit oder Integrität verletzt. Jedem Schadensszenario wird eine Auswirkungsbewertung zugewiesen. Für jede Cybersicherheitseigenschaft eines Assets (Cybersecurity Property of Asset, CSPA) werden die möglichen Schadensszenarien angegeben. In der nächsten Aktivität werden Bedrohungen für die CSPA, Angriffswege zur Verwirklichung dieser Bedrohungen und Schutzmaßnahmen zu ihrer Minderung identifiziert. Die Bewertung der Angriffsmachbarkeit jeder Bedrohung und Schutzmaßnahme wird anhand eines auf dem Angriffspotenzial basierenden Ansatzes geschätzt [148]. Bedrohungs- und Maßnahmenkataloge können verwendet werden, um vergleichbare Ergebnisse über mehrere CRAs hinweg zu erzielen. In der letzten Aktivität wird für jede Bedrohung ein Risikowert ermittelt, indem die Auswirkungsbewertungen aller bedrohten CSPA mit der Bewertung der Angriffsmachbarkeit der Bedrohung gemäß einer definierten Risikomatrix kombiniert werden.

### 2.1.18.3 Security-Risikoanalyse eines automatisierten Fahrsystems des Level 4

In den folgenden Unterabschnitten werden die relevantesten Aspekte unserer Security-Risikoanalyse vorgestellt.

#### Systemmodell

Wir haben das Systemmodell für das ADS auf der Grundlage von Experteninterviews mit Mitarbeitern eines globalen Lkw-Herstellers erstellt. Das ADS besteht aus sechs Hauptkomponenten: Wahrnehmung, Prädiktion, Planung und Steuerung bilden den Regelkreis, der die Umgebungswahrnehmung und das autonome Fahren innerhalb des Einsatzbereichs (Operational Design Domain, ODD) des autonomen Fahrsystems (ADS) ermöglicht. Darüber hinaus überwacht das System Management den Zustand der ADS-relevanten Komponenten und leitet bei Bedarf minimale Risikomanöver (Minimum Risk Maneuvers, MRMs) ein. Darüber hinaus stellt die Mission Control die Kommunikation mit dem externen CC her. Tabelle 16, Tabelle 17, Tabelle 18 und Tabelle 19

enthalten Einzelheiten zu den Funktionen, Daten, Komponenten und Kommunikationstechnologien des Analysegegenstands, und Abbildung 47 zeigt einen Überblick über die Architektur.

Tabelle 16: Funktionen des automatisierten Fahrsystems. Wenn Dx oder Nx in Spalte Architektur eingetragen ist, bedeutet dies, dass das Datum Dx oder der Datenfluss Nx für die Funktion relevant sind. Dies ist auch der Fall, wenn die ID einer Komponente, z. B. CC, aufgeführt ist.

| ID | Name                                              | Beschreibung                                                                                                                                                                                                                                                                                         | Architektur                                                                                                                                     |
|----|---------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| F1 | Datenerfassung                                    | Sensoren, Control Center und Basisfahrzeugüberwachung übertragen Fahrzeug- und Umgebungsdaten an Perception. Darüber hinaus kann das Control Center weitere Umgebungsdaten vom Fahrzeug anfordern.                                                                                                   | N1, N2, N3, N4, N5, N6, N7, N8, N9, SNS, PER, D1, D2, CC, MCON, D3, D9, D10, BVM, D14, TRK, ADS, TRK                                            |
| F2 | Objekt- und Ereigniserkennung und Reaktion        | Die ADS-Kernkomponenten interagieren miteinander, um Trajektorien zu planen und Steuerbefehle an die Aktoren zu senden. Darüber hinaus sendet das Control Center ein Navigationsziel, und das Fahrzeug kann Unterstützung vom Control Center anfordern, z. B. beim Überqueren durchgezogener Linien. | N10, N11, N12, N13, N14, N50, N15, N16, N17, N18, N19, N20, N21, PER, PRE, D4, CC, MCON, D25, PLA, D5, D6, CON, D8, D11, D12, ACT, D7, ADS, TRK |
| F3 | Zustandsüberwachung                               | Alle Geräte mit Zustandsüberwachung senden ihren Zustandsstatus an die System Management.                                                                                                                                                                                                            | N22, HMD, SM, D13, TRK, SNS, PER, PRE, PLA, CON, MCON, HMI, ACT, ADS, TRK                                                                       |
| F4 | Anzeige der Bordinformationen                     | Informationen wie der Gesundheitszustand oder die geplante Fahrtroute werden dem Testfahrer oder Disponenten über ein bordeigenes HMI angezeigt.                                                                                                                                                     | N23, N24, N25, BVM, HMI, D14, SM, D13, PLA, D6, TRK, ADS, TRK                                                                                   |
| F5 | Minimales Risikomanöver (MRM) durchführen         | Ein MRM wird beispielsweise vom Control Center oder vom System Management ausgelöst und anschließend vom Fahrzeug ausgeführt.                                                                                                                                                                        | N26, N27, N28, N29, N30, N31, CC, MCON, D15, SM, PLA, HMI, CON, ACT, ADS, TRK                                                                   |
| F6 | Aktivierung des automatisierten Fahrsystems (ADS) | Das ADS wird über einen Befehl des Control Centers aktiviert, die ECUs werden aktiviert und ein Dispatcher sendet einen Aktivierungsstatus zurück an das Control Center.                                                                                                                             | N32, N33, N34, N35, N36, N37, CC, MCON, D16, HMD, D17, SM, HMI, D18, D19, ADS, TRK, SNS, PER, PRE, PLA, CON, MCON, ACT, TRK, ADS                |
| F7 | Überwachung von ADS                               | Betriebsinformationen werden an das Control Center gesendet. Darüber hinaus kann das Control Center einen detaillierten Fahrzeugstatus sowie EDR-Daten anfordern.                                                                                                                                    | N38, N39, N40, N41, N42, N43, N44, N45, N46, N47, SM, MCON, D20, CC, D21, D22, D23, D24, ADS, TRK                                               |
| F8 | Autorisierter Fahrzeugzugang                      | Ein technischer Supervisor des Control Centers sendet nach Autorisierung des Kontakts einen Befehl zum Entsperren des Fahrzeugs.                                                                                                                                                                     | N48, CC, MCON, D26, ADS, TRK                                                                                                                    |
| F9 | Deaktivierung von ADS                             | Ein technischer Supervisor des Control Centers sendet einen Deaktivierungsbefehl, nachdem das Fahrzeug sein Ziel erreicht hat.                                                                                                                                                                       | N49, CC, MCON, D27, ADS, TRK                                                                                                                    |

Tabelle 17: Daten des automatisierten Fahrsystems

| ID  | Name                                         | Beschreibung                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-----|----------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| D1  | Rohvideofeed                                 | Über Kameras erfasste Umgebungsdaten                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| D2  | Sensordaten                                  | Fahrzeug- und Umgebungsdaten<br>Z. B. Radar- und Lidar-Daten, Reifendruck, Daten der Trägheitsmesseinheit                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| D3  | Virtuelle Sensordaten                        | Sensoreingabe des Control Centers an ADS, z. B. digitale Kartendaten (einschließlich Live-Verkehrsdaten), V2X-Kommunikation (einschließlich Ampelstatus)<br><br>Hinweis: Eine Manipulation von D3 Virtuelle Sensordaten einschließlich der V2X-Kommunikation wird beispielsweise in den Bedrohungen T27 und T28 behandelt. Da sich diese Risikoanalyse auf die ADS-Funktionalität konzentriert, wird die V2X/V2I-Kommunikation nicht weiter analysiert. Es wird jedoch davon ausgegangen, dass bei der Entwicklung des vollständig autonomen Lkw V2X-Richtlinien wie die folgenden der Europäischen Kommission berücksichtigt werden: CPOC Protocol, ITS Security Policy, Certificate Policy |
| D4  | Zusammengeführte Sensordaten                 | D1, D2, D3 Plausibilitätsprüfung und Fusion                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| D5  | Objektbahnen                                 | Vorhergesagte Trajektorien von Objekten                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| D6  | Geplante Trajektorie                         | Die geplante Trajektorie des Lkw auf der Grundlage von fusionierten Sensordaten und Objekt-Trajektorien                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| D7  | Ausgabe des Basisfahrzeugs                   | Steuerbefehle der automatisierten Fahrfunktion an die Aktoren, z. B. Bremsen oder Lenken                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| D8  | Dynamische Anpassung                         | Wenn die geplante Fahrbahn nicht befahren werden kann (z. B. weil der Reifendruck nicht optimal ist oder die Batterie nicht genügend Leistung liefert), wird die Planungsdynamik angepasst                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| D9  | Anforderung weiterer Umgebungsdaten          | Anforderung weiterer Umgebungsdaten durch das Control Center                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| D10 | Weitere Umgebungsdaten                       | Z. B. Kamerabilder                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| D11 | Vorschlag für zu genehmigende Trajektorie    | Dies kann auch ein Kamerabild sein, das eine durchgezogene Linie und die Umgebung des Lkw anstelle einer Trajektorie zeigt. Nachdem der Technischer Supervisor das Bild genehmigt hat, wird die Trajektorie im Lkw geplant.                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| D12 | Genehmigung der zu genehmigenden Trajektorie | Genehmigung durch einen Technischer Supervisor, dass die Trajektorie oder die vorgeschlagene Aufgabe vom Lkw ausgeführt werden kann.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| D13 | Gesundheitszustand                           | Die aktuelle Fähigkeit einer ECU, ihre Funktionen auszuführen                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| D14 | Eingabe des Basisfahrzeugs                   | Z. B. Batteriestatus, Reichweite, Navigationsinformationen, Ego- und Selbstwahrnehmung (z. B. Radgeschwindigkeit)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| D15 | MRM initiieren                               | Auslöser zur Ausführung eines MRM                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |

|     |                                        |                                                                                                                                                                                                                                                                                                   |
|-----|----------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| D16 | Aktivierungsbefehl                     | Befehl des Control Centers zur Aktivierung des Lkw                                                                                                                                                                                                                                                |
| D17 | Weckfunktion                           | Aktivierung von ECUs im Ruhemodus                                                                                                                                                                                                                                                                 |
| D18 | Aktivierungsbereiter Status            | Nachdem der Dispatcher die Betriebsbereitschaft des Lkw überprüft hat, wird dieser Befehl an das Control Center gesendet                                                                                                                                                                          |
| D19 | Antriebsbefehl                         | Befehl des Control Centers, der dem Lkw das Fahren erlaubt                                                                                                                                                                                                                                        |
| D20 | Betriebsinformationen                  | Z. B. Standortdaten, Ladeinformationen                                                                                                                                                                                                                                                            |
| D21 | Detaillierten Fahrzeugstatus anfordern | Anfrage des Control Centers nach detailliertem Fahrzeugstatus                                                                                                                                                                                                                                     |
| D22 | Detaillierter Fahrzeugstatus           | Detaillierte Fahrzeugzustands- und Fehlerprotokolle von ADS                                                                                                                                                                                                                                       |
| D23 | EDR-Daten anfordern                    | Anforderung des Control Centers für EDR-Daten                                                                                                                                                                                                                                                     |
| D24 | EDR-Daten                              | Die dynamischen Zeitreihendaten des Fahrzeugs während des Zeitraums unmittelbar vor einem Unfallereignis (z. B. Fahrzeuggeschwindigkeit im Verhältnis zur Zeit) oder während eines Unfallereignisses (z. B. Delta-V im Verhältnis zur Zeit), die nach dem Unfallereignis abgerufen werden sollen. |
| D25 | Navigationsziel                        | Der Ort, zu dem der Lkw fahren soll                                                                                                                                                                                                                                                               |
| D26 | Befehl zum Entriegeln des Fahrzeugs    | Befehl zum Entriegeln des Fahrzeugs                                                                                                                                                                                                                                                               |
| D27 | Befehl zur Deaktivierung               | Befehl zur Deaktivierung des Fahrzeugs                                                                                                                                                                                                                                                            |

Tabelle 18: Komponenten des automatisierten Fahrsystems

| ID  | Name                             | Beschreibung                                                                                                                                                                                               | Teil von | Mitglied von              |
|-----|----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|---------------------------|
| TRK | Lkw                              | Ein mit ADS ausgestatteter Lkw, der für den fahrerlosen Betrieb unter routinemäßigen/normalen Betriebsbedingungen während aller Fahrten innerhalb seines vorgegebenen Einsatzbereichs (ODD) ausgelegt ist. |          |                           |
| ADS | Automatisiertes Fahrsystem (ADS) | Die Hardware und Software, die gemeinsam in der Lage sind, die gesamte dynamische Fahraufgabe (DDT) dauerhaft auszuführen; Fahrassistenzsystem der Stufe 4.                                                | Lkw      |                           |
| SNS | Sensoren                         | Z. B. Kameras, Radargeräte, Lidars, Reifendrucksensoren, Trägheitsmesseinheit                                                                                                                              | Lkw      | Zustandsüberwachte Geräte |
| CC  | Control Center                   | Bietet eine Schnittstelle zur Fernsteuerung und Überwachung von fahrerlosen Lkw.                                                                                                                           |          |                           |



|      |                                |                                                                                                                                                                                                                                                          |                                  |                           |
|------|--------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------|---------------------------|
| PER  | Wahrnehmung                    | Sammelt Informationen und extrahiert relevante Erkenntnisse aus der Umgebung. Zu den Aufgaben gehören das Auffinden von Hindernissen, das Erkennen von Verkehrszeichen und Markierungen oder die Bestimmung der Position des Lkw innerhalb der Umgebung. | Automatisiertes Fahrsystem (ADS) | Zustandsüberwachte Geräte |
| PRE  | Prädiktion                     | Sagt zukünftige Zustände der Fahrumgebung voraus, z. B. Objektbahnen.                                                                                                                                                                                    | Automatisiertes Fahrsystem (ADS) | Zustandsüberwachte Geräte |
| PLA  | Planung                        | Trifft zielgerichtete Entscheidungen, um das Fahrzeug von einem Startort zu einem Zielort zu bringen und dabei Hindernissen auszuweichen.                                                                                                                | Automatisiertes Fahrsystem (ADS) | Zustandsüberwachte Geräte |
| CON  | Control                        | Führt die geplanten Aktionen durch Befehle an die Aktoren aus.                                                                                                                                                                                           | Automatisiertes Fahrsystem (ADS) | Zustandsüberwachte Geräte |
| MCON | Mission Control                | Teil des ADS, der für die Kommunikation mit dem Control Center zuständig ist.                                                                                                                                                                            | Automatisiertes Fahrsystem (ADS) | Zustandsüberwachte Geräte |
| SM   | System Management              | Teil des ADS, der für die Zustandsüberwachung und die Initiierung von MRMs zuständig ist.                                                                                                                                                                | Automatisiertes Fahrsystem (ADS) |                           |
| HMI  | onboard-HMI                    | Zeigt Informationen für einen Testfahrer oder Disponenten an.                                                                                                                                                                                            | Automatisiertes Fahrsystem (ADS) | Zustandsüberwachte Geräte |
| ACT  | Aktuatoren                     | Z. B. Bremse oder Lenkung                                                                                                                                                                                                                                | Lkw                              | Zustandsüberwachte Geräte |
| HMD  | Zustandsüberwachte Geräte      | Gruppe von Komponenten, die ihren Gesundheitszustand an das System Management senden.                                                                                                                                                                    | Lkw                              |                           |
| BVM  | Überwachung des Basisfahrzeugs | ECUs, die Eingaben wie Ego- und Selbstwahrnehmungsdaten an die Wahrnehmung senden.                                                                                                                                                                       | Lkw                              |                           |

Tabelle 19: Kommunikationstechnologien des automatisierten Fahrsystems

| ID   | Name                      | Beschreibung                                                                                 |
|------|---------------------------|----------------------------------------------------------------------------------------------|
| VBUS | Fahrzeugbus               | Verschiedene Fahrzeugbusse, wie CAN, FlexRay, LIN oder Automotive Ethernet.                  |
| IPC  | Interprozesskommunikation | Kommunikation zwischen zwei Softwarekomponenten innerhalb einer ECU, z. B. über AUTOSAR RTE. |
| MCOM | Mobilkommunikation        | Kommunikation über Mobilfunknetze wie 4G, 5G oder WiFi.                                      |

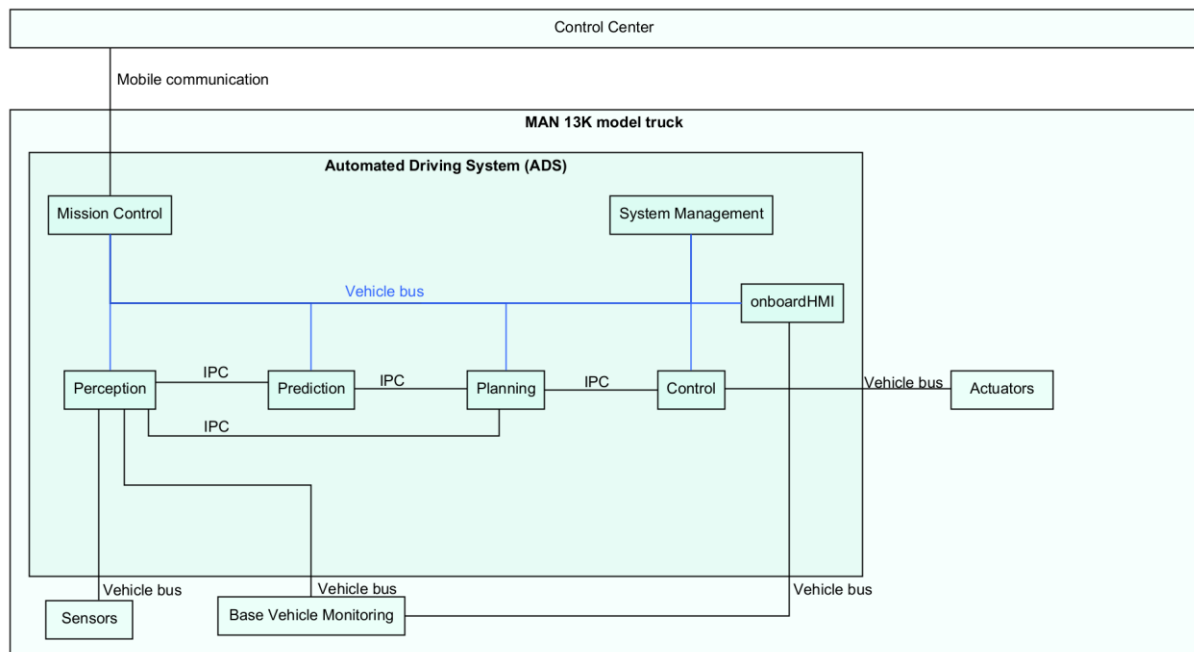


Abbildung 47: ADS Diagramm, das die Komponenten und ihre Verbindungen zeigt. IPC steht für Interprozesskommunikation.

Im Allgemeinen verläuft die Kommunikation zur Durchführung der dynamischen Fahraufgabe (Dynamic Driving Task, DDT) wie folgt: Sensoren, Basisfahrzeugüberwachung und CC übertragen Informationen über die Umgebung und das Fahrzeug an den Regelkreis. Der Regelkreis verarbeitet die Informationen und sendet Steuerbefehle an die Aktoren. MRMs können durch das System Management oder CC ausgelöst werden. Die Kommunikationsflüsse sind in Tabelle 20 aufgeführt und in Abbildung 48 dargestellt.

Tabelle 20: Kommunikationsflüsse des automatisierten Fahrsystems

| ID | Sender          | Empfänger       | Datum                                  | Datumsbeschreibung                                                                                                                           | Kommunikationstechnologie | Auslöser                     | Kommentar            |
|----|-----------------|-----------------|----------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------|---------------------------|------------------------------|----------------------|
| N1 | Sensoren        | Wahrnehmung     | D1 Rohvideodaten                       | D1 Über Kameras erfasste Umgebungsdaten                                                                                                      | Fahrzeugbus               | Kontinuierlich               | >> F1 Datenerfassung |
| N2 | Sensoren        | Wahrnehmung     | D2 Sensordaten                         | D2 Fahrzeug- und Umgebungsdaten<br>z. B. Radar- und Lidar-Daten, Reifendruck, Daten der Trägheitsmess-einheit                                | VBUS Fahrzeugbus          | Kontinuierlich               |                      |
| N3 | Control Center  | Mission Control | D3 Virtuelle Sensordaten               | D3 Sensoreingaben des Control Centers an ADS, z. B. digitale Karten-daten (inkl. Live-Verkehrsdaten), V2X-Kommunikation (inkl. Ampel-status) | MCOM Mobilkommunikation   | Kontinuierlich               |                      |
| N4 | Mission Control | Wahrnehmung     | D3 Virtuelle Sensordaten               | D3 Sensoreingaben des Control Centers an ADS, z. B. digitale Karten-daten (inkl. Live-Verkehrsdaten), V2X-Kommunikation (inkl. Ampel-status) | VBUS Fahrzeugbus          | N3                           |                      |
| N5 | Control Center  | Mission Control | D9 Anforderung weiterer Umgebungsdaten | D9 Anforderung weiterer Umgebungsdaten durch das Control Center.                                                                             | MCOM Mobilkommunikation   | Remote Assistent Interaktion |                      |
| N6 | Mission Control | Wahrnehmung     | D9 Anforderung weiterer Umgebungsdaten | D9 Anforderung weiterer Umgebungsdaten durch das Control Center.                                                                             | VBUS Fahrzeugbus          | N5                           |                      |

|     |                          |                 |                                      |                                                                                                                       |                               |                              |                                                  |
|-----|--------------------------|-----------------|--------------------------------------|-----------------------------------------------------------------------------------------------------------------------|-------------------------------|------------------------------|--------------------------------------------------|
| N7  | Wahrnehmung              | Mission Control | D10 Weitere Umgebungsdaten           | D10 z. B. Kamerabilder.                                                                                               | VBUS Fahrzeugbus              | N6                           |                                                  |
| N8  | Mission Control          | Control Center  | D10 Weitere Umgebungsdaten           | D10 z. B. Kamerabilder.                                                                                               | MCOM Mobilkommunikation       | N7                           |                                                  |
| N9  | Basisfahrzeugüberwachung | Wahrnehmung     | D14 Eingangsdaten des Basisfahrzeugs | D14 z. B. Batteriestatus, Reichweite, Navigationsinformationen, Ego- und Selbstwahrnehmung (z. B. Radgeschwindigkeit) | VBUS Fahrzeugbus              | Kontinuierlich               |                                                  |
| N10 | Wahrnehmung              | Prädiktion      | D4 Zusammengeführte Sensordaten      | D4 D1, D2, D3 auf Plausibilität geprüft und zusammengeführt                                                           | IPC Interprozesskommunikation | N1 UND N2 UND N4 UND N9      | >> F2 Objekt- und Ereigniserkennung und Reaktion |
| N11 | Control Center           | Mission Control | D25 Navigationsziel                  | D25 Der Zielort, zu dem der Lkw fahren soll.                                                                          | MCOM Mobilkommunikation       | Remote Assistent Interaktion |                                                  |
| N12 | Mission Control          | Planung         | D25 Navigationsziel                  | D25 Der Zielort, zu dem der Lkw fahren soll.                                                                          | VBUS Fahrzeugbus              | N11                          |                                                  |
| N13 | Prädiktion               | Planung         | D5 Objekttrajektorien                | D5 Prognostizierte Trajektorien von Objekten                                                                          | IPC Interprozesskommunikation | N10 UND N12 UND N50          |                                                  |

|     |             |                 |                                                    |                                                                                                                                                                                                                          |                               |                                                                                                                                                                                                                                                     |                                                                                                                                                  |
|-----|-------------|-----------------|----------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------|
| N14 | Wahrnehmung | Planung         | D4 Zusammengeführte Sensordaten                    | D4 D1, D2, D3 auf Plausibilität geprüft und zusammengeführt                                                                                                                                                              | IPC Interprozesskommunikation | N1 UND N2 UND N4 UND N9                                                                                                                                                                                                                             |                                                                                                                                                  |
| N50 | Planung     | Prädiktion      | D6 Geplante Trajektorie                            | D6 Die geplante Trajektorie des Lkw auf Basis der zusammengeführten Sensordaten und Objekttrajektorien                                                                                                                   | IPC Interprozesskommunikation | N13 UND N14                                                                                                                                                                                                                                         | Die Planung sendet mögliche Fahrwege zurück an die Prädiktion, um Feedback darüber zu erhalten, wie andere Verkehrsteilnehmer reagieren könnten. |
| N15 | Planung     | Steuerung       | D6 Geplante Trajektorie                            | D6 Die geplante Trajektorie des Lkw auf Basis der zusammengeführten Sensordaten und Objekttrajektorien                                                                                                                   | IPC Interprozesskommunikation | N13                                                                                                                                                                                                                                                 |                                                                                                                                                  |
| N16 | Steuerung   | Planung         | D8 Dynamische Anpassung                            | D8 Wenn die geplante Trajektorie nicht ausgeführt werden kann (z. B. weil der Reifendruck nicht optimal ist oder die Batterie nicht genügend Leistung liefern kann), wird die Planungsdynamik angepasst.                 | IPC Interprozesskommunikation | N15 UND die geplante Trajektorie kann nicht ausgeführt werden, z. B. weil der Reifendruck nicht optimal ist oder die Batterie nicht genügend Leistung liefern kann.                                                                                 |                                                                                                                                                  |
| N17 | Planung     | Mission Control | D11 Vorschlag für eine zu genehmigende Trajektorie | D11 Dies kann auch ein Kamerabild sein, das anstelle einer Fahrbahn eine durchgezogene Linie und die Umgebung des Lkw zeigt. Nachdem der Technische Supervisor das Bild genehmigt hat, wird die Fahrbahn im Lkw geplant. | VBUS Fahrzeugbus              | Situation, in der das Fahrzeug Hilfe oder Erlaubnis vom Control Center benötigt, z. B. wenn sich das Fahrzeug in einer Baustelle mit einer durchgehenden Linie befindet und das Control Center fragt, ob es die durchgehende Linie überqueren darf. |                                                                                                                                                  |

|     |                           |                   |                                                    |                                                                                                                                                                                                                           |                                                 |                |                           |
|-----|---------------------------|-------------------|----------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------|----------------|---------------------------|
| N18 | Mission Control           | Control Center    | D11 Vorschlag für eine zu genehmigende Trajektorie | D11 Dies kann auch ein Kamerabild sein, das anstelle einer Fahrbahn eine durchgezogene Linie und die Umgebung des Lkw zeigt. Nachdem der Technischer Supervisor das Bild genehmigt hat, wird die Fahrbahn im Lkw geplant. | MCOM Mobilkommunikation                         | N17            |                           |
| N19 | Control Center            | Mission Control   | D12 Genehmigung der zu genehmigten Trajektorie     | D12 Genehmigung durch einen Technischer Supervisor, dass die Trajektorie oder die vorgeschlagene Aufgabe vom Lkw ausgeführt werden kann.                                                                                  | MCOM Mobilkommunikation                         | N18            |                           |
| N20 | Mission Control           | Planung           | D12 Genehmigung der zu genehmigten Trajektorie     | D12 Genehmigung durch einen Technischer Supervisor, dass die Trajektorie oder die vorgeschlagene Aufgabe vom Lkw ausgeführt werden kann.                                                                                  | VBUS Fahrzeugbus                                | N19            |                           |
| N21 | Steuerung                 | Aktuatoren        | D7 Basisfahrzeugausgabe                            | D7 Steuerbefehle der automatisierten Fahrfunktion an die Aktoren, z. B. Bremsen oder Lenken                                                                                                                               | VBUS Fahrzeugbus                                | N15 UND N20    |                           |
| N22 | Zustandsüberwachte Geräte | System Management | D13 Zustand                                        | D13 Aktuelle Fähigkeit einer ECU, ihre Funktionen auszuführen                                                                                                                                                             | VBUS Fahrzeugbus, IPC Interprozesskommunikation | Kontinuierlich | >> F3 Zustandsüberwachung |



|     |                          |                   |                                      |                                                                                                                       |                         |                                                |                                                                                                                                                              |
|-----|--------------------------|-------------------|--------------------------------------|-----------------------------------------------------------------------------------------------------------------------|-------------------------|------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|
| N23 | Basisfahrzeugüberwachung | onboard-HMI       | D14 Eingangsdaten des Basisfahrzeugs | D14 z. B. Batteriestatus, Reichweite, Navigationsinformationen, Ego- und Selbstwahrnehmung (z. B. Radgeschwindigkeit) | VBUS Fahrzeugbus        | Kontinuierlich                                 | >> F4 Anzeige der Bordinformationen<br><br>Hinweis: Dieser Datenfluss existiert nicht für den vollständig autonomen Lkw, der ohne Testfahrer in Betrieb ist. |
| N24 | System Management        | onboard-HMI       | D13 Zustand                          | D13 Aktuelle Fähigkeit einer ECU, ihre Funktionen auszuführen                                                         | VBUS Fahrzeugbus        | N22                                            | Hinweis: Dieser Datenfluss existiert nicht für den vollständig autonomen Lkw, der ohne Testfahrer in Betrieb ist.                                            |
| N25 | Planung                  | onboard-HMI       | D6 Geplante Trajektorie              | D6 Die geplante Trajektorie des Lkw auf Basis der zusammengeführten Sensordaten und Objekttrajektorien                | VBUS Fahrzeugbus        | N13                                            | Hinweis: Dieser Datenfluss existiert nicht für den vollständig autonomen Lkw, der ohne Testfahrer in Betrieb ist.                                            |
| N26 | Control Center           | Mission Control   | D15 MRM initiieren                   | D15 Auslöser zur Durchführung eines MRM                                                                               | MCOM Mobilkommunikation | Remote Assistent Interaktion                   | >> F5 Minimales Risiko-Manöver (MRM) durchführen                                                                                                             |
| N27 | Mission Control          | System Management | D15 MRM initiieren                   | D15 Auslöser zur Durchführung eines MRM                                                                               | VBUS Fahrzeugbus        | N26                                            |                                                                                                                                                              |
| N28 | System Management        | Planung           | D15 MRM initiieren                   | D15 Auslöser zur Durchführung eines MRM                                                                               | VBUS Fahrzeugbus        | N27 ODER (N22 UND kritischer Zustand) ODER N29 |                                                                                                                                                              |

|     |                 |                           |                        |                                                        |                                                 |                               |                                                                                                                   |
|-----|-----------------|---------------------------|------------------------|--------------------------------------------------------|-------------------------------------------------|-------------------------------|-------------------------------------------------------------------------------------------------------------------|
| N29 | onboard-HMI     | System Management         | D15 MRM initiieren     | D15 Auslöser zur Durchführung eines MRM                | VBUS Fahrzeugbus                                | Sicherheitsfahrer Interaktion | Hinweis: Dieser Datenfluss existiert nicht für den vollständig autonomen Lkw, der ohne Testfahrer in Betrieb ist. |
| N30 | Planung         | Steuerung                 | D15 MRM initiieren     | D15 Auslöser zur Durchführung eines MRM                | IPC Interprozesskommunikation                   | N28                           |                                                                                                                   |
| N31 | Steuerung       | Aktuatoren                | D15 MRM initiieren     | D15 Auslöser zur Durchführung eines MRM                | VBUS Fahrzeugbus                                | N30                           |                                                                                                                   |
| N32 | Control Center  | Mission Control           | D16 Aktivierungsbefehl | D16 Befehl des Control Centers zur Aktivierung des Lkw | MCOM Mobilkommunikation                         | Remote Assistent Interaktion  | >> F6 Aktivierung des automatisierten Fahrsystems (ADS)                                                           |
| N33 | Mission Control | Zustandsüberwachte Geräte | D17 Weckbefehl         | D17 Aktivierung von ECUs im Schlafmodus                | VBUS Fahrzeugbus, IPC Interprozesskommunikation | N32                           |                                                                                                                   |
| N34 | Mission Control | System Management         | D17 Weckbefehl         | D17 Aktivierung von ECUs im Schlafmodus                | VBUS Fahrzeugbus                                | N32                           |                                                                                                                   |

|     |                   |                   |                                                     |                                                                                                                              |                         |                                                                                                              |                           |
|-----|-------------------|-------------------|-----------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------|-------------------------|--------------------------------------------------------------------------------------------------------------|---------------------------|
| N35 | onboard-HMI       | Mission Control   | D18 Aktivierungsbereiter Status                     | D18 Nachdem der Disponent die Betriebsbereitschaft des Lkw überprüft hat, wird dieser Befehl an das Control Center gesendet. | VBUS Fahrzeugbus        | Dispatcher Interaktion                                                                                       |                           |
| N36 | Mission Control   | Control Center    | D18 Aktivierungsbereiter Status                     | D18 Nachdem der Disponent die Betriebsbereitschaft des Lkw überprüft hat, wird dieser Befehl an das Control Center gesendet. | MCOM Mobilkommunikation | N35                                                                                                          |                           |
| N37 | Control Center    | Mission Control   | D19 Fahrbe-<br>fehl                                 | D19 Befehl des Control Centers, der dem Lkw das Fahren erlaubt.                                                              | MCOM Mobilkommunikation | N36 UND Remote Assistent Interaktion                                                                         |                           |
| N38 | System Management | Mission Control   | D20 Betriebsinformationen                           | D20 Z. B. Standortdaten, Ladeinformationen.                                                                                  | VBUS Fahrzeugbus        | Kontinuierlich                                                                                               | >> F7 Überwachung des ADS |
| N39 | Mission Control   | Control Center    | D20 Betriebsinformationen                           | D20 Z. B. Standortdaten, Ladeinformationen.                                                                                  | MCOM Mobilkommunikation | N38                                                                                                          |                           |
| N40 | Control Center    | Mission Control   | D21 Anforderung detaillierter Fahrzeugzustandsdaten | D21 Anforderung detaillierter Fahrzeugzustandsdaten durch das Control Center.                                                | MCOM Mobilkommunikation | Remote Assistent Interaktion, z. B. wenn weitere Informationen zu einer ECU-Fehlermeldung angefordert werden |                           |
| N41 | Mission Control   | System Management | D21 Anforderung detaillierter                       | D21 Anforderung detaillierter Fahrzeugzustandsdaten durch das Control Center.                                                | VBUS Fahrzeugbus        | N40                                                                                                          |                           |

|     |                           |                           | Fahrzeugzu-<br>standsdaten                            |                                                                                                                                                                                                                                                                                                                                                                            |                                      |                              |  |
|-----|---------------------------|---------------------------|-------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------|------------------------------|--|
| N42 | System<br>Manage-<br>ment | Mission<br>Control        | D22 Detail-<br>lierte Fahr-<br>zeugzu-<br>standsdaten | D22 Detaillierter Fahrzeugstatus und Fehlerproto-<br>kolle von ADS                                                                                                                                                                                                                                                                                                         | VBUS<br>Fahrzeug-<br>bus             | N41                          |  |
| N43 | Mission<br>Control        | Control<br>Center         | D22 Detail-<br>lierte Fahr-<br>zeugzu-<br>standsdaten | D22 Detaillierter Fahrzeugstatus und Fehlerproto-<br>kolle von ADS                                                                                                                                                                                                                                                                                                         | MCOM<br>Mobilkom-<br>munika-<br>tion | N42                          |  |
| N44 | Control<br>Center         | Mission<br>Control        | D23 Anforde-<br>rung von<br>EDR-Daten                 | D23 Anforderung von EDR-Daten durch das Con-<br>trol Center                                                                                                                                                                                                                                                                                                                | MCOM<br>Mobilkom-<br>munika-<br>tion | Remote Assistent Interaktion |  |
| N45 | Mission<br>Control        | System<br>Manage-<br>ment | D23 Anforde-<br>rung von<br>EDR-Daten                 | D23 Anforderung von EDR-Daten durch das Con-<br>trol Center                                                                                                                                                                                                                                                                                                                | VBUS<br>Fahrzeug-<br>bus             | N44                          |  |
| N46 | System<br>Manage-<br>ment | Mission<br>Control        | D24 EDR-Da-<br>ten                                    | D24 Die dynamischen Zeitreihendaten des Fahr-<br>zeugs während des Zeitraums unmittelbar vor ei-<br>nem Unfallereignis (z. B. Fahrzeuggeschwindigkeit<br>im Verhältnis zur Zeit) oder während eines Unfal-<br>lereignisses (z. B. Delta-V im Verhältnis zur Zeit),<br>die nach dem Unfallereignis abgerufen werden sol-<br>len (NHTSA, 49 CFR 563 – Event Data Recorders). | VBUS<br>Fahrzeug-<br>bus             | N45                          |  |

|     |                 |                 |                          |                                                                                                                                                                                                                                                                                                                                                  |                            |                                                                           |                                    |
|-----|-----------------|-----------------|--------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------|---------------------------------------------------------------------------|------------------------------------|
| N47 | Mission Control | Control Center  | D24 EDR-Daten            | D24 Die dynamischen Zeitreihendaten des Fahrzeugs während des Zeitraums unmittelbar vor einem Unfallereignis (z. B. Fahrzeuggeschwindigkeit im Verhältnis zur Zeit) oder während eines Unfallereignisses (z. B. Delta-V im Verhältnis zur Zeit), die nach dem Unfallereignis abgerufen werden sollen (NHTSA, 49 CFR 563 – Event Data Recorders). | MCOM<br>Mobilkommunikation | N46                                                                       |                                    |
| N48 | Control Center  | Mission Control | D26 Entriegelungsbefehl  | D26 Befehl zum Entriegeln des Fahrzeugs                                                                                                                                                                                                                                                                                                          | MCOM<br>Mobilkommunikation | Remote Assistant Interaktion, nach Autorisierung des Kontakts             | >> F8 Autorisierter Fahrzeugzugang |
| N49 | Control Center  | Mission Control | D27 Deaktivierungsbefehl | D27 Befehl zum Deaktivieren des Fahrzeugs                                                                                                                                                                                                                                                                                                        | MCOM<br>Mobilkommunikation | Remote Assistant Interaktion, nachdem das Fahrzeug sein Ziel erreicht hat | >> F9 Deaktivierung des ADS        |

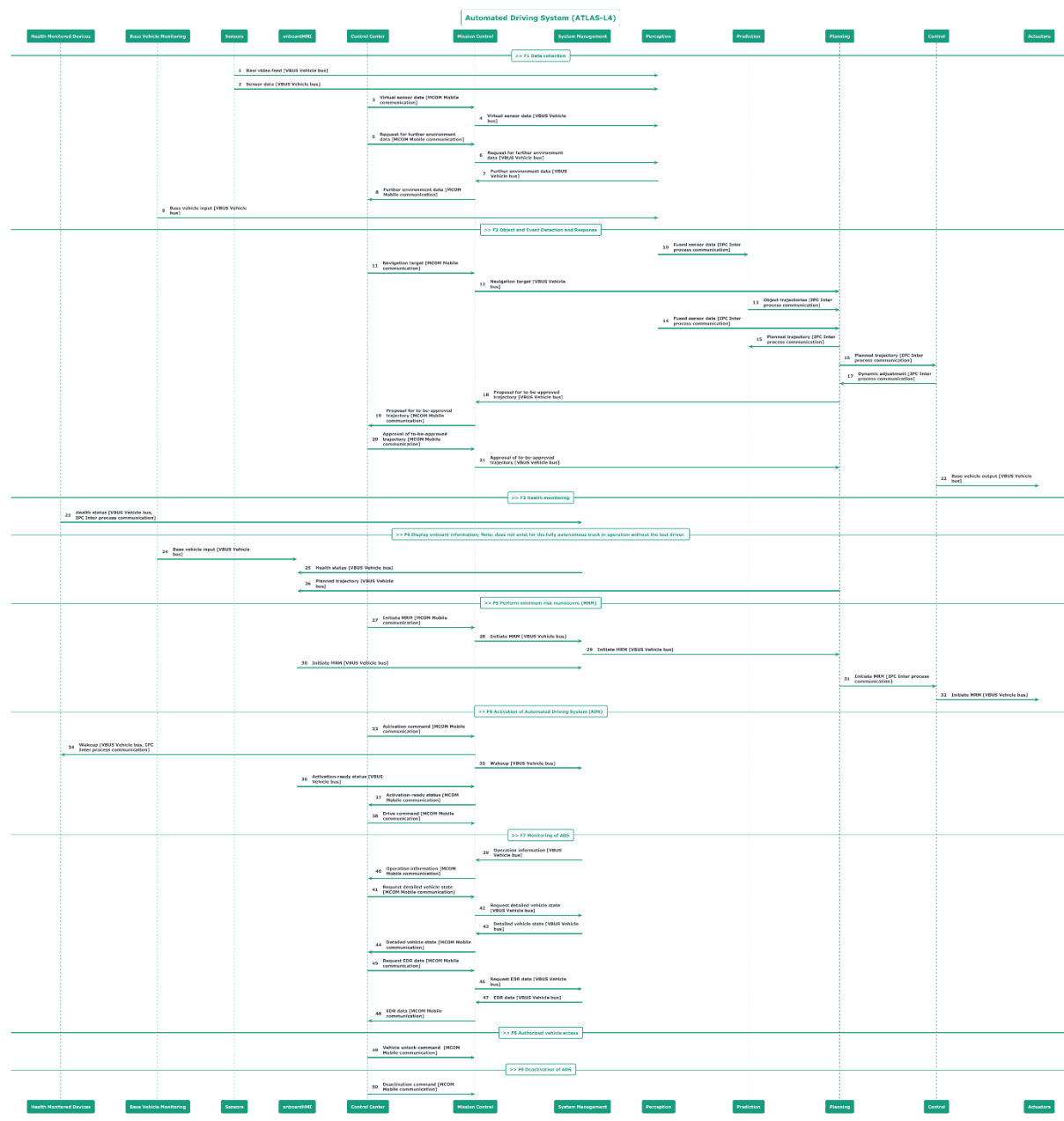


Abbildung 48: Sequenzdiagramm des automatisierten Fahrsystems

## Schadensszenarien und Schutzziele

Wenn es einem Angreifer gelingt, die Sicherheitseigenschaften Vertraulichkeit, Integrität oder Verfügbarkeit von Teilen des TOE zu verletzen, kann dies zu einer Reihe von Schadensszenarien in den Auswirkungsklassen Sicherheit (S), Finanzen (F), Betrieb (O) und Datenschutz (P) mit Auswirkungsgraden auf einer Skala von 0 bis 3 führen, die in Tabelle 21 aufgeführt sind.

Tabelle 21: Schadensszenarien für das automatisierte Fahrsystem; Auswirkungsklassen: S-Sicherheit, F-Finanziell, O-Betrieb, P-Datenschutz; Auswirkungsgrade: 0-Vernachlässigbar, 1-Mäßig, 2-Erheblich, 3-Schwerwiegend.

| ID | Name | Beschreibung und Begründung | Auswirkungsgrad |
|----|------|-----------------------------|-----------------|
|----|------|-----------------------------|-----------------|



|      |                                                                     |                                                                                                                                                                                                                                                          |                  |
|------|---------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------|
| DS1  | Offenlegung von Videodaten                                          | P2: Mehrere Personen könnten erkennbar sein, Verstoß gegen die DSGVO                                                                                                                                                                                     | Erheblich        |
| DS2  | Offenlegung von Infrastrukturinformationen                          | F0OEM: Verlust von geistigem Eigentum in Kartendaten                                                                                                                                                                                                     | Vernachlässigbar |
| DS3  | Verlust von geistigem Eigentum von ADS                              | F3: Das geistige Eigentum von ADS wird für den OEM als finanziell sehr wertvoll angesehen.                                                                                                                                                               | Schwerwiegend    |
| DS4  | Verlust des geistigen Eigentums von Health Monitoring               | F1: Es wird davon ausgegangen, dass das geistige Eigentum von Health Monitoring für den OEM einen mittleren finanziellen Wert hat.                                                                                                                       | Mäßig            |
| DS5  | Verlust der ADS-Funktion im Ruhezustand                             | O2: Fahrzeugstart nicht möglich                                                                                                                                                                                                                          | Erheblich        |
| DS6  | Ausfall der ADS-Funktion während der Fahrt                          | S3: Kollisionen möglich, Verkehrsteilnehmer können lebensgefährliche Verletzungen erleiden                                                                                                                                                               | Schwerwiegend    |
| DS7  | Fehlerhafte Auslösung eines MRM                                     | O2: Fahrzeug hält auf dem Standstreifen                                                                                                                                                                                                                  | Erheblich        |
| DS8  | ADS-Funktion eingeschränkt oder Verlust von Unterkomponenten        | O1: Wartung erforderlich, um volle Funktionsfähigkeit wiederherzustellen                                                                                                                                                                                 | Mäßig            |
| DS9  | Betrieb der Fahrzeugflotte nicht möglich                            | O3: Regressansprüche auf Schadensersatz von OEM-Kunden/CC-Nutzern, Imageschaden                                                                                                                                                                          | Schwerwiegend    |
| DS10 | Erhöhter Batterie- oder Kraftstoffverbrauch für Fahrzeugflotte      | F1: Deaktivierung des Control Centers nicht für die gesamte Flotte verfügbar                                                                                                                                                                             | Mäßig            |
| DS11 | Fahrzeug kann im Ruhezustand nicht ferngesteuert deaktiviert werden | O1: Lokale Deaktivierung durch Servicepersonal erforderlich                                                                                                                                                                                              | Mäßig            |
| DS12 | Gefährliche Fahrmanöver                                             | S3: Manipulierte ADS-Funktionalität kann zu Kollisionen führen, Verkehrsteilnehmer können lebensgefährliche Verletzungen erleiden                                                                                                                        | Schwerwiegend    |
| DS13 | Aktivierung außerhalb des ODD                                       | S3: Unsichere Fahrbedingungen auf bestimmten Straßenabschnitten, auf denen automatisiertes Fahren nicht erlaubt ist, könnten zu lebensbedrohlichen Verletzungen führen.<br>F3: Verstöße gegen Gesetze könnten zu erheblichen finanziellen Schäden führen | Schwerwiegend    |
| DS14 | Falsche Routenplanung für ein einzelnes Fahrzeug                    | F0: Erhöhter Batterieverbrauch, unzufriedene Kunden                                                                                                                                                                                                      | Vernachlässigbar |
| DS15 | Falsche Routenplanung für Fahrzeugflotte                            | F2: Ein Angreifer leitet die Fahrzeugflotte zu einem Ort um, an dem er die Ladung stiehlt. Es ist zu erwarten, dass der Kunde den OEM für die Verluste verklagt.                                                                                         | Erheblich        |

|      |                                                            |                                                                                                                                                                 |                  |
|------|------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------|
| DS16 | Offenlegung der Bewegungsprofile der Fahrzeugflotte        | F2: Ein Angreifer kennt die Routen einer Fahrzeugflotte und stiehlt die Ladung unterwegs. Es ist zu erwarten, dass der Kunde den OEM für die Verluste verklagt. | Erheblich        |
| DS17 | Vorübergehende Störung                                     | O0: Vorübergehende Störung ohne weitere Auswirkungen                                                                                                            | Vernachlässigbar |
| DS18 | Offenlegung des Bewegungsprofils eines einzelnen Fahrzeugs | F1: Ein Angreifer kennt die Route eines einzelnen Fahrzeugs und stiehlt die Ladung unterwegs                                                                    | Mäßig            |

Tabelle 22 zeigt auf, welche Schadensszenarien bei einem Asset (Daten, Komponenten) entstehen können, wenn deren Sicherheitseigenschaften Vertraulichkeit, Integrität, oder Verfügbarkeit verletzt werden. Dies wird als Schutzziel bezeichnet. Hier werden die Auswirkungen von Annahmen und Schutzmaßnahmen noch nicht berücksichtigt.

Tabelle 22: Schutzziele für das automatisierte Fahrsystem; Auswirkungsklassen: S-Sicherheit, F-Finanziell, O-Betrieb, P-Datenschutz; Auswirkungsgrade: 0-Vernachlässigbar, 1-Mäßig, 2-Erheblich, 3-Schwerwiegend.

| ID     | Name                                       | Schadensszenarien                                                              | Auswirkungsgrad  | Kommentar     |
|--------|--------------------------------------------|--------------------------------------------------------------------------------|------------------|---------------|
| CNF.D1 | Vertraulichkeit der Rohvideodaten          | DS1 [P2]                                                                       | Erheblich        |               |
| AVA.D1 | Verfügbarkeit von Rohvideomaterial         | DS5 [O2], DS6 [S3 F2OEM], DS7 [O2], DS8 [O1]                                   | Schwerwiegend    |               |
| INT.D1 | Integrität der Rohvideodaten               | DS5 [O2], DS6 [S3 F2OEM], DS7 [O2], DS8 [O1], DS12 [S3 F2OEM], DS13 [S3 F3OEM] | Schwerwiegend    |               |
|        | Vertraulichkeit der Sensordaten            |                                                                                |                  | Keine Schäden |
| AVA.D2 | Verfügbarkeit der Sensordaten              | DS5 [O2], DS6 [S3 F2OEM], DS7 [O2], DS8 [O1]                                   | Schwerwiegend    |               |
| INT.D2 | Integrität der Sensordaten                 | DS5 [O2], DS6 [S3 F2OEM], DS7 [O2], DS8 [O1], DS12 [S3 F2OEM]                  | Schwerwiegend    |               |
| CNF.D3 | Vertraulichkeit der Virtuellen Sensordaten | DS2 [F0OEM]                                                                    | Vernachlässigbar |               |
| AVA.D3 | Verfügbarkeit virtueller Sensordaten       | DS7 [O2], DS8 [O1]                                                             | Erheblich        |               |
| INT.D3 | Integrität der Virtuellen Sensordaten      | DS5 [O2], DS7 [O2], DS8 [O1], DS12 [S3 F2OEM], DS13 [S3 F3OEM], DS14 [F0RU]    | Schwerwiegend    |               |

|        |                                                         |                                                                                             |               |               |
|--------|---------------------------------------------------------|---------------------------------------------------------------------------------------------|---------------|---------------|
|        | Vertraulichkeit der fusionierten Sensordaten            |                                                                                             |               | Keine Schäden |
| AVA.D4 | Verfügbarkeit der fusionierten Sensordaten              | DS5 [O2], DS6 [S3 F2OEM], DS7 [O2]                                                          | Schwerwiegend |               |
| INT.D4 | Integrität der fusionierten Sensordaten                 | DS5 [O2], DS6 [S3 F2OEM], DS7 [O2], DS8 [O1], DS12 [S3 F2OEM], DS13 [S3 F3OEM], DS14 [F0RU] | Schwerwiegend |               |
|        | Vertraulichkeit von Objektbahnen                        |                                                                                             |               | Keine Schäden |
| AVA.D5 | Verfügbarkeit von Objektbahnen                          | DS5 [O2], DS6 [S3 F2OEM], DS7 [O2]                                                          | Schwerwiegend |               |
| INT.D5 | Integrität der Objektbahnen                             | DS5 [O2], DS6 [S3 F2OEM], DS7 [O2], DS8 [O1], DS12 [S3 F2OEM], DS13 [S3 F3OEM], DS14 [F0RU] | Schwerwiegend |               |
|        | Vertraulichkeit der geplanten Trajektorie               |                                                                                             |               | Keine Schäden |
| AVA.D6 | Verfügbarkeit der geplanten Bahn                        | DS5 [O2], DS6 [S3 F2OEM], DS7 [O2]                                                          | Schwerwiegend |               |
| INT.D6 | Integrität der geplanten Bahn                           | DS5 [O2], DS6 [S3 F2OEM], DS7 [O2], DS8 [O1], DS12 [S3 F2OEM], DS13 [S3 F3OEM], DS14 [F0RU] | Schwerwiegend |               |
|        | Vertraulichkeit der Basisfahrzeugleistung               |                                                                                             |               | Keine Schäden |
| AVA.D7 | Verfügbarkeit der Leistung des Basisfahrzeugs           | DS5 [O2], DS6 [S3 F2OEM], DS7 [O2]                                                          | Schwerwiegend |               |
| INT.D7 | Integrität der Basisfahrzeugleistung                    | DS5 [O2], DS6 [S3 F2OEM], DS7 [O2], DS8 [O1], DS12 [S3 F2OEM], DS13 [S3 F3OEM], DS14 [F0RU] | Schwerwiegend |               |
|        | Vertraulichkeit der dynamischen Anpassung               |                                                                                             |               | Keine Schäden |
| AVA.D8 | Verfügbarkeit der dynamischen Anpassung                 | DS7 [O2], DS8 [O1]                                                                          | Erheblich     |               |
| INT.D8 | Integrität der dynamischen Anpassung                    | DS7 [O2], DS8 [O1], DS12 [S3 F2OEM]                                                         | Schwerwiegend |               |
|        | Vertraulichkeit der Anforderung weiterer Umgebungsdaten |                                                                                             |               | Keine Schäden |

|         |                                                                    |                                                            |               |                                                                                                                                                                                                               |
|---------|--------------------------------------------------------------------|------------------------------------------------------------|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AVA.D9  | Verfügbarkeit der Anfrage nach weiteren Umgebungsdaten             | DS8 [O1]                                                   | Mäßig         |                                                                                                                                                                                                               |
| INT.D9  | Integrität der Anfrage nach weiteren Umweltdaten                   | DS8 [O1]                                                   | Mäßig         |                                                                                                                                                                                                               |
| CNF.D10 | Vertraulichkeit weiterer Umweltdaten                               | DS1 [P2], DS2 [F0OEM]                                      | Erheblich     |                                                                                                                                                                                                               |
| AVA.D10 | Verfügbarkeit weiterer Umweltdaten                                 | DS7 [O2], DS8 [O1]                                         | Erheblich     |                                                                                                                                                                                                               |
| INT.D10 | Integrität weiterer Umweltdaten                                    | DS5 [O2], DS7 [O2], DS8 [O1]                               | Erheblich     |                                                                                                                                                                                                               |
|         | Vertraulichkeit des Vorschlags für die zu genehmigende Trajektorie |                                                            |               | DS2 nicht abgebildet, da davon ausgegangen wird, dass Anfragen nach Notfalltrajektorien selten vorkommen und deren Verfolgung daher nicht zur Offenlegung von Bewegungsprofilen der Fahrzeugflotte führt      |
| AVA.D11 | Verfügbarkeit des Vorschlags für die zu genehmigende Trajektorie   | DS5 [O2], DS8 [O1]                                         | Erheblich     |                                                                                                                                                                                                               |
| INT.D11 | Integrität des Vorschlags für die zu genehmigende Trajektorie      | DS5 [O2], DS7 [O2], DS8 [O1], DS12 [S3 F2OEM], DS14 [F0RU] | Schwerwiegend | Wird von einem Supervisor des Control Centers überprüft. Menschliche Fehler können jedoch nicht vollständig ausgeschlossen werden.                                                                            |
|         | Vertraulichkeit der Genehmigung der zu genehmigenden Trajektorie   |                                                            |               | Keine Schäden                                                                                                                                                                                                 |
| AVA.D12 | Verfügbarkeit der Genehmigung der zu genehmigenden Trajektorie     | DS5 [O2], DS8 [O1]                                         | Erheblich     |                                                                                                                                                                                                               |
| INT.D12 | Integrität der Genehmigung der zu genehmigenden Trajektorie        | DS5 [O2], DS8 [O1]                                         | Erheblich     | Die Trajektorie wird von den ADS-Kernkomponenten validiert, sobald sie vom Control Center an das Fahrzeug zurückgesendet wird.<br><br>Die an das Fahrzeug zurückgesendeten Informationen lauten in etwa: „Die |

|         |                                               |                                                               |               |                                                                                                                         |
|---------|-----------------------------------------------|---------------------------------------------------------------|---------------|-------------------------------------------------------------------------------------------------------------------------|
|         |                                               |                                                               |               | Trajektorie mit der ID 1 kann sicher ausgeführt werden".                                                                |
|         | Vertraulichkeit des Gesundheitszustands       |                                                               |               | Keine Schäden                                                                                                           |
| AVA.D13 | Verfügbarkeit des Gesundheitszustands         | DS5 [O2], DS7 [O2], DS8 [O1]                                  | Erheblich     |                                                                                                                         |
| INT.D13 | Integrität des Gesundheitszustands            | DS5 [O2], DS7 [O2], DS8 [O1], DS12 [S3 F2OEM]                 | Schwerwiegend |                                                                                                                         |
|         | Vertraulichkeit der Eingabe zum Basisfahrzeug |                                                               |               | Keine Schäden                                                                                                           |
| AVA.D14 | Verfügbarkeit der Eingaben zum Basisfahrzeug  | DS5 [O2], DS6 [S3 F2OEM], DS7 [O2], DS8 [O1]                  | Schwerwiegend |                                                                                                                         |
| INT.D14 | Integrität der Eingaben zum Basisfahrzeug     | DS5 [O2], DS6 [S3 F2OEM], DS7 [O2], DS8 [O1], DS12 [S3 F2OEM] | Schwerwiegend |                                                                                                                         |
|         | Vertraulichkeit der MRM-Initiierung           |                                                               |               | Keine Schäden                                                                                                           |
| AVA.D15 | Verfügbarkeit von Initiate MRM                | DS6 [S3 F2OEM]                                                | Schwerwiegend | Der Angreifer wartet, bis ein lebensbedrohliches Szenario eintritt, das ein MRM erfordert, und verweigert dann das MRM. |
| INT.D15 | Integrität der MRM-Initiierung                | DS6 [S3 F2OEM], DS7 [O2]                                      | Schwerwiegend | Der Angreifer wartet, bis ein lebensbedrohliches Szenario eintritt, das ein MRM erfordert, und verweigert dann das MRM. |
|         | Vertraulichkeit des Aktivierungsbefehls       |                                                               |               | Keine Schäden                                                                                                           |
| AVA.D16 | Verfügbarkeit des Aktivierungsbefehls         | DS5 [O2]                                                      | Erheblich     |                                                                                                                         |
| INT.D16 | Integrität des Aktivierungsbefehls            | DS5 [O2], DS11 [O1]                                           | Erheblich     |                                                                                                                         |
|         | Vertraulichkeit des Wakeup-Befehls            |                                                               |               | Keine Schäden                                                                                                           |
| AVA.D17 | Verfügbarkeit des Wakeup-Befehls              | DS5 [O2]                                                      | Erheblich     |                                                                                                                         |
| INT.D17 | Integrität des Wakeup-Befehls                 | DS5 [O2], DS11 [O1]                                           | Erheblich     |                                                                                                                         |

|         |                                                            |                              |                  |                                |
|---------|------------------------------------------------------------|------------------------------|------------------|--------------------------------|
|         | Vertraulichkeit des Aktivierungsstatus                     |                              |                  | Keine Schäden                  |
| AVA.D18 | Verfügbarkeit des Aktivierungsstatus                       | DS5 [O2]                     | Erheblich        |                                |
| INT.D18 | Integrität des Aktivierungsstatus                          | DS5 [O2]                     | Erheblich        |                                |
|         | Vertraulichkeit des Laufwerksbefehls                       |                              |                  | Keine Schäden                  |
| AVA.D19 | Verfügbarkeit des Laufwerksbefehls                         | DS5 [O2]                     | Erheblich        |                                |
| INT.D19 | Integrität des Laufwerksbefehls                            | DS5 [O2]                     | Erheblich        |                                |
| CNF.D20 | Vertraulichkeit der Betriebsinformationen                  | DS18 [F1RU]                  | Mäßig            |                                |
| AVA.D20 | Verfügbarkeit von Betriebsinformationen                    | DS5 [O2], DS7 [O2], DS8 [O1] | Erheblich        |                                |
| INT.D20 | Integrität der Betriebsinformationen                       | DS5 [O2], DS7 [O2], DS8 [O1] | Erheblich        |                                |
|         | Vertraulichkeit der Abfrage detaillierter Fahrzeugzustände |                              |                  | Keine Schäden                  |
| AVA.D21 | Verfügbarkeit detaillierter Fahrzeugzustandsanfragen       | DS7 [O2], DS8 [O1]           | Erheblich        |                                |
| INT.D21 | Integrität der Abfrage detaillierter Fahrzeugzustände      | DS7 [O2], DS8 [O1]           | Erheblich        |                                |
| CNF.D22 | Vertraulichkeit detaillierter Fahrzeugzustandsdaten        | DS2 [F0OEM]                  | Vernachlässigbar |                                |
| AVA.D22 | Verfügbarkeit detaillierter Fahrzeugzustandsdaten          | DS7 [O2], DS8 [O1]           | Erheblich        |                                |
| INT.D22 | Integrität detaillierter Fahrzeugzustand                   | DS7 [O2], DS8 [O1]           | Erheblich        |                                |
|         | Vertraulichkeit der EDR-Datenanforderung                   |                              |                  | Keine Schäden                  |
| AVA.D23 | Verfügbarkeit der angeforderten EDR-Daten                  |                              |                  | Keine Schäden, vgl. Annahme A9 |
| INT.D23 | Integrität der angeforderten EDR-Daten                     |                              |                  | Keine Schäden, vgl. Annahme A9 |
|         | Vertraulichkeit der EDR-Daten                              |                              |                  | Keine Schäden                  |



|         |                                                          |                       |           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|---------|----------------------------------------------------------|-----------------------|-----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|         |                                                          |                       |           | „Ein Ereignisdatenschreiber (EDR) ist ein Gerät oder eine Funktion in einem Fahrzeug, das/die die dynamischen Zeitreihendaten des Fahrzeugs während des Zeitraums unmittelbar vor einem Unfallereignis (z. B. Fahrzeuggeschwindigkeit im Verhältnis zur Zeit) oder während eines Unfallereignisses (z. B. Delta-V im Verhältnis zur Zeit) aufzeichnet, um sie nach dem Unfallereignis abzurufen. Im Sinne dieser Definition umfassen die Ereignisdaten keine Audio- und Videodaten.“ – NHTSA, 49 CFR 563 – Ereignisdatenrekorder |
| AVA.D24 | Verfügbarkeit der EDR-Daten                              |                       |           | Keine Schäden, vgl. Annahme A9                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| INT.D24 | Integrität der EDR-Daten                                 |                       |           | Keine Schäden, vgl. Annahme A9                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| CNF.D25 | Vertraulichkeit des Navigationsziels                     | DS18 [F1RU]           | Mäßig     | Weniger kritisch als das tatsächliche Bewegungsprofil. Im schlimmsten Fall könnte ein Angreifer jedoch immer noch DS18 erreichen, da der Lkw wahrscheinlich die schnellste Route zum Navigationsziel nimmt.                                                                                                                                                                                                                                                                                                                      |
| AVA.D25 | Verfügbarkeit des Navigationsziels                       | DS5 [O2]              | Erheblich |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| INT.D25 | Integrität des Navigationsziels                          | DS5 [O2], DS14 [F0RU] | Erheblich |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|         | Vertraulichkeit des Befehls zum Entriegeln des Fahrzeugs |                       |           | Keine Schäden und nicht im Geltungsbereich von SRA ADS                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| AVA.D26 | Verfügbarkeit des Befehls zum Entriegeln des Fahrzeugs   | DS5 [O2]              | Erheblich |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| INT.D26 | Integrität des Befehls zum Entriegeln des Fahrzeugs      | DS5 [O2]              | Erheblich | Andere Schäden, wie das Entriegeln/Stehlen eines Lkw, sind nicht im Umfang                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

|         |                                                       |                                                                                                        |               |                                                                                                                      |
|---------|-------------------------------------------------------|--------------------------------------------------------------------------------------------------------|---------------|----------------------------------------------------------------------------------------------------------------------|
|         |                                                       |                                                                                                        |               | enthalten, da das ADS nur die von anderen Komponenten bereitgestellten Lkw-Zugangs-/Wegfahr-sperrenfunktionen nutzt. |
|         | Vertraulichkeit des Deaktivierungsbefehls             |                                                                                                        |               | Keine Schäden                                                                                                        |
| AVA.D27 | Verfügbarkeit des Deaktivierungsbefehls               | DS11 [O1]                                                                                              | Mäßig         |                                                                                                                      |
| INT.D27 | Integrität des Deaktivierungsbefehls                  | DS5 [O2], DS11 [O1]                                                                                    | Erheblich     |                                                                                                                      |
|         | Vertraulichkeit von Lkw                               |                                                                                                        |               | Vollständiger Lkw nicht im Anwendungsbereich, relevante Unterkomponenten werden bewertet                             |
|         | Verfügbarkeit des Lkw                                 |                                                                                                        |               | Vollständiger Lkw nicht im Anwendungsbereich, relevante Unterkomponenten werden bewertet                             |
|         | Integrität des Lkw                                    |                                                                                                        |               | Vollständiger Lkw nicht im Anwendungsbereich, relevante Unterkomponenten werden bewertet                             |
| CNF.ADS | Vertraulichkeit des automatisierten Fahrsystems (ADS) | DS1 [P2], DS2 [F0OEM], DS3 [F3OEM], DS4 [F1OEM], DS18 [F1RU]                                           | Schwerwiegend |                                                                                                                      |
| AVA.ADS | Verfügbarkeit des automatisierten Fahrsystems (ADS)   | DS5 [O2], DS6 [S3 F2OEM], DS7 [O2], DS8 [O1], DS11 [O1]                                                | Schwerwiegend |                                                                                                                      |
| INT.ADS | Integrität des automatisierten Fahrsystems (ADS)      | DS5 [O2], DS6 [S3 F2OEM], DS7 [O2], DS8 [O1], DS11 [O1], DS12 [S3 F2OEM], DS13 [S3 F3OEM], DS14 [F0RU] | Schwerwiegend |                                                                                                                      |
| CNF.SNS | Vertraulichkeit der Sensoren                          | DS1 [P2]                                                                                               | Erheblich     |                                                                                                                      |
| AVA.SNS | Verfügbarkeit der Sensoren                            | DS5 [O2], DS6 [S3 F2OEM], DS7 [O2], DS8 [O1]                                                           | Schwerwiegend |                                                                                                                      |
| INT.SNS | Integrität der Sensoren                               | DS5 [O2], DS6 [S3 F2OEM], DS7 [O2], DS8 [O1], DS12 [S3 F2OEM], DS13 [S3 F3OEM]                         | Schwerwiegend |                                                                                                                      |

|         |                                     |                                                                                                                                              |               |  |
|---------|-------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------|---------------|--|
| CNF.CC  | Vertraulichkeit des Control Centers | DS1 [P2], DS2 [F0OEM], DS16 [F2OEM], DS18 [F1RU]                                                                                             | Erheblich     |  |
| AVA.CC  | Verfügbarkeit des Control Centers   | DS5 [O2], DS6 [S3 F2OEM], DS7 [O2], DS8 [O1], DS11 [O1], DS9 [O3], DS10 [F1OEM]                                                              | Schwerwiegend |  |
| INT.CC  | Integrität des Control Centers      | DS5 [O2], DS6 [S3 F2OEM], DS7 [O2], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS11 [O1], DS12 [S3 F2OEM], DS13 [S3 F3OEM], DS14 [F0RU], DS15 [F2OEM] | Schwerwiegend |  |
| CNF.PER | Vertraulichkeit der Wahrnehmung     | DS1 [P2], DS2 [F0OEM], DS3 [F3OEM]                                                                                                           | Schwerwiegend |  |
| AVA.PER | Verfügbarkeit der Wahrnehmung       | DS5 [O2], DS6 [S3 F2OEM], DS7 [O2], DS8 [O1]                                                                                                 | Schwerwiegend |  |
| INT.PER | Integrität der Wahrnehmung          | DS5 [O2], DS6 [S3 F2OEM], DS7 [O2], DS8 [O1], DS12 [S3 F2OEM], DS13 [S3 F3OEM], DS14 [F0RU]                                                  | Schwerwiegend |  |
| CNF.PRE | Vertraulichkeit der Prädiktion      | DS3 [F3OEM]                                                                                                                                  | Schwerwiegend |  |
| AVA.PRE | Verfügbarkeit der Prädiktion        | DS5 [O2], DS6 [S3 F2OEM], DS7 [O2]                                                                                                           | Schwerwiegend |  |
| INT.PRE | Integrität der Prädiktion           | DS5 [O2], DS6 [S3 F2OEM], DS7 [O2], DS8 [O1], DS12 [S3 F2OEM], DS13 [S3 F3OEM], DS14 [F0RU]                                                  | Schwerwiegend |  |
| CNF.PLA | Vertraulichkeit der Planung         | DS3 [F3OEM], DS18 [F1RU]                                                                                                                     | Schwerwiegend |  |
| AVA.PLA | Verfügbarkeit der Planung           | DS5 [O2], DS6 [S3 F2OEM], DS7 [O2], DS8 [O1]                                                                                                 | Schwerwiegend |  |
| INT.PLA | Integrität der Planung              | DS5 [O2], DS6 [S3 F2OEM], DS7 [O2], DS8 [O1], DS12 [S3 F2OEM], DS13 [S3 F3OEM], DS14 [F0RU]                                                  | Schwerwiegend |  |
| CNF.CON | Vertraulichkeit von Control         | DS3 [F3OEM]                                                                                                                                  | Schwerwiegend |  |

|          |                                       |                                                                                             |               |                                                                                                                                                                                                                                                                    |
|----------|---------------------------------------|---------------------------------------------------------------------------------------------|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AVA.CON  | Verfügbarkeit von Control             | DS5 [O2], DS6 [S3 F2OEM], DS7 [O2], DS8 [O1]                                                | Schwerwiegend |                                                                                                                                                                                                                                                                    |
| INT.CON  | Integrität von Control                | DS5 [O2], DS6 [S3 F2OEM], DS7 [O2], DS8 [O1], DS12 [S3 F2OEM], DS13 [S3 F3OEM], DS14 [F0RU] | Schwerwiegend |                                                                                                                                                                                                                                                                    |
| CNF.MCON | Vertraulichkeit der Mission Control   | DS1 [P2], DS2 [F0OEM], DS18 [F1RU]                                                          | Erheblich     |                                                                                                                                                                                                                                                                    |
| AVA.MCON | Verfügbarkeit der Mission Control     | DS5 [O2], DS7 [O2], DS8 [O1], DS11 [O1]                                                     | Erheblich     |                                                                                                                                                                                                                                                                    |
| INT.MCON | Integrität der Mission Control        | DS5 [O2], DS7 [O2], DS8 [O1], DS11 [O1], DS12 [S3 F2OEM], DS13 [S3 F3OEM], DS14 [F0RU]      | Schwerwiegend | Beachten Sie, dass INT.D11 nicht unterstützt wird, da DS12, das durch eine manipulierte, vom CC genehmigte Fahrbahn verursacht werden kann, durch Control M20 verhindert wird. DS12 kann jedoch weiterhin durch Manipulation der virtuellen Sensordaten auftreten. |
| CNF.SM   | Vertraulichkeit der System Management | DS2 [F0OEM], DS4 [F1OEM], DS18 [F1RU]                                                       | Mäßig         |                                                                                                                                                                                                                                                                    |
| AVA.SM   | Verfügbarkeit der System Management   | DS5 [O2], DS6 [S3 F2OEM], DS7 [O2], DS8 [O1]                                                | Schwerwiegend |                                                                                                                                                                                                                                                                    |
| INT.SM   | Integrität der System Management      | DS5 [O2], DS6 [S3 F2OEM], DS7 [O2], DS8 [O1], DS11 [O1], DS12 [S3 F2OEM]                    | Schwerwiegend |                                                                                                                                                                                                                                                                    |
|          | Vertraulichkeit der integrierten HMI  |                                                                                             |               | Keine Schäden                                                                                                                                                                                                                                                      |
| AVA.HMI  | Verfügbarkeit der bordeigenen HMI     | DS5 [O2]                                                                                    | Erheblich     | Keine weiteren Schäden im Betrieb ohne Testfahrer, was dem Anwendungsfall entspricht.                                                                                                                                                                              |
| INT.HMI  | Integrität der bordeigenen HMI        | DS5 [O2]                                                                                    | Erheblich     | Keine weiteren Schäden im Betrieb ohne Testfahrer, was dem Anwendungsfall entspricht.                                                                                                                                                                              |
|          | Vertraulichkeit der Aktoren           |                                                                                             |               | Keine Schäden                                                                                                                                                                                                                                                      |
| AVA.BVM  | Verfügbarkeit der Aktoren             | DS5 [O2], DS6 [S3 F2OEM], DS7 [O2]                                                          | Schwerwiegend |                                                                                                                                                                                                                                                                    |

|         |                                                     |                                                                                             |               |                                                                                                                                                                                                                                                                                                                                                                                           |
|---------|-----------------------------------------------------|---------------------------------------------------------------------------------------------|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| INT.BVM | Integrität der Aktoren                              | DS5 [O2], DS6 [S3 F2OEM], DS7 [O2], DS8 [O1], DS12 [S3 F2OEM], DS13 [S3 F3OEM], DS14 [F0RU] | Schwerwiegend |                                                                                                                                                                                                                                                                                                                                                                                           |
|         | Vertraulichkeit von Geräten mit Zustandsüberwachung |                                                                                             |               | Gruppe nicht im Anwendungsbereich, Unterkomponenten werden bewertet                                                                                                                                                                                                                                                                                                                       |
|         | Verfügbarkeit von gesundheitsüberwachten Geräten    |                                                                                             |               | Gruppe nicht im Anwendungsbereich, Unterkomponenten werden bewertet                                                                                                                                                                                                                                                                                                                       |
|         | Integrität von Geräten mit Gesundheitsüberwachung   |                                                                                             |               | Gruppe nicht im Anwendungsbereich, Unterkomponenten werden bewertet                                                                                                                                                                                                                                                                                                                       |
|         | Vertraulichkeit der Überwachung des Basisfahrzeugs  |                                                                                             |               | Keine Schäden                                                                                                                                                                                                                                                                                                                                                                             |
| AVA.CVM | Verfügbarkeit der Überwachung des Basisfahrzeugs    | DS5 [O2], DS6 [S3 F2OEM], DS7 [O2], DS8 [O1]                                                | Schwerwiegend |                                                                                                                                                                                                                                                                                                                                                                                           |
| INT.CVM | Integrität der Basisfahrzeugüberwachung             | DS5 [O2], DS6 [S3 F2OEM], DS7 [O2], DS8 [O1], DS12 [S3 F2OEM]                               | Schwerwiegend |                                                                                                                                                                                                                                                                                                                                                                                           |
| INT.P5  |                                                     |                                                                                             |               | Dieses Schutzziel zeigt, welche Schutzmaßnahmen gebrochen werden, wenn ein Angreifer mehr als eine Verbindung angreift, um die Sensorfusion oder Redundanzen zu überwinden:<br><br>C3 Validierung von Sensordaten durch Sensorfusion,<br><br>C4 Redundanz für sicherheitskritische Kommunikation der ADS-Kernkomponenten,<br><br>C5 Redundanz gegen Aktivierung von ADS außerhalb von ODD |
| INT.T51 |                                                     |                                                                                             |               | Dieses Schutzziel zeigt, welche Schutzmaßnahmen gebrochen werden, wenn ein Angreifer die Sequenznummer manipuliert, um                                                                                                                                                                                                                                                                    |

|         |  |  |  |                                                                                                                                                                                                                                                                                                                      |
|---------|--|--|--|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|         |  |  |  | die Erkennung fehlender Nachrichten zu umgehen:<br>C9 Sequenznummer zur Erkennung fehlender Nachrichten                                                                                                                                                                                                              |
| CNF.P12 |  |  |  | Dieses Schutzziel zeigt, welche Schutzmaßnahmen gebrochen werden, wenn ein Angreifer private Entschlüsselungsschlüssel extrahiert, um den verschlüsselten Speicher von Software zu überwinden:<br>C8 Verschlüsselte Speicherung der ADS-Software,<br>C10 Verschlüsselte Speicherung der Zustandsüberwachungssoftware |

### Annahmen und Schutzmaßnahmen

Die Bedrohungsszenarien werden durch Annahmen behandelt, die entweder Schadensszenarien mindern oder transformieren oder sich auf die Bewertung der Durchführbarkeit von Angriffen auswirken. Annahmen beziehen sich auf den Umfang der Analyse, z. B. „Angriffe auf das CC sind nicht im Umfang enthalten“, oder auf das Angreifer-Modell, z. B. „Begrenzter Umfang für Tuning-Angriffe“. Darüber hinaus werden wichtige implementierungsrelevante Aspekte, die während der Entwicklung des TOE überprüft werden müssen, in Annahmen als Ansprüche (Claims) spezifiziert, z. B. „Remote-Angriffe werden selektiv berücksichtigt“, was angibt, an welchen Fahrzeugbus eine fernzugängliche ECU angeschlossen ist, oder „MRM, ausgelöst durch CC, sind nicht sicherheitskritisch“. Sie sind in Tabelle 23 aufgeführt.

Tabelle 23: Annahmen für das automatisierte Fahrsystem

| ID | Name                                                       | Beschreibung                                                                                         | Auswirkungsminde-<br>rung | Maxi-<br>ma-<br>ler<br>Risi-<br>ko-<br>wert | Bedrohungen                                        | Kom-<br>mentar<br>/ ver-<br>ant-<br>wortli-<br>che<br>Stelle |
|----|------------------------------------------------------------|------------------------------------------------------------------------------------------------------|---------------------------|---------------------------------------------|----------------------------------------------------|--------------------------------------------------------------|
| A1 | Angriffe auf das Control Center fallen nicht in den Umfang | Es wird davon ausgegangen, dass das Control Center gegen interne und externe Angriffe geschützt ist. |                           | 2                                           | T74 Angriffe auf oder ausgehend vom Control Center | Control Center IT                                            |



|    | dieser Risiko-analyse                                                               |                                                                                                                                                                                                                                                                                                                              |                                                                                                                                                                                                  |                                                                                                                                                                                                                                                                                                           |                       |
|----|-------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|
| A2 | Begrenzter Scope für Tuning-Angriffe                                                | Ein Fahrzeugbesitzer/Tuner verursacht nur Schadensszenarien, die in seinem Interesse liegen.                                                                                                                                                                                                                                 | Entfernt:<br>DS1 [P2],<br>DS5 [O2],<br>DS6 [S3 F2OEM],<br>DS7 [O2],<br>DS8 [O1],<br>DS9 [O3],<br>DS10 [F1OEM],<br>DS11 [O1],<br>DS12 [S3 F2OEM],<br>DS14 [F0RU],<br>DS15 [F2OEM],<br>DS18 [F1RU] | P1 Erlangung physischen Zugriffs auf die Fahrzeugelektronik als Fahrzeugbesitzer/Tuner                                                                                                                                                                                                                    | Angreifer-Modell      |
| A3 | Qualitätsschäden werden im Falle eines kompromittierten Lkw selektiv berücksichtigt | Wenn der Angreifer Zugang zu einem Lkw-Bus oder einer Komponente hat, sind Qualitäts-/Betriebschäden, die durch die TOE verursacht werden, nicht weiter relevant. Wenn der Lkw durch einen Angreifer kompromittiert wird, sollte ohnehin eine Werkstatt aufgesucht werden, um den ursprünglichen Zustand wiederherzustellen. | Entfernt:<br>DS5 [O2],<br>DS7 [O2],<br>DS8 [O1],<br>DS11 [O1]                                                                                                                                    | P2 Erlangung physischen Zugriffs auf die Fahrzeugelektronik als externer Angreifer<br>P3 Erlangung des Zugriffs auf einen Offline-Fahrzeugbus durch Fernkompromittierung einer verbundenen ECU<br>P4 Erlangung des Zugriffs auf einen Online-Fahrzeugbus durch Fernkompromittierung einer verbundenen ECU | Schadensplausibilität |
| A4 | Begrenzte Störung des Mobilfunks                                                    | Ein Angreifer kann Mobilfunkverbindungen nur vorübergehend und in der Nähe des Lkw stören. Störangriffe auf stehende Lkw können erkannt und weitere Maßnahmen ergriffen werden.                                                                                                                                              | Verwandelt:<br>DS5 [O2]<br>-----> DS17 [Q0]<br>DS7 [O2]<br>-----> DS17 [Q0]<br>DS8 [O1]<br>-----> DS17 [Q0]<br>DS11 [O1]                                                                         | T22 Störung der nicht sicherheitskritischen Kommunikation über die MCOM-Verbindung                                                                                                                                                                                                                        | Angreifer-Modell      |

|    |                                                                                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | -----> DS17<br>[Q0]                                                 |   |                                                                                                                                                                 |                 |
|----|------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------|---|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|
| A5 | Fernangriffe werden selektiv berücksichtigt                                              | Die Anschlüsse des Lkw sind in Online-Busse, an die mindestens ein Steuergerät mit drahtlosen Schnittstellen (z. B. WiFi) angeschlossen ist, und Offline-Busse unterteilt. Es wird davon ausgegangen, dass Steuergeräte mit drahtlosen Schnittstellen aus der Ferne kompromittiert werden können und Angriffe über die angeschlossenen Online-Busse möglich sind. Es wird ferner davon ausgegangen, dass Fernangriffe auf Offline-Busse und die daran angeschlossenen Steuergeräte nicht möglich sind. Wenn es wahrscheinlich erscheint, dass ein Offline-Bus mit einem Nachrüstgerät mit drahtlosen Schnittstellen ausgestattet wird, wird er wie ein Online-Bus behandelt. |                                                                     | 1 | P3 Erlangung des Zugriffs auf einen Offline-Fahrzeugbus durch Fernkompromittierung einer angeschlossenen ECU                                                    | OEM             |
| A6 | Lokale Angreifer                                                                         | Der Schutz vor Angriffen durch einen externen Angreifer, der physischen Zugriff auf ADS-relevante Verbindungen und Komponenten benötigt, ist durch Schutzmaßnahmen nicht wirksam, da der Angreifer einfachere Möglichkeiten hat, lebensbedrohliche Schäden zu verursachen (z. B. durch Trennen der Bremsleitungen).                                                                                                                                                                                                                                                                                                                                                          | Entfernt:<br>DS6 [S3 F2OEM],<br>DS12 [S3 F2OEM],<br>DS13 [S3 F3OEM] |   | P2 Erlangung physischen Zugriffs auf die Fahrzeugelektronik als externer Angreifer                                                                              | Angrifer-Modell |
| A8 | Vertrauliche Daten werden nur während der Übertragung verarbeitet und nicht gespeichert. | Hardware-Angriffe auf Komponenten, auf die diese Behauptung zutrifft können nicht zur Offenlegung von Videodaten führen, da diese Daten nur während der Übertragung verarbeitet und nicht gespeichert werden.                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Entfernt:<br>DS1 [P2],<br>DS18 [F1RU]                               |   | T75 Extrahieren von Daten aus zentralen ADS-Komponenten<br>T76 Extrahieren von Daten aus Mission Control<br>T77 Extrahieren von Daten aus dem System Management | OEM             |
| A9 | Keine gesetzlichen Anforderungen für die Übertragung von                                 | Zum Zeitpunkt dieser Analyse gibt es keine gesetzlichen Anforderungen, dass EDR-Daten an das CC gesendet werden müssen. Daher wird davon ausgegangen, dass keine                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |                                                                     |   |                                                                                                                                                                 | OEM             |

|     |                                                        |                                                                                                                                                                                                                                                                                                                   |                          |   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |     |
|-----|--------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|---|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|
|     | EDR-Daten an das CC                                    | <p>relevanten Schäden entstehen, wenn ein Angreifer die Übertragung stört oder manipuliert. EDR-Daten können nach einem Unfall aus den Protokollen im Fahrzeug abgerufen werden.</p> <p>Die Protokolle im Fahrzeug sind ausreichend gegen Angriffe geschützt, was jedoch nicht Gegenstand dieser Analyse ist.</p> |                          |   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |     |
| A10 | Durch CC ausgelöste MRM sind nicht sicherheitskritisch | MRM, die vom Control Center ausgelöst werden, sind nicht sicherheitskritisch. Zusammenfassend lässt sich sagen, dass keine Sicherheitsschäden auftreten können, wenn ein Angreifer die Übertragung dieses Signals stört.                                                                                          | Entfernt: DS6 [S3 F2OEM] |   | <p>T16 Störung MRM auf der MCOM-Verbindung zwischen Control Center und Mission Control initiieren,</p> <p>T17 Störung MRM auf der VBUS-Verbindung zwischen Mission Control und System Management initiieren,</p> <p>T50 Spoofing oder Manipulation MRM als MitM auf der MCOM-Verbindung zwischen Control Center und Mission Control initiieren,</p> <p>T51 Spoofing oder Manipulation von Initiate MRM als MitM auf der VBUS-Verbindung zwischen Mission Control und System Management</p> | OEM |
| A11 | Risiko unabhängig von ADS                              | Risiken, denen diese Behauptung zugeordnet wird, bestehen unabhängig vom ADS, insbesondere: Manipulation von Steuerbefehlen an Aktoren                                                                                                                                                                            |                          | 2 | T45 Spoofing oder Manipulation der Basisausgabe des Fahrzeugs als MitM auf der VBUS-Verbindung zwischen Steuerung und Aktoren                                                                                                                                                                                                                                                                                                                                                              | OEM |

Die Bedrohungsszenarien werden auch durch Schutzmaßnahmen behandelt, die sich auf Schadensszenarien oder die Bewertung der Durchführbarkeit von Angriffen auswirken. Sicherheitsmaßnahmen wie die Erkennung von Systemausfällen sowie Schutzmaßnahmen wie die authentische und verschlüsselte Übertragung oder Schutz vor Denial-of-Service-Angriffen (DoS) für sicherheitskritische Komponenten, sind erforderlich, um die Risikowerte auf ein akzeptables Maß zu senken. Die Schutzmaßnahmen sind in Tabelle 24 aufgeführt.

Tabelle 24: Schutzmaßnahmen für das automatisierte Fahrsystem

| ID | Name                                             | Beschreibung                                                                                                                                                                                                                                                                                                                                                                                    | Maßnahmen-<br>gruppe | Geschützte<br>Cybersi-<br>cherheitsei-<br>genschaft | Geminderte Bedrohungen                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | Auswir-<br>kungsmin-<br>derung                                                   | Angriffs-<br>mach-<br>barkeit |
|----|--------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------|-----------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------|-------------------------------|
| C1 | Erkennung von Systemausfällen                    | <p>Angriffe auf die Verfügbarkeit eines sicherheitsrelevanten Signals gefährden nicht die Sicherheit, sondern lösen lediglich ein MRM aus.</p> <p>Der Lkw führt auch dann ein MRM durch, wenn die Verbindung zum Control Center während der Fahrt für einige Minuten unterbrochen ist.</p>                                                                                                      | Safety               | AVA Verfüg-<br>barkeit                              | <p>T6 Störung des Rohvideofeeds auf der VBUS-Verbindung zwischen Sensoren und Wahrnehmung,</p> <p>T7 Störung der Sensordaten auf der VBUS-Verbindung zwischen Sensoren und Wahrnehmung,</p> <p>T8 Unterbrechung der Basis-Fahrzeugeingabe auf der VBUS-Verbindung zwischen Basis-Fahrzeugüberwachung und Wahrnehmung</p>                                                                                                                                                                   | <p>Transfor-<br/>mationen:<br/>DS6<br/>[S3 F2OEM]<br/>-----&gt; DS7<br/>[O2]</p> | Hoch                          |
| C2 | mTLS zwischen Control Center und Mission Control | Die mobile Verbindung zwischen Control Center und Mission Control wird durch gegenseitig authentifizierte Transport Layer Security in Version 1.3 oder höher gesichert. Es werden sichere, vertrauenswürdige Zertifizierungsstellen verwendet. Die Zertifikate werden validiert. Es werden vertrauenswürdige, eingeschränkte Trust Stores verwendet. Private Schlüssel werden sicher behandelt. | Security             | CNF Vertraulichkeit,<br>INT Integrität              | <p>T1 Abhören der MCOM-Verbindung zwischen Mission Control und Control Center,</p> <p>T27 Spoofing oder Manipulation virtueller Sensordaten als MitM auf der MCOM-Verbindung zwischen Control Center und Mission Control,</p> <p>T29 Spoofing oder Manipulation von Anfragen nach weiteren Umgebungsdaten als MitM auf der MCOM-Verbindung zwischen Control Center und Mission Control,</p> <p>T32 Spoofing oder Manipulation weiterer Umgebungsdaten als MitM auf der MCOM-Verbindung</p> |                                                                                  | Sehr gering                   |

|  |  |  |  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |  |
|--|--|--|--|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|
|  |  |  |  | <p>zwischen Mission Control und Control Center,<br/>T35 Spoofing oder Manipulation von Navigationszielen als MitM auf der MCOM-Verbindung zwischen Control Center und Mission Control,<br/>T42 Spoofing oder Manipulation des Vorschlags für die zu genehmigende Trajektorie als MitM auf der MCOM-Verbindung zwischen Mission Control und Control Center,<br/>T43 Spoofing oder Manipulation der Genehmigung der zu genehmigenden Trajektorie als MitM auf der MCOM-Verbindung zwischen Control Center und Mission Control,<br/>T50 Spoofing oder Manipulation der MRM-Initiierung als MitM auf der MCOM-Verbindung zwischen Control Center und Mission Control,<br/>T56 Spoofing oder Manipulation des Aktivierungsbefehls als MitM auf der MCOM-Verbindung zwischen Control Center und Mission Control,<br/>T60 Spoofing oder Manipulation des Aktivierungsstatus als MitM auf der MCOM-Verbindung zwischen Mission Control und Control Center,<br/>T61 Spoofing oder Manipulation des Fahrbefehls als MitM auf der MCOM-Verbindung zwischen Control Center und Mission Control,<br/>T63 Spoofing oder Manipulation von Betriebsinformationen als MitM auf der MCOM-Verbindung zwischen Mission Control und Control Center,<br/>T64 Spoofing oder Manipulation der detaillierten Fahrzeugzustandsanforderung als MitM auf der MCOM-Verbindung zwischen Control Center und</p> |  |
|--|--|--|--|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|

|    |                                                |                                                                                                                                    |        |                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                                                                                                                                                       |      |
|----|------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------|--------|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|------|
|    |                                                |                                                                                                                                    |        |                | <p>Mission Control,</p> <p>T67 Spoofing oder Manipulation detaillierter Fahrzeugzustandsdaten als MitM auf der MCOM-Verbindung zwischen Mission Control und Control Center,</p> <p>T68 Spoofing oder Manipulation von EDR-Datenanfragen als MitM auf der MCOM-Verbindung zwischen Control Center und Mission Control,</p> <p>T71 Spoofing oder Manipulation von EDR-Daten als MitM auf der MCOM-Verbindung zwischen Mission Control und Control Center,</p> <p>T72 Spoofing oder Manipulation des Befehls zum Entsperren des Fahrzeugs als MitM auf der MCOM-Verbindung zwischen Control Center und Mission Control,</p> <p>T73 Spoofing oder Manipulation des Deaktivierungsbefehls als MitM auf der MCOM-Verbindung zwischen Control Center und Mission Control</p> |                                                                                                                                                       |      |
| C3 | Validierung von Sensordaten durch Sensorfusion | Angriffe auf die Integrität der Daten eines einzelnen Sensors gefährden nicht die Sicherheit, sondern lösen lediglich ein MRM aus. | Safety | INT Integrität | <p>T25 Spoofing oder Manipulation von Rohvideodaten als MitM auf der VBUS-Verbindung zwischen Sensoren und Wahrnehmung,</p> <p>T26 Spoofing oder Manipulation von Sensordaten als MitM auf der VBUS-Verbindung zwischen Sensoren und Wahrnehmung,</p> <p>T27 Spoofing oder Manipulation virtueller Sensordaten als MitM auf der MCOM-Verbindung zwischen Control Center und Mission Control,</p> <p>T28 Spoofing oder Manipulation virtueller Sensordaten als MitM auf der VBUS-Verbindung zwischen Mission Control und Wahrnehmung,</p> <p>T33 Spoofing oder Manipulation der Eingaben des</p>                                                                                                                                                                       | <p>Transformationen:</p> <p>DS6</p> <p>[S3 F2OEM]</p> <p>-----&gt; DS7</p> <p>[O2]</p> <p>DS12</p> <p>[S3 F2OEM]</p> <p>-----&gt; DS7</p> <p>[O2]</p> | Hoch |



|    |                                                                          |                                                                                                                                                                                                                                                                   |          |                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |                                                                                        |      |
|----|--------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|-------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------|------|
|    |                                                                          |                                                                                                                                                                                                                                                                   |          |                   | Basisfahrzeugs als MitM auf der VBUS-Verbindung zwischen der Überwachung des Basisfahrzeugs und der Wahrnehmung                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |                                                                                        |      |
| C4 | Redundanz für sicherheitskritische Kommunikation der ADS-Kernkomponenten | <p>Angriffe auf die Verfügbarkeit eines sicherheitsrelevanten Signals gefährden nicht die Sicherheit, sondern lösen lediglich ein MRM aus.</p> <p>Das MRM wird mit Daten durchgeführt, die über einen redundanten Bus eingehen, der nicht kompromittiert ist.</p> | Safety   | AVA Verfügbarkeit | <p>T9 Unterbrechung der fusionierten Sensordaten auf der IPC-Verbindung zwischen Wahrnehmung und Prädiktion,</p> <p>T10 Störung der Objektbahnen auf der IPC-Verbindung zwischen Prädiktion und Planung,</p> <p>T11 Störung der fusionierten Sensordaten auf der IPC-Verbindung zwischen Wahrnehmung und Planung,</p> <p>T12 Störung der geplanten Bahn auf der IPC-Verbindung zwischen Planung und Steuerung oder zwischen Planung und Prädiktion,</p> <p>T13 Störung der Basisfahrzeugleistung auf der VBUS-Verbindung zwischen Steuerung und Aktoren,</p> <p>T17 Störung der MRM-Initiierung auf der VBUS-Verbindung zwischen Mission Control und System Management,</p> <p>T18 Störung der MRM-Initiierung auf der VBUS-Verbindung zwischen System Management und Planung,</p> <p>T20 Störung der MRM-Initiierung auf der IPC-Verbindung zwischen Planung und Steuerung,</p> <p>T21 Unterbrechung von Initiate MRM auf der VBUS-Verbindung zwischen Steuerung und Aktoren</p> | <p>Transformationen:</p> <p>DS6</p> <p>[S3 F2OEM]</p> <p>-----&gt; DS7</p> <p>[O2]</p> | Hoch |
| C5 | Redundanz gegen Aktivierung                                              | Das Spoofing oder die Manipulation eines einzelnen Eingangssignals, das zur Bestimmung der ODD-Grenzen verwendet wird,                                                                                                                                            | Security | INT Integrität    | T25 Spoofing oder Manipulation von Rohvideodaten als MitM auf der VBUS-Verbindung zwischen Sensoren und Wahrnehmung,                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | <p>Entfernt:</p> <p>DS13</p> <p>[S3 F3OEM]</p>                                         | Hoch |

|    |                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |          |                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |  |             |
|----|-------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|-------------|
|    | von ADS außerhalb von ODD     | <p>kann nicht zu einer Aktivierung des ADS außerhalb des ODD führen.</p> <p>Die ODD-Grenzen werden vom Fahrzeug durch</p> <ul style="list-style-type: none"> <li>*Lokalisierung (GNSS usw.)</li> <li>*Sensordaten (Fahrspuren, Verkehrszeichen usw.)</li> </ul>                                                                                                                                                                                                                                                                                                   |          |                | <p>T26 Spoofing oder Manipulation von Sensordaten als MitM auf der VBUS-Verbindung zwischen Sensoren und Wahrnehmung,</p> <p>T27 Spoofing oder Manipulation virtueller Sensordaten als MitM auf der MCOM-Verbindung zwischen Control Center und Mission Control,</p> <p>T28 Spoofing oder Manipulation virtueller Sensordaten als MitM auf der VBUS-Verbindung zwischen Mission Control und Wahrnehmung,</p> <p>T33 Spoofing oder Manipulation der Eingaben des Basisfahrzeugs als MitM auf der VBUS-Verbindung zwischen der Überwachung des Basisfahrzeugs und der Wahrnehmung</p>                                                                                                                                                                                                    |  |             |
| C6 | Authentische Datenübertragung | <p>Authentische Datenübertragung. Die Daten werden vom Absender signiert und die Signatur vom Empfänger überprüft.</p> <p>Einschließlich:</p> <ul style="list-style-type: none"> <li>*D3 Virtuelle Sensordaten</li> <li>*D4 Geführte Sensordaten</li> <li>*D5 Objektbahnen</li> <li>*D6 Geplante Bahn</li> <li>*D7 Basisfahrzeugleistung</li> <li>*D11 Vorschlag für zu genehmigende Trajektorie</li> <li>*D13 Gesundheitszustand</li> <li>*D14 Eingabe des Basisfahrzeugs</li> <li>*D25 Navigationsziel</li> </ul> <p>D3 zur Verhinderung von Angriffen, bei</p> | Security | INT Integrität | <p>T28 Spoofing oder Manipulation virtueller Sensordaten als MitM auf der VBUS-Verbindung zwischen Mission Control und Wahrnehmung,</p> <p>T34 Spoofing oder Manipulation von fusionierten Sensordaten als MitM auf der IPC-Verbindung zwischen Perception und Prediction,</p> <p>T36 Spoofing oder Manipulation des Navigationsziels als MitM auf der VBUS-Verbindung zwischen Mission Control und Planung,</p> <p>T37 Spoofing oder Manipulation von Objektbahnen als MitM auf der IPC-Verbindung zwischen Prädiktion und Planung,</p> <p>T38 Spoofing oder Manipulation von fusionierten Sensordaten als MitM auf der IPC-Verbindung zwischen Perception und Planning,</p> <p>T39 Spoofing oder Manipulation der geplanten Trajektorie als MitM auf der IPC-Verbindung zwischen</p> |  | Sehr gering |

|    |                                                |                                                                                                                                                                                                                                                                                                                                            |          |                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                                         |      |
|----|------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|---------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------|------|
|    |                                                | denen mehrere Daten gefälscht werden, um DS12 oder DS13 zu verursachen, vgl. Risiken bei Vorbereitungsangriffen P5.                                                                                                                                                                                                                        |          |                     | Planung und Steuerung oder zwischen Planung und Prädiktion,<br>T41 Spoofing oder Manipulation des Vorschlags für die zu genehmigende Trajektorie als MitM auf der VBUS-Verbindung zwischen Planung und Mission Control,<br>T45 Spoofing oder Manipulation der Basisfahrzeugleistung als MitM auf der VBUS-Verbindung zwischen Steuerung und Aktoren,<br>T46 Spoofing oder Manipulation des Gesundheitszustands als MitM auf der VBUS-, IPC-Verbindung zwischen den gesundheitsüberwachten Geräten und dem System Management,<br>T47 Spoofing oder Manipulation der Eingabe des Basisfahrzeugs als MitM auf der VBUS-Verbindung zwischen der Basisfahrzeugüberwachung und dem Onboard-HMI,<br>T48 Spoofing oder Manipulation des Gesundheitszustands als MitM auf der VBUS-Verbindung zwischen System Management und Onboard-HMI |                                         |      |
| C7 | Verschlüsselte Übertragung vertraulicher Daten | <p>Verschlüsselte Übertragung vertraulicher Daten zum Schutz der Privatsphäre von Verkehrsteilnehmern und Navigationszielen von Lkw</p> <p>Einschließlich:</p> <ul style="list-style-type: none"> <li>*D1 Rohvideodaten</li> <li>*D10 Weitere Umgebungsdaten</li> <li>*D20 Betriebsinformationen</li> <li>*D25 Navigationsdaten</li> </ul> | Security | CNF Vertraulichkeit | <p>T2 Abhören der VBUS-Verbindung zwischen Sensoren und Wahrnehmung,</p> <p>T3 Abhören der VBUS-Verbindung zwischen Mission Control und Wahrnehmung,</p> <p>T4 Abhören der VBUS-Verbindung zwischen Mission Control und Planung,</p> <p>T5 Abhören der VBUS-Verbindung zwischen Mission Control und System Management,</p> <p>T76 Extrahieren von Daten aus der Mission Control,</p>                                                                                                                                                                                                                                                                                                                                                                                                                                            | Entfernt:<br>DS1 [P2]<br>DS18<br>[F1RU] | Hoch |

|     |                                                               |                                                                                                                                                                                                                                                                                   |          |                     |                                                                                                                                                                                                        |                                                  |             |
|-----|---------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|---------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------|-------------|
|     |                                                               |                                                                                                                                                                                                                                                                                   |          |                     | T83 Manipulation von Daten, Parametern oder Software der Mission Control                                                                                                                               |                                                  |             |
| C8  | Verschlüsselte Speicherung der ADS-Software                   | ADS-Software mit hohem geistigen Eigentumswert wird verschlüsselt gespeichert und nur beim Starten des Fahrzeugs entschlüsselt                                                                                                                                                    | Security | CNF Vertraulichkeit | T75 Extrahieren von Daten aus zentralen ADS-Komponenten                                                                                                                                                | Entfernt: DS3 [F3OEM]                            | Hoch        |
| C10 | Verschlüsselte Speicherung der Health Monitoring-Software     | Health-Monitoring-Software mit mittlerem geistigen Eigentum wird verschlüsselt gespeichert und nur während des Fahrzeugstarts entschlüsselt                                                                                                                                       | Security | CNF Vertraulichkeit | T77 Extrahieren von Daten aus dem System Management                                                                                                                                                    | Entfernt: DS4 [F1OEM]                            | Hoch        |
| C11 | Denial-of-Service-Schutz für sicherheitskritische Komponenten | Angriffe auf ECUs, bei denen diese Schutzmaßnahme angewendet wird, können nicht zum Verlust der Verfügbarkeit der MRM-Funktionalität führen.<br><br>Einfache Flooding-Angriffe werden erkannt und die Kommunikation mit den sendenden Steuergeräten wird gedrosselt oder beendet. | Security | AVA Verfügbarkeit   | T78 Denial-of-Service-Angriff auf zentrale ADS-Komponenten,<br>T79 Denial-of-Service-Angriff auf die Mission Control über verbundene Busse,<br>T81 Denial-of-Service-Angriff auf das System Management | Transformationen: DS6 [S3 F2OEM] -----> DS7 [O2] | Hoch        |
| C12 | Zugriffskontrolle auf Remote-Schnittstellen                   | Nur Nachrichten von autorisierten Kommunikationspartnern werden vollständig verarbeitet, andere werden verworfen. Zusätzliche Schutzmaßnahmen, wie z. B. Whitelisting, werden implementiert.                                                                                      | Security | AVA Verfügbarkeit   | T80 Denial-of-Service-Angriff auf Mission Control über Remote-Schnittstellen                                                                                                                           |                                                  | Sehr gering |
| C13 | Signierte Software-Updates und Parameter                      | Software-Updates und Parameter werden vom IT-Backend signiert und von den Ziel-Steuergeräten verifiziert.                                                                                                                                                                         | Security | INT Integrität      | P6 Angriff über lokalen Diagnosezugriff, P7 Angriff über Remote-Diagnosezugriff                                                                                                                        |                                                  | Sehr gering |

|     |                                                                 |                                                                                                                                                                                                                                                                                                            |          |                |                                                                                 |  |             |
|-----|-----------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|----------------|---------------------------------------------------------------------------------|--|-------------|
| C14 | Signierte Token zur Autorisierung von Diagnose-diensten         | Zur Autorisierung von Diagnosediensten sind Token erforderlich, die vom IT-Backend kryptografisch signiert sind.<br><br>Wird nur in Verbindung mit C13 verwendet, daher keinen individuellen Effekt zugewiesen.                                                                                            | Security | INT Integrität | P6 Angriff über lokalen Diagnosezugriff, P7 Angriff über Remote-Diagnosezugriff |  |             |
| C15 | Sichere Debugging-, Entwicklungs- und Produktionsschnittstellen | Entweder vollständig entfernt oder nur nach vorheriger Autorisierung zugänglich.                                                                                                                                                                                                                           | Security | INT Integrität | P8 Angriff über Debugging-, Entwicklungs- oder Produktionsschnittstellen        |  | Sehr gering |
| C16 | Sicherer Start                                                  | Die Software eines Steuergeräts wird beim Starten des Fahrzeugs auf ihre Signatur durch das IT-Backend überprüft. Wenn die Überprüfung fehlschlägt, startet das Steuergerät nicht.                                                                                                                         | Security | INT Integrität | P9 Angriff über direkten Speicherzugriff                                        |  | Sehr gering |
| C17 | Entfernung unnötiger Internet-Ports                             | Entfernung aller unnötigen Internet-Ports.                                                                                                                                                                                                                                                                 | Security | INT Integrität | P10 Angriff über unnötige Internet-Ports                                        |  | Sehr gering |
| C18 | Absicherung gegen Fernangriffe                                  | Robuste Implementierung von Software unter Einhaltung sicherer Codierungsrichtlinien, Sicherheits- (Penetrations-)Tests und Codeüberprüfungen, um die Wahrscheinlichkeit von Software-Schwachstellen zu verringern.<br><br>Die Wahrscheinlichkeit einer Software-Sicherheitslücke kann auch dann bestehen, | Security | INT Integrität | P11 Angriff über Remote-Schnittstellen                                          |  | Gering      |

|     |                                                                          | wenn Vorsichtsmaß-nahmen getroffen werden.                                                                                                                                                               |          |                                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |                                                       |             |
|-----|--------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|----------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------|-------------|
| C19 | Speicherung von kryptografischem Material in Hardware-Sicherheitsmodulen | Private Schlüssel sind vor Extraktion geschützt, öffentliche Schlüssel sind vor Manipulation geschützt.<br><br>Der Angriff wird unpraktisch, wenn modernste Hardware-Sicherheitsmodule verwendet werden. | Security | CNF Vertraulichkeit,<br>INT Integrität | P12 Extrahieren von kryptografischem Material<br>P13 Manipulation von kryptografischem Material                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |                                                       | Sehr gering |
| C20 | Überprüfung der genehmigten Trajektorie                                  | Nachdem das Control Center die (manipulierte) Trajektorie (D11, D12) genehmigt hat, überprüft das ADS noch einmal, ob die Trajektorie sicher ausgeführt werden kann.                                     | Safety   | INT Integrität                         | T41 Spoofing oder Manipulation des Vorschlags für die zu genehmigende Trajektorie als MitM auf der VBUS-Verbindung zwischen Planung und Mission Control,<br><br>T42 Spoofing oder Manipulation des Vorschlags für die zu genehmigende Trajektorie als MitM auf der MCOM-Verbindung zwischen Mission Control und Control Center,<br><br>T43 Spoofing oder Manipulation der Genehmigung der zu genehmigenden Trajektorie als MitM auf der MCOM-Verbindung zwischen Control Center und Mission Control,<br><br>T44 Spoofing oder Manipulation der Genehmigung der zu genehmigenden Trajektorie als MitM auf der VBUS-Verbindung zwischen Mission Control und Planung | Entfernt:<br>DS12<br>[S3 F2OEM]                       | Hoch        |
| C21 | End-to-End-Signatur virtueller Sensordaten                               | Virtuelle Sensordaten (D3) werden vom Control Center signiert und die Signatur wird von Perception überprüft. Dadurch wird verhindert, dass ein Angreifer seine eigenen Kartendaten einspeist,           | Security | INT Integrität                         | T27 Spoofing oder Manipulation virtueller Sensordaten als MitM auf der MCOM-Verbindung zwischen Control Center und Mission Control,<br><br>T28 Spoofing oder Manipulation virtueller Sensordaten als MitM auf der VBUS-Verbindung zwischen                                                                                                                                                                                                                                                                                                                                                                                                                        | Entfernt:<br>DS12<br>[S3 F2OEM]<br>DS13<br>[S3 F3OEM] | Hoch        |



|  |                                                                                                                                                                                                                                                                                                                                   |  |                                                                                                                 |  |
|--|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|-----------------------------------------------------------------------------------------------------------------|--|
|  | <p>möglicherweise durch Kompromittierung der Mission Control, was zu gefährlichen Fahrmanövern führen könnte (DS12).</p> <p>Beachten Sie, dass Kartendaten anhand von Landmarken usw. auf Plausibilität mit Sensordaten überprüft werden. Daher ist es für einen Angreifer möglicherweise nicht möglich, DS12 zu verursachen.</p> |  | <p>Mission Control und Perception, T83 Manipulation von Daten, Parametern oder Software von Mission Control</p> |  |
|--|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|-----------------------------------------------------------------------------------------------------------------|--|

### Bedrohungsszenarien und Risiken

Die Sicherheitseigenschaften des TOE werden durch insgesamt 216 Bedrohungsszenarien gefährdet, die sich aus einer Kombination von 84 Hauptangriffsschritten und 13 Vorbereitungsschritten zusammensetzen. Die Hauptangriffsschritte gefährden systematisch die Vertraulichkeit, Verfügbarkeit und Integrität der Datenflüsse und Komponenten des TOE, während die Vorbereitungsschritte bestimmen, wie auf sie zugegriffen wird (z. B. physisch oder aus der Ferne) und durch welche Art von Angreifer (z. B. Fahrzeugbesitzer/Tuner oder externer Angreifer). Die Bewertung der Angriffsmachbarkeiten wurde anhand eines auf dem Angriffspotenzial basierenden Ansatzes gemäß ISO/IEC 18045:2022 und gemäß des vertraulichen Bedrohungskatalogs des OEM geschätzt, der nicht in diesem Abschlussbericht enthalten ist. Die Bewertung der Angriffsmachbarkeiten für die meisten Bedrohungen wird mit „hoch“ eingeschätzt, um Risiken nicht zu unterschätzen. Die 216 Bedrohungsszenarien sowie die Anwendung der Annahmen und Schutzmaßnahmen auf die Bedrohungsszenarien und ihre Auswirkungen auf Schadensszenarien, Angriffsmöglichkeiten und Risikowerte sind in Tabelle 25 dargestellt. Unter Berücksichtigung der Annahmen und Schutzmaßnahmen führt die Realisierung dieser Bedrohungsszenarien nur zu einem einzigen signifikanten Risiko. Das verbleibende Risiko mit dem Wert 3 betrifft die Ausnutzung von Software-Schwachstellen in Mission Control, dem Endpunkt für die externe Kommunikation. Im Rahmen dieser CRA ist nicht auszuschließen, dass diese aus der Ferne zugängliche Komponente durch eine Software-Schwachstelle kompromittiert wird. Um die Wahrscheinlichkeit so weit wie möglich zu reduzieren, wird jedoch eine Absicherung gegen Fernangriffe vorgeschlagen, die eine robuste Implementierung der Software, die Einhaltung sicherer Codierungsrichtlinien, Cybersicherheits- (Penetrations-)Tests und Codeüberprüfungen umfasst. Darüber hinaus können Safety-Auswirkungen verhindert werden, indem die virtuellen Sensordaten vom CC durchgehend signiert und die Signaturen in Perception überprüft werden.

Tabelle 25: Bedrohungsszenarien und Risiken für das automatisierte Fahrsystem; SZ<sub>v</sub>/SZ<sub>n</sub>-Schadensszenarien vor/nach Schutzmaßnahmen; AG<sub>v</sub>/AG<sub>n</sub>-Auswirkungsgrad vor/nach Schutzmaßnahmen, V-Vernachlässigbar, M-Mäßig, E-Erheblich, S-Schwerwiegend; AM<sub>v</sub>/AM<sub>n</sub>-Angriffsmachbarkeit vor/nach Schutzmaßnahmen, SG-Sehr gering, G-Gering, M-Mittel, H-Hoch; R<sub>v</sub>/R<sub>n</sub>-Risikowert vor/nach Schutzmaßnahmen; Hinweis: Wenn in den Spalten SZ<sub>v</sub>/SZ<sub>n</sub> zwei durchgezogene Linien vorhanden sind, ist dies so zu

interpretieren, dass oberhalb der ersten Linie die Schadensszenarien ohne Berücksichtigung von Annahmen, darunter die durch Annahmen entfernten oder transformierten Schadensszenarien und ganz unten die Schadensszenarien unter Berücksichtigung von Annahmen aufgeführt sind.

| ID+Name                                                                                                                                                                               | Schutzmaßnahmen und Annahmen                                                                                                                                        | SZ <sub>v</sub>                                                                                          | AG <sub>v</sub> | AM <sub>v</sub> | R <sub>v</sub> | SZ <sub>n</sub>                                                                                                     | AG <sub>n</sub> | AM <sub>n</sub> | R <sub>n</sub> |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------|-----------------|-----------------|----------------|---------------------------------------------------------------------------------------------------------------------|-----------------|-----------------|----------------|
| R1: T1 Abhören der MCOM-Verbindung zwischen Mission Control und Control Center                                                                                                        | C2 mTLS zwischen Control Center und Mission Control                                                                                                                 | DS1 [P2], DS2 [F0OEM], DS18 [F1RU]                                                                       | E               | H               | 4              | DS1 [P2], DS2 [F0OEM], DS18 [F1RU]                                                                                  | E               | SG              | 2              |
| R2: T2 Abhören der VBUS-Verbindung zwischen Sensoren und Wahrnehmung Vorbereitung durch P2 Erlangung physischen Zugriffs auf die Fahrzeugelektronik als externer Angreifer            | C7 Verschlüsselte Übertragung vertraulicher Daten<br>A3 Qualitätsschäden werden im Falle eines kompromittierten Lkw selektiv berücksichtigt.<br>A6 Lokale Angreifer | DS1 [P2]<br>DS5, DS7, DS8, DS11, DS6, DS12, DS13<br>DS1 [P2]                                             | E               | H               | 4              | DS1 [P2]<br>DS1, DS18, DS5, DS7, DS8, DS11, DS6, DS12, DS13                                                         |                 | H               | 1              |
| R3: T2 Abhören der VBUS-Verbindung zwischen Sensoren und Wahrnehmung Vorbereitung durch P3 Zugriff auf einen Offline-Fahrzeugbus durch Fernkompromittierung einer angeschlossenen ECU | C7 Verschlüsselte Übertragung vertraulicher Daten<br>A3 Qualitätsschäden werden im Falle eines kompromittierten Lkw selektiv berücksichtigt.<br>A5 Domänentrennung  | DS1 [P2]<br>DS5, DS7, DS8, DS11<br>DS1 [P2]                                                              | E               | H               | 1              | DS1 [P2]<br>DS1, DS18, DS5, DS7, DS8, DS11                                                                          |                 | H               | 1              |
| R4: T3 Abhören der VBUS-Verbindung zwischen Mission Control und Perception prep. durch P1 Erlangung physischen Zugriffs auf die Fahrzeugelektronik als Fahrerhalter/Tuner             | C7 Verschlüsselte Übertragung vertraulicher Daten<br>A2 Begrenzter Spielraum für Tuning-Angriffe                                                                    | DS1 [P2], DS2 [F0OEM]<br>DS1, DS5, DS6, DS7, DS8, DS9, DS10, DS11, DS12, DS14, DS15, DS18<br>DS2 [F0OEM] | V               | H               | 2              | DS1 [P2], DS2 [F0OEM]<br>DS1, DS18, DS1, DS5, DS6, DS7, DS8, DS9, DS10, DS11, DS12, DS14, DS15, DS18<br>DS2 [F0OEM] | V               | H               | 2              |

|                                                                                                                                                                                             |                                                                                                                                                                     |                                                                                        |   |   |   |                                                                                            |   |   |   |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------|---|---|---|--------------------------------------------------------------------------------------------|---|---|---|
| R5: T3 Abhören der VBUS-Verbindung zwischen Mission Control und Perception prep. durch P2 Erlangung physischen Zugriffs auf die Fahrzeugelektronik als externer Angreifer                   | C7 Verschlüsselte Übertragung vertraulicher Daten<br>A3 Qualitätsschäden werden im Falle eines kompromittierten Lkw selektiv berücksichtigt.<br>A6 Lokale Angreifer | DS1 [P2], DS2 [F0OEM]<br>DS5, DS7, DS8, DS11, DS6, DS12, DS13<br>DS1 [P2], DS2 [F0OEM] | E | H | 4 | DS1 [P2], DS2 [F0OEM]<br>DS1, DS18, DS5, DS7, DS8, DS11, DS6, DS12, DS13<br>DS2 [F0OEM]    | V | H | 2 |
| R6: T3 Abhören der VBUS-Verbindung zwischen Mission Control und Wahrnehmung Vorbereitung durch P4 Zugriff auf einen Online-Fahrzeugbus durch Fernkompromittierung einer angeschlossenen ECU | C7 Verschlüsselte Übertragung vertraulicher Daten<br>A3 Qualitätsschäden werden im Falle eines kompromittierten Lkw selektiv berücksichtigt                         | DS1 [P2], DS2 [F0OEM]<br>DS5, DS7, DS8, DS11<br>DS1 [P2], DS2 [F0OEM]                  | E | H | 4 | DS1 [P2], DS2 [F0OEM]<br>DS1, DS18, DS5, DS7, DS8, DS11<br>DS2 [F0OEM]                     | V | H | 2 |
| R7: T4 Abhören der VBUS-Verbindung zwischen Mission Control und Planungsvorbereitung durch P1 Erlangung physischen Zugriffs auf die Fahrzeugelektronik als Fahrzeugbesitzer/Tuner           | C7 Verschlüsselte Übertragung vertraulicher Daten<br>A2 Begrenzter Spielraum für Tuning-Angriffe                                                                    | DS18 [F1RU]<br>DS1, DS5, DS6, DS7, DS8, DS9, DS10, DS11, DS12, DS14, DS15, DS18        |   | H | 1 | DS18 [F1RU]<br>DS1, DS18, DS1, DS5, DS6, DS7, DS8, DS9, DS10, DS11, DS12, DS14, DS15, DS18 |   | H | 1 |
| R8: T4 Abhören der VBUS-Verbindung zwischen Mission Control und Planning prep. durch P2 Erlangung physischen Zugriffs auf die Fahrzeugelektronik als externer Angreifer                     | C7 Verschlüsselte Übertragung vertraulicher Daten<br>A3 Qualitätsschäden werden im Falle eines kompromittierten Lkw selektiv berücksichtigt.<br>A6 Lokale Angreifer | DS18 [F1RU]<br>DS5, DS7, DS8, DS11, DS6, DS12, DS13<br>DS18 [F1RU]                     | M | H | 3 | DS18 [F1RU]<br>DS1, DS18, DS5, DS7, DS8, DS11, DS6, DS12, DS13                             |   | H | 1 |

|                                                                                                                                                                                                                 |                                                                                                                                                                         |                                                                                                                     |   |   |   |                                                                                                                                |   |   |   |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------|---|---|---|--------------------------------------------------------------------------------------------------------------------------------|---|---|---|
| R9: T4 Abhören der VBUS-Verbindung zwischen Mission Control und Planungsvorbereitung durch P4 Zugriff auf einen Online-Fahrzeugbus durch Fernkompromittierung einer angeschlossenen ECU                         | C7 Verschlüsselte Übertragung vertraulicher Daten<br><br>A3 Qualitätsschäden werden im Falle eines kompromittierten Lkw selektiv berücksichtigt                         | DS18 [F1RU]<br><br>DS5, DS7, DS8, DS11<br><br>DS18 [F1RU]                                                           | M | H | 3 | DS18 [F1RU]<br><br>DS1, DS18, DS5, DS7, DS8, DS11                                                                              |   | H | 1 |
| R10: T5 Abhören der VBUS-Verbindung zwischen Mission Control und System Management Vorbereitung durch P1 Erlangung physischen Zugriffs auf die Fahrzeugelektronik als Fahrzeughalter/Tuner                      | C7 Verschlüsselte Übertragung vertraulicher Daten<br><br>A2 Begrenzter Spielraum für Tuning-Angriffe                                                                    | DS2 [F0OEM], DS18 [F1RU]<br><br>DS1, DS5, DS6, DS7, DS8, DS9, DS10, DS11, DS12, DS14, DS15, DS18<br><br>DS2 [F0OEM] | V | H | 2 | DS2 [F0OEM], DS18 [F1RU]<br><br>DS1, DS18, DS1, DS5, DS6, DS7, DS8, DS9, DS10, DS11, DS12, DS14, DS15, DS18<br><br>DS2 [F0OEM] | V | H | 2 |
| R11: T5 Abhören der VBUS-Verbindung zwischen Mission Control und System Management prep. von P2 Erlangen von physischem Zugriff auf die Fahrzeugelektronik als externer Angreifer                               | C7 Verschlüsselte Übertragung vertraulicher Daten<br><br>A3 Qualitätsschäden werden im Falle eines kompromittierten Lkw selektiv berücksichtigt.<br>A6 Lokale Angreifer | DS2 [F0OEM], DS18 [F1RU]<br><br>DS5, DS7, DS8, DS11, DS6, DS12, DS13<br><br>DS2 [F0OEM], DS18 [F1RU]                | M | H | 3 | DS2 [F0OEM], DS18 [F1RU]<br><br>DS1, DS18, DS5, DS7, DS8, DS11, DS6, DS12, DS13<br><br>DS2 [F0OEM]                             | V | H | 2 |
| R12: T5 Abhören der VBUS-Verbindung zwischen Mission Control und System Management, vorbereitet durch P4 Erlangen von Zugriff auf einen Online-Fahrzeugbus durch Fernkompromittierung einer angeschlossenen ECU | C7 Verschlüsselte Übertragung vertraulicher Daten<br><br>A3 Qualitätsschäden werden im Falle eines kompromittierten Lkw selektiv berücksichtigt                         | DS2 [F0OEM], DS18 [F1RU]<br><br>DS5, DS7, DS8, DS11                                                                 | M | H | 3 | DS2 [F0OEM], DS18 [F1RU]<br><br>DS1, DS18, DS5, DS7, DS8, DS11                                                                 | V | H | 2 |

|                                                                                                                                                                                                                                        |                                                                                                                                                  | DS2 [F0OEM], DS18 [F1RU]                                                              |   |   |   | DS2 [F0OEM]                                                                                   |  |   |   |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---|---|---|-----------------------------------------------------------------------------------------------|--|---|---|
| R13: T6 Störung der Rohvideodatenübertragung auf der VBUS-Verbindung zwischen Sensoren und Wahrnehmung Vorbereitung durch P2 Erlangung physischen Zugriffs auf die Fahrzeugelektronik als externer Angreifer                           | C1 Erkennung von Systemfehlern<br>A3 Qualitätsschäden werden im Falle eines kompromittierten Lkw selektiv berücksichtigt.<br>A6 Lokale Angreifer | DS5 [O2], DS6 [S3 F2OEM], DS7 [O2], DS8 [O1]<br>DS5, DS7, DS8, DS11, DS6, DS12, DS13  |   | H | 1 | DS5 [O2], DS6 [S3 F2OEM], DS7 [O2], DS8 [O1]<br>DS6>DS7, DS5, DS7, DS8, DS11, DS6, DS12, DS13 |  | H | 1 |
| R14: T6 Störung der Rohvideodatenübertragung auf der VBUS-Verbindung zwischen Sensoren und Wahrnehmung Vorbereitung durch P3 Erlangung des Zugriffs auf einen Offline-Fahrzeugbus durch Fernkompromittierung einer angeschlossenen ECU | C1 Erkennung von Systemausfällen<br>A3 Qualitätsmängel werden im Falle eines kompromittierten Lkw selektiv berücksichtigt.<br>A5 Domänentrennung | DS5 [O2], DS6 [S3 F2OEM], DS7 [O2], DS8 [O1]<br>DS5, DS7, DS8, DS11<br>DS6 [S3 F2OEM] | S | H | 1 | DS5 [O2], DS6 [S3 F2OEM], DS7 [O2], DS8 [O1]<br>DS6>DS7, DS5, DS7, DS8, DS11                  |  | H | 1 |
| R15: T7 Störung der Sensordaten auf der VBUS-Verbindung zwischen Sensoren und Wahrnehmung Vorbereitung durch P2 Erlangung physischen Zugriffs auf die Fahrzeugelektronik als externer Angreifer                                        | C1 Erkennung von Systemfehlern<br>A3 Qualitätsschäden werden im Falle eines kompromittierten Lkw selektiv berücksichtigt.<br>A6 Lokale Angreifer | DS5 [O2], DS6 [S3 F2OEM], DS7 [O2], DS8 [O1]<br>DS5, DS7, DS8, DS11, DS6, DS12, DS13  |   | H | 1 | DS5 [O2], DS6 [S3 F2OEM], DS7 [O2], DS8 [O1]<br>DS6>DS7, DS5, DS7, DS8, DS11, DS6, DS12, DS13 |  | H | 1 |
| R16: T7 Störung der Sensordaten auf der VBUS-Verbindung zwischen Sensoren und Wahrnehmung Vorbereitung durch P3 Erlangung des Zugriffs auf einen Offline-                                                                              | C1 Erkennung von Systemausfällen                                                                                                                 | DS5 [O2], DS6 [S3 F2OEM], DS7 [O2], DS8 [O1]                                          | S | H | 1 | DS5 [O2], DS6 [S3 F2OEM], DS7 [O2], DS8 [O1]                                                  |  | H | 1 |

|                                                                                                                                                                                                                                                     |                                                                                                                                                                                               |                                                                                       |   |   |   |                                                                                               |  |   |   |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---|---|---|-----------------------------------------------------------------------------------------------|--|---|---|
| Fahrzeugbus durch Fernkompromittierung einer verbundenen ECU                                                                                                                                                                                        | A3 Qualitätsmängel werden im Falle eines kompromittierten Lkw selektiv berücksichtigt.<br>A5 Domänentrennung                                                                                  | DS5, DS7, DS8, DS11<br>DS6 [S3 F2OEM]                                                 |   |   |   | DS6>DS7, DS5, DS7, DS8, DS11                                                                  |  |   |   |
| R17: T8 Störung der Basisfahrzeug-Eingabe auf der VBUS-Verbindung zwischen Basisfahrzeugüberwachung und Wahrnehmung Vorbereitung durch P2 Erlangung physischen Zugriffs auf die Fahrzeugelektronik als externer Angreifer                           | C1 Erkennung von Systemfehlern<br>A3 Qualitätsschäden werden im Falle eines kompromittierten Lkw selektiv berücksichtigt.<br>A6 Lokale Angreifer                                              | DS5 [O2], DS6 [S3 F2OEM], DS7 [O2], DS8 [O1]<br>DS5, DS7, DS8, DS11, DS6, DS12, DS13  |   | H | 1 | DS5 [O2], DS6 [S3 F2OEM], DS7 [O2], DS8 [O1]<br>DS6>DS7, DS5, DS7, DS8, DS11, DS6, DS12, DS13 |  | H | 1 |
| R18: T8 Störung der Basis-Fahrzeugeingabe auf der VBUS-Verbindung zwischen Basis-Fahrzeugüberwachung und Wahrnehmungsvorbereitung durch P4 Erlangung des Zugriffs auf einen Online-Fahrzeugbus durch Fernkompromittierung einer angeschlossenen ECU | C1 Erkennung von Systemfehlern<br>A3 Bei einem beschädigten Lkw werden Qualitätsschäden selektiv berücksichtigt.                                                                              | DS5 [O2], DS6 [S3 F2OEM], DS7 [O2], DS8 [O1]<br>DS5, DS7, DS8, DS11<br>DS6 [S3 F2OEM] | S | H | 5 | DS5 [O2], DS6 [S3 F2OEM], DS7 [O2], DS8 [O1]<br>DS6>DS7, DS5, DS7, DS8, DS11                  |  | H | 1 |
| R19: T9 Störung der fusionierten Sensordaten auf der IPC-Verbindung zwischen Wahrnehmung und Prädiktion, vorbereitet durch P2 Erlangung physischen Zugriffs auf die Fahrzeugelektronik als externer Angreifer                                       | C4 Redundanz für sicherheitskritische Kommunikation der ADS-Kernkomponenten<br>A3 Qualitätsschäden werden im Falle eines kompromittierten Lkw selektiv berücksichtigt.<br>A6 Lokale Angreifer | DS5 [O2], DS6 [S3 F2OEM], DS7 [O2]<br>DS5, DS7, DS8, DS11, DS6, DS12, DS13            |   | H | 1 | DS5 [O2], DS6 [S3 F2OEM], DS7 [O2]<br>DS6>DS7, DS5, DS7, DS8, DS11, DS6, DS12, DS13           |  | H | 1 |

|                                                                                                                                                                                                                                                                                                                                                    |                                                                                                                                                                                              |                                                                             |   |   |   |                                                                                |   |   |   |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------|---|---|---|--------------------------------------------------------------------------------|---|---|---|
| R20: T9 Störung der fusionierten Sensordaten auf der IPC-Verbindung zwischen Wahrnehmung und Prädiktion Vorbereitung durch P3 Zugriff auf einen Offline-Fahrzeugbus durch Fernkompromittierung einer verbundenen ECU                                                                                                                               | C4 Redundanz für sicherheitskritische Kommunikation von ADS-Kernkomponenten<br>A3 Qualitätsschäden werden im Falle eines kompromittierten Lkw selektiv berücksichtigt.<br>A5 Domänentrennung | DS5 [O2], DS6 [S3 F2OEM], DS7 [O2]<br>DS5, DS7, DS8, DS11<br>DS6 [S3 F2OEM] | S | H | 1 | DS5 [O2], DS6 [S3 F2OEM], DS7 [O2]<br>DS6>DS7, DS5, DS7, DS8, DS11             | H | 1 |   |
| R21: T9 Störung der fusi-onierten Sensordaten auf der IPC-Verbindung zwi-schen Wahrnehmung und Prädiktion Vorbereitung durch P5 Angriff auf mehr als eine Verbindung, um die Sensorfusion (C3) oder Redundanzen (C4, C5) zu überwinden<br>P2 Erlangung physischen Zugriffs auf die Fahrzeu-gelektronik als externer Angreifer                      | A3 Qualitätsschäden werden im Falle eines kompromittierten Lkw selektiv berücksichtigt,<br>A6 Lokale Angreifer                                                                               | DS5 [O2], DS6 [S3 F2OEM], DS7 [O2]<br>DS5, DS7, DS8, DS11, DS6, DS12, DS13  |   | M | 1 | DS5 [O2], DS6 [S3 F2OEM], DS7 [O2]<br>DS5, DS7, DS8, DS11, DS6, DS12, DS13     | M | 1 |   |
| R22: T9 Störung der fusi-onierten Sensordaten auf der IPC-Verbindung zwi-schen Wahrnehmung und Prädiktion Vorbereitung durch P5 Angriff auf mehr als eine Verbindung, um die Sensorfusion (C3) oder Redundanzen (C4, C5) zu überwinden,<br>P3 Erlangen von Zugriff auf einen Offline-Fahrzeugbus durch Fern-kompromittierung einer verbundenen ECU | A3 Qualitätsmängel werden im Falle eines kompromittierten Lkw selektiv berücksichtigt.<br>A5 Domänentrennung                                                                                 | DS5 [O2], DS6 [S3 F2OEM], DS7 [O2]<br>DS5, DS7, DS8, DS11<br>DS6 [S3 F2OEM] | S | M | 1 | DS5 [O2], DS6 [S3 F2OEM], DS7 [O2]<br>DS5, DS7, DS8, DS11<br>DS6 [S3 F2OEM]    | S | M | 1 |
| R23: T10 Störung der Objektbahnen auf der IPC-Verbindung zwischen Prädiktion und Planung Vorbereitung durch P2 Erlangung physischen Zugriffs auf die Fahrzeugelektronik als externer Angreifer                                                                                                                                                     | C4 Redundanz für sicherheitskritische Kommunikation der ADS-Kernkomponenten<br>A3 Qualitätsschäden werden                                                                                    | DS5 [O2], DS6 [S3 F2OEM], DS7 [O2]<br>DS5, DS7, DS8, DS11,                  |   | H | 1 | DS5 [O2], DS6 [S3 F2OEM], DS7 [O2]<br>DS6>DS7, DS5, DS7, DS8, DS11, DS6, DS12, | H | 1 |   |



|                                                                                                                                                                                                                                                                                                                                    |                                                                                                                                                                                                       |                                                                                               |   |   |   |                                                                                               |   |   |   |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------|---|---|---|-----------------------------------------------------------------------------------------------|---|---|---|
|                                                                                                                                                                                                                                                                                                                                    | im Falle eines kompromittierten Lkw selektiv berücksichtigt.<br>A6 Lokale Angreifer                                                                                                                   | DS6, DS12, DS13<br>_____                                                                      |   |   |   | DS13<br>_____                                                                                 |   |   |   |
| R24: T10 Störung der Objektbahnen auf der IPC-Verbindung zwischen Prädiktion und Planung Vorbereitung durch P3 Erlangung des Zugriffs auf einen Offline-Fahrzeugbus durch Fernkompromittierung einer verbundenen ECU                                                                                                               | C4 Redundanz für sicherheitskritische Kommunikation von ADS-Kernkomponenten<br>_____<br>A3 Qualitätsschäden werden im Falle eines kompromittierten Lkw selektiv berücksichtigt.<br>A5 Domänentrennung | DS5 [O2], DS6 [S3 F2OEM], DS7 [O2]<br>_____<br>DS5, DS7, DS8, DS11<br>_____<br>DS6 [S3 F2OEM] | S | H | 1 | DS5 [O2], DS6 [S3 F2OEM], DS7 [O2]<br>_____<br>DS6>DS7, DS5, DS7, DS8, DS11<br>_____          |   | H | 1 |
| R25: T10 Störung der Objektbahnen auf der IPC-Verbindung zwischen Prädiktion und Planung, vorbereitet durch P5 Angriff auf mehr als eine Verbindung, um die Sensorfusion (C3) oder Redundanzen (C4, C5) zu überwinden,<br>P2 Erlangung physischen Zugriffs auf die Fahrzeugelektronik als externer Angreifer                       | A3 Qualitätsschäden werden im Falle eines kompromittierten Lkw selektiv berücksichtigt,<br>A6 Lokale Angreifer                                                                                        | DS5 [O2], DS6 [S3 F2OEM], DS7 [O2]<br>_____<br>DS5, DS7, DS8, DS11, DS6, DS12, DS13<br>_____  |   | M | 1 | DS5 [O2], DS6 [S3 F2OEM], DS7 [O2]<br>_____<br>DS5, DS7, DS8, DS11, DS6, DS12, DS13<br>_____  |   | M | 1 |
| R26: T10 Störung der Objektbahnen auf der IPC-Verbindung zwischen Prädiktion und Planung Vorbereitung durch P5 Angriff auf mehr als eine Verbindung, um die Sensorfusion (C3) oder Redundanzen (C4, C5) zu überwinden,<br>P3 Erlangung des Zugriffs auf einen Offline-Fahrzeugbus durch Fernkompromittierung einer verbundenen ECU | A3 Qualitätsmängel werden im Falle eines kompromittierten Lkw selektiv berücksichtigt.<br>A5 Domänentrennung                                                                                          | DS5 [O2], DS6 [S3 F2OEM], DS7 [O2]<br>_____<br>DS5, DS7, DS8, DS11<br>_____<br>DS6 [S3 F2OEM] | S | M | 1 | DS5 [O2], DS6 [S3 F2OEM], DS7 [O2]<br>_____<br>DS5, DS7, DS8, DS11<br>_____<br>DS6 [S3 F2OEM] | S | M | 1 |
| R27: T11 Störung der fusionierten Sensordaten auf der IPC-Verbindung zwischen Wahrnehmung und Planung                                                                                                                                                                                                                              | C4 Redundanz für sicherheitskritische Kommunikation                                                                                                                                                   | DS5 [O2], DS6 [S3 F2OEM], DS7 [O2]                                                            |   | H | 1 | DS5 [O2], DS6 [S3 F2OEM], DS7 [O2]                                                            |   | H | 1 |

|                                                                                                                                                                                                                                                                                                                                                  |                                                                                                                                                                                                |                                                                               |   |   |   |                                                                               |   |   |   |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------|---|---|---|-------------------------------------------------------------------------------|---|---|---|
| Vorbereitung durch P2 Erlangung physischen Zugriffs auf die Fahrzeugelektronik als externer Angreifer                                                                                                                                                                                                                                            | der ADS-Kernkomponenten<br>A3 Qualitätsschäden werden im Falle eines kompromittierten Lkw selektiv berücksichtigt.<br>A6 Lokale Angreifer                                                      | DS5, DS7, DS8, DS11,<br>DS6, DS12, DS13                                       |   |   |   | DS6>DS7, DS5, DS7,<br>DS8, DS11, DS6, DS12,<br>DS13                           |   |   |   |
| R28: T11 Störung der fusionierten Sensordaten auf der IPC-Verbindung zwischen Wahrnehmung und Planung<br>Vorbereitung durch P3 Erlangung des Zugriffs auf einen Offline-Fahrzeugbus durch Fernkompromittierung einer verbundenen ECU                                                                                                             | C4 Redundanz für sicherheitskritische Kommunikation von ADS-Kernkomponenten<br>A3 Qualitätsschäden werden im Falle eines kompromittierten Lkw selektiv berücksichtigt.<br>A5 Domänenentrennung | DS5 [O2], DS6 [S3 F2OEM], DS7 [O2]<br>DS5, DS7, DS8, DS11<br>DS6 [S3 F2OEM]   | S | H | 1 | DS5 [O2], DS6 [S3 F2OEM], DS7 [O2]<br>DS6>DS7, DS5, DS7,<br>DS8, DS11         |   | H | 1 |
| R29: T11 Störung der fusionierten Sensordaten auf der IPC-Verbindung zwischen Wahrnehmung und Planung, vorbereitet durch P5 Angriff auf mehr als eine Verbindung, um die Sensorfusion (C3) oder Redundanzen (C4, C5) zu überwinden,<br>P2 Erlangung physischen Zugriffs auf die Fahrzeugelektronik als externer Angreifer                        | A3 Qualitätsschäden werden im Falle eines kompromittierten Lkw selektiv berücksichtigt,<br>A6 Lokale Angreifer                                                                                 | DS5 [O2], DS6 [S3 F2OEM], DS7 [O2]<br>DS5, DS7, DS8, DS11,<br>DS6, DS12, DS13 |   | M | 1 | DS5 [O2], DS6 [S3 F2OEM], DS7 [O2]<br>DS5, DS7, DS8, DS11,<br>DS6, DS12, DS13 |   | M | 1 |
| R30: T11 Störung der fusionierten Sensordaten auf der IPC-Verbindung zwischen Wahrnehmung und Planung<br>Vorbereitung durch P5 Angriff auf mehr als eine Verbindung, um die Sensorfusion (C3) oder Redundanzen (C4, C5) zu überwinden,<br>P3 Erlangen von Zugriff auf einen Offline-Fahrzeugbus durch Fernkompromittierung einer verbundenen ECU | A3 Qualitätsmängel werden im Falle eines kompromittierten Lkw selektiv berücksichtigt.<br>A5 Domänenentrennung                                                                                 | DS5 [O2], DS6 [S3 F2OEM], DS7 [O2]<br>DS5, DS7, DS8, DS11<br>DS6 [S3 F2OEM]   | S | M | 1 | DS5 [O2], DS6 [S3 F2OEM], DS7 [O2]<br>DS5, DS7, DS8, DS11<br>DS6 [S3 F2OEM]   | S | M | 1 |

|                                                                                                                                                                                                                                                                                                                                                       |                                                                                                                                                                                                   |                                                                                     |   |   |   |                                                                                         |   |   |   |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|---|---|---|-----------------------------------------------------------------------------------------|---|---|---|
| R31: T12 Störung der geplanten Trajektorie auf der IPC-Verbindung zwischen Planung und Steuerung oder zwischen Planung und Prädiktion Vorbereitung durch P2 Erlangung physischen Zugriffs auf die Fahrzeugelektronik als externer Angreifer                                                                                                           | C4 Redundanz für sicherheitskritische Kommunikation der ADS-Kernkomponenten<br><br>A3 Qualitätsschäden werden im Falle eines kompromittierten Lkw selektiv berücksichtigt.<br>A6 Lokale Angreifer | DS5 [O2], DS6 [S3 F2OEM], DS7 [O2]<br><br>DS5, DS7, DS8, DS11, DS6, DS12, DS13      |   | H | 1 | DS5 [O2], DS6 [S3 F2OEM], DS7 [O2]<br><br>DS6>DS7, DS5, DS7, DS8, DS11, DS6, DS12, DS13 |   | H | 1 |
| R32: T12 Störung der geplanten Trajektorie auf der IPC-Verbindung zwischen Planung und Steuerung oder zwischen Planung und Prädiktion Vorbereitung durch P3 Erlangung des Zugriffs auf einen Offline-Fahrzeugbus durch Fernkompromittierung einer verbundenen ECU                                                                                     | C4 Redundanz für sicherheitskritische Kommunikation von ADS-Kernkomponenten<br><br>A3 Qualitätsschäden werden im Falle eines kompromittierten Lkw selektiv berücksichtigt.<br>A5 Domänentrennung  | DS5 [O2], DS6 [S3 F2OEM], DS7 [O2]<br><br>DS5, DS7, DS8, DS11<br><br>DS6 [S3 F2OEM] | S | H | 1 | DS5 [O2], DS6 [S3 F2OEM], DS7 [O2]<br><br>DS6>DS7, DS5, DS7, DS8, DS11                  |   | H | 1 |
| R33: T12 Störung der geplanten Trajektorie auf der IPC-Verbindung zwischen Planung und Steuerung oder zwischen Planung und Prädiktionvorbereitung durch P5 Angriff auf mehr als eine Verbindung, um die Sensorfusion (C3) oder Redundanzen (C4, C5) zu überwinden, P2 Erlangung physischen Zugriffs auf die Fahrzeugelektronik als externer Angreifer | A3 Qualitätsschäden werden im Falle eines kompromittierten Lkw selektiv berücksichtigt,<br>A6 Lokale Angreifer                                                                                    | DS5 [O2], DS6 [S3 F2OEM], DS7 [O2]<br><br>DS5, DS7, DS8, DS11, DS6, DS12, DS13      |   | M | 1 | DS5 [O2], DS6 [S3 F2OEM], DS7 [O2]<br><br>DS5, DS7, DS8, DS11, DS6, DS12, DS13          |   | M | 1 |
| R34: T12 Störung der geplanten Trajektorie auf der IPC-Verbindung zwischen Planung und Steuerung oder zwischen Planung und Prädiktion, vorbereitet durch P5 Angriff auf mehr als eine Verbindung, um die Sensorfusion (C3) oder Redundanzen (C4, C5) zu überwinden. P3 Erlangung des Zugriffs auf einen Offline-                                      | A3 Qualitätsmängel werden im Falle eines kompromittierten Lkw selektiv berücksichtigt.<br>A5 Domänentrennung                                                                                      | DS5 [O2], DS6 [S3 F2OEM], DS7 [O2]<br><br>DS5, DS7, DS8, DS11<br><br>DS6 [S3 F2OEM] | S | M | 1 | DS5 [O2], DS6 [S3 F2OEM], DS7 [O2]<br><br>DS5, DS7, DS8, DS11<br><br>DS6 [S3 F2OEM]     | S | M | 1 |

|                                                                                                                                                                                                                                                                                                                   |                                                                                                                                                                                                   |                                                                                     |   |   |   |                                                                                         |   |   |   |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|---|---|---|-----------------------------------------------------------------------------------------|---|---|---|
| Fahrzeugbus durch Fernkompromittierung einer verbundenen ECU                                                                                                                                                                                                                                                      |                                                                                                                                                                                                   |                                                                                     |   |   |   |                                                                                         |   |   |   |
| R35: T13 Störung der Basisfahrzeugleistung auf der VBUS-Verbindung zwischen Steuerung und Aktoren<br>Vorbereitung durch P2 Erlangung physischen Zugriffs auf die Fahrzeugelektronik als externer Angreifer                                                                                                        | C4 Redundanz für sicherheitskritische Kommunikation der ADS-Kernkomponenten<br><br>A3 Qualitätsschäden werden im Falle eines kompromittierten Lkw selektiv berücksichtigt.<br>A6 Lokale Angreifer | DS5 [O2], DS6 [S3 F2OEM], DS7 [O2]<br><br>DS5, DS7, DS8, DS11, DS6, DS12, DS13      |   | H | 1 | DS5 [O2], DS6 [S3 F2OEM], DS7 [O2]<br><br>DS6>DS7, DS5, DS7, DS8, DS11, DS6, DS12, DS13 |   | H | 1 |
| R36: T13 Störung der Basisausgabe des Fahrzeugs über die VBUS-Verbindung zwischen Steuerung und Aktoren, vorbereitet durch P3 Erlangung des Zugriffs auf einen Offline-Fahrzeugbus durch Fernkompromittierung einer angeschlossenen ECU                                                                           | C4 Redundanz für sicherheitskritische Kommunikation von ADS-Kernkomponenten<br><br>A3 Qualitätsschäden werden im Falle eines kompromittierten Lkw selektiv berücksichtigt.<br>A5 Domänentrennung  | DS5 [O2], DS6 [S3 F2OEM], DS7 [O2]<br><br>DS5, DS7, DS8, DS11<br><br>DS6 [S3 F2OEM] | S | H | 1 | DS5 [O2], DS6 [S3 F2OEM], DS7 [O2]<br><br>DS6>DS7, DS5, DS7, DS8, DS11                  |   | H | 1 |
| R37: T13 Störung der Basisfahrzeugleistung auf der VBUS-Verbindung zwischen Steuerung und Aktoren, vorbereitet durch P5 Angriff auf mehr als eine Verbindung, um Sensorfusion (C3) oder Redundanzen (C4, C5) zu überwinden,<br>P2 Erlangung physischen Zugriffs auf die Fahrzeugelektronik als externer Angreifer | A3 Qualitätsschäden werden im Falle eines kompromittierten Lkw selektiv berücksichtigt,<br>A6 Lokale Angreifer                                                                                    | DS5 [O2], DS6 [S3 F2OEM], DS7 [O2]<br><br>DS5, DS7, DS8, DS11, DS6, DS12, DS13      |   | M | 1 | DS5 [O2], DS6 [S3 F2OEM], DS7 [O2]<br><br>DS5, DS7, DS8, DS11, DS6, DS12, DS13          |   | M | 1 |
| R38: T13 Störung der Basisausgabe des Fahrzeugs an der VBUS-Verbindung zwischen Steuerung und Aktoren, vorbereitet durch P5 Angriff auf mehr als eine                                                                                                                                                             | A3 Qualitätsmängel werden im Falle eines kompromittierten                                                                                                                                         | DS5 [O2], DS6 [S3 F2OEM], DS7 [O2]                                                  | S | M | 1 | DS5 [O2], DS6 [S3 F2OEM], DS7 [O2]                                                      | S | M | 1 |

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                                                                                                                |                                                           |  |   |   |                                                           |  |   |   |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------|--|---|---|-----------------------------------------------------------|--|---|---|
| Verbindung, um die Sensorfusion (C3) oder Redundanzen (C4, C5) zu überwinden,<br>P3 Erlangung des Zugriffs auf einen Offline-Fahrzeugbus durch Fernkompromittierung einer angeschlossenen ECU                                                                                                                                                                                                                                                                         | Lkw selektiv berücksichtigt.<br>A5 Domänentrennung                                                             | DS5, DS7, DS8, DS11<br>_____<br>DS6 [S3 F2OEM]            |  |   |   | DS5, DS7, DS8, DS11<br>_____<br>DS6 [S3 F2OEM]            |  |   |   |
| R39: T14 Störung der Basisfahrzeug-Eingabe auf der VBUS-Verbindung zwischen Basisfahrzeugüberwachung und Onboard-HMI Vorbereitung durch P2 Erlangung physischen Zugriffs auf die Fahrzeugelektronik als externer Angreifer<br><br>Hinweis: Es wurden keine Sicherheitsziele oder Schadensszenarien zugewiesen, da der durch diese Bedrohung gefährdete Datenfluss für den vollständig autonomen Lkw im Betrieb ohne Testfahrer nicht existiert.                       | A3 Qualitätsschäden werden im Falle eines kompromittierten Lkw selektiv berücksichtigt,<br>A6 Lokale Angreifer | _____<br>DS5, DS7, DS8, DS11,<br>DS6, DS12, DS13<br>_____ |  | H | 1 | _____<br>DS5, DS7, DS8, DS11,<br>DS6, DS12, DS13<br>_____ |  | H | 1 |
| R40: T14 Störung der Basis-Fahrzeugeingabe auf der VBUS-Verbindung zwischen Basis-Fahrzeugüberwachung und Onboard-HMI-Vorbereitung durch P4 Erlangung des Zugriffs auf einen Online-Fahrzeugbus durch Fernkompromittierung einer verbundenen ECU<br><br>Hinweis: Es wurden keine Sicherheitsziele oder Schadensszenarien zugewiesen, da der durch diese Bedrohung gefährdete Datenfluss für den vollständig autonomen Lkw im Betrieb ohne Testfahrer nicht existiert. | A3 Bei einem kompromittierten Lkw werden Qualitätsschäden selektiv berücksichtigt.                             | _____<br>DS5, DS7, DS8, DS11<br>_____                     |  | H | 1 | _____<br>DS5, DS7, DS8, DS11<br>_____                     |  | H | 1 |
| R41: T15 Störung der geplanten Fahrbahn auf der VBUS-Verbindung zwischen Planung und Onboard-                                                                                                                                                                                                                                                                                                                                                                         | A3 Qualitätsschäden werden im Falle eines                                                                      | _____<br>DS5, DS7, DS8, DS11,                             |  | H | 1 | _____<br>DS5, DS7, DS8, DS11,                             |  | H | 1 |

|                                                                                                                                                                                                                                |                                                                                    |                                |  |   |   |                                |  |   |   |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------|--------------------------------|--|---|---|--------------------------------|--|---|---|
| HMI-Vorbereitung durch P2 Erlangung physischen Zugriffs auf die Fahrzeugelektronik als externer Angreifer                                                                                                                      | kompromittierten Lkw selektiv berücksichtigt,<br>A6 Lokale Angreifer               | DS6, DS12, DS13<br>_____       |  |   |   | DS6, DS12, DS13<br>_____       |  |   |   |
| Hinweis: Es wurden keine Sicherheitsziele oder Schadensszenarien zugewiesen, da der durch diese Bedrohung gefährdete Datenfluss für den vollständig autonomen Lkw im Betrieb ohne Testfahrer nicht existiert.                  |                                                                                    |                                |  |   |   |                                |  |   |   |
| R42: T15 Störung der geplanten Trajektorie auf der VBUS-Verbindung zwischen Planung und Onboard-HMI-Vorbereitung durch P4 Erlangung des Zugriffs auf einen Online-Fahrzeugbus durch Fernkompromittierung einer verbundenen ECU | A3 Bei einem kompromittierten Lkw werden Qualitätsschäden selektiv berücksichtigt. | DS5, DS7, DS8, DS11<br>_____   |  | H | 1 | DS5, DS7, DS8, DS11<br>_____   |  | H | 1 |
| Hinweis: Es wurden keine Sicherheitsziele oder Schadensszenarien zugewiesen, da der durch diese Bedrohung gefährdete Datenfluss für den vollständig autonomen Lkw im Betrieb ohne Testfahrer nicht existiert.                  |                                                                                    |                                |  |   |   |                                |  |   |   |
| R43: T16 Störung Initiieren von MRM auf der MCOM-Verbindung zwischen Control Center und Mission Control                                                                                                                        | A10 Durch CC ausgelöste MRM sind nicht sicherheitskritisch.                        | DS6 [S3 F2OEM]<br>DS6<br>_____ |  | G | 1 | DS6 [S3 F2OEM]<br>DS6<br>_____ |  | G | 1 |
| Hinweis: Schwieriges Zeitfenster, da der Angriff genau in dem Moment ausgeführt werden muss, in dem das Control Center das Signal „MRM initiieren“ sendet und sich der Lkw in einem Zustand befindet, der ein MRM erfordert.   |                                                                                    |                                |  |   |   |                                |  |   |   |
| R44: T17 Unterbrechung Initiieren von MRM auf der VBUS-Verbindung zwischen Mission Control und                                                                                                                                 | C4 Redundanz für sicherheitskritische Kommunikation                                | DS6 [S3 F2OEM]<br>_____        |  | H | 1 | DS6 [S3 F2OEM]<br>_____        |  | H | 1 |

|                                                                                                                                                                                                                                                                                                                            |                                                                                                                                                                                                                                  |                                                                |  |   |   |                                                                |  |   |   |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------|--|---|---|----------------------------------------------------------------|--|---|---|
| System Management Vorbereitung durch P2 Erlangen von physischem Zugriff auf die Fahrzeugelektronik als externer Angreifer                                                                                                                                                                                                  | von ADS-Kernkomponenten<br>A10 Durch CC ausgelöste MRM sind nicht sicherheitskritisch.<br>A3 Qualitätsschäden werden im Falle eines kompromittierten Lkw selektiv berücksichtigt.<br>A6 Lokale Angreifer                         | DS6, DS5, DS7, DS8,<br>DS11, DS6, DS12, DS13                   |  |   |   | DS6>DS7, DS6, DS5,<br>DS7, DS8, DS11, DS6,<br>DS12, DS13       |  |   |   |
| R45: T17 Störung Initiieren von MRM auf der VBUS-Verbindung zwischen Mission Control und System Management Vorbereitung durch P4 Erlangen von Zugriff auf einen Online-Fahrzeugbus durch Fernkompromittierung einer verbundenen ECU                                                                                        | C4 Redundanz für sicherheitskritische Kommunikation von ADS-Kernkomponenten<br>A10 Durch CC ausgelöste MRM sind nicht sicherheitskritisch.<br>A3 Qualitätsschäden werden im Falle eines beschädigten Lkw selektiv berücksichtigt | DS6 [S3 F2OEM]<br>DS6, DS5, DS7, DS8,<br>DS11                  |  | H | 1 | DS6 [S3 F2OEM]<br>DS6>DS7, DS6, DS5,<br>DS7, DS8, DS11         |  | H | 1 |
| R46: T17 Störung Initiierung von MRM auf der VBUS-Verbindung zwischen Mission Control und System Management Vorbereitung durch P5 Angriff auf mehr als eine Verbindung, um Sensorfusion (C3) oder Redundanzen (C4, C5) zu überwinden<br>P2 Erlangung physischen Zugriffs auf die Fahrzeugelektronik als externer Angreifer | A10 Durch CC ausgelöste MRM sind nicht sicherheitskritisch.<br>A3 Qualitätsschäden werden im Falle eines kompromittierten Lkw selektiv berücksichtigt.<br>A6 Lokale Angreifer                                                    | DS6 [S3 F2OEM]<br>DS6, DS5, DS7, DS8,<br>DS11, DS6, DS12, DS13 |  | M | 1 | DS6 [S3 F2OEM]<br>DS6, DS5, DS7, DS8,<br>DS11, DS6, DS12, DS13 |  | M | 1 |
| R47: T17 Störung Initiieren von MRM auf der VBUS-Verbindung zwischen Mission Control und System Management Vorbereitung durch P5 Angriff auf mehr als eine Verbindung, um Sensorfusion (C3) oder Redundanzen (C4, C5) zu überwinden,                                                                                       | A10 Durch CC ausgelöste MRM sind nicht sicherheitskritisch.<br>A3 Qualitätsschäden werden im Falle eines                                                                                                                         | DS6 [S3 F2OEM]<br>DS6, DS5, DS7, DS8,<br>DS11, DS6, DS12, DS13 |  | M | 1 | DS6 [S3 F2OEM]<br>DS6, DS5, DS7, DS8,<br>DS11, DS6, DS12, DS13 |  | M | 1 |



|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |                                                                                                                                                       |                                                                 |  |   |   |                                                                 |  |   |   |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------|--|---|---|-----------------------------------------------------------------|--|---|---|
| T51 Spoofing oder Manipulation Initiieren von MRM als MitM auf der VBUS-Verbindung zwischen Mission Control und System Management,<br>P2 Erlangung physischen Zugriffs auf die Fahrzeugelektronik als externer Angreifer                                                                                                                                                                                                                                                                                                                                                                                                                                                                | kompromittierten Lkw selektiv berücksichtigt.<br>A6 Lokale Angreifer                                                                                  |                                                                 |  |   |   |                                                                 |  |   |   |
| R48: T17 Störung Initiierung von MRM auf der VBUS-Verbindung zwischen Mission Control und System Management Vorbereitung durch P5 Angriff auf mehr als eine Verbindung, um Sensorfusion (C3) oder Redundanzen (C4, C5) zu überwinden,<br>P4 Erlangung des Zugriffs auf einen Online-Fahrzeugbus durch Fernkompromittierung einer angeschlossenen ECU                                                                                                                                                                                                                                                                                                                                    | A10 Durch CC ausgelöste MRM sind nicht sicherheitskritisch.<br>A3 Qualitätsschäden werden im Falle eines kompromittierten Lkw selektiv berücksichtigt | DS6 [S3 F2OEM]<br>_____<br>DS6, DS5, DS7, DS8,<br>DS11<br>_____ |  | M | 1 | DS6 [S3 F2OEM]<br>_____<br>DS6, DS5, DS7, DS8,<br>DS11<br>_____ |  | M | 1 |
| R49: T17 Störung der MRM-Initiierung auf der VBUS-Verbindung zwischen Mission Control und System Management, vorbereitet durch P5 Angriff auf mehr als eine Verbindung, um Sensorfusion (C3) oder Redundanzen (C4, C5) zu überwinden,<br>T51 Spoofing oder Manipulation Initiieren von MRM als MitM auf der VBUS-Verbindung zwischen Mission Control und System Management,<br>P4 Zugriff auf einen Online-Fahrzeugbus durch Fernkompromittierung einer angeschlossenen ECU<br><br>Hinweis: T51 wurde als zusätzliche Angriffsvorbereitung hinzugefügt, um zu veranschaulichen, dass ein Angreifer die Sequenznummer nicht manipulieren kann, um die Erkennung fehlender Nachrichten zu | A10 Durch CC ausgelöste MRM sind nicht sicherheitskritisch.<br>A3 Qualitätsschäden werden im Falle eines kompromittierten Lkw selektiv berücksichtigt | DS6 [S3 F2OEM]<br>_____<br>DS6, DS5, DS7, DS8,<br>DS11<br>_____ |  | M | 1 | DS6 [S3 F2OEM]<br>_____<br>DS6, DS5, DS7, DS8,<br>DS11<br>_____ |  | M | 1 |

|                                                                                                                                                                                                                                                                                                                  |                                                                                                                                                                                                   |                                                                 |   |   |   |                                                                     |   |   |   |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------|---|---|---|---------------------------------------------------------------------|---|---|---|
| verhindern, wenn die initiiierende MRM authentisch übertragen wird.                                                                                                                                                                                                                                              |                                                                                                                                                                                                   |                                                                 |   |   |   |                                                                     |   |   |   |
| R50: T18 Störung des Initiate MRM auf der VBUS-Verbindung zwischen System Management und Planung Vorbereitung durch P2 Erlangung physischen Zugriffs auf die Fahrzeugelektronik als externer Angreifer                                                                                                           | C4 Redundanz für sicherheitskritische Kommunikation der ADS-Kernkomponenten<br><br>A3 Qualitätsschäden werden im Falle eines kompromittierten Lkw selektiv berücksichtigt.<br>A6 Lokale Angreifer | DS6 [S3 F2OEM]<br><br>DS5, DS7, DS8, DS11, DS6, DS12, DS13      |   | H | 1 | DS6 [S3 F2OEM]<br><br>DS6>DS7, DS5, DS7, DS8, DS11, DS6, DS12, DS13 |   | H | 1 |
| R51: T18 Störung von Initiate MRM auf der VBUS-Verbindung zwischen System Management und Planung, vorbereitet durch P3 Erlangung des Zugriffs auf einen Offline-Fahrzeugbus durch Fernkompromittierung einer angeschlossenen ECU                                                                                 | C4 Redundanz für sicherheitskritische Kommunikation von ADS-Kernkomponenten<br><br>A3 Qualitätsschäden werden im Falle eines kompromittierten Lkw selektiv berücksichtigt.<br>A5 Domänentrennung  | DS6 [S3 F2OEM]<br><br>DS5, DS7, DS8, DS11<br><br>DS6 [S3 F2OEM] | S | H | 1 | DS6 [S3 F2OEM]<br><br>DS6>DS7, DS5, DS7, DS8, DS11                  |   | H | 1 |
| R52: T18 Störung Initiierung von MRM auf der VBUS-Verbindung zwischen System Management und Planungsvorbereitung durch P5 Angriff auf mehr als eine Verbindung, um Sensorfusion (C3) oder Redundanzen (C4, C5) zu überwinden, P2 Erlangung physischen Zugriffs auf die Fahrzeugelektronik als externer Angreifer | A3 Qualitätsschäden werden im Falle eines kompromittierten Lkw selektiv berücksichtigt, A6 Lokale Angreifer                                                                                       | DS6 [S3 F2OEM]<br><br>DS5, DS7, DS8, DS11, DS6, DS12, DS13      |   | M | 1 | DS6 [S3 F2OEM]<br><br>DS5, DS7, DS8, DS11, DS6, DS12, DS13          |   | M | 1 |
| R53: T18 Störung Initiieren von MRM auf der VBUS-Verbindung zwischen System Management und Planungsvorbereitung durch P5 Angriff auf mehr als eine                                                                                                                                                               | A3 Qualitätsmängel werden im Falle eines kompromittierten                                                                                                                                         | DS6 [S3 F2OEM]<br><br>DS5, DS7, DS8, DS11                       | S | M | 1 | DS6 [S3 F2OEM]<br><br>DS5, DS7, DS8, DS11                           | S | M | 1 |

|                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                                                                                                                |                                         |  |   |   |                                         |  |   |   |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------|-----------------------------------------|--|---|---|-----------------------------------------|--|---|---|
| Verbindung, um Sensorfusion (C3) oder Redundanzen (C4, C5) zu überwinden,<br>P3 Erlangen von Zugriff auf einen Offline-Fahrzeugbus durch Fernkompromittierung einer verbundenen ECU                                                                                                                                                                                                                                                                  | Lkw selektiv berücksichtigt.<br>A5 Domänentrennung                                                             | DS6 [S3 F2OEM]                          |  |   |   | DS6 [S3 F2OEM]                          |  |   |   |
| R54: T19 Störung Initiieren von MRM auf der VBUS-Verbindung zwischen Onboard-HMI und System Management Vorbereitung durch P2 Erlangen von physischem Zugriff auf die Fahrzeugelektronik als externer Angreifer<br><br>Hinweis: Es wurden keine Sicherheitsziele oder Schadensszenarien zugewiesen, da der durch diese Bedrohung gefährdete Datenfluss für den vollständig autonomen Lkw im Betrieb ohne Testfahrer nicht existiert.                  | A3 Qualitätsschäden werden im Falle eines kompromittierten Lkw selektiv berücksichtigt,<br>A6 Lokale Angreifer | DS5, DS7, DS8, DS11,<br>DS6, DS12, DS13 |  | H | 1 | DS5, DS7, DS8, DS11,<br>DS6, DS12, DS13 |  | H | 1 |
| R55: T19 Störung Initiieren von MRM auf der VBUS-Verbindung zwischen Onboard-HMI und System Management Vorbereitung durch P4 Erlangen von Zugriff auf einen Online-Fahrzeugbus durch Fernkompromittierung einer verbundenen ECU<br><br>Hinweis: Es wurden keine Sicherheitsziele oder Schadensszenarien zugewiesen, da der durch diese Bedrohung gefährdete Datenfluss für den vollständig autonomen Lkw im Betrieb ohne Testfahrer nicht existiert. | A3 Bei einem kompromittierten Lkw werden Qualitätsschäden selektiv berücksichtigt.                             | DS5, DS7, DS8, DS11                     |  | H | 1 | DS5, DS7, DS8, DS11                     |  | H | 1 |
| R56: T19 Störung Initiieren von MRM auf der VBUS-Verbindung zwischen Onboard-HMI und System Management Vorbereitung durch P5 Angriff auf mehr als eine Verbindung, um Sensorfusion (C3) oder Redundanzen (C4, C5) zu überwinden                                                                                                                                                                                                                      | A3 Qualitätsschäden werden im Falle eines kompromittierten Lkw selektiv berücksichtigt,<br>A6 Lokale Angreifer | DS5, DS7, DS8, DS11,<br>DS6, DS12, DS13 |  | M | 1 | DS5, DS7, DS8, DS11,<br>DS6, DS12, DS13 |  | M | 1 |

|                                                                                                                                                                                                                                                                                                                                  |                                                                                                                                                                                                       |                                                            |  |   |   |                                                                     |  |   |   |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------|--|---|---|---------------------------------------------------------------------|--|---|---|
| P2 Erlangung physischen Zugriffs auf die Fahrzeugelektronik als externer Angreifer                                                                                                                                                                                                                                               |                                                                                                                                                                                                       |                                                            |  |   |   |                                                                     |  |   |   |
| Hinweis: Es wurden keine Sicherheitsziele oder Schadensszenarien zugewiesen, da der durch diese Bedrohung gefährdete Datenfluss für den vollständig autonomen Lkw im Betrieb ohne Testfahrer nicht existiert.                                                                                                                    |                                                                                                                                                                                                       |                                                            |  |   |   |                                                                     |  |   |   |
| R57: T19 Störung Initiierung von MRM auf der VBUS-Verbindung zwischen Onboard-HMI und System Management Vorbereitung durch P5 Angriff auf mehr als eine Verbindung, um Sensorfusion (C3) oder Redundanzen (C4, C5) zu überwinden<br><br>P4 Zugriff auf einen Online-Fahrzeugbus durch Fernkompromittierung einer verbundenen ECU | A3 Bei einem kompromittierten Lkw werden Qualitätsschäden selektiv berücksichtigt.                                                                                                                    | DS5, DS7, DS8, DS11                                        |  | M | 1 | DS5, DS7, DS8, DS11                                                 |  | M | 1 |
| Hinweis: Es wurden keine Sicherheitsziele oder Schadensszenarien zugewiesen, da der durch diese Bedrohung gefährdete Datenfluss für den vollständig autonomen Lkw im Betrieb ohne Testfahrer nicht existiert.                                                                                                                    |                                                                                                                                                                                                       |                                                            |  |   |   |                                                                     |  |   |   |
| R58: T20 Störung Initiieren Sie MRM auf der IPC-Verbindung zwischen Planung und Steuerung Vorbereitung durch P2 Erlangen Sie als externer Angreifer physischen Zugriff auf die Fahrzeugelektronik                                                                                                                                | C4 Redundanz für sicherheitskritische Kommunikation der ADS-Kernkomponenten<br><br>A3 Qualitätsschäden werden im Falle eines kompromittierten Lkw selektiv berücksichtigt.<br><br>A6 Lokale Angreifer | DS6 [S3 F2OEM]<br><br>DS5, DS7, DS8, DS11, DS6, DS12, DS13 |  | H | 1 | DS6 [S3 F2OEM]<br><br>DS6>DS7, DS5, DS7, DS8, DS11, DS6, DS12, DS13 |  | H | 1 |

|                                                                                                                                                                                                                                                                                                                                     |                                                                                                                                                                                                  |                                                                           |   |   |   |                                                                                   |   |   |   |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------|---|---|---|-----------------------------------------------------------------------------------|---|---|---|
| R59: T20 Störung Initiieren von MRM auf der IPC-Verbindung zwischen Planung und Steuerung Vorbereitung durch P3 Erlangen von Zugriff auf einen Offline-Fahrzeugbus durch Fernkompromittierung einer verbundenen ECU                                                                                                                 | C4 Redundanz für sicherheitskritische Kommunikation von ADS-Kernkomponenten<br><br>A3 Qualitätsschäden werden im Falle eines kompromittierten Lkw selektiv berücksichtigt.<br>A5 Domänentrennung | DS6 [S3 F2OEM]<br>_____<br>DS5, DS7, DS8, DS11<br>_____<br>DS6 [S3 F2OEM] | S | H | 1 | DS6 [S3 F2OEM]<br>_____<br>DS6>DS7, DS5, DS7, DS8, DS11<br>_____                  |   | H | 1 |
| R60: T20 Störung Initiieren von MRM auf der IPC-Verbindung zwischen Planung und Steuerung Vorbereitung durch P5 Angriff auf mehr als eine Verbindung, um Sensorfusion (C3) oder Redundanzen (C4, C5) zu überwinden,<br>P2 Erlangung physischen Zugriffs auf die Fahrzeugelektronik als externer Angreifer                           | A3 Qualitätsschäden werden im Falle eines kompromittierten Lkw selektiv berücksichtigt,<br>A6 Lokale Angreifer                                                                                   | DS6 [S3 F2OEM]<br>_____<br>DS5, DS7, DS8, DS11, DS6, DS12, DS13<br>_____  |   | M | 1 | DS6 [S3 F2OEM]<br>_____<br>DS5, DS7, DS8, DS11, DS6, DS12, DS13<br>_____          |   | M | 1 |
| R61: T20 Störung Initiierung von MRM auf der IPC-Verbindung zwischen Planung und Steuerung Vorbereitung durch P5 Angriff auf mehr als eine Verbindung, um die Sensorfusion (C3) oder Redundanzen (C4, C5) zu überwinden<br>P3 Erlangung des Zugriffs auf einen Offline-Fahrzeugbus durch Fernkompromittierung einer verbundenen ECU | A3 Qualitätsmängel werden im Falle eines kompromittierten Lkw selektiv berücksichtigt.<br>A5 Domänentrennung                                                                                     | DS6 [S3 F2OEM]<br>_____<br>DS5, DS7, DS8, DS11<br>_____<br>DS6 [S3 F2OEM] | S | M | 1 | DS6 [S3 F2OEM]<br>_____<br>DS5, DS7, DS8, DS11<br>_____<br>DS6 [S3 F2OEM]         | S | M | 1 |
| R62: T21 Störung Initiieren von MRM auf der VBUS-Verbindung zwischen Steuerung und Aktoren Vorbereitung durch P2 Erlangen von physischem Zugriff auf die Fahrzeugelektronik als externer Angreifer                                                                                                                                  | C4 Redundanz für sicherheitskritische Kommunikation der ADS-Kernkomponenten<br><br>A3 Qualitätsschäden werden im Falle eines                                                                     | DS6 [S3 F2OEM]<br>_____<br>DS5, DS7, DS8, DS11, DS6, DS12, DS13<br>_____  |   | H | 1 | DS6 [S3 F2OEM]<br>_____<br>DS6>DS7, DS5, DS7, DS8, DS11, DS6, DS12, DS13<br>_____ |   | H | 1 |

|                                                                                                                                                                                                                                                                                                                                |                                                                                                                                                                                                  |                                                                           |   |   |   |                                                                           |   |   |   |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------|---|---|---|---------------------------------------------------------------------------|---|---|---|
|                                                                                                                                                                                                                                                                                                                                | kompromittierten Lkw selektiv berücksichtigt.<br>A6 Lokale Angreifer                                                                                                                             |                                                                           |   |   |   |                                                                           |   |   |   |
| R63: T21 Störung Initiieren von MRM auf der VBUS-Verbindung zwischen Steuerung und Aktoren Vorbereitung durch P3 Erlangen von Zugriff auf einen Offline-Fahrzeugbus durch Fernkompromittierung einer verbundenen ECU                                                                                                           | C4 Redundanz für sicherheitskritische Kommunikation von ADS-Kernkomponenten<br><br>A3 Qualitätsschäden werden im Falle eines kompromittierten Lkw selektiv berücksichtigt.<br>A5 Domänentrennung | DS6 [S3 F2OEM]<br>_____<br>DS5, DS7, DS8, DS11<br>_____<br>DS6 [S3 F2OEM] | S | H | 1 | DS6 [S3 F2OEM]<br>_____<br>DS6>DS7, DS5, DS7, DS8, DS11<br>_____          |   | H | 1 |
| R64: T21 Störung Initiierung von MRM auf der VBUS-Verbindung zwischen Steuerung und Aktoren Vorbereitung durch P5 Angriff auf mehr als eine Verbindung, um Sensorfusion (C3) oder Redundanzen (C4, C5) zu überwinden,<br>P2 Erlangung physischen Zugriffs auf die Fahrzeugelektronik als externer Angreifer                    | A3 Qualitätsschäden werden im Falle eines kompromittierten Lkw selektiv berücksichtigt,<br>A6 Lokale Angreifer                                                                                   | DS6 [S3 F2OEM]<br>_____<br>DS5, DS7, DS8, DS11, DS6, DS12, DS13<br>_____  |   | M | 1 | DS6 [S3 F2OEM]<br>_____<br>DS5, DS7, DS8, DS11, DS6, DS12, DS13<br>_____  |   | M | 1 |
| R65: T21 Störung Initiieren von MRM auf der VBUS-Verbindung zwischen Steuerung und Aktoren Vorbereitung durch P5 Angriff auf mehr als eine Verbindung, um Sensorfusion (C3) oder Redundanzen (C4, C5) zu überwinden,<br>P3 Erlangen von Zugriff auf einen Offline-Fahrzeugbus durch Fernkompromittierung einer verbundenen ECU | A3 Qualitätsmängel werden im Falle eines kompromittierten Lkw selektiv berücksichtigt.<br>A5 Domänentrennung                                                                                     | DS6 [S3 F2OEM]<br>_____<br>DS5, DS7, DS8, DS11<br>_____<br>DS6 [S3 F2OEM] | S | M | 1 | DS6 [S3 F2OEM]<br>_____<br>DS5, DS7, DS8, DS11<br>_____<br>DS6 [S3 F2OEM] | S | M | 1 |
| R66: T22 Störung der nicht sicherheitskritischen Kommunikation auf der MCOM-Verbindung                                                                                                                                                                                                                                         | A4 Begrenzte Störung des Mobilfunks                                                                                                                                                              | DS5 [O2], DS7 [O2], DS8 [O1], DS11 [O1]<br>_____                          | V | H | 2 | DS5 [O2], DS7 [O2], DS8 [O1], DS11 [O1]<br>_____                          | V | H | 2 |

|                                                                                                                                                                                                                         |                                                                                                             |                                                                                              |   |   |   |                                                                                              |  |   |   |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------|---|---|---|----------------------------------------------------------------------------------------------|--|---|---|
|                                                                                                                                                                                                                         |                                                                                                             | DS5>DS17, DS7>DS17,<br>DS8>DS17, DS11>DS17<br>_____<br>DS17 [Q0]                             |   |   |   | DS5>DS17, DS7>DS17,<br>DS8>DS17, DS11>DS17<br>_____<br>DS17 [Q0]                             |  |   |   |
| R67: T23 Störung der nicht sicherheitskritischen Kommunikation auf einer VBUS-Verbindung Vorbereitung durch P2 Erlangung physischen Zugriffs auf die Fahrzeugelektronik als externer Angreifer                          | A3 Qualitätsschäden werden im Falle eines kompromittierten Lkw selektiv berücksichtigt, A6 Lokale Angreifer | DS5 [O2], DS7 [O2],<br>DS8 [O1]<br>_____<br>DS5, DS7, DS8, DS11,<br>DS6, DS12, DS13<br>_____ |   | H | 1 | DS5 [O2], DS7 [O2],<br>DS8 [O1]<br>_____<br>DS5, DS7, DS8, DS11,<br>DS6, DS12, DS13<br>_____ |  | H | 1 |
| R68: T23 Störung der nicht sicherheitskritischen Kommunikation auf einer VBUS-Verbindung Vorbereitung durch P4 Erlangung des Zugriffs auf einen Online-Fahrzeugbus durch Fernkompromittierung einer angeschlossenen ECU | A3 Bei einem kompromittierten Lkw werden Qualitätsschäden selektiv berücksichtigt.                          | DS5 [O2], DS7 [O2],<br>DS8 [O1]<br>_____<br>DS5, DS7, DS8, DS11<br>_____                     |   | H | 1 | DS5 [O2], DS7 [O2],<br>DS8 [O1]<br>_____<br>DS5, DS7, DS8, DS11<br>_____                     |  | H | 1 |
| R69: T24 Störung der nicht sicherheitskritischen Kommunikation auf einer IPC-Verbindung Vorbereitung durch P2 Erlangung physischen Zugriffs auf die Fahrzeugelektronik als externer Angreifer                           | A3 Qualitätsschäden werden im Falle eines kompromittierten Lkw selektiv berücksichtigt, A6 Lokale Angreifer | DS5 [O2], DS7 [O2],<br>DS8 [O1]<br>_____<br>DS5, DS7, DS8, DS11,<br>DS6, DS12, DS13<br>_____ |   | H | 1 | DS5 [O2], DS7 [O2],<br>DS8 [O1]<br>_____<br>DS5, DS7, DS8, DS11,<br>DS6, DS12, DS13<br>_____ |  | H | 1 |
| R70: T24 Störung der nicht sicherheitskritischen Kommunikation auf einer IPC-Verbindung Vorbereitung durch P3 Erlangung des Zugriffs auf einen Offline-Fahrzeugbus durch Fernkompromittierung einer verbundenen ECU     | A3 Qualitätsmängel werden im Falle eines kompromittierten Lkw selektiv berücksichtigt. A5 Domänentrennung   | DS5 [O2], DS7 [O2],<br>DS8 [O1]<br>_____<br>DS5, DS7, DS8, DS11<br>_____                     |   | H | 1 | DS5 [O2], DS7 [O2],<br>DS8 [O1]<br>_____<br>DS5, DS7, DS8, DS11<br>_____                     |  | H | 1 |
| R71: T25 Spoofing oder Manipulation von Rohvideodaten als MitM auf der VBUS-Verbindung zwischen                                                                                                                         | C3 Validierung von Sensordaten durch Sensorfusion,                                                          | DS5 [O2], DS6<br>[S3 F2OEM], DS7 [O2],                                                       | S | H | 5 | DS5 [O2], DS6<br>[S3 F2OEM], DS7 [O2],                                                       |  | H | 1 |



|                                                                                                                                                                                                                                                      |                                                                                                             |                                                                                     |   |   |   |                                                                                           |  |   |   |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|---|---|---|-------------------------------------------------------------------------------------------|--|---|---|
| Sensoren und Wahrnehmung Vorbereitung durch P1 Erlangung physischen Zugriffs auf die Fahrzeugelektronik als Fahrzeugbesitzer/Tuner                                                                                                                   | C5 Redundanz gegen Aktivierung von ADS außerhalb von ODD                                                    | DS8 [O1], DS12 [S3 F3OEM], DS13 [S3 F3OEM]                                          |   |   |   | DS8 [O1], DS12 [S3 F3OEM], DS13 [S3 F3OEM]                                                |  |   |   |
|                                                                                                                                                                                                                                                      | A2 Begrenzter Spielraum für Tuning-Angriffe                                                                 | DS1, DS5, DS6, DS7, DS8, DS9, DS10, DS11, DS12, DS14, DS15, DS18<br>DS13 [S3 F3OEM] |   |   |   | DS6>DS7, DS12>DS7, DS13, DS1, DS5, DS6, DS7, DS8, DS9, DS10, DS11, DS12, DS14, DS15, DS18 |  |   |   |
| R72: T25 Spoofing oder Manipulation von Rohvideodaten als MitM auf der VBUS-Verbindung zwischen Sensoren und Wahrnehmung Vorbereitung durch P2 Erlangung physischen Zugriffs auf die Fahrzeugelektronik als externer Angreifer                       | C3 Validierung von Sensordaten durch Sensorfusion, C5 Redundanz gegen Aktivierung von ADS außerhalb von ODD | DS5 [O2], DS6 [S3 F2OEM], DS7 [O2], DS8 [O1], DS12 [S3 F3OEM], DS13 [S3 F3OEM]      |   | H | 1 | DS5 [O2], DS6 [S3 F2OEM], DS7 [O2], DS8 [O1], DS12 [S3 F3OEM], DS13 [S3 F3OEM]            |  | H | 1 |
|                                                                                                                                                                                                                                                      | A3 Qualitätsschäden werden im Falle eines kompromittierten Lkw selektiv berücksichtigt, A6 Lokale Angreifer | DS5, DS7, DS8, DS11, DS6, DS12, DS13                                                |   |   |   | DS6>DS7, DS12>DS7, DS13, DS5, DS7, DS8, DS11, DS6, DS12, DS13                             |  |   |   |
| R73: T25 Spoofing oder Manipulation von Rohvideodaten als MitM auf der VBUS-Verbindung zwischen Sensoren und Wahrnehmung Vorbereitung durch P3 Erlangung des Zugriffs auf einen Offline-Fahrzeugbus durch Fernkompromittierung einer verbundenen ECU | C3 Validierung von Sensordaten durch Sensorfusion, C5 Redundanz gegen Aktivierung von ADS außerhalb von ODD | DS5 [O2], DS6 [S3 F2OEM], DS7 [O2], DS8 [O1], DS12 [S3 F3OEM], DS13 [S3 F3OEM]      | S | H | 1 | DS5 [O2], DS6 [S3 F2OEM], DS7 [O2], DS8 [O1], DS12 [S3 F3OEM], DS13 [S3 F3OEM]            |  | H | 1 |
|                                                                                                                                                                                                                                                      | A3 Qualitätsschäden werden im Falle eines                                                                   | DS5, DS7, DS8, DS11<br>DS6 [S3 F2OEM], DS12                                         |   |   |   | DS6>DS7, DS12>DS7, DS13, DS5, DS7, DS8,                                                   |  |   |   |

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |                                                                                                                                                                                                                |                                                                                                                                                                                                              |   |   |   |                                                                                                                                                                                                       |   |    |   |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|---|---|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|----|---|
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | kompromittierten Lkw selektiv berücksichtigt,<br>A5 Domänenentrennung                                                                                                                                          | [S3 F2OEM], DS13<br>[S3 F3OEM]                                                                                                                                                                               |   |   |   | DS11<br>_____                                                                                                                                                                                         |   |    |   |
| R74: T25 Spoofing oder Manipulation von Rohvideodaten als MitM auf der VBUS-Verbindung zwischen Sensoren und Wahrnehmung Vorbereitung durch P5 Angriff auf mehr als eine Verbindung, um die Sensorfusion (C3) oder Redundanzen (C4, C5) zu überwinden<br>T28 Spoofing oder Manipulation virtueller Sensordaten als MitM auf der VBUS-Verbindung zwischen Mission Control und Wahrnehmung,<br>P1 Erlangung physischen Zugriffs auf die Fahrzeugelektronik als Fahrzeugbesitzer/Tuner | C6 Authentische Datenübertragung,<br>C21 End-to-End-Signatur virtueller Sensordaten<br>_____<br>A2 Begrenzter Spielraum für Tuning-Angriffe                                                                    | DS5 [O2], DS6<br>[S3 F2OEM], DS7 [O2],<br>DS8 [O1], DS12<br>[S3 F3OEM], DS13<br>[S3 F3OEM]<br>_____<br>DS1, DS5, DS6, DS7,<br>DS8, DS9, DS10, DS11,<br>DS12, DS14, DS15,<br>DS18<br>_____<br>DS13 [S3 F3OEM] | S | M | 4 | DS5 [O2], DS6<br>[S3 F2OEM], DS7 [O2],<br>DS8 [O1], DS12<br>[S3 F3OEM], DS13<br>[S3 F3OEM]<br>_____<br>DS12, DS13, DS1, DS5,<br>DS6, DS7, DS8, DS9,<br>DS10, DS11, DS12,<br>DS14, DS15, DS18<br>_____ |   | SG | 1 |
| R75: T25 Spoofing oder Manipulation von Rohvideodaten als MitM auf der VBUS-Verbindung zwischen Sensoren und Perception prep. durch P5 Angriff auf mehr als eine Verbindung, um die Sensorfusion (C3) oder Redundanzen (C4, C5) zu überwinden.<br>T28 Spoofing oder Manipulation virtueller Sensordaten als MitM auf der VBUS-Verbindung zwischen Mission Control und Wahrnehmung,<br>P2 Erlangung physischen Zugriffs auf die Fahrzeugelektronik als externer Angreifer            | C6 Authentische Datenübertragung,<br>C21 End-to-End-Signatur virtueller Sensordaten<br>_____<br>A3 Qualitätsschäden werden im Falle eines kompromittierten Lkw selektiv berücksichtigt,<br>A6 Lokale Angreifer | DS5 [O2], DS6<br>[S3 F2OEM], DS7 [O2],<br>DS8 [O1], DS12<br>[S3 F3OEM], DS13<br>[S3 F3OEM]<br>_____<br>DS5, DS7, DS8, DS11,<br>DS6, DS12, DS13<br>_____                                                      |   | M | 1 | DS5 [O2], DS6<br>[S3 F2OEM], DS7 [O2],<br>DS8 [O1], DS12<br>[S3 F3OEM], DS13<br>[S3 F3OEM]<br>_____<br>DS12, DS13, DS5, DS7,<br>DS8, DS11, DS6, DS12,<br>DS13<br>_____                                |   | SG | 1 |
| R76: T25 Spoofing oder Manipulation von Rohvideodaten als MitM auf der VBUS-Verbindung zwischen Sensoren und Wahrnehmung Vorbereitung durch P5 Angriff auf mehr als eine Verbindung, um die Sensorfusion                                                                                                                                                                                                                                                                            | C6 Authentische Datenübertragung,<br>C21 End-to-End-Signatur virtueller Sensordaten                                                                                                                            | DS5 [O2], DS6<br>[S3 F2OEM], DS7 [O2],<br>DS8 [O1], DS12<br>[S3 F3OEM], DS13                                                                                                                                 | S | M | 1 | DS5 [O2], DS6<br>[S3 F2OEM], DS7 [O2],<br>DS8 [O1], DS12<br>[S3 F3OEM], DS13                                                                                                                          | S | SG | 1 |

|                                                                                                                                                                                                                                                                                           |                                                                                                                            |                                                                               |   |   |   |                                                                        |  |    |   |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------|---|---|---|------------------------------------------------------------------------|--|----|---|
| (C3) oder Redundanzen (C4, C5) zu überwinden,<br>T28 Spoofing oder Manipulation virtueller Sensordaten<br>als MitM auf der VBUS-Verbindung zwischen Mission<br>Control und Wahrnehmung,<br>P3 Zugriff auf einen Offline-Fahrzeugbus durch Fern-<br>kompromittierung einer verbundenen ECU | _____                                                                                                                      | [S3 F3OEM]                                                                    |   |   |   | [S3 F3OEM]                                                             |  |    |   |
|                                                                                                                                                                                                                                                                                           | A3 Qualitätsschäden werden<br>im Falle eines beschädigten<br>Lkw selektiv berücksichtigt,<br>A5 Domänentrennung            | DS5, DS7, DS8, DS11<br>DS6 [S3 F2OEM], DS12<br>[S3 F2OEM], DS13<br>[S3 F3OEM] |   |   |   | DS12, DS13, DS5, DS7,<br>DS8, DS11<br>DS6 [S3 F2OEM]                   |  |    |   |
| R77: T26 Spoofing oder Manipulation von Sensordaten<br>als MitM auf der VBUS-Verbindung zwischen Sensoren<br>und Wahrnehmung Vorbereitung durch P2 Erlangung<br>physischen Zugriffs auf die Fahrzeugelektronik als ex-<br>terner Angreifer                                                | C3 Validierung von Sensordaten durch Sensorfusion,<br>C5 Redundanz gegen Aktivierung von ADS außerhalb von<br>ODD<br>_____ | DS5 [O2], DS6<br>[S3 F2OEM], DS7 [O2],<br>DS8 [O1], DS12<br>[S3 F3OEM]        |   | H | 1 | DS5 [O2], DS6<br>[S3 F2OEM], DS7 [O2],<br>DS8 [O1], DS12<br>[S3 F3OEM] |  | H  | 1 |
|                                                                                                                                                                                                                                                                                           | A3 Qualitätsschäden werden<br>im Falle eines kompromittierten Lkw selektiv berücksichtigt,<br>A6 Lokale Angreifer          | DS5, DS7, DS8, DS11,<br>DS6, DS12, DS13                                       |   |   |   | DS6>DS7, DS12>DS7,<br>DS13, DS5, DS7, DS8,<br>DS11, DS6, DS12, DS13    |  |    |   |
| R78: T26 Spoofing oder Manipulation von Sensordaten<br>als MitM auf der VBUS-Verbindung zwischen Sensoren<br>und Wahrnehmung Vorbereitung durch P3 Erlangung<br>des Zugriffs auf einen Offline-Fahrzeugbus durch Fern-<br>kompromittierung einer verbundenen ECU                          | C3 Validierung von Sensordaten durch Sensorfusion,<br>C5 Redundanz gegen Aktivierung von ADS außerhalb von<br>ODD<br>_____ | DS5 [O2], DS6<br>[S3 F2OEM], DS7 [O2],<br>DS8 [O1], DS12<br>[S3 F3OEM]        | S | H | 1 | DS5 [O2], DS6<br>[S3 F2OEM], DS7 [O2],<br>DS8 [O1], DS12<br>[S3 F3OEM] |  | H  | 1 |
|                                                                                                                                                                                                                                                                                           | A3 Qualitätsschäden werden<br>im Falle eines kompromittierten Lkw selektiv berücksichtigt,<br>A5 Domänentrennung           | DS5, DS7, DS8, DS11<br>DS6 [S3 F2OEM], DS12<br>[S3 F2OEM]                     |   |   |   | DS6>DS7, DS12>DS7,<br>DS13, DS5, DS7, DS8,<br>DS11                     |  |    |   |
| R79: T26 Spoofing oder Manipulation von Sensordaten<br>als MitM auf der VBUS-Verbindung zwischen Sensoren                                                                                                                                                                                 | C6 Authentische Datenübertragung,                                                                                          | DS5 [O2], DS6<br>[S3 F2OEM], DS7 [O2],                                        |   | M | 1 | DS5 [O2], DS6<br>[S3 F2OEM], DS7 [O2],                                 |  | SG | 1 |

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                                                                                                                                                                                                                           |                                                                                                                                 |   |   |   |                                                                                                                                                                         |   |    |   |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------|---|---|---|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|----|---|
| und Wahrnehmung Vorbereitung durch P5 Angriff auf mehr als eine Verbindung, um die Sensorfusion (C3) oder Redundanzen (C4, C5) zu überwinden<br>T28 Spoofing oder Manipulation virtueller Sensordaten als MitM auf der VBUS-Verbindung zwischen Mission Control und Wahrnehmung,<br>P2 Erlangung physischen Zugriffs auf die Fahrzeugelektronik als externer Angreifer                                                                                                                | C21 End-to-End-Signatur virtueller Sensordaten<br><br>A3 Qualitätsschäden werden im Falle eines kompromittierten Lkw selektiv berücksichtigt,<br>A6 Lokale Angreifer                                                      | DS8 [O1], DS12 [S3 F3OEM]<br><br>DS5, DS7, DS8, DS11, DS6, DS12, DS13                                                           |   |   |   | DS8 [O1], DS12 [S3 F3OEM]<br><br>DS12, DS13, DS5, DS7, DS8, DS11, DS6, DS12, DS13                                                                                       |   |    |   |
| R80: T26 Spoofing oder Manipulation von Sensordaten als MitM auf der VBUS-Verbindung zwischen Sensoren und Wahrnehmung Vorbereitung durch P5 Angriff auf mehr als eine Verbindung, um die Sensorfusion (C3) oder Redundanzen (C4, C5) zu überwinden,<br>T28 Spoofing oder Manipulation virtueller Sensordaten als MitM auf der VBUS-Verbindung zwischen Mission Control und Wahrnehmung,<br>P3 Zugriff auf einen Offline-Fahrzeugbus durch Fernkompromittierung einer verbundenen ECU | C6 Authentische Datenübertragung,<br>C21 End-to-End-Signatur virtueller Sensordaten<br><br>A3 Qualitätsschäden werden im Falle eines beschädigten Lkw selektiv berücksichtigt,<br>A5 Domänentrennung                      | DS5 [O2], DS6 [S3 F2OEM], DS7 [O2], DS8 [O1], DS12 [S3 F3OEM]<br><br>DS5, DS7, DS8, DS11<br><br>DS6 [S3 F2OEM], DS12 [S3 F2OEM] | S | M | 1 | DS5 [O2], DS6 [S3 F2OEM], DS7 [O2], DS8 [O1], DS12 [S3 F3OEM]<br><br>DS12, DS13, DS5, DS7, DS8, DS11<br><br>DS6 [S3 F2OEM]                                              | S | SG | 1 |
| R81: T27 Spoofing oder Manipulation virtueller Sensordaten als MitM auf der MCOM-Verbindung zwischen Control Center und Mission Control                                                                                                                                                                                                                                                                                                                                               | C2 mTLS zwischen Control Center und Mission Control,<br>C3 Validierung der Sensordaten durch Sensorfusion,<br>C5 Redundanz gegen Aktivierung von ADS außerhalb von ODD,<br>C21 End-to-End-Signatur virtueller Sensordaten | DS5 [O2], DS7 [O2], DS8 [O1], DS12 [S3 F2OEM], DS13 [S3 F3OEM], DS14 [F0RU]                                                     | S | H | 5 | DS5 [O2], DS7 [O2], DS8 [O1], DS12 [S3 F3OEM], DS13 [S3 F3OEM], DS14 [F0RU]<br><br>DS6>DS7, DS12>DS7, DS13, DS12, DS13<br><br>DS5 [O2], DS7 [O2], DS8 [O1], DS14 [F0RU] | E | SG | 2 |

|                                                                                                                                                                                                                                                                  |                                                                                                                                                                                                                                                       |                                                                                                                                                                            |   |   |   |                                                                                                                                                                                          |   |    |   |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|---|---|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|----|---|
| R82: T27 Spoofing oder Manipulation virtueller Sensordaten als MitM auf der MCOM-Verbindung zwischen Control Center und Mission Control, vorbereitet durch P5 Angriff auf mehr als eine Verbindung, um Sensorfusion (C3) oder Redundanzen (C4, C5) zu überwinden | C2 mTLS zwischen Control Center und Mission Control, C21 End-to-End-Signatur virtueller Sensordaten                                                                                                                                                   | DS5 [O2], DS7 [O2], DS8 [O1], DS12 [S3 F2OEM], DS13 [S3 F3OEM], DS14 [F0RU]                                                                                                | S | M | 4 | DS5 [O2], DS7 [O2], DS8 [O1], DS12 [S3 F3OEM], DS13 [S3 F3OEM], DS14 [F0RU]<br><br>DS12, DS13<br><br>DS5 [O2], DS7 [O2], DS8 [O1], DS14 [F0RU]                                           | E | SG | 2 |
| R83: T28 Spoofing oder Manipulation virtueller Sensordaten als MitM auf der VBUS-Verbindung zwischen Mission Control und Wahrnehmung Vorbereitung durch P1 Erlangung physischen Zugriffs auf die Fahrzeugelektronik als Fahrzeugbesitzer/Tuner                   | C3 Validierung von Sensordaten durch Sensorfusion, C5 Redundanz gegen Aktivierung von ADS außerhalb von ODD, C6 Authentische Übertragung von Daten, C21 End-to-End-Signatur virtueller Sensordaten<br><br>A2 Begrenzter Spielraum für Tuning-Angriffe | DS5 [O2], DS7 [O2], DS8 [O1], DS12 [S3 F3OEM], DS13 [S3 F3OEM], DS14 [F0RU]<br><br>DS1, DS5, DS6, DS7, DS8, DS9, DS10, DS11, DS12, DS14, DS15, DS18<br><br>DS13 [S3 F3OEM] | S | H | 5 | DS5 [O2], DS7 [O2], DS8 [O1], DS12 [S3 F3OEM], DS13 [S3 F3OEM], DS14 [F0RU]<br><br>DS6>DS7, DS12>DS7, DS13, DS12, DS13, DS1, DS5, DS6, DS7, DS8, DS9, DS10, DS11, DS12, DS14, DS15, DS18 |   | SG | 1 |
| R84: T28 Spoofing oder Manipulation virtueller Sensordaten als MitM auf der VBUS-Verbindung zwischen Mission Control und Wahrnehmung Vorbereitung durch P2 Erlangung physischen Zugriffs auf die Fahrzeugelektronik als externer Angreifer                       | C3 Validierung von Sensordaten durch Sensorfusion, C5 Redundanz gegen Aktivierung von ADS außerhalb von ODD, C6 Authentische Übertragung                                                                                                              | DS5 [O2], DS7 [O2], DS8 [O1], DS12 [S3 F3OEM], DS13 [S3 F3OEM], DS14 [F0RU]                                                                                                | V | H | 2 | DS5 [O2], DS7 [O2], DS8 [O1], DS12 [S3 F3OEM], DS13 [S3 F3OEM], DS14 [F0RU]                                                                                                              | V | SG | 1 |

|                                                                                                                                                                                                                                                                                                                                                       |                                                                                                                                                                                                                                                                                                                 |                                                                                                                                                                                            |   |   |   |                                                                                                                                                                                                     |   |    |   |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|---|---|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|----|---|
|                                                                                                                                                                                                                                                                                                                                                       | <p>von Daten,<br/>C21 End-to-End-Signatur virtueller Sensordaten</p> <p>A3 Qualitätsschäden werden im Falle eines kompromittierten Lkw selektiv berücksichtigt,<br/>A6 Lokale Angreifer</p>                                                                                                                     | <p>DS5, DS7, DS8, DS11,<br/>DS6, DS12, DS13</p> <p>DS14 [F0RU]</p>                                                                                                                         |   |   |   | <p>DS6&gt;DS7, DS12&gt;DS7,<br/>DS13, DS12, DS13,<br/>DS5, DS7, DS8, DS11,<br/>DS6, DS12, DS13</p> <p>DS14 [F0RU]</p>                                                                               |   |    |   |
| R85: T28 Spoofing oder Manipulation virtueller Sensordaten als MitM auf der VBUS-Verbindung zwischen Mission Control und Perception prep. von P4 Erlangung des Zugriffs auf einen Online-Fahrzeugbus durch Fernkompromittierung einer angeschlossenen ECU                                                                                             | <p>C3 Validierung von Sensordaten durch Sensorfusion,<br/>C5 Redundanz gegen Aktivierung von ADS außerhalb von ODD,<br/>C6 Authentische Übertragung von Daten,<br/>C21 End-to-End-Signatur virtueller Sensordaten</p> <p>A3 Qualitätsschäden werden im Falle eines beschädigten Lkw selektiv berücksichtigt</p> | <p>DS5 [O2], DS7 [O2],<br/>DS8 [O1], DS12<br/>[S3 F3OEM], DS13<br/>[S3 F3OEM], DS14<br/>[F0RU]</p> <p>DS5, DS7, DS8, DS11</p> <p>DS12 [S3 F2OEM],<br/>DS13 [S3 F3OEM],<br/>DS14 [F0RU]</p> | S | H | 5 | <p>DS5 [O2], DS7 [O2],<br/>DS8 [O1], DS12<br/>[S3 F3OEM], DS13<br/>[S3 F3OEM], DS14<br/>[F0RU]</p> <p>DS6&gt;DS7, DS12&gt;DS7,<br/>DS13, DS12, DS13,<br/>DS5, DS7, DS8, DS11</p> <p>DS14 [F0RU]</p> | V | SG | 1 |
| R86: T28 Spoofing oder Manipulation virtueller Sensordaten als MitM auf der VBUS-Verbindung zwischen Mission Control und Wahrnehmung Vorbereitung durch P5 Angriff auf mehr als eine Verbindung, um Sensorfusion (C3) oder Redundanzen (C4, C5) zu überwinden, P1 Erlangung physischen Zugriffs auf die Fahrzeugelektronik als Fahrzeugbesitzer/Tuner | <p>C6 Authentische Datenübertragung,<br/>C21 End-to-End-Signatur virtueller Sensordaten</p> <p>A2 Begrenzter Spielraum für Tuning-Angriffe</p>                                                                                                                                                                  | <p>DS5 [O2], DS7 [O2],<br/>DS8 [O1], DS12<br/>[S3 F3OEM], DS13<br/>[S3 F3OEM], DS14<br/>[F0RU]</p> <p>DS1, DS5, DS6, DS7,<br/>DS8, DS9, DS10, DS11,</p>                                    | S | M | 4 | <p>DS5 [O2], DS7 [O2],<br/>DS8 [O1], DS12<br/>[S3 F3OEM], DS13<br/>[S3 F3OEM], DS14<br/>[F0RU]</p> <p>DS12, DS13, DS1, DS5,<br/>DS6, DS7, DS8, DS9,</p>                                             |   | SG | 1 |

|                                                                                                                                                                                                                                                                                                                                                                |                                                                                                                                                                                                                |                                                                                                                                                                                         |   |   |   |                                                                                                                                                                                    |   |    |   |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|---|---|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|----|---|
|                                                                                                                                                                                                                                                                                                                                                                |                                                                                                                                                                                                                | DS12, DS14, DS15,<br>DS18<br>_____<br>DS13 [S3 F3OEM]                                                                                                                                   |   |   |   | DS10, DS11, DS12,<br>DS14, DS15, DS18<br>_____                                                                                                                                     |   |    |   |
| R87: T28 Spoofing oder Manipulation virtueller Sensordaten als MitM auf der VBUS-Verbindung zwischen Mission Control und Wahrnehmung Vorbereitung durch P5 Angriff auf mehr als eine Verbindung, um Sensorfusion (C3) oder Redundanzen (C4, C5) zu überwinden, P2 Erlangung physischen Zugriffs auf die Fahrzeugelektronik als externer Angreifer              | C6 Authentische Datenübertragung,<br>C21 End-to-End-Signatur virtueller Sensordaten<br>_____<br>A3 Qualitätsschäden werden im Falle eines kompromittierten Lkw selektiv berücksichtigt,<br>A6 Lokale Angreifer | DS5 [O2], DS7 [O2],<br>DS8 [O1], DS12<br>[S3 F3OEM], DS13<br>[S3 F3OEM], DS14<br>[F0RU]<br>_____<br>DS5, DS7, DS8, DS11,<br>DS6, DS12, DS13<br>_____<br>DS14 [F0RU]                     | V | M | 2 | DS5 [O2], DS7 [O2],<br>DS8 [O1], DS12<br>[S3 F3OEM], DS13<br>[S3 F3OEM], DS14<br>[F0RU]<br>_____<br>DS12, DS13, DS5, DS7,<br>DS8, DS11, DS6, DS12,<br>DS13<br>_____<br>DS14 [F0RU] | V | SG | 1 |
| R88: T28 Spoofing oder Manipulation virtueller Sensordaten als MitM auf der VBUS-Verbindung zwischen Mission Control und Perception Prep. durch P5 Angriff auf mehr als eine Verbindung, um Sensorfusion (C3) oder Redundanzen (C4, C5) zu überwinden, P4 Erlangung des Zugriffs auf einen Online-Fahrzeugbus durch Fernkompromittierung einer verbundenen ECU | C6 Authentische Datenübertragung,<br>C21 End-to-End-Signatur virtueller Sensordaten<br>_____<br>A3 Bei einem beschädigten Lkw werden Qualitätsschäden selektiv berücksichtigt                                  | DS5 [O2], DS7 [O2],<br>DS8 [O1], DS12<br>[S3 F3OEM], DS13<br>[S3 F3OEM], DS14<br>[F0RU]<br>_____<br>DS5, DS7, DS8, DS11<br>_____<br>DS12 [S3 F2OEM],<br>DS13 [S3 F3OEM],<br>DS14 [F0RU] | S | M | 4 | DS5 [O2], DS7 [O2],<br>DS8 [O1], DS12<br>[S3 F3OEM], DS13<br>[S3 F3OEM], DS14<br>[F0RU]<br>_____<br>DS12, DS13, DS5, DS7,<br>DS8, DS11<br>_____<br>DS14 [F0RU]                     | V | SG | 1 |
| R89: T29 Spoofing oder Manipulation Anfrage nach weiteren Umgebungsdaten als MitM auf der MCOM-Verbindung zwischen Control Center und Mission Control                                                                                                                                                                                                          | C2 mTLS zwischen Control Center und Mission Control                                                                                                                                                            | DS8 [O1]                                                                                                                                                                                | M | H | 3 | DS8 [O1]                                                                                                                                                                           | M | SG | 1 |



|                                                                                                                                                                                                                                                                            |                                                                                                             |                                                                                              |   |   |   |                                                                                              |   |    |   |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------|---|---|---|----------------------------------------------------------------------------------------------|---|----|---|
| R90: T30 Spoofing oder Manipulation Anfrage nach weiteren Umgebungsdaten als MitM auf der VBUS-Verbindung zwischen Mission Control und Wahrnehmung Vorbereitung durch P2 Erlangung physischen Zugriffs auf die Fahrzeugelektronik als externer Angreifer                   | A3 Qualitätsschäden werden im Falle eines kompromittierten Lkw selektiv berücksichtigt, A6 Lokale Angreifer | DS8 [O1]<br>_____<br>DS5, DS7, DS8, DS11,<br>DS6, DS12, DS13<br>_____                        |   | H | 1 | DS8 [O1]<br>_____<br>DS5, DS7, DS8, DS11,<br>DS6, DS12, DS13<br>_____                        |   | H  | 1 |
| R91: T30 Spoofing oder Manipulation von Anfragen nach weiteren Umgebungsdaten als MitM auf der VBUS-Verbindung zwischen Mission Control und Perception prep. durch P4 Erlangung des Zugriffs auf einen Online-Fahrzeugbus durch Fernkompromittierung einer verbundenen ECU | A3 Bei einem kompromittierten Lkw werden Qualitätsschäden selektiv berücksichtigt.                          | DS8 [O1]<br>_____<br>DS5, DS7, DS8, DS11<br>_____                                            |   | H | 1 | DS8 [O1]<br>_____<br>DS5, DS7, DS8, DS11<br>_____                                            |   | H  | 1 |
| R92: T31 Spoofing oder Manipulation weiterer Umgebungsdaten als MitM auf der VBUS-Verbindung zwischen Perception und Mission Control Vorbereitung durch P2 Erlangung physischen Zugriffs auf die Fahrzeugelektronik als externer Angreifer                                 | A3 Qualitätsschäden werden im Falle eines kompromittierten Lkw selektiv berücksichtigt, A6 Lokale Angreifer | DS5 [O2], DS7 [O2],<br>DS8 [O1]<br>_____<br>DS5, DS7, DS8, DS11,<br>DS6, DS12, DS13<br>_____ |   | H | 1 | DS5 [O2], DS7 [O2],<br>DS8 [O1]<br>_____<br>DS5, DS7, DS8, DS11,<br>DS6, DS12, DS13<br>_____ |   | H  | 1 |
| R93: T31 Spoofing oder Manipulation weiterer Umgebungsdaten als MitM auf der VBUS-Verbindung zwischen Wahrnehmung und Mission Control Vorbereitung durch P4 Erlangung des Zugriffs auf einen Online-Fahrzeugbus durch Fernkompromittierung einer verbundenen ECU           | A3 Bei einem kompromittierten Lkw werden Qualitätsschäden selektiv berücksichtigt.                          | DS5 [O2], DS7 [O2],<br>DS8 [O1]<br>_____<br>DS5, DS7, DS8, DS11<br>_____                     |   | H | 1 | DS5 [O2], DS7 [O2],<br>DS8 [O1]<br>_____<br>DS5, DS7, DS8, DS11<br>_____                     |   | H  | 1 |
| R94: T32 Spoofing oder Manipulation weiterer Umgebungsdaten als MitM auf der MCOM-Verbindung zwischen Mission Control und Control Center                                                                                                                                   | C2 mTLS zwischen Control Center und Mission Control                                                         | DS5 [O2], DS7 [O2],<br>DS8 [O1]<br>_____                                                     | E | H | 4 | DS5 [O2], DS7 [O2],<br>DS8 [O1]<br>_____                                                     | E | SG | 2 |
| R95: T33 Spoofing oder Manipulation der Eingaben des Basisfahrzeugs als MitM auf der VBUS-Verbindung                                                                                                                                                                       | C3 Validierung von Sensordaten durch Sensorfusion,                                                          | DS5 [O2], DS6<br>[S3 F2OEM], DS7 [O2],<br>_____                                              |   | H | 1 | DS5 [O2], DS6<br>[S3 F2OEM], DS7 [O2],<br>_____                                              |   | H  | 1 |

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |                                                                                                                                                                                                       |                                                                                                                                 |   |   |   |                                                                                                                       |  |    |   |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------|---|---|---|-----------------------------------------------------------------------------------------------------------------------|--|----|---|
| zwischen der Überwachung des Basisfahrzeugs und der Wahrnehmung, vorbereitet durch P2 Erlangung physischen Zugriffs auf die Fahrzeugelektronik als externer Angreifer                                                                                                                                                                                                                                                                                                                                    | C5 Redundanz gegen Aktivierung von ADS außerhalb von ODD<br><br>A3 Qualitätsschäden werden im Falle eines kompromittierten Lkw selektiv berücksichtigt, A6 Lokale Angreifer                           | DS8 [O1], DS12 [S3 F3OEM]<br><br>DS5, DS7, DS8, DS11, DS6, DS12, DS13                                                           |   |   |   | DS8 [O1], DS12 [S3 F3OEM]<br><br>DS6>DS7, DS12>DS7, DS13, DS5, DS7, DS8, DS11, DS6, DS12, DS13                        |  |    |   |
| R96: T33 Spoofing oder Manipulation der Eingaben des Basisfahrzeugs als MitM auf der VBUS-Verbindung zwischen der Überwachung des Basisfahrzeugs und der Wahrnehmung, vorbereitet durch P4 Erlangung des Zugriffs auf einen Online-Fahrzeugbus durch Fernkompromittierung einer verbundenen ECU                                                                                                                                                                                                          | C3 Validierung von Sensordaten durch Sensorfusion, C5 Redundanz gegen Aktivierung von ADS außerhalb von ODD<br><br>A3 Qualitätsschäden werden im Falle eines beschädigten Lkw selektiv berücksichtigt | DS5 [O2], DS6 [S3 F2OEM], DS7 [O2], DS8 [O1], DS12 [S3 F3OEM]<br><br>DS5, DS7, DS8, DS11<br><br>DS6 [S3 F2OEM], DS12 [S3 F2OEM] | S | H | 5 | DS5 [O2], DS6 [S3 F2OEM], DS7 [O2], DS8 [O1], DS12 [S3 F3OEM]<br><br>DS6>DS7, DS12>DS7, DS13, DS5, DS7, DS8, DS11     |  | H  | 1 |
| R97: T33 Spoofing oder Manipulation der Eingaben des Basisfahrzeugs als MitM auf der VBUS-Verbindung zwischen Basisfahrzeugüberwachung und Wahrnehmung, vorbereitet durch P5 Angriff auf mehr als eine Verbindung, um die Sensorfusion (C3) oder Redundanzen (C4, C5) zu überwinden, T28 Spoofing oder Manipulation virtueller Sensordaten als MitM auf der VBUS-Verbindung zwischen Mission Control und Wahrnehmung, P2 Erlangung physischen Zugriffs auf die Fahrzeugelektronik als externer Angreifer | C6 Authentische Datenübertragung, C21 End-to-End-Signatur virtueller Sensordaten<br><br>A3 Qualitätsschäden werden im Falle eines kompromittierten Lkw selektiv berücksichtigt, A6 Lokale Angreifer   | DS5 [O2], DS6 [S3 F2OEM], DS7 [O2], DS8 [O1], DS12 [S3 F3OEM]<br><br>DS5, DS7, DS8, DS11, DS6, DS12, DS13                       |   | M | 1 | DS5 [O2], DS6 [S3 F2OEM], DS7 [O2], DS8 [O1], DS12 [S3 F3OEM]<br><br>DS12, DS13, DS5, DS7, DS8, DS11, DS6, DS12, DS13 |  | SG | 1 |

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                                                                                                                                                                                           |                                                                                                                                                                                                               |   |   |   |                                                                                                                                                                                                               |   |    |   |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|---|---|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|----|---|
| <p>R98: T33 Spoofing oder Manipulation der Basisfahrzeug-Eingabe als MitM auf der VBUS-Verbindung zwischen Basisfahrzeugüberwachung und Wahrnehmung Vorbereitung durch P5 Angriff auf mehr als eine Verbindung, um die Sensorfusion (C3) oder Redundanzen (C4, C5) zu überwinden,</p> <p>T28 Spoofing oder Manipulation virtueller Sensordaten als MitM auf der VBUS-Verbindung zwischen Mission Control und Wahrnehmung,</p> <p>P4 Zugriff auf einen Online-Fahrzeugbus durch Fernkompromittierung einer verbundenen ECU</p> | <p>C6 Authentische Datenübertragung,</p> <p>C21 End-to-End-Signatur virtueller Sensordaten</p> <hr/> <p>A3 Bei einem beschädigten Lkw werden Qualitätsschäden selektiv berücksichtigt</p> | <p>DS5 [O2], DS6 [S3 F2OEM], DS7 [O2], DS8 [O1], DS12 [S3 F3OEM]</p> <hr/> <p>DS5, DS7, DS8, DS11</p> <hr/> <p>DS6 [S3 F2OEM], DS12 [S3 F2OEM]</p>                                                            | S | M | 4 | <p>DS5 [O2], DS6 [S3 F2OEM], DS7 [O2], DS8 [O1], DS12 [S3 F3OEM]</p> <hr/> <p>DS12, DS13, DS5, DS7, DS8, DS11</p> <hr/> <p>DS6 [S3 F2OEM]</p>                                                                 | S | SG | 2 |
| <p>R99: T34 Spoofing oder Manipulation von fusionierten Sensordaten als MitM auf der IPC-Verbindung zwischen Wahrnehmung und Prädiktion, vorbereitet durch P1 Erlangung physischen Zugriffs auf die Fahrzeugelektronik als Fahrzeugbesitzer/Tuner</p> <p>Hinweis: Die Manipulation der zwischen den zentralen ADS-Komponenten ausgetauschten Daten erfordert einen erhöhten Aufwand, da die interne Kommunikation der ECU angegriffen werden muss.</p>                                                                        | <p>C6 Authentische Übertragung von Daten</p> <hr/> <p>A2 Begrenzter Spielraum für Tuning-Angriffe</p>                                                                                     | <p>DS5 [O2], DS6 [S3 F2OEM], DS7 [O2], DS8 [O1], DS12 [S3 F3OEM], DS13 [S3 F3OEM], DS14 [F0RU]</p> <hr/> <p>DS1, DS5, DS6, DS7, DS8, DS9, DS10, DS11, DS12, DS14, DS15, DS18</p> <hr/> <p>DS13 [S3 F3OEM]</p> | S | M | 4 | <p>DS5 [O2], DS6 [S3 F2OEM], DS7 [O2], DS8 [O1], DS12 [S3 F3OEM], DS13 [S3 F3OEM], DS14 [F0RU]</p> <hr/> <p>DS1, DS5, DS6, DS7, DS8, DS9, DS10, DS11, DS12, DS14, DS15, DS18</p> <hr/> <p>DS13 [S3 F3OEM]</p> | S | SG | 2 |
| <p>R100: T34 Spoofing oder Manipulation von Fused-Sensordaten als MitM auf der IPC-Verbindung zwischen Wahrnehmung und Prädiktion, vorbereitet durch P2 Erlangung physischen Zugriffs auf die Fahrzeugelektronik als externer Angreifer</p>                                                                                                                                                                                                                                                                                   | <p>C6 Authentische Datenübertragung</p> <hr/> <p>A3 Qualitätsschäden werden im Falle eines</p>                                                                                            | <p>DS5 [O2], DS6 [S3 F2OEM], DS7 [O2], DS8 [O1], DS12 [S3 F3OEM], DS13 [S3 F3OEM], DS14</p>                                                                                                                   | V | M | 2 | <p>DS5 [O2], DS6 [S3 F2OEM], DS7 [O2], DS8 [O1], DS12 [S3 F3OEM], DS13 [S3 F3OEM], DS14</p>                                                                                                                   | V | SG | 1 |

|                                                                                                                                                                                                                                                                                                                                                                                                                                                             |                                                                                                                                                              |                                                                                                                                                                                                       |   |   |   |                                                                                                                                                                                                       |   |    |   |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|---|---|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|----|---|
| Hinweis: Die Manipulation der zwischen den zentralen ADS-Komponenten ausgetauschten Daten erfordert einen erhöhten Aufwand, da die interne Kommunikation der ECU angegriffen werden muss.                                                                                                                                                                                                                                                                   | kompromittierten Lkw selektiv berücksichtigt.<br>A6 Lokale Angreifer                                                                                         | [F0RU]<br>_____<br>DS5, DS7, DS8, DS11,<br>DS6, DS12, DS13<br>_____<br>DS14 [F0RU]                                                                                                                    |   |   |   | [F0RU]<br>_____<br>DS5, DS7, DS8, DS11,<br>DS6, DS12, DS13<br>_____<br>DS14 [F0RU]                                                                                                                    |   |    |   |
| R101: T34 Spoofing oder Manipulation von Fused-Sensordaten als MitM auf der IPC-Verbindung zwischen Wahrnehmung und Prädiktion Vorbereitung durch P3 Erlangung des Zugriffs auf einen Offline-Fahrzeugbus durch Fernkompromittierung einer verbundenen ECU<br><br>Hinweis: Die Manipulation der zwischen den zentralen ADS-Komponenten ausgetauschten Daten erfordert einen erhöhten Aufwand, da die interne Kommunikation der ECU angegriffen werden muss. | C6 Authentische Übertragung von Daten<br>_____<br>A3 Qualitätsschäden werden im Falle eines kompromittierten Lkw selektiv berücksichtigt, A5 Domänentrennung | DS5 [O2], DS6 [S3 F2OEM], DS7 [O2], DS8 [O1], DS12 [S3 F3OEM], DS13 [S3 F3OEM], DS14 [F0RU]<br>_____<br>DS5, DS7, DS8, DS11<br>_____<br>DS6 [S3 F2OEM], DS12 [S3 F2OEM], DS13 [S3 F3OEM], DS14 [F0RU] | S | M | 1 | DS5 [O2], DS6 [S3 F2OEM], DS7 [O2], DS8 [O1], DS12 [S3 F3OEM], DS13 [S3 F3OEM], DS14 [F0RU]<br>_____<br>DS5, DS7, DS8, DS11<br>_____<br>DS6 [S3 F2OEM], DS12 [S3 F2OEM], DS13 [S3 F3OEM], DS14 [F0RU] | S | SG | 1 |
| R102: T35 Spoofing oder Manipulation des Navigationsziels als MitM auf der MCOM-Verbindung zwischen Control Center und Mission Control                                                                                                                                                                                                                                                                                                                      | C2 mTLS zwischen Control Center und Mission Control                                                                                                          | DS5 [O2], DS14 [F0RU]                                                                                                                                                                                 | E | H | 4 | DS5 [O2], DS14 [F0RU]                                                                                                                                                                                 | E | SG | 2 |
| R103: T36 Spoofing oder Manipulation des Navigationsziels als MitM auf der VBUS-Verbindung zwischen Mission Control und Planungsvorbereitung durch P2 Erlangung physischen Zugriffs auf die Fahrzeugelektronik als externer Angreifer                                                                                                                                                                                                                       | C6 Authentische Datenübertragung<br>_____<br>A3 Qualitätsschäden werden im Falle eines kompromittierten Lkw selektiv berücksichtigt. A6 Lokale Angreifer     | DS5 [O2], DS14 [F0RU]<br>_____<br>DS5, DS7, DS8, DS11,<br>DS6, DS12, DS13<br>_____<br>DS14 [F0RU]                                                                                                     | V | H | 2 | DS5 [O2], DS14 [F0RU]<br>_____<br>DS5, DS7, DS8, DS11,<br>DS6, DS12, DS13<br>_____<br>DS14 [F0RU]                                                                                                     | V | SG | 1 |

|                                                                                                                                                                                                                                                                                                                                                                                                                                         |                                                                                                                                                                   |                                                                                                                                                                                                   |   |   |   |                                                                                                                                                                                                   |   |    |   |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|---|---|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|----|---|
| <p>R104: T36 Spoofing oder Manipulation des Navigationsziels als MitM auf der VBUS-Verbindung zwischen Mission Control und Planungsvorbereitung durch P4 Erlangung des Zugriffs auf einen Online-Fahrzeugbus durch Fernkompromittierung einer angeschlossenen ECU</p>                                                                                                                                                                   | <p>C6 Authentische Übertragung von Daten</p> <p>A3 Bei einem beschädigten Lkw werden Qualitätsschäden selektiv berücksichtigt.</p>                                | <p>DS5 [O2], DS14 [F0RU]</p> <p>DS5, DS7, DS8, DS11</p> <p>DS14 [F0RU]</p>                                                                                                                        | V | H | 2 | <p>DS5 [O2], DS14 [F0RU]</p> <p>DS5, DS7, DS8, DS11</p> <p>DS14 [F0RU]</p>                                                                                                                        | V | SG | 1 |
| <p>R105: T37 Spoofing oder Manipulation von Objektbahnen als MitM auf der IPC-Verbindung zwischen Prädiktion und Planung Vorbereitung durch P1 Erlangung physischen Zugriffs auf die Fahrzeugelektronik als Fahrzeugbesitzer/Tuner</p> <p>Hinweis: Die Manipulation der zwischen den zentralen ADS-Komponenten ausgetauschten Daten erfordert einen erhöhten Aufwand, da die interne Kommunikation der ECU angegriffen werden muss.</p> | <p>C6 Authentische Übertragung von Daten</p> <p>A2 Begrenzter Spielraum für Tuning-Angriffe</p>                                                                   | <p>DS5 [O2], DS6 [S3 F2OEM], DS7 [O2], DS8 [O1], DS12 [S3 F3OEM], DS13 [S3 F3OEM], DS14 [F0RU]</p> <p>DS1, DS5, DS6, DS7, DS8, DS9, DS10, DS11, DS12, DS14, DS15, DS18</p> <p>DS13 [S3 F3OEM]</p> | S | M | 4 | <p>DS5 [O2], DS6 [S3 F2OEM], DS7 [O2], DS8 [O1], DS12 [S3 F3OEM], DS13 [S3 F3OEM], DS14 [F0RU]</p> <p>DS1, DS5, DS6, DS7, DS8, DS9, DS10, DS11, DS12, DS14, DS15, DS18</p> <p>DS13 [S3 F3OEM]</p> | S | SG | 2 |
| <p>R106: T37 Spoofing oder Manipulation von Objektbahnen als MitM auf der IPC-Verbindung zwischen Prädiktion und Planungsvorbereitung durch P2 Erlangung physischen Zugriffs auf die Fahrzeugelektronik als externer Angreifer</p> <p>Hinweis: Die Manipulation der zwischen den zentralen ADS-Komponenten ausgetauschten Daten erfordert einen erhöhten Aufwand, da die interne Kommunikation der ECU angegriffen werden muss.</p>     | <p>C6 Authentische Datenübertragung</p> <p>A3 Qualitätsschäden werden im Falle eines kompromittierten Lkw selektiv berücksichtigt.</p> <p>A6 Lokale Angreifer</p> | <p>DS5 [O2], DS6 [S3 F2OEM], DS7 [O2], DS8 [O1], DS12 [S3 F3OEM], DS13 [S3 F3OEM], DS14 [F0RU]</p> <p>DS5, DS7, DS8, DS11, DS6, DS12, DS13</p>                                                    | V | M | 2 | <p>DS5 [O2], DS6 [S3 F2OEM], DS7 [O2], DS8 [O1], DS12 [S3 F3OEM], DS13 [S3 F3OEM], DS14 [F0RU]</p> <p>DS5, DS7, DS8, DS11, DS6, DS12, DS13</p>                                                    | V | SG | 1 |

|                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                                                                                                                                                                | DS14 [F0RU]                                                                                                                                                                                        |   |   |   | DS14 [F0RU]                                                                                                                                                                                        |   |    |   |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|---|---|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|----|---|
| <p>R107: T37 Spoofing oder Manipulation von Objektbahnen als MitM auf der IPC-Verbindung zwischen Prädiktion und Planung, vorbereitet durch P3 Erlangung des Zugriffs auf einen Offline-Fahrzeugbus durch Fernkompromittierung einer verbundenen ECU</p> <p>Hinweis: Die Manipulation der zwischen den zentralen ADS-Komponenten ausgetauschten Daten erfordert einen erhöhten Aufwand, da die interne Kommunikation der ECU angegriffen werden muss.</p> | <p>C6 Authentische Übertragung von Daten</p> <p>A3 Qualitätsschäden werden im Falle eines kompromittierten Lkw selektiv berücksichtigt, A5 Domänentrennung</p> | <p>DS5 [O2], DS6 [S3 F2OEM], DS7 [O2], DS8 [O1], DS12 [S3 F3OEM], DS13 [S3 F3OEM], DS14 [F0RU]</p> <p>DS5, DS7, DS8, DS11</p> <p>DS6 [S3 F2OEM], DS12 [S3 F2OEM], DS13 [S3 F3OEM], DS14 [F0RU]</p> | S | M | 1 | <p>DS5 [O2], DS6 [S3 F2OEM], DS7 [O2], DS8 [O1], DS12 [S3 F3OEM], DS13 [S3 F3OEM], DS14 [F0RU]</p> <p>DS5, DS7, DS8, DS11</p> <p>DS6 [S3 F2OEM], DS12 [S3 F2OEM], DS13 [S3 F3OEM], DS14 [F0RU]</p> | S | SG | 1 |
| <p>R108: T38 Spoofing oder Manipulation von fusionierten Sensordaten als MitM auf der IPC-Verbindung zwischen Wahrnehmung und Planung Vorbereitung durch P1 Erlangung physischen Zugriffs auf die Fahrzeugelektronik als Fahrzeugbesitzer/Tuner</p> <p>Hinweis: Die Manipulation der zwischen den zentralen ADS-Komponenten ausgetauschten Daten erfordert einen erhöhten Aufwand, da die interne Kommunikation der ECU angegriffen werden muss.</p>      | <p>C6 Authentische Übertragung von Daten</p> <p>A2 Begrenzter Spielraum für Tuning-Angriffe</p>                                                                | <p>DS5 [O2], DS6 [S3 F2OEM], DS7 [O2], DS8 [O1], DS12 [S3 F3OEM], DS13 [S3 F3OEM], DS14 [F0RU]</p> <p>DS1, DS5, DS6, DS7, DS8, DS9, DS10, DS11, DS12, DS14, DS15, DS18</p> <p>DS13 [S3 F3OEM]</p>  | S | M | 4 | <p>DS5 [O2], DS6 [S3 F2OEM], DS7 [O2], DS8 [O1], DS12 [S3 F3OEM], DS13 [S3 F3OEM], DS14 [F0RU]</p> <p>DS1, DS5, DS6, DS7, DS8, DS9, DS10, DS11, DS12, DS14, DS15, DS18</p> <p>DS13 [S3 F3OEM]</p>  | S | SG | 2 |

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                                                                                                                                                                       |                                                                                                                                                                                                    |   |   |   |                                                                                                                                                                                                    |   |    |   |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|---|---|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|----|---|
| <p>R109: T38 Spoofing oder Manipulation von Fused-Sensordaten als MitM auf der IPC-Verbindung zwischen Wahrnehmung und Planung, vorbereitet durch P2 Erlangung physischen Zugriffs auf die Fahrzeugelektronik als externer Angreifer</p> <p>Hinweis: Die Manipulation der zwischen den zentralen ADS-Komponenten ausgetauschten Daten erfordert einen erhöhten Aufwand, da die interne Kommunikation der ECU angegriffen werden muss.</p>                       | <p>C6 Authentische Datenübertragung</p> <p>A3 Qualitätsschäden werden im Falle eines kompromittierten Lkw selektiv berücksichtigt.</p> <p>A6 Lokale Angreifer</p>     | <p>DS5 [O2], DS6 [S3 F2OEM], DS7 [O2], DS8 [O1], DS12 [S3 F3OEM], DS13 [S3 F3OEM], DS14 [F0RU]</p> <p>DS5, DS7, DS8, DS11, DS6, DS12, DS13</p> <p>DS14 [F0RU]</p>                                  | V | M | 2 | <p>DS5 [O2], DS6 [S3 F2OEM], DS7 [O2], DS8 [O1], DS12 [S3 F3OEM], DS13 [S3 F3OEM], DS14 [F0RU]</p> <p>DS5, DS7, DS8, DS11, DS6, DS12, DS13</p> <p>DS14 [F0RU]</p>                                  | V | SG | 1 |
| <p>R110: T38 Spoofing oder Manipulation von Fused-Sensordaten als MitM auf der IPC-Verbindung zwischen Wahrnehmung und Planung Vorbereitung durch P3 Erlangung des Zugriffs auf einen Offline-Fahrzeugbus durch Fernkompromittierung einer verbundenen ECU</p> <p>Hinweis: Die Manipulation der zwischen den zentralen ADS-Komponenten ausgetauschten Daten erfordert einen erhöhten Aufwand, da die interne Kommunikation der ECU angegriffen werden muss.</p> | <p>C6 Authentische Übertragung von Daten</p> <p>A3 Qualitätsschäden werden im Falle eines kompromittierten Lkw selektiv berücksichtigt,</p> <p>A5 Domänentrennung</p> | <p>DS5 [O2], DS6 [S3 F2OEM], DS7 [O2], DS8 [O1], DS12 [S3 F3OEM], DS13 [S3 F3OEM], DS14 [F0RU]</p> <p>DS5, DS7, DS8, DS11</p> <p>DS6 [S3 F2OEM], DS12 [S3 F2OEM], DS13 [S3 F3OEM], DS14 [F0RU]</p> | S | M | 1 | <p>DS5 [O2], DS6 [S3 F2OEM], DS7 [O2], DS8 [O1], DS12 [S3 F3OEM], DS13 [S3 F3OEM], DS14 [F0RU]</p> <p>DS5, DS7, DS8, DS11</p> <p>DS6 [S3 F2OEM], DS12 [S3 F2OEM], DS13 [S3 F3OEM], DS14 [F0RU]</p> | S | SG | 1 |
| <p>R111: T39 Spoofing oder Manipulation der geplanten Trajektorie als MitM auf der IPC-Verbindung zwischen Planung und Steuerung oder zwischen Planung und Prädiktion Vorbereitung durch P1 Erlangung physischen</p>                                                                                                                                                                                                                                            | <p>C6 Authentische Übertragung von Daten</p> <p>A2 Begrenzter Spielraum für Tuning-Angriffe</p>                                                                       | <p>DS5 [O2], DS6 [S3 F2OEM], DS7 [O2], DS8 [O1], DS12 [S3 F3OEM], DS13 [S3 F3OEM], DS14</p>                                                                                                        | S | M | 4 | <p>DS5 [O2], DS6 [S3 F2OEM], DS7 [O2], DS8 [O1], DS12 [S3 F3OEM], DS13 [S3 F3OEM], DS14</p>                                                                                                        | S | SG | 2 |



|                                                                                                                                                                                                                                                                                               |                                                                                                                                                         |                                                                                             |   |   |   |                                                                                             |   |    |   |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------|---|---|---|---------------------------------------------------------------------------------------------|---|----|---|
| Zugriffs auf die Fahrzeugelektronik als Fahrzeugbesitzer/Tuner                                                                                                                                                                                                                                |                                                                                                                                                         | [F0RU]                                                                                      |   |   |   | [F0RU]                                                                                      |   |    |   |
| Hinweis: Die Manipulation der zwischen den zentralen ADS-Komponenten ausgetauschten Daten erfordert einen erhöhten Aufwand, da die interne Kommunikation der ECU angegriffen werden muss.                                                                                                     |                                                                                                                                                         | DS1, DS5, DS6, DS7, DS8, DS9, DS10, DS11, DS12, DS14, DS15, DS18                            |   |   |   | DS1, DS5, DS6, DS7, DS8, DS9, DS10, DS11, DS12, DS14, DS15, DS18                            |   |    |   |
|                                                                                                                                                                                                                                                                                               |                                                                                                                                                         | DS13 [S3 F3OEM]                                                                             |   |   |   | DS13 [S3 F3OEM]                                                                             |   |    |   |
| R112: T39 Spoofing oder Manipulation der geplanten Trajektorie als MitM auf der IPC-Verbindung zwischen Planung und Steuerung oder zwischen Planung und Prädiktion, vorbereitet durch P2 Erlangung physischen Zugriffs auf die Fahrzeugelektronik als externer Angreifer                      | C6 Authentische Datenübertragung<br><br>A3 Qualitätsschäden werden im Falle eines kompromittierten Lkw selektiv berücksichtigt.<br>A6 Lokale Angreifer  | DS5 [O2], DS6 [S3 F2OEM], DS7 [O2], DS8 [O1], DS12 [S3 F3OEM], DS13 [S3 F3OEM], DS14 [F0RU] | V | M | 2 | DS5 [O2], DS6 [S3 F2OEM], DS7 [O2], DS8 [O1], DS12 [S3 F3OEM], DS13 [S3 F3OEM], DS14 [F0RU] | V | SG | 1 |
| Hinweis: Die Manipulation der zwischen den zentralen ADS-Komponenten ausgetauschten Daten erfordert einen erhöhten Aufwand, da die interne Kommunikation der ECU angegriffen werden muss.                                                                                                     |                                                                                                                                                         | DS5, DS7, DS8, DS11, DS6, DS12, DS13                                                        |   |   |   | DS5, DS7, DS8, DS11, DS6, DS12, DS13                                                        |   |    |   |
|                                                                                                                                                                                                                                                                                               |                                                                                                                                                         | DS14 [F0RU]                                                                                 |   |   |   | DS14 [F0RU]                                                                                 |   |    |   |
| R113: T39 Spoofing oder Manipulation der geplanten Trajektorie als MitM auf der IPC-Verbindung zwischen Planung und Steuerung oder zwischen Planung und Prädiktionvorbereitung durch P3 Erlangung des Zugriffs auf einen Offline-Fahrzeugbus durch Fernkompromittierung einer verbundenen ECU | C6 Authentische Übertragung von Daten<br><br>A3 Qualitätsschäden werden im Falle eines kompromittierten Lkw selektiv berücksichtigt, A5 Domänentrennung | DS5 [O2], DS6 [S3 F2OEM], DS7 [O2], DS8 [O1], DS12 [S3 F3OEM], DS13 [S3 F3OEM], DS14 [F0RU] | S | M | 1 | DS5 [O2], DS6 [S3 F2OEM], DS7 [O2], DS8 [O1], DS12 [S3 F3OEM], DS13 [S3 F3OEM], DS14 [F0RU] | S | SG | 1 |
| Hinweis: Die Manipulation der zwischen den zentralen ADS-Komponenten ausgetauschten Daten erfordert                                                                                                                                                                                           |                                                                                                                                                         | DS5, DS7, DS8, DS11                                                                         |   |   |   | DS5, DS7, DS8, DS11                                                                         |   |    |   |
|                                                                                                                                                                                                                                                                                               |                                                                                                                                                         | DS6 [S3 F2OEM], DS12                                                                        |   |   |   | DS6 [S3 F2OEM], DS12                                                                        |   |    |   |

|                                                                                                                                                                                                                                                                                                                                                                                                                                                            |                                                                                                             |                                                                                                     |   |   |   |                                                                                                     |   |    |   |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------|---|---|---|-----------------------------------------------------------------------------------------------------|---|----|---|
| einen erhöhten Aufwand, da die interne Kommunikation der ECU angegriffen werden muss.                                                                                                                                                                                                                                                                                                                                                                      |                                                                                                             | [S3 F2OEM], DS13<br>[S3 F3OEM], DS14<br>[F0RU]                                                      |   |   |   | [S3 F2OEM], DS13<br>[S3 F3OEM], DS14<br>[F0RU]                                                      |   |    |   |
| R114: T40 Spoofing oder Manipulation der dynamischen Anpassung als MitM auf der IPC-Verbindung zwischen Steuerung und Planung Vorbereitung durch P2 Erlangung physischen Zugriffs auf die Fahrzeugelektronik als externer Angreifer<br><br>Hinweis: Die Manipulation der zwischen den zentralen ADS-Komponenten ausgetauschten Daten erfordert einen erhöhten Aufwand, da die interne Kommunikation der ECU angegriffen werden muss.                       | A3 Qualitätsschäden werden im Falle eines kompromittierten Lkw selektiv berücksichtigt, A6 Lokale Angreifer | DS7 [O2], DS8 [O1],<br>DS12 [S3 F3OEM]<br>_____<br>DS5, DS7, DS8, DS11,<br>DS6, DS12, DS13<br>_____ |   | M | 1 | DS7 [O2], DS8 [O1],<br>DS12 [S3 F3OEM]<br>_____<br>DS5, DS7, DS8, DS11,<br>DS6, DS12, DS13<br>_____ |   | M  | 1 |
| R115: T40 Spoofing oder Manipulation der dynamischen Anpassung als MitM auf der IPC-Verbindung zwischen Steuerung und Planung Vorbereitung durch P3 Erlangung des Zugriffs auf einen Offline-Fahrzeugbus durch Fernkompromittierung einer verbundenen ECU<br><br>Hinweis: Die Manipulation der zwischen den zentralen ADS-Komponenten ausgetauschten Daten erfordert einen erhöhten Aufwand, da die interne Kommunikation der ECU angegriffen werden muss. | A3 Qualitätsmängel werden im Falle eines kompromittierten Lkw selektiv berücksichtigt. A5 Domänentrennung   | DS7 [O2], DS8 [O1],<br>DS12 [S3 F3OEM]<br>_____<br>DS5, DS7, DS8, DS11<br>_____<br>DS12 [S3 F2OEM]  | S | M | 1 | DS7 [O2], DS8 [O1],<br>DS12 [S3 F3OEM]<br>_____<br>DS5, DS7, DS8, DS11<br>_____<br>DS12 [S3 F2OEM]  | S | M  | 1 |
| R116: T41 Spoofing oder Manipulation des zu genehmigenden Flugplans als MitM auf der VBUS-Verbindung zwischen Planung und Mission Control Vorbereitung durch P1 Erlangung physischen Zugriffs auf die Fahrzeugelektronik als Fahrzeugbesitzer/Tuner                                                                                                                                                                                                        | C6 Authentische Datenübertragung, C20 Überprüfung der genehmigten Trajektorie<br>_____                      | DS5 [O2], DS7 [O2],<br>DS8 [O1], DS12<br>[S3 F3OEM], DS14<br>[F0RU]<br>_____                        |   | H | 1 | DS5 [O2], DS7 [O2],<br>DS8 [O1], DS12<br>[S3 F3OEM], DS14<br>[F0RU]<br>_____                        |   | SG | 1 |

|                                                                                                                                                                                                                                                                                        |                                                                                                                                                                                                        |                                                                                                                           |   |   |   |                                                                                                                                 |   |    |   |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------|---|---|---|---------------------------------------------------------------------------------------------------------------------------------|---|----|---|
|                                                                                                                                                                                                                                                                                        | A2 Begrenzter Spielraum für Tuning-Angriffe                                                                                                                                                            | DS1, DS5, DS6, DS7, DS8, DS9, DS10, DS11, DS12, DS14, DS15, DS18                                                          |   |   |   | DS12, DS1, DS5, DS6, DS7, DS8, DS9, DS10, DS11, DS12, DS14, DS15, DS18                                                          |   |    |   |
| R117: T41 Spoofing oder Manipulation Vorschlag für eine zu genehmigende Trajektorie als MitM auf der VBUS-Verbindung zwischen Planung und Mission Control, vorbereitet von P2 Erlangung physischen Zugriffs auf die Fahrzeugelektronik als externer Angreifer                          | C6 Authentische Datenübertragung,<br>C20 Überprüfung der genehmigten Trajektorie<br><br>A3 Qualitätsschäden werden im Falle eines kompromittierten Lkw selektiv berücksichtigt,<br>A6 Lokale Angreifer | DS5 [O2], DS7 [O2], DS8 [O1], DS12 [S3 F3OEM], DS14 [F0RU]<br><br>DS5, DS7, DS8, DS11, DS6, DS12, DS13<br><br>DS14 [F0RU] | V | H | 2 | DS5 [O2], DS7 [O2], DS8 [O1], DS12 [S3 F3OEM], DS14 [F0RU]<br><br>DS12, DS5, DS7, DS8, DS11, DS6, DS12, DS13<br><br>DS14 [F0RU] | V | SG | 1 |
| R118: T41 Spoofing oder Manipulation Vorschlag für eine zu genehmigende Trajektorie als MitM auf der VBUS-Verbindung zwischen Planung und Mission Control, vorbereitet von P4 Erlangung des Zugriffs auf einen Online-Fahrzeugbus durch Fernkompromittierung einer angeschlossenen ECU | C6 Authentische Datenübertragung,<br>C20 Überprüfung der genehmigten Trajektorie<br><br>A3 Qualitätsschäden werden im Falle eines kompromittierten Lkw selektiv berücksichtigt                         | DS5 [O2], DS7 [O2], DS8 [O1], DS12 [S3 F3OEM], DS14 [F0RU]<br><br>DS5, DS7, DS8, DS11<br><br>DS12 [S3 F2OEM], DS14 [F0RU] | S | H | 5 | DS5 [O2], DS7 [O2], DS8 [O1], DS12 [S3 F3OEM], DS14 [F0RU]<br><br>DS12, DS5, DS7, DS8, DS11<br><br>DS14 [F0RU]                  | V | SG | 1 |
| R119: T42 Spoofing oder Manipulation Vorschlag für eine zu genehmigende Trajektorie als MitM auf der MCOM-Verbindung zwischen Mission Control und Control Center                                                                                                                       | C2 mTLS zwischen Control Center und Mission Control,<br>C20 Überprüfung der genehmigten Trajektorie                                                                                                    | DS5 [O2], DS7 [O2], DS8 [O1], DS12 [S3 F2OEM], DS14 [F0RU]                                                                | S | H | 5 | DS5 [O2], DS7 [O2], DS8 [O1], DS12 [S3 F3OEM], DS14 [F0RU]<br><br>DS12                                                          | E | SG | 2 |

|                                                                                                                                                                                                                                                                                            |                                                                                                                                                              |                                                                                                            |   |   |   |                                                                                                            |   |    |   |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------|---|---|---|------------------------------------------------------------------------------------------------------------|---|----|---|
|                                                                                                                                                                                                                                                                                            |                                                                                                                                                              |                                                                                                            |   |   |   | DS5 [O2], DS7 [O2],<br>DS8 [O1], DS14 [F0RU]                                                               |   |    |   |
| R120: T43 Spoofing oder Manipulation der Genehmigung der zu genehmigenden Trajektorie als MitM auf der MCOM-Verbindung zwischen Control Center und Mission Control                                                                                                                         | C2 mTLS zwischen Control Center und Mission Control, C20 Überprüfung der genehmigten Trajektorie                                                             | DS5 [O2], DS8 [O1]                                                                                         | E | H | 4 | DS5 [O2], DS8 [O1]<br><br>DS12<br><br>DS5 [O2], DS8 [O1]                                                   | E | SG | 2 |
| R121: T44 Spoofing oder Manipulation der Genehmigung der zu genehmigenden Trajektorie als MitM auf der VBUS-Verbindung zwischen Mission Control und Planungsvorbereitung durch P2 Erlangung physischen Zugriffs auf die Fahrzeugelektronik als externer Angreifer                          | C20 Überprüfung der genehmigten Trajektorie<br><br>A3 Bei einem kompromittierten Lkw werden Qualitätsschäden selektiv berücksichtigt.<br>A6 Lokale Angreifer | DS5 [O2], DS8 [O1]<br><br>DS5, DS7, DS8, DS11,<br>DS6, DS12, DS13                                          |   | H | 1 | DS5 [O2], DS8 [O1]<br><br>DS12, DS5, DS7, DS8,<br>DS11, DS6, DS12, DS13                                    |   | H  | 1 |
| R122: T44 Spoofing oder Manipulation der Genehmigung der zu genehmigenden Trajektorie als MitM auf der VBUS-Verbindung zwischen Mission Control und Planungsvorbereitung durch P4 Erlangung des Zugriffs auf einen Online-Fahrzeugbus durch Fernkompromittierung einer angeschlossenen ECU | C20 Überprüfung der genehmigten Trajektorie<br><br>A3 Bei einem beschädigten Lkw werden Qualitätsschäden selektiv berücksichtigt.                            | DS5 [O2], DS8 [O1]<br><br>DS5, DS7, DS8, DS11                                                              |   | H | 1 | DS5 [O2], DS8 [O1]<br><br>DS12, DS5, DS7, DS8,<br>DS11                                                     |   | H  | 1 |
| R123: T45 Spoofing oder Manipulation der Basisfahrzeugleistung als MitM auf der VBUS-Verbindung zwischen Steuerung und Aktoren Vorbereitung durch P1 Erlangung physischen Zugriffs auf die Fahrzeugelektronik als Fahrzeugbesitzer/Tuner                                                   | C6 Authentische Datenübertragung<br><br>A11 Risiko unabhängig von ADS,<br>A2 Begrenzter Spielraum für Tuning-Angriffe                                        | DS5 [O2], DS6<br>[S3 F2OEM], DS7 [O2],<br>DS8 [O1], DS12<br>[S3 F3OEM], DS13<br>[S3 F3OEM], DS14<br>[F0RU] | S | H | 2 | DS5 [O2], DS6<br>[S3 F2OEM], DS7 [O2],<br>DS8 [O1], DS12<br>[S3 F3OEM], DS13<br>[S3 F3OEM], DS14<br>[F0RU] | S | SG | 2 |

|                                                                                                                                                                                                                                                                       |                                                                                                                                                                                               |                                                                                                                                                                                  |   |   |   |                                                                                                                                                                                  |   |    |   |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|---|---|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|----|---|
|                                                                                                                                                                                                                                                                       |                                                                                                                                                                                               | DS1, DS5, DS6, DS7,<br>DS8, DS9, DS10, DS11,<br>DS12, DS14, DS15,<br>DS18<br>_____<br>DS13 [S3 F3OEM]                                                                            |   |   |   | DS1, DS5, DS6, DS7,<br>DS8, DS9, DS10, DS11,<br>DS12, DS14, DS15,<br>DS18<br>_____<br>DS13 [S3 F3OEM]                                                                            |   |    |   |
| R124: T45 Spoofing oder Manipulation der Basisfahrzeugleistung als MitM auf der VBUS-Verbindung zwischen Steuerung und Aktoren, vorbereitet durch P2 Erlangung physischen Zugriffs auf die Fahrzeugelektronik als externer Angreifer                                  | C6 Authentische Datenübertragung<br>_____<br>A11 Risiko unabhängig von ADS,<br>A3 Qualitätsschäden werden im Falle eines kompromittierten Lkw selektiv berücksichtigt,<br>A6 Lokale Angreifer | DS5 [O2], DS6 [S3 F2OEM], DS7 [O2],<br>DS8 [O1], DS12 [S3 F3OEM], DS13 [S3 F3OEM], DS14 [F0RU]<br>_____<br>DS5, DS7, DS8, DS11, DS6, DS12, DS13<br>_____<br>DS14 [F0RU]          | V | H | 2 | DS5 [O2], DS6 [S3 F2OEM], DS7 [O2],<br>DS8 [O1], DS12 [S3 F3OEM], DS13 [S3 F3OEM], DS14 [F0RU]<br>_____<br>DS5, DS7, DS8, DS11, DS6, DS12, DS13<br>_____<br>DS14 [F0RU]          | V | SG | 1 |
| R125: T45 Spoofing oder Manipulation der Basisausgabe des Fahrzeugs als MitM auf der VBUS-Verbindung zwischen Steuerung und Aktoren Vorbereitung durch P3 Erlangung des Zugriffs auf einen Offline-Fahrzeuga-bus durch Fernkompromittierung einer angeschlossenen ECU | C6 Authentische Datenübertragung<br>_____<br>A11 Risiko unabhängig von ADS,<br>A3 Qualitätsschäden werden im Falle eines kompromittierten Lkw selektiv berücksichtigt.<br>A5 Domänentrennung  | DS5 [O2], DS6 [S3 F2OEM], DS7 [O2],<br>DS8 [O1], DS12 [S3 F3OEM], DS13 [S3 F3OEM], DS14 [F0RU]<br>_____<br>DS5, DS7, DS8, DS11<br>_____<br>DS6 [S3 F2OEM], DS12 [S3 F2OEM], DS13 | S | H | 1 | DS5 [O2], DS6 [S3 F2OEM], DS7 [O2],<br>DS8 [O1], DS12 [S3 F3OEM], DS13 [S3 F3OEM], DS14 [F0RU]<br>_____<br>DS5, DS7, DS8, DS11<br>_____<br>DS6 [S3 F2OEM], DS12 [S3 F2OEM], DS13 | S | SG | 1 |

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |                                                                                                                                                        | [S3 F3OEM], DS14<br>[F0RU]                                                                            |   |   |   | [S3 F3OEM], DS14<br>[F0RU]                                                                            |   |    |   |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------|---|---|---|-------------------------------------------------------------------------------------------------------|---|----|---|
| R126: T46 Spoofing oder Manipulation des Gesundheitszustands als MitM auf der VBUS-, IPC-Verbindung zwischen gesundheitsüberwachten Geräten und System Management Vorbereitung durch P2 Erlangung physischen Zugriffs auf die Fahrzeugelektronik als externer Angreifer                                                                                                                                                                                                                     | C6 Authentische Datenübertragung<br><br>A3 Qualitätsschäden werden im Falle eines kompromittierten Lkw selektiv berücksichtigt.<br>A6 Lokale Angreifer | DS5 [O2], DS7 [O2],<br>DS8 [O1], DS12<br>[S3 F3OEM]<br><br>DS5, DS7, DS8, DS11,<br>DS6, DS12, DS13    |   | H | 1 | DS5 [O2], DS7 [O2],<br>DS8 [O1], DS12<br>[S3 F3OEM]<br><br>DS5, DS7, DS8, DS11,<br>DS6, DS12, DS13    |   | SG | 1 |
| R127: T46 Spoofing oder Manipulation des Gesundheitszustands als MitM auf dem VBUS, IPC-Verbindung zwischen gesundheitsüberwachten Geräten und System Management Vorbereitung durch P4 Erlangung des Zugriffs auf einen Online-Fahrzeugbus durch Fernkompromittierung einer angeschlossenen ECU                                                                                                                                                                                             | C6 Authentische Übertragung von Daten<br><br>A3 Bei einem beschädigten Lkw werden Qualitätsschäden selektiv berücksichtigt.                            | DS5 [O2], DS7 [O2],<br>DS8 [O1], DS12<br>[S3 F3OEM]<br><br>DS5, DS7, DS8, DS11<br><br>DS12 [S3 F2OEM] | S | H | 5 | DS5 [O2], DS7 [O2],<br>DS8 [O1], DS12<br>[S3 F3OEM]<br><br>DS5, DS7, DS8, DS11<br><br>DS12 [S3 F2OEM] | S | SG | 2 |
| R128: T47 Spoofing oder Manipulation der Eingaben des Basisfahrzeugs als MitM auf der VBUS-Verbindung zwischen der Basisfahrzeugüberwachung und der On-board-HMI-Vorbereitung durch P2 Erlangung physischen Zugriffs auf die Fahrzeugelektronik als externer Angreifer<br><br>Hinweis: Es wurden keine Sicherheitsziele oder Schadensszenarien zugewiesen, da der durch diese Bedrohung gefährdete Datenfluss für den vollständig autonomen Lkw im Betrieb ohne Testfahrer nicht existiert. | A3 Qualitätsschäden werden im Falle eines kompromittierten Lkw selektiv berücksichtigt,<br>A6 Lokale Angreifer                                         | DS5, DS7, DS8, DS11,<br>DS6, DS12, DS13                                                               |   | H | 1 | DS5, DS7, DS8, DS11,<br>DS6, DS12, DS13                                                               |   | SG | 1 |

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |                                                                                                                    |                                             |   |   |                                             |    |   |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------|---------------------------------------------|---|---|---------------------------------------------|----|---|
| <p>R129: T47 Spoofing oder Manipulation der Basis-Fahrzeugeingabe als MitM auf der VBUS-Verbindung zwischen der Basis-Fahrzeugüberwachung und der On-board-HMI-Vorbereitung durch P4 Erlangung des Zugriffs auf einen Online-Fahrzeugbus durch Fernkompromittierung einer verbundenen ECU</p> <p>Hinweis: Es wurden keine Sicherheitsziele oder Schadensszenarien zugewiesen, da der durch diese Bedrohung gefährdete Datenfluss für den vollständig autonomen Lkw im Betrieb ohne Testfahrer nicht existiert.</p> | <p>A3 Bei einem kompromittierten Lkw werden Qualitätsschäden selektiv berücksichtigt.</p>                          | <p>DS5, DS7, DS8, DS11</p>                  | H | 1 | <p>DS5, DS7, DS8, DS11</p>                  | SG | 1 |
| <p>R130: T48 Spoofing oder Manipulation des Gesundheitszustands als MitM auf der VBUS-Verbindung zwischen System Management und onboardHMI prep. durch P2 Erlangung physischen Zugriffs auf die Fahrzeugelektronik als externer Angreifer</p> <p>Hinweis: Es wurden keine Sicherheitsziele oder Schadensszenarien zugewiesen, da der durch diese Bedrohung gefährdete Datenfluss für den vollständig autonomen Lkw im Betrieb ohne Testfahrer nicht existiert.</p>                                                 | <p>A3 Qualitätsschäden werden im Falle eines kompromittierten Lkw selektiv berücksichtigt, A6 Lokale Angreifer</p> | <p>DS5, DS7, DS8, DS11, DS6, DS12, DS13</p> | H | 1 | <p>DS5, DS7, DS8, DS11, DS6, DS12, DS13</p> | SG | 1 |
| <p>R131: T48 Spoofing oder Manipulation des Gesundheitszustands als MitM auf der VBUS-Verbindung zwischen System Management und Onboard-HMI Vorbereitung durch P4 Erlangung des Zugriffs auf einen Online-Fahrzeugbus durch Fernkompromittierung einer angeschlossenen ECU</p>                                                                                                                                                                                                                                     | <p>A3 Bei einem kompromittierten Lkw werden Qualitätsschäden selektiv berücksichtigt.</p>                          | <p>DS5, DS7, DS8, DS11</p>                  | H | 1 | <p>DS5, DS7, DS8, DS11</p>                  | SG | 1 |



|                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                                                                                                             |                                                                  |  |   |   |                                                                  |  |   |   |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------|--|---|---|------------------------------------------------------------------|--|---|---|
| Hinweis: Es wurden keine Sicherheitsziele oder Schadensszenarien zugewiesen, da der durch diese Bedrohung gefährdete Datenfluss für den vollständig autonomen Lkw im Betrieb ohne Testfahrer nicht existiert.                                                                                                                                                                                                                                                   |                                                                                                             |                                                                  |  |   |   |                                                                  |  |   |   |
| R132: T49 Spoofing oder Manipulation der geplanten Trajektorie als MitM auf der VBUS-Verbindung zwischen Planung und Onboard-HMI Vorbereitung durch P1 Erlangung physischen Zugriffs auf die Fahrzeugelektronik als Fahrzeugbesitzer/Tuner<br><br>Hinweis: Es wurden keine Sicherheitsziele oder Schadensszenarien zugewiesen, da der durch diese Bedrohung gefährdete Datenfluss für den vollständig autonomen Lkw im Betrieb ohne Testfahrer nicht existiert. | A2 Begrenzter Spielraum für Tuning-Angriffe                                                                 | DS1, DS5, DS6, DS7, DS8, DS9, DS10, DS11, DS12, DS14, DS15, DS18 |  | H | 1 | DS1, DS5, DS6, DS7, DS8, DS9, DS10, DS11, DS12, DS14, DS15, DS18 |  | H | 1 |
| R133: T49 Spoofing oder Manipulation der geplanten Fahrbahn als MitM auf der VBUS-Verbindung zwischen Planung und Onboard-HMI-Vorbereitung durch P2 Erlangung physischen Zugriffs auf die Fahrzeugelektronik als externer Angreifer<br><br>Hinweis: Es wurden keine Sicherheitsziele oder Schadensszenarien zugewiesen, da der durch diese Bedrohung gefährdete Datenfluss für den vollständig autonomen Lkw im Betrieb ohne Testfahrer nicht existiert.        | A3 Qualitätsschäden werden im Falle eines kompromittierten Lkw selektiv berücksichtigt, A6 Lokale Angreifer | DS5, DS7, DS8, DS11, DS6, DS12, DS13                             |  | H | 1 | DS5, DS7, DS8, DS11, DS6, DS12, DS13                             |  | H | 1 |
| R134: T49 Spoofing oder Manipulation der geplanten Trajektorie als MitM auf der VBUS-Verbindung zwischen Planung und Onboard-HMI-Vorbereitung durch P4                                                                                                                                                                                                                                                                                                          | A3 Bei einem kompromittierten Lkw werden Qualitätsschäden selektiv berücksichtigt.                          | DS5, DS7, DS8, DS11                                              |  | H | 1 | DS5, DS7, DS8, DS11                                              |  | H | 1 |

|                                                                                                                                                                                                                                                 |                                                                                                                                                                               |                                                                       |   |   |   |                                                                       |   |    |   |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------|---|---|---|-----------------------------------------------------------------------|---|----|---|
| Erlangung des Zugriffs auf einen Online-Fahrzeugbus durch Fernkompromittierung einer verbundenen ECU                                                                                                                                            |                                                                                                                                                                               |                                                                       |   |   |   |                                                                       |   |    |   |
| Hinweis: Es wurden keine Sicherheitsziele oder Schadensszenarien zugewiesen, da der durch diese Bedrohung gefährdete Datenfluss für den vollständig autonomen Lkw im Betrieb ohne Testfahrer nicht existiert.                                   |                                                                                                                                                                               |                                                                       |   |   |   |                                                                       |   |    |   |
| R135: T50 Spoofing oder Manipulation von MRM als MitM auf der MCOM-Verbindung zwischen Control Center und Mission Control                                                                                                                       | C2 mTLS zwischen Control Center und Mission Control                                                                                                                           | DS6 [S3 F2OEM], DS7 [O2]                                              | E | H | 4 | DS6 [S3 F2OEM], DS7 [O2]                                              | E | SG | 2 |
|                                                                                                                                                                                                                                                 | A10 Von CC ausgelöste MRM sind nicht sicherheitskritisch                                                                                                                      | DS6<br>DS7 [O2]                                                       |   |   |   | DS6<br>DS7 [O2]                                                       |   |    |   |
| R136: T51 Spoofing oder Manipulation MRM als MitM auf der VBUS-Verbindung zwischen Mission Control und System Management initiieren Vorbereitung durch P2 Erlangung physischen Zugriffs auf die Fahrzeugelektronik als externer Angreifer       | A10 Durch CC ausgelöste MRM sind nicht sicherheitskritisch.<br>A3 Qualitätsschäden werden im Falle eines kompromittierten Lkw selektiv berücksichtigt.<br>A6 Lokale Angreifer | DS6 [S3 F2OEM], DS7 [O2]<br>DS6, DS5, DS7, DS8, DS11, DS6, DS12, DS13 |   | H | 1 | DS6 [S3 F2OEM], DS7 [O2]<br>DS6, DS5, DS7, DS8, DS11, DS6, DS12, DS13 |   | H  | 1 |
| R137: T51 Spoofing oder Manipulation MRM als MitM auf der VBUS-Verbindung zwischen Mission Control und System Management initiieren Vorbereitung durch P4 Zugriff auf einen Online-Fahrzeugbus durch Fernkompromittierung einer verbundenen ECU | A10 Durch CC ausgelöste MRM sind nicht sicherheitskritisch.<br>A3 Qualitätsschäden werden im Falle eines kompromittierten Lkw selektiv berücksichtigt                         | DS6 [S3 F2OEM], DS7 [O2]<br>DS6, DS5, DS7, DS8, DS11                  |   | H | 1 | DS6 [S3 F2OEM], DS7 [O2]<br>DS6, DS5, DS7, DS8, DS11                  |   | H  | 1 |
| R138: T52 Spoofing oder Manipulation MRM als MitM auf der VBUS-Verbindung zwischen System                                                                                                                                                       | A3 Qualitätsschäden werden im Falle eines                                                                                                                                     | DS6 [S3 F2OEM], DS7 [O2]                                              |   | H | 1 | DS6 [S3 F2OEM], DS7 [O2]                                              |   | H  | 1 |

|                                                                                                                                                                                                                                                                                                                                                                                                                                                            |                                                                                                                |                                                                                     |   |   |   |                                                                                     |   |   |   |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|---|---|---|-------------------------------------------------------------------------------------|---|---|---|
| Management und Planning prep. durch P2 initiieren<br>Physischer Zugriff auf die Fahrzeugelektronik als externer Angreifer                                                                                                                                                                                                                                                                                                                                  | kompromittierten Lkw selektiv berücksichtigt,<br>A6 Lokale Angreifer                                           | DS5, DS7, DS8, DS11,<br>DS6, DS12, DS13<br>_____                                    |   |   |   | DS5, DS7, DS8, DS11,<br>DS6, DS12, DS13<br>_____                                    |   |   |   |
| R139: T52 Spoofing oder Manipulation MRM als MitM auf der VBUS-Verbindung zwischen System Management und Planungsvorbereitung durch P3 initiieren. Zugriff auf einen Offline-Fahrzeugbus durch Fernkompromittierung einer verbundenen ECU erlangen.                                                                                                                                                                                                        | A3 Qualitätsmängel werden im Falle eines kompromittierten Lkw selektiv berücksichtigt.<br>A5 Domänentrennung   | DS6 [S3 F2OEM], DS7 [O2]<br>_____<br>DS5, DS7, DS8, DS11<br>_____<br>DS6 [S3 F2OEM] | S | H | 1 | DS6 [S3 F2OEM], DS7 [O2]<br>_____<br>DS5, DS7, DS8, DS11<br>_____<br>DS6 [S3 F2OEM] | S | H | 1 |
| R140: T53 Spoofing oder Manipulation MRM als MitM auf der VBUS-Verbindung zwischen Onboard-HMI und System Management initiieren Vorbereitung durch P2 Erlangung physischen Zugriffs auf die Fahrzeugelektronik als externer Angreifer<br><br>Hinweis: Es wurden keine Sicherheitsziele oder Schadensszenarien zugewiesen, da der durch diese Bedrohung gefährdete Datenfluss für den vollständig autonomen Lkw im Betrieb ohne Testfahrer nicht existiert. | A3 Qualitätsschäden werden im Falle eines kompromittierten Lkw selektiv berücksichtigt,<br>A6 Lokale Angreifer | _____<br>DS5, DS7, DS8, DS11,<br>DS6, DS12, DS13<br>_____                           |   | H | 1 | _____<br>DS5, DS7, DS8, DS11,<br>DS6, DS12, DS13<br>_____                           |   | H | 1 |
| R141: T53 Spoofing oder Manipulation MRM als MitM auf der VBUS-Verbindung zwischen Onboard-HMI und System Management initiieren Vorbereitung durch P4 Zugriff auf einen Online-Fahrzeugbus durch Fernkompromittierung einer verbundenen ECU<br><br>Hinweis: Es wurden keine Sicherheitsziele oder Schadensszenarien zugewiesen, da der durch diese Bedro-                                                                                                  | A3 Bei einem kompromittierten Lkw werden Qualitätsschäden selektiv berücksichtigt.                             | _____<br>DS5, DS7, DS8, DS11<br>_____                                               |   | H | 1 | _____<br>DS5, DS7, DS8, DS11<br>_____                                               |   | H | 1 |

|                                                                                                                                                                                                                                      |                                                                                                             |                                                                                     |   |   |   |                                                                                     |   |   |   |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|---|---|---|-------------------------------------------------------------------------------------|---|---|---|
| hung gefährdete Datenfluss für den vollständig autonomen Lkw im Betrieb ohne Testfahrer nicht existiert.                                                                                                                             |                                                                                                             |                                                                                     |   |   |   |                                                                                     |   |   |   |
| R142: T54 Spoofing oder Manipulation MRM als MitM auf der IPC-Verbindung zwischen Planung und Steuerung initiieren Vorbereitung durch P2 Physischer Zugriff auf die Fahrzeugelektronik als externer Angreifer                        | A3 Qualitätsschäden werden im Falle eines kompromittierten Lkw selektiv berücksichtigt, A6 Lokale Angreifer | DS6 [S3 F2OEM], DS7 [O2]<br>_____<br>DS5, DS7, DS8, DS11, DS6, DS12, DS13<br>_____  |   | H | 1 | DS6 [S3 F2OEM], DS7 [O2]<br>_____<br>DS5, DS7, DS8, DS11, DS6, DS12, DS13<br>_____  |   | H | 1 |
| R143: T54 Spoofing oder Manipulation MRM als MitM auf der IPC-Verbindung zwischen Planung und Steuerung vorbereiten durch P3 Zugriff auf einen Offline-Fahrzeugbus durch Fernkompromittierung einer verbundenen ECU erlangen         | A3 Qualitätsmängel werden im Falle eines kompromittierten Lkw selektiv berücksichtigt. A5 Domänentrennung   | DS6 [S3 F2OEM], DS7 [O2]<br>_____<br>DS5, DS7, DS8, DS11<br>_____<br>DS6 [S3 F2OEM] | S | H | 1 | DS6 [S3 F2OEM], DS7 [O2]<br>_____<br>DS5, DS7, DS8, DS11<br>_____<br>DS6 [S3 F2OEM] | S | H | 1 |
| R144: T55 Spoofing oder Manipulation MRM als MitM auf der VBUS-Verbindung zwischen Steuerung und Aktoren initiieren Vorbereitung durch P2 Erlangung physischen Zugriffs auf die Fahrzeugelektronik als externer Angreifer            | A3 Qualitätsschäden werden im Falle eines kompromittierten Lkw selektiv berücksichtigt, A6 Lokale Angreifer | DS6 [S3 F2OEM], DS7 [O2]<br>_____<br>DS5, DS7, DS8, DS11, DS6, DS12, DS13<br>_____  |   | H | 1 | DS6 [S3 F2OEM], DS7 [O2]<br>_____<br>DS5, DS7, DS8, DS11, DS6, DS12, DS13<br>_____  |   | H | 1 |
| R145: T55 Spoofing oder Manipulation MRM als MitM auf der VBUS-Verbindung zwischen Steuerung und Aktoren initiieren Vorbereitung durch P3 Zugriff auf einen Offline-Fahrzeugbus durch Fernkompromittierung einer angeschlossenen ECU | A3 Qualitätsmängel werden im Falle eines kompromittierten Lkw selektiv berücksichtigt. A5 Domänentrennung   | DS6 [S3 F2OEM], DS7 [O2]<br>_____<br>DS5, DS7, DS8, DS11<br>_____<br>DS6 [S3 F2OEM] | S | H | 1 | DS6 [S3 F2OEM], DS7 [O2]<br>_____<br>DS5, DS7, DS8, DS11<br>_____<br>DS6 [S3 F2OEM] | S | H | 1 |

|                                                                                                                                                                                                                                                                                             |                                                                                                                        |                                                                                  |   |   |   |                                                                                  |   |    |   |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------|---|---|---|----------------------------------------------------------------------------------|---|----|---|
| R146: T56 Spoofing oder Manipulation Aktivierungsbe-<br>fehl als MitM auf der MCOM-Verbindung zwischen Con-<br>trol Center und Mission Control                                                                                                                                              | C2 mTLS zwischen Control<br>Center und Mission Control                                                                 | DS5 [O2], DS11 [O1]                                                              | E | H | 4 | DS5 [O2], DS11 [O1]                                                              | E | SG | 2 |
| R147: T57 Spoofing oder Manipulation von Wakeup als<br>MitM auf der VBUS-, IPC-Verbindung zwischen Mission<br>Control und Gesundheitsüberwachungsgeräten, vorbe-<br>reitet durch P2 Erlangung physischen Zugriffs auf die<br>Fahrzeugelektronik als externer Angreifer                      | A3 Qualitätsschäden werden<br>im Falle eines kompromittier-<br>ten Lkw selektiv berücksichtigt,<br>A6 Lokale Angreifer | DS5 [O2], DS11 [O1]<br>_____<br>DS5, DS7, DS8, DS11,<br>DS6, DS12, DS13<br>_____ |   | H | 1 | DS5 [O2], DS11 [O1]<br>_____<br>DS5, DS7, DS8, DS11,<br>DS6, DS12, DS13<br>_____ |   | H  | 1 |
| R148: T57 Spoofing oder Manipulation von Wakeup als<br>MitM auf dem VBUS, IPC-Verbindung zwischen Mission<br>Control und Health Monitored Devices, vorbereitet von<br>P4 Erlangung des Zugriffs auf einen Online-Fahrzeug-<br>bus durch Fernkompromittierung einer angeschlosse-<br>nen ECU | A3 Bei einem kompromittierten<br>Lkw werden Qualitätsschäden<br>selektiv berücksichtigt.                               | DS5 [O2], DS11 [O1]<br>_____<br>DS5, DS7, DS8, DS11<br>_____                     |   | H | 1 | DS5 [O2], DS11 [O1]<br>_____<br>DS5, DS7, DS8, DS11<br>_____                     |   | H  | 1 |
| R149: T58 Spoofing oder Manipulation von Wakeup als<br>MitM auf der VBUS-Verbindung zwischen Mission Con-<br>trol und System Management Vorbereitung durch P2 Er-<br>langung physischen Zugriffs auf die Fahrzeugelektronik<br>als externer Angreifer                                       | A3 Qualitätsschäden werden<br>im Falle eines kompromittier-<br>ten Lkw selektiv berücksichtigt,<br>A6 Lokale Angreifer | DS5 [O2], DS11 [O1]<br>_____<br>DS5, DS7, DS8, DS11,<br>DS6, DS12, DS13<br>_____ |   | H | 1 | DS5 [O2], DS11 [O1]<br>_____<br>DS5, DS7, DS8, DS11,<br>DS6, DS12, DS13<br>_____ |   | H  | 1 |
| R150: T58 Spoofing oder Manipulation von Wakeup als<br>MitM auf der VBUS-Verbindung zwischen Mission Con-<br>trol und System Management, vorbereitet von P4 Erlan-<br>gung des Zugriffs auf einen Online-Fahrzeugbus durch<br>Fernkompromittierung einer angeschlossenen ECU                | A3 Bei einem kompromittierten<br>Lkw werden Qualitätsschäden<br>selektiv berücksichtigt.                               | DS5 [O2], DS11 [O1]<br>_____<br>DS5, DS7, DS8, DS11<br>_____                     |   | H | 1 | DS5 [O2], DS11 [O1]<br>_____<br>DS5, DS7, DS8, DS11<br>_____                     |   | H  | 1 |
| R151: T59 Spoofing oder Manipulation des Aktivie-<br>rungsstatus als MitM auf der VBUS-Verbindung zwi-<br>schen Onboard-HMI und Mission Control Vorbereitung                                                                                                                                | A3 Qualitätsschäden werden<br>im Falle eines kompromittier-<br>ten Lkw selektiv berücksichtigt,<br>A6 Lokale Angreifer | DS5 [O2]<br>_____<br>DS5, DS7, DS8, DS11,<br>A6 Lokale Angreifer                 |   | H | 1 | DS5 [O2]<br>_____<br>DS5, DS7, DS8, DS11,<br>A6 Lokale Angreifer                 |   | H  | 1 |

|                                                                                                                                                                                                                                                                               |                                                                                                             |                                                                      |   |   |   |                                                                      |   |    |   |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------|---|---|---|----------------------------------------------------------------------|---|----|---|
| durch P2 Erlangung physischen Zugriffs auf die Fahrzeugelektronik als externer Angreifer                                                                                                                                                                                      |                                                                                                             | DS6, DS12, DS13                                                      |   |   |   | DS6, DS12, DS13                                                      |   |    |   |
| R152: T59 Spoofing oder Manipulation des Aktivierungsstatus als MitM auf der VBUS-Verbindung zwischen Onboard-HMI und Mission Control Vorbereitung durch P4 Erlangung des Zugriffs auf einen Online-Fahrzeugbus durch Fernkompromittierung einer verbundenen ECU              | A3 Bei einem kompromittierten Lkw werden Qualitätsschäden selektiv berücksichtigt.                          | DS5 Verlust der ADS-Funktion in Ruhe<br>DS5, DS7, DS8, DS11          |   | H | 1 | DS5 Verlust der ADS-Funktion in Ruhe<br>DS5, DS7, DS8, DS11          |   | H  | 1 |
| R153: T60 Spoofing oder Manipulation des Aktivierungsstatus als MitM auf der MCOM-Verbindung zwischen Mission Control und Control Center                                                                                                                                      | C2 mTLS zwischen Control Center und Mission Control                                                         | DS5 [O2]                                                             | E | H | 4 | DS5 [O2]                                                             | E | SG | 2 |
| R154: T61 Spoofing oder Manipulation von Fahrbefehlen als MitM auf der MCOM-Verbindung zwischen Control Center und Mission Control                                                                                                                                            | C2 mTLS zwischen Control Center und Mission Control                                                         | DS5 [O2]                                                             | E | H | 4 | DS5 [O2]                                                             | E | SG | 2 |
| R155: T62 Spoofing oder Manipulation von Betriebsinformationen als MitM auf der VBUS-Verbindung zwischen System Management und Mission Control, vorbereitet durch P2 Erlangung physischen Zugriffs auf die Fahrzeugelektronik als externer Angreifer                          | A3 Qualitätsschäden werden im Falle eines kompromittierten Lkw selektiv berücksichtigt, A6 Lokale Angreifer | DS5 [O2], DS7 [O2], DS8 [O1]<br>DS5, DS7, DS8, DS11, DS6, DS12, DS13 |   | H | 1 | DS5 [O2], DS7 [O2], DS8 [O1]<br>DS5, DS7, DS8, DS11, DS6, DS12, DS13 |   | H  | 1 |
| R156: T62 Spoofing oder Manipulation von Betriebsinformationen als MitM auf der VBUS-Verbindung zwischen System Management und Mission Control Vorbereitung durch P4 Erlangung des Zugriffs auf einen Online-Fahrzeugbus durch Fernkompromittierung einer angeschlossenen ECU | A3 Bei einem kompromittierten Lkw werden Qualitätsschäden selektiv berücksichtigt.                          | DS5 [O2], DS7 [O2], DS8 [O1]<br>DS5, DS7, DS8, DS11                  |   | H | 1 | DS5 [O2], DS7 [O2], DS8 [O1]<br>DS5, DS7, DS8, DS11                  |   | H  | 1 |

|                                                                                                                                                                                                                                                                                          |                                                                                                             |                                                            |   |   |   |                                                            |   |    |   |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------|------------------------------------------------------------|---|---|---|------------------------------------------------------------|---|----|---|
| R157: T63 Spoofing oder Manipulation von Betriebsinformationen als MitM auf der MCOM-Verbindung zwischen Mission Control und Control Center                                                                                                                                              | C2 mTLS zwischen Control Center und Mission Control                                                         | DS5 [O2], DS7 [O2], DS8 [O1]                               | E | H | 4 | DS5 [O2], DS7 [O2], DS8 [O1]                               | E | SG | 2 |
| R158: T64 Spoofing oder Manipulation der Abfrage des detaillierten Fahrzeugzustands als MitM auf der MCOM-Verbindung zwischen Control Center und Mission Control                                                                                                                         | C2 mTLS zwischen Control Center und Mission Control                                                         | DS7 [O2], DS8 [O1]                                         | E | H | 4 | DS7 [O2], DS8 [O1]                                         | E | SG | 2 |
| R159: T65 Spoofing oder Manipulation von Anfragen zum detaillierten Fahrzeugstatus als MitM auf der VBUS-Verbindung zwischen Mission Control und System Management, vorbereitet durch P2 Erlangung physischen Zugriffs auf die Fahrzeugelektronik als externer Angreifer                 | A3 Qualitätsschäden werden im Falle eines kompromittierten Lkw selektiv berücksichtigt, A6 Lokale Angreifer | DS7 [O2], DS8 [O1]<br>DS5, DS7, DS8, DS11, DS6, DS12, DS13 |   | H | 1 | DS7 [O2], DS8 [O1]<br>DS5, DS7, DS8, DS11, DS6, DS12, DS13 |   | H  | 1 |
| R160: T65 Spoofing oder Manipulation Anforderung detaillierter Fahrzeugzustandsdaten als MitM auf der VBUS-Verbindung zwischen Mission Control und System Management prep. durch P4 Erlangung des Zugriffs auf einen Online-Fahrzeugbus durch Fernkompromittierung einer verbundenen ECU | A3 Bei einem kompromittierten Lkw werden Qualitätsschäden selektiv berücksichtigt.                          | DS7 [O2], DS8 [O1]<br>DS5, DS7, DS8, DS11                  |   | H | 1 | DS7 [O2], DS8 [O1]<br>DS5, DS7, DS8, DS11                  |   | H  | 1 |
| R161: T66 Spoofing oder Manipulation des detaillierten Fahrzeugzustands als MitM auf der VBUS-Verbindung zwischen System Management und Mission Control Vorbereitung durch P2 Erlangung physischen Zugriffs auf die Fahrzeugelektronik als externer Angreifer                            | A3 Qualitätsschäden werden im Falle eines kompromittierten Lkw selektiv berücksichtigt, A6 Lokale Angreifer | DS7 [O2], DS8 [O1]<br>DS5, DS7, DS8, DS11, DS6, DS12, DS13 |   | H | 1 | DS7 [O2], DS8 [O1]<br>DS5, DS7, DS8, DS11, DS6, DS12, DS13 |   | H  | 1 |
| R162: T66 Spoofing oder Manipulation des detaillierten Fahrzeugzustands als MitM auf der VBUS-Verbindung zwischen System Management und Mission Control Vorbereitung durch P4 Erlangung des Zugriffs auf einen                                                                           | A3 Bei einem kompromittierten Lkw werden Qualitätsschäden selektiv berücksichtigt.                          | DS7 [O2], DS8 [O1]<br>DS5, DS7, DS8, DS11                  |   | H | 1 | DS7 [O2], DS8 [O1]<br>DS5, DS7, DS8, DS11                  |   | H  | 1 |



|                                                                                                                                                                                                                                                            |                                                                                                             |                                      |   |   |   |                                      |   |    |   |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------|--------------------------------------|---|---|---|--------------------------------------|---|----|---|
| Online-Fahrzeugbus durch Fernkompromittierung einer verbundenen ECU                                                                                                                                                                                        |                                                                                                             |                                      |   |   |   |                                      |   |    |   |
| R163: T67 Spoofing oder Manipulation des detaillierten Fahrzeugzustands als MitM auf der MCOM-Verbindung zwischen Mission Control und Control Center                                                                                                       | C2 mTLS zwischen Control Center und Mission Control                                                         | DS7 [O2], DS8 [O1]                   | E | H | 4 | DS7 [O2], DS8 [O1]                   | E | SG | 2 |
| R164: T68 Spoofing oder Manipulation von Request-EDR-Daten als MitM auf der MCOM-Verbindung zwischen Control Center und Mission Control                                                                                                                    | C2 mTLS zwischen Control Center und Mission Control                                                         |                                      |   | H | 1 |                                      |   | SG | 1 |
| R165: T69 Spoofing oder Manipulation von Request-EDR-Daten als MitM auf der VBUS-Verbindung zwischen Mission Control und System Management, vorbereitet durch P2 Erlangung physischen Zugriffs auf die Fahrzeugelektronik als externer Angreifer           | A3 Qualitätsschäden werden im Falle eines kompromittierten Lkw selektiv berücksichtigt, A6 Lokale Angreifer | DS5, DS7, DS8, DS11, DS6, DS12, DS13 |   | H | 1 | DS5, DS7, DS8, DS11, DS6, DS12, DS13 |   | H  | 1 |
| R166: T69 Spoofing oder Manipulation von EDR-Daten als MitM auf der VBUS-Verbindung zwischen Mission Control und System Management prep. durch P4 Erlangung des Zugriffs auf einen Online-Fahrzeugbus durch Fernkompromittierung einer angeschlossenen ECU | A3 Bei einem kompromittierten Lkw werden Qualitätsschäden selektiv berücksichtigt.                          | DS5, DS7, DS8, DS11                  |   | H | 1 | DS5, DS7, DS8, DS11                  |   | H  | 1 |
| R167: T70 Spoofing oder Manipulation von EDR-Daten als MitM auf der VBUS-Verbindung zwischen System Management und Mission Control Vorbereitung durch P2 Erlangung physischen Zugriffs auf die Fahrzeugelektronik als externer Angreifer                   | A3 Qualitätsschäden werden im Falle eines kompromittierten Lkw selektiv berücksichtigt, A6 Lokale Angreifer | DS5, DS7, DS8, DS11, DS6, DS12, DS13 |   | H | 1 | DS5, DS7, DS8, DS11, DS6, DS12, DS13 |   | H  | 1 |
| R168: T70 Spoofing oder Manipulation von EDR-Daten als MitM auf der VBUS-Verbindung zwischen System Management und Mission Control Vorbereitung durch P4 Erlangung des Zugriffs auf einen Online-                                                          | A3 Bei einem kompromittierten Lkw werden Qualitätsschäden selektiv berücksichtigt.                          | DS5, DS7, DS8, DS11                  |   | H | 1 | DS5, DS7, DS8, DS11                  |   | H  | 1 |

|                                                                                                                                                                                     |                                                                                                               |                                                                  |   |   |   |                                                                  |   |    |   |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------|---|---|---|------------------------------------------------------------------|---|----|---|
| Fahrzeugbus durch Fernkompromittierung einer verbundenen ECU                                                                                                                        |                                                                                                               |                                                                  |   |   |   |                                                                  |   |    |   |
| R169: T71 Spoofing oder Manipulation von EDR-Daten als MitM auf der MCOM-Verbindung zwischen Mission Control und Control Center                                                     | C2 mTLS zwischen Control Center und Mission Control                                                           |                                                                  |   | H | 1 |                                                                  |   | SG | 1 |
| R170: T72 Spoofing oder Manipulation des Fahrzeugen- triegelungsbefehls als MitM auf der MCOM-Verbindung zwischen Control Center und Mission Control                                | C2 mTLS zwischen Control Center und Mission Control                                                           | DS5 [O2]                                                         | E | H | 4 | DS5 [O2]                                                         | E | SG | 2 |
| R171: T73 Spoofing oder Manipulation des Deaktivie- rungsbefehls als MitM auf der MCOM-Verbindung zwi- schen Control Center und Mission Control                                     | C2 mTLS zwischen Control Center und Mission Control                                                           | DS5 [O2], DS11 [O1]                                              | E | H | 4 | DS5 [O2], DS11 [O1]                                              | E | SG | 2 |
| R172: P1 Erlangung physischen Zugriffs auf die Fahr- zeugelektronik als Fahrzeughalter/Tuner<br><br>Hinweis: Dieser Vorbereitungsschritt allein verursacht keine Schadensszenarien. | A2 Begrenzter Spielraum für Tu- ning-Angriffe                                                                 | DS1, DS5, DS6, DS7, DS8, DS9, DS10, DS11, DS12, DS14, DS15, DS18 |   | H | 1 | DS1, DS5, DS6, DS7, DS8, DS9, DS10, DS11, DS12, DS14, DS15, DS18 |   | H  | 1 |
| R173: P2 Erlangung physischen Zugriffs auf die Fahr- zeugelektronik als externer Angreifer<br><br>Hinweis: Dieser Vorbereitungsschritt allein verursacht keine Schadensszenarien.   | A3 Qualitätsschäden werden im Falle eines kompromittier- ten Lkw selektiv berücksichtigt, A6 Lokale Angreifer | DS5, DS7, DS8, DS11, DS6, DS12, DS13                             |   | H | 1 | DS5, DS7, DS8, DS11, DS6, DS12, DS13                             |   | H  | 1 |
| R174: P3 Zugriff auf einen Offline-Fahrzeugbus durch Fernkompromittierung einer verbundenen ECU                                                                                     | A3 Qualitätsmängel werden im Falle eines kompromittierten Lkw selektiv berücksichtigt. A5 Domänentrennung     | DS5, DS7, DS8, DS11                                              |   | H | 1 | DS5, DS7, DS8, DS11                                              |   | H  | 1 |

|                                                                                                                                                                                   |                                                                                     |                                                                                                                                                             |   |   |   |                                                                                                                                                             |   |   |   |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|---|---|---|-------------------------------------------------------------------------------------------------------------------------------------------------------------|---|---|---|
| Hinweis: Dieser Vorbereitungsschritt allein verursacht keine Schadensszenarien.                                                                                                   |                                                                                     |                                                                                                                                                             |   |   |   |                                                                                                                                                             |   |   |   |
| R175: P4 Zugriff auf einen Online-Fahrzeugbus durch Fernkompromittierung einer verbundenen ECU                                                                                    | A3 Bei einem kompromittierten Lkw werden Qualitätsschäden selektiv berücksichtigt.  | DS5, DS7, DS8, DS11                                                                                                                                         |   | H | 1 | DS5, DS7, DS8, DS11                                                                                                                                         |   | H | 1 |
| Hinweis: Dieser Vorbereitungsschritt allein verursacht keine Schadensszenarien.                                                                                                   |                                                                                     |                                                                                                                                                             |   |   |   |                                                                                                                                                             |   |   |   |
| R176: P5 Angriff auf mehr als eine Verbindung, um die Sensorfusion (C3) oder Redundanzen (C4, C5) zu überwinden                                                                   |                                                                                     |                                                                                                                                                             |   | M | 1 |                                                                                                                                                             |   | M | 1 |
| Hinweis: Der Angriff auf mehr als eine Verbindung zur Umgehung bestimmter Schutzmaßnahmen erfordert im Vergleich zum Angriff auf eine einzelne Verbindung einen erhöhten Aufwand. |                                                                                     |                                                                                                                                                             |   |   |   |                                                                                                                                                             |   |   |   |
| Hinweis: Dieser Vorbereitungsschritt allein verursacht keine Schadensszenarien.                                                                                                   |                                                                                     |                                                                                                                                                             |   |   |   |                                                                                                                                                             |   |   |   |
| R177: T74 Angriffe auf oder ausgehend vom Control Center                                                                                                                          | A1 Angriffe auf das Control Center fallen nicht in den Umfang dieser Risikoanalyse. | DS1 [P2], DS2 [F0OEM], DS5 [O2], DS6 [S3 F2OEM], DS7 [O2], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS11 [O1], DS12 [S3 F2OEM], DS13 [S3 F3OEM], DS14 [F0RU], DS15 | S | H | 2 | DS1 [P2], DS2 [F0OEM], DS5 [O2], DS6 [S3 F2OEM], DS7 [O2], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS11 [O1], DS12 [S3 F2OEM], DS13 [S3 F3OEM], DS14 [F0RU], DS15 | S | H | 2 |

|                                                                                                                                                                                 |                                                                                             | [F2OEM], DS16<br>[F2OEM], DS18 [F1RU]           |   |   |   | [F2OEM], DS16<br>[F2OEM], DS18 [F1RU]           |   |    |   |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------|-------------------------------------------------|---|---|---|-------------------------------------------------|---|----|---|
| R178: T75 Extraktion von Daten aus zentralen ADS-Komponenten                                                                                                                    | C8 Verschlüsselte Speicherung der ADS-Software                                              | DS1 [P2], DS2 [F0OEM], DS3 [F3OEM], DS18 [F1RU] | S | M | 4 | DS1 [P2], DS2 [F0OEM], DS3 [F3OEM], DS18 [F1RU] | V | M  | 2 |
| Hinweis: Das Extrahieren von Informationen aus dem Speicher einer Komponente erfordert im Vergleich zum Abhören von Informationen auf einem Fahrzeugbus einen erhöhten Aufwand. | A8 Vertrauliche Daten werden nur während der Übertragung verarbeitet und nicht gespeichert. | DS1, DS18<br>DS2 [F0OEM], DS3 [F3OEM]           |   |   |   | DS3, DS1, DS18<br>DS2 [F0OEM]                   |   |    |   |
| R179: T75 Extrahieren von Daten aus zentralen ADS-Komponenten Vorbereitung durch P12 Extrahieren von kryptografischem Material                                                  | C19 Speicherung von kryptografischem Material in Hardware-Sicherheitsmodulen                | DS1 [P2], DS2 [F0OEM], DS3 [F3OEM], DS18 [F1RU] | S | M | 4 | DS1 [P2], DS2 [F0OEM], DS3 [F3OEM], DS18 [F1RU] | S | SG | 2 |
| Hinweis: Das Extrahieren von Informationen aus dem Speicher einer Komponente erfordert im Vergleich zum Abhören von Informationen auf einem Fahrzeugbus einen erhöhten Aufwand. | A8 Vertrauliche Daten werden nur während der Übertragung verarbeitet und nicht gespeichert. | DS1, DS18<br>DS2 [F0OEM], DS3 [F3OEM]           |   |   |   | DS1, DS18<br>DS2 [F0OEM], DS3 [F3OEM]           |   |    |   |
| Hinweis: Durch P12 wirkt C8 Verschlüsselte Speicherung der ADS-Software nicht.                                                                                                  |                                                                                             |                                                 |   |   |   |                                                 |   |    |   |
| R180: T76 Extrahieren von Daten aus der Mission Control                                                                                                                         | C7 Verschlüsselte Übertragung vertraulicher Daten                                           | DS1 [P2], DS2 [F0OEM], DS18 [F1RU]              | V | M | 2 | DS1 [P2], DS2 [F0OEM], DS18 [F1RU]              | V | M  | 2 |
| Hinweis: Das Extrahieren von Informationen aus dem Speicher einer Komponente erfordert im Vergleich zum                                                                         | A8 Vertrauliche Daten werden nur während der Übertragung verarbeitet und nicht gespeichert  | DS1, DS18<br>DS2 [F0OEM]                        |   |   |   | DS1, DS18, DS1, DS18<br>DS2 [F0OEM]             |   |    |   |

|                                                                                                                                                                                                                                                                                                                          |                                                                                                                                                                                                                                          |                                                                                               |   |   |   |                                                                                               |   |    |   |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------|---|---|---|-----------------------------------------------------------------------------------------------|---|----|---|
| Abhören von Informationen auf einem Fahrzeugbus einen erhöhten Aufwand.                                                                                                                                                                                                                                                  |                                                                                                                                                                                                                                          |                                                                                               |   |   |   |                                                                                               |   |    |   |
| <p>R181: T76 Extrahieren von Daten aus Mission Control prep. durch P12 Extrahieren von kryptografischem Material</p> <p>Hinweis: Das Extrahieren von Informationen aus dem Speicher einer Komponente erfordert im Vergleich zum Abhören von Informationen auf einem Fahrzeugbus einen erhöhten Aufwand.</p>              | <p>C7 Verschlüsselte Übertragung vertraulicher Daten, C19 Speicherung von kryptografischem Material in Hardware-Sicherheitsmodulen</p> <p>A8 Vertrauliche Daten werden nur während der Übertragung verarbeitet und nicht gespeichert</p> | <p>DS1 [P2], DS2 [F0OEM], DS18 [F1RU]</p> <p>DS1, DS18</p> <p>DS2 [F0OEM]</p>                 | V | M | 2 | <p>DS1 [P2], DS2 [F0OEM], DS18 [F1RU]</p> <p>DS1, DS18, DS1, DS18</p> <p>DS2 [F0OEM]</p>      | V | SG | 1 |
| <p>R182: T77 Extrahieren von Daten aus der System Management</p> <p>Hinweis: Das Extrahieren von Informationen aus dem Speicher einer Komponente erfordert im Vergleich zum Abhören von Informationen auf einem Fahrzeugbus einen erhöhten Aufwand.</p>                                                                  | <p>C10 Verschlüsselte Speicherung der Gesundheitsüberwachungssoftware</p> <p>A8 Vertrauliche Daten werden nur während der Übertragung verarbeitet und nicht gespeichert.</p>                                                             | <p>DS2 [F0OEM], DS4 [F1OEM], DS18 [F1RU]</p> <p>DS1, DS18</p> <p>DS2 [F0OEM], DS4 [F1OEM]</p> | M | M | 3 | <p>DS2 [F0OEM], DS4 [F1OEM], DS18 [F1RU]</p> <p>DS4, DS1, DS18</p> <p>DS2 [F0OEM]</p>         | V | M  | 2 |
| <p>R183: T77 Extrahieren von Daten aus der System Management Vorbereitung durch P12 Extrahieren von kryptografischem Material</p> <p>Hinweis: Das Extrahieren von Informationen aus dem Speicher einer Komponente erfordert im Vergleich zum Abhören von Informationen auf einem Fahrzeugbus einen erhöhten Aufwand.</p> | <p>C19 Speicherung von kryptografischem Material in Hardware-Sicherheitsmodulen</p> <p>A8 Vertrauliche Daten werden nur während der Übertragung verarbeitet und nicht gespeichert.</p>                                                   | <p>DS2 [F0OEM], DS4 [F1OEM], DS18 [F1RU]</p> <p>DS1, DS18</p> <p>DS2 [F0OEM], DS4 [F1OEM]</p> | M | M | 3 | <p>DS2 [F0OEM], DS4 [F1OEM], DS18 [F1RU]</p> <p>DS1, DS18</p> <p>DS2 [F0OEM], DS4 [F1OEM]</p> | M | SG | 1 |

|                                                                                                                                                                                                                                                                                                                       |                                                                                                                                                                                         |                                                                                               |   |   |   |                                                                                                   |  |     |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------|---|---|---|---------------------------------------------------------------------------------------------------|--|-----|
| Hinweis: Durch P12 wirkt C10 Verschlüsselte Speicherung von Health Monitoring Software nicht.                                                                                                                                                                                                                         |                                                                                                                                                                                         |                                                                                               |   |   |   |                                                                                                   |  |     |
| R184: T78 Denial-of-Service-Angriff auf zentrale ADS-Komponenten Vorbereitung durch P2 Erlangung physischen Zugriffs auf die Fahrzeugelektronik als externer Angreifer                                                                                                                                                | C11 Denial-of-Service-Schutz für sicherheitskritische Komponenten<br><br>A3 Qualitätsschäden werden im Falle eines kompromittierten Lkw selektiv berücksichtigt.<br>A6 Lokale Angreifer | DS5 [O2], DS6 [S3 F2OEM], DS7 [O2], DS8 [O1]<br><br>DS5, DS7, DS8, DS11, DS6, DS12, DS13      |   | H | 1 | DS5 [O2], DS6 [S3 F2OEM], DS7 [O2], DS8 [O1]<br><br>DS6>DS7, DS5, DS7, DS8, DS11, DS6, DS12, DS13 |  | H 1 |
| R185: T78 Denial-of-Service-Angriff auf zentrale ADS-Komponenten, vorbereitet durch P4 Erlangung des Zugriffs auf einen Online-Fahrzeugbus durch Fernkompromittierung einer verbundenen ECU<br><br>Hinweis: Ein Angreifer muss beide redundanten ADS-Steuergeräte angreifen, um die Schadensszenarien zu verursachen. | C11 Denial-of-Service-Schutz für sicherheitskritische Komponenten<br><br>A3 Qualitätsschäden werden im Falle eines kompromittierten Lkw selektiv berücksichtigt                         | DS5 [O2], DS6 [S3 F2OEM], DS7 [O2], DS8 [O1]<br><br>DS5, DS7, DS8, DS11<br><br>DS6 [S3 F2OEM] | S | H | 5 | DS5 [O2], DS6 [S3 F2OEM], DS7 [O2], DS8 [O1]<br><br>DS6>DS7, DS5, DS7, DS8, DS11                  |  | H 1 |
| R186: T79 Denial-of-Service-Angriff auf die Mission Control über verbundene Busse, vorbereitet durch P2 Erlangung physischen Zugriffs auf die Fahrzeugelektronik als externer Angreifer                                                                                                                               | C11 Denial-of-Service-Schutz für sicherheitskritische Komponenten<br><br>A3 Qualitätsschäden werden im Falle eines kompromittierten Lkw selektiv berücksichtigt.<br>A6 Lokale Angreifer | DS5 [O2], DS7 [O2], DS8 [O1], DS11 [O1]<br><br>DS5, DS7, DS8, DS11, DS6, DS12, DS13           |   | H | 1 | DS5 [O2], DS7 [O2], DS8 [O1], DS11 [O1]<br><br>DS6>DS7, DS5, DS7, DS8, DS11, DS6, DS12, DS13      |  | H 1 |

|                                                                                                                                                                                                                                                                                                                                                              |                                                                                                                                                                                         |                                                                                                                                              |   |   |   |                                                                                                                                              |   |    |   |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------|---|---|---|----------------------------------------------------------------------------------------------------------------------------------------------|---|----|---|
| R187: T80 Denial-of-Service-Angriff auf die Mission Control über Fernschnittstellen                                                                                                                                                                                                                                                                          | C12 Zugriffskontrolle auf Remote-Schnittstellen                                                                                                                                         | DS5 [O2], DS7 [O2], DS8 [O1], DS11 [O1]                                                                                                      | E | H | 4 | DS5 [O2], DS7 [O2], DS8 [O1], DS11 [O1]                                                                                                      | E | SG | 2 |
| R188: T81 Denial-of-Service-Angriff auf die System Management, vorbereitet durch P2 Erlangung physischen Zugriffs auf die Fahrzeugelektronik als externer Angreifer                                                                                                                                                                                          | C11 Denial-of-Service-Schutz für sicherheitskritische Komponenten<br><br>A3 Qualitätsschäden werden im Falle eines kompromittierten Lkw selektiv berücksichtigt.<br>A6 Lokale Angreifer | DS5 [O2], DS6 [S3 F2OEM], DS7 [O2], DS8 [O1]<br><br>DS5, DS7, DS8, DS11, DS6, DS12, DS13                                                     |   | H | 1 | DS5 [O2], DS6 [S3 F2OEM], DS7 [O2], DS8 [O1]<br><br>DS6>DS7, DS5, DS7, DS8, DS11, DS6, DS12, DS13                                            |   | H  | 1 |
| R189: T81 Denial-of-Service-Angriff auf das System Management, vorbereitet durch P4 Erlangung des Zugriffs auf einen Online-Fahrzeugbus durch Fernkompromittierung einer angeschlossenen ECU                                                                                                                                                                 | C11 Denial-of-Service-Schutz für sicherheitskritische Komponenten<br><br>A3 Qualitätsschäden werden im Falle eines kompromittierten Lkw selektiv berücksichtigt                         | DS5 [O2], DS6 [S3 F2OEM], DS7 [O2], DS8 [O1]<br><br>DS5, DS7, DS8, DS11<br>DS6 [S3 F2OEM]                                                    | S | H | 5 | DS5 [O2], DS6 [S3 F2OEM], DS7 [O2], DS8 [O1]<br><br>DS6>DS7, DS5, DS7, DS8, DS11                                                             |   | H  | 1 |
| R190: T82 Manipulation von Daten, Parametern oder Software von ADS-Kernkomponenten Vorbereitung durch P6 Angriff über lokalen Diagnosezugriff<br><br>Hinweis: Die Manipulation von Informationen aus dem Speicher einer Komponente erfordert im Vergleich zum Spoofing oder zur Manipulation von Informationen auf einem Fahrzeugbus einen erhöhten Aufwand. | C13 Signierte Software-Updates und Parameter<br>C14 Signierte Token für die Autorisierung von Diagnosediensten                                                                          | DS1 [P2], DS2 [F0OEM], DS3 [F3OEM], DS5 [O2], DS6 [S3 F2OEM], DS7 [O2], DS8 [O1], DS12 [S3 F2OEM], DS13 [S3 F3OEM], DS14 [F0RU], DS18 [F1RU] | S | M | 4 | DS1 [P2], DS2 [F0OEM], DS3 [F3OEM], DS5 [O2], DS6 [S3 F2OEM], DS7 [O2], DS8 [O1], DS12 [S3 F2OEM], DS13 [S3 F3OEM], DS14 [F0RU], DS18 [F1RU] | S | SG | 2 |
| R191: T82 Manipulation von Daten, Parametern oder Software von ADS-Kernkomponenten, vorbereitet durch P7 Angriff über Ferndiagnosezugriff                                                                                                                                                                                                                    | C13 Signierte Software-Updates und Parameter<br>C14 Signierte Token für die                                                                                                             | DS1 [P2], DS2 [F0OEM], DS3 [F3OEM], DS5 [O2], DS6 [S3 F2OEM], DS7                                                                            | S | M | 4 | DS1 [P2], DS2 [F0OEM], DS3 [F3OEM], DS5 [O2], DS6 [S3 F2OEM], DS7                                                                            | S | SG | 2 |



|                                                                                                                                                                                                                                                                                                                                                                                               |                                                                         |                                                                                                                                              |   |   |   |                                                                                                                                              |   |    |   |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------|---|---|---|----------------------------------------------------------------------------------------------------------------------------------------------|---|----|---|
| Hinweis: Die Manipulation von Informationen aus dem Speicher einer Komponente erfordert im Vergleich zum Spoofing oder zur Manipulation von Informationen auf einem Fahrzeugbus einen erhöhten Aufwand.                                                                                                                                                                                       | Autorisierung von Diagnose-diensten                                     | [O2], DS8 [O1], DS12 [S3 F2OEM], DS13 [S3 F3OEM], DS14 [F0RU], DS18 [F1RU]                                                                   |   |   |   | [O2], DS8 [O1], DS12 [S3 F2OEM], DS13 [S3 F3OEM], DS14 [F0RU], DS18 [F1RU]                                                                   |   |    |   |
| R192: T82 Manipulation von Daten, Parametern oder Software von ADS-Kernkomponenten, vorbereitet durch P8 Angriff über Debugging-, Entwicklungs- oder Produktionsschnittstellen<br><br>Hinweis: Die Manipulation von Informationen aus dem Speicher einer Komponente erfordert im Vergleich zum Spoofing oder zur Manipulation von Informationen auf einem Fahrzeugbus einen erhöhten Aufwand. | C15 Gesicherte Debugging-, Entwicklungs- und Produkti-onsschnittstellen | DS1 [P2], DS2 [F0OEM], DS3 [F3OEM], DS5 [O2], DS6 [S3 F2OEM], DS7 [O2], DS8 [O1], DS12 [S3 F2OEM], DS13 [S3 F3OEM], DS14 [F0RU], DS18 [F1RU] | S | M | 4 | DS1 [P2], DS2 [F0OEM], DS3 [F3OEM], DS5 [O2], DS6 [S3 F2OEM], DS7 [O2], DS8 [O1], DS12 [S3 F2OEM], DS13 [S3 F3OEM], DS14 [F0RU], DS18 [F1RU] | S | SG | 2 |
| R193: T82 Manipulation von Daten, Parametern oder Software von ADS-Kernkomponenten, vorbereitet durch P9 Angriff über direkten Speicherzugriff<br><br>Hinweis: Die Manipulation von Informationen aus dem Speicher einer Komponente erfordert im Vergleich zum Spoofing oder zur Manipulation von Informationen auf einem Fahrzeugbus einen erhöhten Aufwand.                                 | C16 Sicherer Startvorgang                                               | DS1 [P2], DS2 [F0OEM], DS3 [F3OEM], DS5 [O2], DS6 [S3 F2OEM], DS7 [O2], DS8 [O1], DS12 [S3 F2OEM], DS13 [S3 F3OEM], DS14 [F0RU], DS18 [F1RU] | S | M | 4 | DS1 [P2], DS2 [F0OEM], DS3 [F3OEM], DS5 [O2], DS6 [S3 F2OEM], DS7 [O2], DS8 [O1], DS12 [S3 F2OEM], DS13 [S3 F3OEM], DS14 [F0RU], DS18 [F1RU] | S | SG | 2 |
| R194: T82 Manipulation von Daten, Parametern oder Software von ADS-Kernkomponenten, vorbereitet durch P10 Angriff über unnötige Internet-Ports                                                                                                                                                                                                                                                | C17 Entfernung unnötiger Inter-net-Ports                                | DS1 [P2], DS2 [F0OEM], DS3 [F3OEM], DS5 [O2], DS6 [S3 F2OEM], DS7 [O2], DS8 [O1], DS12 [S3 F2OEM], DS13                                      | S | M | 4 | DS1 [P2], DS2 [F0OEM], DS3 [F3OEM], DS5 [O2], DS6 [S3 F2OEM], DS7 [O2], DS8 [O1], DS12 [S3 F2OEM], DS13                                      | S | SG | 2 |

|                                                                                                                                                                                                         |                                                                                                                                                                                                                       |                                                                                                                                              |   |   |   |                                                                                                                                                                                                                                  |   |    |   |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------|---|---|---|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|----|---|
| Hinweis: Die Manipulation von Informationen aus dem Speicher einer Komponente erfordert im Vergleich zum Spoofing oder zur Manipulation von Informationen auf einem Fahrzeugbus einen erhöhten Aufwand. |                                                                                                                                                                                                                       | [S3 F3OEM], DS14<br>[F0RU], DS18 [F1RU]                                                                                                      |   |   |   | [S3 F3OEM], DS14<br>[F0RU], DS18 [F1RU]                                                                                                                                                                                          |   |    |   |
| R195: T82 Manipulation von Daten, Parametern oder Software von ADS-Kernkomponenten, vorbereitet durch P13 Manipulation von kryptografischem Material                                                    | C19 Speicherung von kryptografischem Material in Hardware-Sicherheitsmodulen                                                                                                                                          | DS1 [P2], DS2 [F0OEM], DS3 [F3OEM], DS5 [O2], DS6 [S3 F2OEM], DS7 [O2], DS8 [O1], DS12 [S3 F2OEM], DS13 [S3 F3OEM], DS14 [F0RU], DS18 [F1RU] | S | M | 4 | DS1 [P2], DS2 [F0OEM], DS3 [F3OEM], DS5 [O2], DS6 [S3 F2OEM], DS7 [O2], DS8 [O1], DS12 [S3 F2OEM], DS13 [S3 F3OEM], DS14 [F0RU], DS18 [F1RU]                                                                                     | S | SG | 2 |
| Hinweis: Die Manipulation von Informationen aus dem Speicher einer Komponente erfordert im Vergleich zum Spoofing oder zur Manipulation von Informationen auf einem Fahrzeugbus einen erhöhten Aufwand. |                                                                                                                                                                                                                       |                                                                                                                                              |   |   |   |                                                                                                                                                                                                                                  |   |    |   |
| R196: T83 Manipulation von Daten, Parametern oder Software der Missionskontrollvorbereitung durch P6 Angriff über lokalen Diagnosezugriff                                                               | C7 Verschlüsselte Übertragung vertraulicher Daten,<br>C21 End-to-End-Signatur virtueller Sensordaten,<br>C13 Signierte Software-Updates und Parameter,<br>C14 Signierte Tokens zur Autorisierung von Diagnosediensten | DS1 [P2], DS2 [F0OEM], DS5 [O2], DS7 [O2], DS8 [O1], DS11 [O1], DS12 [S3 F2OEM], DS13 [S3 F3OEM], DS14 [F0RU], DS18 [F1RU]                   | S | M | 4 | DS1 [P2], DS2 [F0OEM], DS5 [O2], DS7 [O2], DS8 [O1], DS11 [O1], DS12 [S3 F3OEM], DS13 [S3 F3OEM], DS14 [F0RU], DS18 [F1RU]<br><br>DS1, DS18, DS12, DS13<br><br>DS2 [F0OEM], DS5 [O2], DS7 [O2], DS8 [O1], DS11 [O1], DS14 [F0RU] | E | SG | 2 |
| Hinweis: Die Manipulation von Informationen aus dem Speicher einer Komponente erfordert im Vergleich zum Spoofing oder zur Manipulation von Informationen auf einem Fahrzeugbus einen erhöhten Aufwand. |                                                                                                                                                                                                                       |                                                                                                                                              |   |   |   |                                                                                                                                                                                                                                  |   |    |   |
| R197: T83 Manipulation von Daten, Parametern oder Software der Mission Control durch P7 Angriff über Ferndiagnosezugriff                                                                                | C7 Verschlüsselte Übertragung vertraulicher Daten,<br>C21 End-to-End-Signatur virtueller Sensordaten,                                                                                                                 | DS1 [P2], DS2 [F0OEM], DS5 [O2], DS7 [O2], DS8 [O1], DS11 [O1], DS12 [S3 F2OEM],                                                             | S | M | 4 | DS1 [P2], DS2 [F0OEM], DS5 [O2], DS7 [O2], DS8 [O1], DS11 [O1], DS12 [S3 F3OEM],                                                                                                                                                 | E | SG | 2 |

|                                                                                                                                                                                                                                                                                                                                                                              |                                                                                                                                                                                 |                                                                                                                                              |   |   |   |                                                                                                                                                                                                                                                          |   |    |   |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------|---|---|---|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|----|---|
| Hinweis: Die Manipulation von Informationen aus dem Speicher einer Komponente erfordert im Vergleich zum Spoofing oder zur Manipulation von Informationen auf einem Fahrzeugbus einen erhöhten Aufwand.                                                                                                                                                                      | C13 Signierte Software-Up-<br>dates und Parameter,<br>C14 Signierte Tokens zur Auto-<br>risierung von Diagnosediensten                                                          | DS13 [S3 F3OEM],<br>DS14 [F0RU], DS18<br>[F1RU]                                                                                              |   |   |   | DS13 [S3 F3OEM],<br>DS14 [F0RU], DS18<br>[F1RU]<br><br>DS1, DS18, DS12, DS13<br><br>DS2 [F0OEM], DS5 [O2],<br>DS7 [O2], DS8 [O1],<br>DS11 [O1], DS14 [F0RU]                                                                                              |   |    |   |
| R198: T83 Manipulation von Daten, Parametern oder Software der Mission Control durch P8 Angriff über Debugging-, Entwicklungs- oder Produktionsschnittstellen<br><br>Hinweis: Die Manipulation von Informationen aus dem Speicher einer Komponente erfordert im Vergleich zum Spoofing oder zur Manipulation von Informationen auf einem Fahrzeugbus einen erhöhten Aufwand. | C7 Verschlüsselte Übertragung vertraulicher Daten,<br>C21 End-to-End-Signatur virtueller Sensordaten,<br>C15 Gesicherte Debugging-, Entwicklungs- und Produktionsschnittstellen | DS1 [P2], DS2 [F0OEM],<br>DS5 [O2], DS7 [O2],<br>DS8 [O1], DS11 [O1],<br>DS12 [S3 F2OEM],<br>DS13 [S3 F3OEM],<br>DS14 [F0RU], DS18<br>[F1RU] | S | M | 4 | DS1 [P2], DS2 [F0OEM],<br>DS5 [O2], DS7 [O2],<br>DS8 [O1], DS11 [O1],<br>DS12 [S3 F3OEM],<br>DS13 [S3 F3OEM],<br>DS14 [F0RU], DS18<br>[F1RU]<br><br>DS1, DS18, DS12, DS13<br><br>DS2 [F0OEM], DS5 [O2],<br>DS7 [O2], DS8 [O1],<br>DS11 [O1], DS14 [F0RU] | E | SG | 2 |
| R199: T83 Manipulation von Daten, Parametern oder Software der Mission Control durch P9 Angriff über direkten Speicherzugriff<br><br>Hinweis: Die Manipulation von Informationen aus dem Speicher einer Komponente erfordert im Vergleich zum                                                                                                                                | C7 Verschlüsselte Übertragung vertraulicher Daten,<br>C21 End-to-End-Signatur virtueller Sensordaten,<br>C16 Sicherer Startvorgang                                              | DS1 [P2], DS2 [F0OEM],<br>DS5 [O2], DS7 [O2],<br>DS8 [O1], DS11 [O1],<br>DS12 [S3 F2OEM],<br>DS13 [S3 F3OEM],<br>DS14 [F0RU], DS18<br>[F1RU] | S | M | 4 | DS1 [P2], DS2 [F0OEM],<br>DS5 [O2], DS7 [O2],<br>DS8 [O1], DS11 [O1],<br>DS12 [S3 F3OEM],<br>DS13 [S3 F3OEM],<br>DS14 [F0RU], DS18<br>[F1RU]                                                                                                             | E | SG | 2 |

|                                                                                                                                                                                                                                                                                                                                                          |                                                                                                                                                  |                                                                                                                            |   |   |   |                                                                                                                                                                                                                                  |   |    |   |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------|---|---|---|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|----|---|
| Spoofing oder zur Manipulation von Informationen auf einem Fahrzeugbus einen erhöhten Aufwand.                                                                                                                                                                                                                                                           |                                                                                                                                                  |                                                                                                                            |   |   |   | DS1, DS18, DS12, DS13                                                                                                                                                                                                            |   |    |   |
|                                                                                                                                                                                                                                                                                                                                                          |                                                                                                                                                  |                                                                                                                            |   |   |   | DS2 [F0OEM], DS5 [O2], DS7 [O2], DS8 [O1], DS11 [O1], DS14 [F0RU]                                                                                                                                                                |   |    |   |
| R200: T83 Manipulation von Daten, Parametern oder Software der Mission Control Vorbereitung durch P10 Angriff über unnötige Internetports<br><br>Hinweis: Die Manipulation von Informationen aus dem Speicher einer Komponente erfordert im Vergleich zum Spoofing oder zur Manipulation von Informationen auf einem Fahrzeugbus einen erhöhten Aufwand. | C7 Verschlüsselte Übertragung vertraulicher Daten,<br>C21 End-to-End-Signatur virtueller Sensordaten,<br>C17 Entfernung unnötiger Internet-Ports | DS1 [P2], DS2 [F0OEM], DS5 [O2], DS7 [O2], DS8 [O1], DS11 [O1], DS12 [S3 F2OEM], DS13 [S3 F3OEM], DS14 [F0RU], DS18 [F1RU] | S | M | 4 | DS1 [P2], DS2 [F0OEM], DS5 [O2], DS7 [O2], DS8 [O1], DS11 [O1], DS12 [S3 F3OEM], DS13 [S3 F3OEM], DS14 [F0RU], DS18 [F1RU]<br><br>DS1, DS18, DS12, DS13<br><br>DS2 [F0OEM], DS5 [O2], DS7 [O2], DS8 [O1], DS11 [O1], DS14 [F0RU] | E | SG | 2 |
| R201: T83 Manipulation von Daten, Parametern oder Software der Mission Control Vorbereitung durch P11 Angriff über Remote-Schnittstellen<br><br>Hinweis: Die Manipulation von Informationen aus dem Speicher einer Komponente erfordert im Vergleich zum Spoofing oder zur Manipulation von Informationen auf einem Fahrzeugbus einen erhöhten Aufwand.  | C7 Verschlüsselte Übertragung vertraulicher Daten,<br>C21 End-to-End-Signatur virtueller Sensordaten,<br>C18 Schutz vor Fernangriffen            | DS1 [P2], DS2 [F0OEM], DS5 [O2], DS7 [O2], DS8 [O1], DS11 [O1], DS12 [S3 F2OEM], DS13 [S3 F3OEM], DS14 [F0RU], DS18 [F1RU] | S | M | 4 | DS1 [P2], DS2 [F0OEM], DS5 [O2], DS7 [O2], DS8 [O1], DS11 [O1], DS12 [S3 F3OEM], DS13 [S3 F3OEM], DS14 [F0RU], DS18 [F1RU]<br><br>DS1, DS18, DS12, DS13                                                                          | E | G  | 3 |

|                                                                                                                                                                                                                                                                                                                                                                        |                                                                                                                                                                                                |                                                                                                                                   |   |   |   |                                                                                                                                                                                                                                         |   |    |   |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------|---|---|---|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|----|---|
|                                                                                                                                                                                                                                                                                                                                                                        |                                                                                                                                                                                                |                                                                                                                                   |   |   |   | DS2 [F0OEM], DS5 [O2],<br>DS7 [O2], DS8 [O1],<br>DS11 [O1], DS14 [F0RU]                                                                                                                                                                 |   |    |   |
| <p>R202: T83 Manipulation von Daten, Parametern oder Software der Mission Control Vorbereitung durch P13 Manipulation von kryptografischem Material</p> <p>Hinweis: Die Manipulation von Informationen aus dem Speicher einer Komponente erfordert im Vergleich zum Spoofing oder zur Manipulation von Informationen auf einem Fahrzeugbus einen erhöhten Aufwand.</p> | <p>C7 Verschlüsselte Übertragung vertraulicher Daten,<br/>C21 End-to-End-Signatur virtueller Sensordaten,<br/>C19 Speicherung von kryptografischem Material in Hardware-Sicherheitsmodulen</p> | <p>DS1 [P2], DS2 [F0OEM], DS5 [O2], DS7 [O2], DS8 [O1], DS11 [O1], DS12 [S3 F2OEM], DS13 [S3 F3OEM], DS14 [F0RU], DS18 [F1RU]</p> | S | M | 4 | <p>DS1 [P2], DS2 [F0OEM], DS5 [O2], DS7 [O2], DS8 [O1], DS11 [O1], DS12 [S3 F3OEM], DS13 [S3 F3OEM], DS14 [F0RU], DS18 [F1RU]</p> <p>DS1, DS18, DS12, DS13</p> <p>DS2 [F0OEM], DS5 [O2], DS7 [O2], DS8 [O1], DS11 [O1], DS14 [F0RU]</p> | E | SG | 2 |
| <p>R203: T84 Manipulation von Daten, Parametern oder Software der System Management durch P6 Angriff über lokalen Diagnosezugriff</p> <p>Hinweis: Die Manipulation von Informationen aus dem Speicher einer Komponente erfordert im Vergleich zum Spoofing oder zur Manipulation von Informationen auf einem Fahrzeugbus einen erhöhten Aufwand.</p>                   | <p>C13 Signierte Software-Updates und Parameter<br/>C14 Signierte Token für die Autorisierung von Diagnosediensten</p>                                                                         | <p>DS2 [F0OEM], DS4 [F1OEM], DS5 [O2], DS6 [S3 F2OEM], DS7 [O2], DS8 [O1], DS11 [O1], DS12 [S3 F2OEM], DS18 [F1RU]</p>            | S | M | 4 | <p>DS2 [F0OEM], DS4 [F1OEM], DS5 [O2], DS6 [S3 F2OEM], DS7 [O2], DS8 [O1], DS11 [O1], DS12 [S3 F2OEM], DS18 [F1RU]</p>                                                                                                                  | S | SG | 2 |
| <p>R204: T84 Manipulation von Daten, Parametern oder Software der System Management durch P7 Angriff über Ferndiagnosezugriff</p>                                                                                                                                                                                                                                      | <p>C13 Signierte Software-Updates und Parameter<br/>C14 Signierte Token für die</p>                                                                                                            | <p>DS2 [F0OEM], DS4 [F1OEM], DS5 [O2], DS6 [S3 F2OEM], DS7 [O2], DS8 [O1], DS11 [O1],</p>                                         | S | M | 4 | <p>DS2 [F0OEM], DS4 [F1OEM], DS5 [O2], DS6 [S3 F2OEM], DS7 [O2], DS8 [O1], DS11 [O1],</p>                                                                                                                                               | S | SG | 2 |

|                                                                                                                                                                                                                                                                                                                                                                                |                                                                        |                                                                                                                 |   |   |   |                                                                                                                 |   |    |   |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------|---|---|---|-----------------------------------------------------------------------------------------------------------------|---|----|---|
| Hinweis: Die Manipulation von Informationen aus dem Speicher einer Komponente erfordert im Vergleich zum Spoofing oder zur Manipulation von Informationen auf einem Fahrzeugbus einen erhöhten Aufwand.                                                                                                                                                                        | Autorisierung von Diagnose-diensten                                    | DS12 [S3 F2OEM], DS18 [F1RU]                                                                                    |   |   |   | DS12 [S3 F2OEM], DS18 [F1RU]                                                                                    |   |    |   |
| R205: T84 Manipulation von Daten, Parametern oder Software der System Management durch P8 Angriff über Debugging-, Entwicklungs- oder Produktionsschnittstellen<br><br>Hinweis: Die Manipulation von Informationen aus dem Speicher einer Komponente erfordert im Vergleich zum Spoofing oder zur Manipulation von Informationen auf einem Fahrzeugbus einen erhöhten Aufwand. | C15 Gesicherte Debugging-, Entwicklungs- und Produktionsschnittstellen | DS2 [F0OEM], DS4 [F1OEM], DS5 [O2], DS6 [S3 F2OEM], DS7 [O2], DS8 [O1], DS11 [O1], DS12 [S3 F2OEM], DS18 [F1RU] | S | M | 4 | DS2 [F0OEM], DS4 [F1OEM], DS5 [O2], DS6 [S3 F2OEM], DS7 [O2], DS8 [O1], DS11 [O1], DS12 [S3 F2OEM], DS18 [F1RU] | S | SG | 2 |
| R206: T84 Manipulation von Daten, Parametern oder Software der System Management durch P9 Angriff über direkten Speicherzugriff<br><br>Hinweis: Die Manipulation von Informationen aus dem Speicher einer Komponente erfordert im Vergleich zum Spoofing oder zur Manipulation von Informationen auf einem Fahrzeugbus einen erhöhten Aufwand.                                 | C16 Sicherer Startvorgang                                              | DS2 [F0OEM], DS4 [F1OEM], DS5 [O2], DS6 [S3 F2OEM], DS7 [O2], DS8 [O1], DS11 [O1], DS12 [S3 F2OEM], DS18 [F1RU] | S | M | 4 | DS2 [F0OEM], DS4 [F1OEM], DS5 [O2], DS6 [S3 F2OEM], DS7 [O2], DS8 [O1], DS11 [O1], DS12 [S3 F2OEM], DS18 [F1RU] | S | SG | 2 |
| R207: T84 Manipulation von Daten, Parametern oder Software der System Management durch P10 Angriff über unnötige Internet-Ports<br><br>Hinweis: Die Manipulation von Informationen aus dem Speicher einer Komponente erfordert im Vergleich zum                                                                                                                                | C17 Entfernung unnötiger Internet-Ports                                | DS2 [F0OEM], DS4 [F1OEM], DS5 [O2], DS6 [S3 F2OEM], DS7 [O2], DS8 [O1], DS11 [O1], DS12 [S3 F2OEM], DS18 [F1RU] | S | M | 4 | DS2 [F0OEM], DS4 [F1OEM], DS5 [O2], DS6 [S3 F2OEM], DS7 [O2], DS8 [O1], DS11 [O1], DS12 [S3 F2OEM], DS18 [F1RU] | S | SG | 2 |

|                                                                                                                                                                                                                                                                                                                                                             |                                                                                                                           |                                                                                                                 |   |   |   |                                                                                                                 |   |    |   |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------|---|---|---|-----------------------------------------------------------------------------------------------------------------|---|----|---|
| Spoofing oder zur Manipulation von Informationen auf einem Fahrzeugbus einen erhöhten Aufwand.                                                                                                                                                                                                                                                              |                                                                                                                           |                                                                                                                 |   |   |   |                                                                                                                 |   |    |   |
| <p>R208: T84 Manipulation von Daten, Parametern oder Software der System Management durch P13 Manipulation von kryptografischem Material</p> <p>Hinweis: Die Manipulation von Informationen aus dem Speicher einer Komponente erfordert im Vergleich zum Spoofing oder zur Manipulation von Informationen auf einem Fahrzeugbus einen erhöhten Aufwand.</p> | C19 Speicherung von kryptografischem Material in Hardware-Sicherheitsmodulen                                              | DS2 [F0OEM], DS4 [F1OEM], DS5 [O2], DS6 [S3 F2OEM], DS7 [O2], DS8 [O1], DS11 [O1], DS12 [S3 F2OEM], DS18 [F1RU] | S | M | 4 | DS2 [F0OEM], DS4 [F1OEM], DS5 [O2], DS6 [S3 F2OEM], DS7 [O2], DS8 [O1], DS11 [O1], DS12 [S3 F2OEM], DS18 [F1RU] | S | SG | 2 |
| <p>R209: P6 Angriff über lokalen Diagnosezugriff</p> <p>Hinweis: Dieser Vorbereitungsschritt allein verursacht keine Schadensszenarien.</p>                                                                                                                                                                                                                 | <p>C13 Signierte Software-Updates und Parameter</p> <p>C14 Signierte Token für die Autorisierung von Diagnosediensten</p> |                                                                                                                 |   | H | 1 |                                                                                                                 |   | SG | 1 |
| <p>R210: P7 Angriff über den Ferndiagnosezugriff</p> <p>Hinweis: Dieser Vorbereitungsschritt allein verursacht keine Schadensszenarien.</p>                                                                                                                                                                                                                 | <p>C13 Signierte Software-Updates und Parameter</p> <p>C14 Signierte Token für die Autorisierung von Diagnosediensten</p> |                                                                                                                 |   | H | 1 |                                                                                                                 |   | SG | 1 |
| <p>R211: P8 Angriff über Debugging-, Entwicklungs- oder Produktionsschnittstellen</p> <p>Hinweis: Dieser Vorbereitungsschritt allein verursacht keine Schadensszenarien.</p>                                                                                                                                                                                | C15 Gesicherte Debugging-, Entwicklungs- und Produktionsschnittstellen                                                    |                                                                                                                 |   | H | 1 |                                                                                                                 |   | SG | 1 |
| R212: P9 Angriff über direkten Speicherzugriff                                                                                                                                                                                                                                                                                                              | C16 Sicherer Startvorgang                                                                                                 |                                                                                                                 |   | H | 1 |                                                                                                                 |   | SG | 1 |



|                                                                                 |                                                                              |  |  |   |   |  |  |    |   |
|---------------------------------------------------------------------------------|------------------------------------------------------------------------------|--|--|---|---|--|--|----|---|
| Hinweis: Dieser Vorbereitungsschritt allein verursacht keine Schadensszenarien. |                                                                              |  |  |   |   |  |  |    |   |
| R213: P10 Angriff über unnötige Internet-Ports                                  | C17 Entfernung unnötiger Internet-Ports                                      |  |  | H | 1 |  |  | SG | 1 |
| Hinweis: Dieser Vorbereitungsschritt allein verursacht keine Schadensszenarien. |                                                                              |  |  |   |   |  |  |    |   |
| R214: P11 Angriff über Remote-Schnittstellen                                    | C18 Schutz vor Fernangriffen                                                 |  |  | H | 1 |  |  | G  | 1 |
| Hinweis: Dieser Vorbereitungsschritt allein verursacht keine Schadensszenarien. |                                                                              |  |  |   |   |  |  |    |   |
| R215: P12 Extrahieren von kryptografischem Material                             | C19 Speicherung von kryptografischem Material in Hardware-Sicherheitsmodulen |  |  | H | 1 |  |  | SG | 1 |
| Hinweis: Dieser Vorbereitungsschritt allein verursacht keine Schadensszenarien. |                                                                              |  |  |   |   |  |  |    |   |
| R216: P13 Manipulation von kryptografischem Material                            | C19 Speicherung von kryptografischem Material in Hardware-Sicherheitsmodulen |  |  | H | 1 |  |  | SG | 1 |
| Hinweis: Dieser Vorbereitungsschritt allein verursacht keine Schadensszenarien. |                                                                              |  |  |   |   |  |  |    |   |

#### **2.1.18.4 Grundsätze für die Durchführung von Security-Risikoanalysen für automatisierte Fahrsysteme**

Wir haben 18 Schadensszenarien, 216 Bedrohungsszenarien, 11 Annahmen und 20 Schutzmaßnahmen identifiziert und diese in mehreren Gesprächen mit einem globalen Lkw-Hersteller verfeinert. Aus unserer CRA haben wir die folgenden Grundsätze abgeleitet, um zukünftigen Cybersicherheitsanalysten zu helfen, sich auf die kritischen Aspekte ihrer CRAs zu ADS zu konzentrieren.

Bedrohungsszenarien, die die Vertraulichkeit von Vermögenswerten verletzen, müssen durch Schutzmaßnahmen angemessen gemindert werden, wenn die Offenlegung von Videodaten durch Abgreifen von Rohvideodaten über mobile Verbindungen, Online-Busse oder Fahrzeugbusse, auf die durch geringfügige Zerstörung von der Fahrzeugaußenseite aus zugegriffen werden kann, hervorgerufen werden kann.

Bedrohungsszenarien, die die Verfügbarkeit von Anlagen beeinträchtigen, müssen durch Schutzmaßnahmen angemessen gemindert werden, wenn der Verlust der ADS-Funktion während des Betriebs durch Datenverlust auf Online-Bussen oder DoS-Angriffe über Online-Busse auf Komponenten ausgelöst werden kann, um deren Funktionalität außer Kraft zu setzen. Schutzmaßnahmen sind auch erforderlich, wenn der Verlust der ADS-Funktion im Ruhezustand oder die falsche Auslösung eines MRM durch DoS-Angriffe auf Komponenten ausgelöst werden kann, die über eine externe drahtlose Schnittstelle (in unserem Beispiel Mission Control) direkt erreichbar sind.

Bedrohungsszenarien, die die Integrität von Anlagen beeinträchtigen, müssen durch Schutzmaßnahmen für alle über mobile Verbindungen übertragenen Daten angemessen gemindert werden. Dies ist ebenfalls erforderlich, wenn eine Aktivierung außerhalb des ODD (Tuning Interest) durch Spoofing oder Manipulation der Eingangssignale zur Wahrnehmung (Rohvideofeed, virtuelle Sensordaten) oder der Signale im ADS-Regelkreis (fusionierte Sensordaten, Objektbahnen, geplante Bahn) ausgelöst werden kann. Schutzmaßnahmen sind auch erforderlich, wenn gefährliche Fahrmanöver oder eine Aktivierung außerhalb des ODD durch Spoofing oder Manipulation von Daten auf Online-Bussen (virtuelle Sensordaten, Eingaben des Basisfahrzeugs) oder durch Fernangriffe ausgelöst werden können, bei denen Komponenten durch Ausnutzung von Software-Schwachstellen kompromittiert werden könnten. Dies gilt insbesondere für Komponenten, die den Endpunkt einer externen Kommunikation bilden (in unserem Beispiel die Mission Control). Hier können Sicherheitsschadensszenarien verhindert werden, indem die virtuellen Sensordaten vom CC durchgehend signiert und in der Wahrnehmung verifiziert werden.

In allen Aspekten muss berücksichtigt werden, dass Angreifer möglicherweise mehr als eine Verbindung angreifen können, sodass Schutzmaßnahmen wie die Validierung von Sensordaten durch Sensorfusion oder Redundanz gegen die Aktivierung von ADS außerhalb von ODD in diesem Fall möglicherweise nicht wirksam sind.

#### **2.1.19 Security-Risikoanalyse eines Control Centers**

##### **2.1.19.1 Kurzfassung**

Wenn es einem Angreifer gelingt, die Cybersicherheitseigenschaften Vertraulichkeit, Integrität oder Verfügbarkeit von Teilen des Bewertungsobjekts (TOE) zu verletzen, können 19 Schadensszenarien in den Auswirkungskategorien Sicherheit, Finanzen, Datenschutz und Betrieb verursacht werden. Beispiele mit hoher Auswirkungsbewertung sind DS1 Offenlegung von Videodaten, DS9

Betrieb der Fahrzeugflotte nicht möglich, DS13s/DS13f Aktivierung außerhalb von ODD, DS15 Falsche Routenplanung für die Fahrzeugflotte und DS21 Falsche Auslösung eines MRM für die Fahrzeugflotte.

Die Cybersicherheitseigenschaften des TOE werden durch insgesamt 208 Bedrohungsszenarien bedroht, die sich aus einer Kombination von 89 Hauptangriffsschritten und 40 Vorbereitungsschritten zusammensetzen. Die Hauptangriffsschritte bedrohen die Datenflüsse und Komponenten des TOE, während die Vorbereitungsschritte bestimmen, wie auf sie zugegriffen wird (z. B. physisch oder aus der Ferne). Ohne jegliche Annahmen oder Schutzmaßnahmen führt die Realisierung dieser Bedrohungsszenarien zu 119 Risiken mit dem Wert 5, 53 Risiken mit dem Wert 4, 24 Risiken mit dem Wert 3, 0 Risiken mit dem Wert 2 und 12 Risiken mit dem Wert 1.

Die Bedrohungsszenarien werden einerseits durch 9 Annahmen behandelt, die entweder Schadensszenarien mindern oder transformieren oder den maximalen Risikowert begrenzen. Annahmen betreffen den Umfang der Analyse, z. B. A1 Angriffe auf den Lkw fallen nicht in den Umfang dieser Risikoanalyse, oder das Angreifer-Modell, z. B. A4 Begrenzte Störung des Mobilfunks. Darüber hinaus werden wichtige implementierungsrelevante Annahmen, die während der Entwicklung des TOE überprüft werden müssen, in Claims spezifiziert, z. B. A10 Durch CC ausgelöste MRM sind nicht sicherheitskritisch.

Andererseits werden die Bedrohungsszenarien durch 16 Schutzmaßnahmen behandelt, die sich ebenfalls auf Schadensszenarien oder die Bewertung der Durchführbarkeit von Angriffen auswirken. Lkw-Schutzmaßnahmen wie C5A/C5I Intrinsische Sicherheit des Lkw oder C20 ADS-Sicherheitsvalidierungen nach Entscheidungen des Control Centers sowie Schutzmaßnahmen des Control Centers wie C18 Härtung von internetfähigen Komponenten gegen Software-Schwachstellen oder C23 Schutz vor Distributed-Denial-of-Service-Angriffen (DDoS) für internetfähige Komponenten sind erforderlich, um die Risikowerte auf ein moderates Niveau zu senken. Mit den Schutzmaßnahmen dieser Maßnahmengruppen bleiben 44 Risiken mit einem Wert von 3 bestehen.

Um diese verbleibenden 44 Risiken auf ein akzeptables Niveau zu senken, d. h. ihren Risikowert auf höchstens 2, sollten weitere Schutzmaßnahmen implementiert werden: End-to-End-Schutzmaßnahmen, nämlich C27 für die Verschlüsselung und C28 für die Authentifizierung, stellen sicher, dass selbst eine kompromittierte Komponente des Control Centers keine Nachrichten vom/zum Lkw lesen oder schreiben kann. Darüber hinaus erhöht C29 Resilienz/Sicherheit durch Diversität die Systemresilienz, sodass die Wahrscheinlichkeit, dass ein einzelner Exploit oder eine einzelne Schwachstelle die Verfügbarkeit des gesamten Control Centers kompromittiert, verringert wird.

Unter Berücksichtigung aller Annahmen und Schutzmaßnahmen bleiben nur Risiken mit einem maximalen Wert von 2 übrig.

### **2.1.19.2 Methode**

Für die Security-Risikoanalyse des Control Centers wurde – analog zur CRA des automatisierten Fahrsystems (Abschnitt 2.1.18.2) – die in Abschnitt 2.1.1 beschriebene, für ATLAS-L4 angepasste MoRA-Methode eingesetzt. MoRA wurde dabei ISO/SAE-21434-konform und zugleich kompatibel zu ISO/IEC-27005 und den IT-/Cloud-Domänenanforderungen ausgelegt, sodass Fahrzeug-CSMS und Backend-ISMS auf einer gemeinsamen Bewertungslogik aufbauen.

Durch die Wiederverwendung derselben MoRA-Metamodelle, Bewertungsmaßstäbe und Kataloge wie in der ADS-Analyse und die Ergänzung um Cloud-/IT-spezifische Bedrohungen und Maßnahmen ergibt sich ein konsistenter, normkonformer Risikoüberblick über Lkw und Control Center hinweg.

### 2.1.19.3 Security-Risikoanalyse eines Control Centers für Lkw mit Level 4 Autonomiegrad

In den folgenden Unterabschnitten werden die relevantesten Aspekte unserer Security-Risikoanalyse vorgestellt.

#### Systemmodell

Ausgangspunkt war die Definition des Target of Evaluation „Control Center“ und dessen Zerlegung in Funktionen, Daten, Komponenten und Kommunikationsflüsse. Auf Basis von Architekturunterlagen und Experteninterviews (MAN, Fraunhofer AISEC) wurden unter anderem folgende Elemente modelliert:

- Komponenten wie Control-Center-Frontend/-Backend, Fahrzeugadapterdienst, Command Service, Event-Busse, API-Gateway, Datenbank, C2/Konnektivität sowie die Einbettung in die AWS-Cloud und angebundene externe Partner.
- Datenobjekte wie Lkw-Daten, Missions- und Routendaten, zusätzliche Umgebungsdaten (Video/Bild), Zustände von Lkw und Control Center, Kundendaten sowie MRM- und Aktivierungs-/Deaktivierungsbefehle.
- Kommunikationspfade (HTTP/gRPC/MQTT) zwischen Lkw, Control Center, AWS-Diensten und externen Systemen (z. B. dynamisches Routenmanagement, Flotten-Backends).

Tabelle 26, Tabelle 27, Tabelle 28 und Tabelle 29 enthalten Einzelheiten zu den Funktionen, Daten, Komponenten und Kommunikationstechnologien des Analysegegenstands, und Abbildung 49 zeigt einen Überblick über die Architektur.

Tabelle 26: Funktionen des Control Centers. Wenn Dx oder Nx in Spalte Architektur eingetragen ist, bedeutet dies, dass das Datum Dx oder der Datenfluss Nx für die Funktion relevant sind. Dies ist auch der Fall, wenn die ID einer Komponente, z. B. CC, aufgeführt ist.

| ID | Name                | Beschreibung                                                                                                                                                           | Architektur                                                                                                                                                                                                |
|----|---------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| F1 | Systemintegration   | Das Control Center ist in externe Systeme integriert und empfängt Informationen von diesen.                                                                            | N1, N2, N3, N4, N5, N6, N7, CCB, CFM, D8, D9, D10, DB, DRM, D6, APIG, D7, CC, AWS                                                                                                                          |
| F2 | Aktivierung des Lkw | Der Lkw wird über einen Befehl des Control Centers aktiviert und geweckt; ein Dispatcher sendet einen Aktivierungsstatus zurück an das Control Center.                 | N8, N9, N10, N11, N12, N13, N14, N15, N16, N17, N18, N19, N20, N21, N22, N23, N24, N25, N26, N27, N28, N29, N30, N31, TSE, CCF, D18, CCBF, CCB, DB, VAS, CS, TRK, C2, D19, CONE, CCE, D2, D4, DRM, CC, AWS |
| F3 | Überwachung des Lkw | Betriebsinformationen und der Zustand des Lkw werden an das Control Center gesendet. Zusätzlich übermittelt jede Komponente des Control Centers ihren eigenen Zustand. | N32, N33, N34, N35, N36, N37, N38, N39, N40, N41, TRK, C2, D3, D23, CONE, D24, VAS, CCE,                                                                                                                   |

|    |                               |                                                                                                                                                                                                                                                                                                             |                                                                                                                                                                                                                                                                                                                        |
|----|-------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|    |                               |                                                                                                                                                                                                                                                                                                             | CCB, DB, DRM, CCBF, CCF, TSE, AWS, CC, AWS                                                                                                                                                                                                                                                                             |
| F4 | Problemhilfe                  | Das Control Center kann weitere Umgebungsdaten und einen detaillierten Status des Lkw anfordern. Darüber hinaus kann der Lkw das Control Center über Funktionsbeeinträchtigungen informieren. Das Control Center kann eine Beeinträchtigung sowie die Position des Lkw an eine externe Stelle weiterleiten. | N42, N43, N44, N45, N46, N47, N48, N49, N50, N51, N52, N53, N54, N55, N56, N57, N58, N59, N60, N61, N62, N63, N64, N65, N66, N67, N68, N69, N70, N71, N72, N73, N74, N75, N76, N77, N78, N79, TSE, CCF, D13, D20, CCBF, CCB, DB, DRM, VAS, CS, TRK, C2, D14, D21, D11, CONE, CCE, EP, APIG, D12, D3, D15, D16, CC, AWS |
| F5 | Minimales Risikomanöver (MRM) | Ein MRM wird vom Control Center ausgelöst und anschließend vom Fahrzeug ausgeführt. Nachdem die Situation geklärt ist, hebt das Control Center das MRM auf.                                                                                                                                                 | N80, N81, N82, N83, N84, N85, N86, N87, N88, N89, N90, N91, N92, N93, N94, N95, TSE, CCF, D17, CCBF, CCB, DB, DRM, VAS, CS, TRK, D1, CC, AWS                                                                                                                                                                           |
| F6 | Deaktivierung des Lkw         | Ein technischer Supervisor sendet einen Deaktivierungsbefehl, nachdem der Lkw sein Ziel erreicht hat.                                                                                                                                                                                                       | N96, N97, N98, N99, N100, N101, N102, N103, TSE, CCF, D22, CCBF, CCB, DB, DRM, VAS, CS, TRK, CC, AWS                                                                                                                                                                                                                   |

Tabelle 27: Daten des Control Centers

| ID  | Name                             | Beschreibung                                                                                                                                    |
|-----|----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| D1  | Befehl zum Löschen von MRM       | Befehl zum Löschen/Freigeben einer bestehenden MRM-Bedingung                                                                                    |
| D2  | Befehl zum Starten einer Mission | Befehl zum Starten einer Mission                                                                                                                |
| D3  | Lkw-Daten                        | Lkw-Daten wie Position, Geschwindigkeit, Ausrichtung, Telemetriedaten und statische Informationen                                               |
| D4  | Missions- und Routendaten        | Mission: Startpunkt und Zielort des Fahrzeugs einschließlich geschätzter Daten wie Ankunftszeit<br><br>Route: Die geplante Route dieser Mission |
| D6  | ODDs/Aktivierte Routen anfordern | Anfrage des Control Centers nach ODDs/freigegebenen Routen                                                                                      |
| D7  | ODDs/Freigegebene Routen         | Routen, die autonome Lkw befahren dürfen                                                                                                        |
| D8  | Anfrage nach Flottendaten        | Anfrage des Control Centers nach Flottendaten                                                                                                   |
| D9  | Kundendaten                      | Informationen über die Fahrzeughalter, Beziehung zu Flotten, sonstige Kontaktdaten                                                              |
| D10 | Hub-Daten                        | Informationen zu den unterstützten Hubs                                                                                                         |

|     |                                               |                                                                                                                                                                                                                             |
|-----|-----------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| D11 | Verschlechterungen                            | Verschlechterungen aus Sicht des Fahrzeugs                                                                                                                                                                                  |
| D12 | Anfrage für Lkw-Daten                         | Anforderung von Lkw-Daten durch externe Partner                                                                                                                                                                             |
| D13 | Anforderung weiterer Umweltdaten              | Anfrage durch das Control Center nach weiteren Umgebungsdaten, die über Kameras als Bilder oder Videos erfasst wurden                                                                                                       |
| D14 | Weitere Umweltdaten                           | Weitere Umgebungsdaten, die über Kameras als Bilder oder Videos erfasst wurden                                                                                                                                              |
| D15 | Vorschlag für die zu genehmigende Fahrstrecke | Dies kann auch ein Kamerabild sein, das anstelle einer Fahrstrecke eine durchgezogene Linie und die Umgebung des Lkw zeigt. Nachdem der Technischer Supervisor das Bild genehmigt hat, wird die Fahrstrecke im Lkw geplant. |
| D16 | Genehmigung der zu genehmigenden Fahrstrecke  | Genehmigung durch einen Technischer Supervisor, dass die Fahrstrecke oder die vorgeschlagene Aufgabe vom Lkw ausgeführt werden kann.                                                                                        |
| D17 | MRM initiieren                                | Auslöser zur Durchführung eines MRM                                                                                                                                                                                         |
| D18 | Aktivierungsbefehl                            | Befehl des Control Centers zur Aktivierung des Lastwagens                                                                                                                                                                   |
| D19 | Aktivierungsbereiter Status                   | Nachdem der Disponent die Betriebsbereitschaft des Lkw überprüft hat, wird dieser Befehl an das Control Center gesendet.                                                                                                    |
| D20 | Anforderung detaillierter Fahrzeugdaten       | Anfrage des Control Centers nach detailliertem Fahrzeugstatus                                                                                                                                                               |
| D21 | Detaillierter Fahrzeugstatus                  | Detaillierte Fahrzeugzustands- und Fehlerprotokolle von ADS                                                                                                                                                                 |
| D22 | Deaktivierungsbefehl                          | Befehl zum Deaktivieren des Fahrzeugs                                                                                                                                                                                       |
| D23 | Zustand des Lkw                               | Die aktuelle Fähigkeit des Lkw, seine Funktionen auszuführen.                                                                                                                                                               |
| D24 | Zustand des Control Centers                   | Die aktuelle Funktionsfähigkeit der einzelnen Komponenten des Control Centers.                                                                                                                                              |

Tabelle 28: Komponenten des Control Centers

| ID   | Name                                | Beschreibung                                                                                    | Teil von       | Mitglied von |
|------|-------------------------------------|-------------------------------------------------------------------------------------------------|----------------|--------------|
| CC   | Control Center                      | Control Center-Anwendung zur Überwachung autonomer Lkw und zum Auslösen von Aktionen für diese. | AWS Cloud      |              |
| CCB  | Backend des Control Centers         | Bietet Funktionen zur Überwachung autonomer Lkw und zum Auslösen von Aktionen.                  | Control Center |              |
| CCF  | Control Center-Frontend             | Einzelseitige Anwendung zur Überwachung autonomer Lkw und zum Auslösen von Aktionen für diese.  | Control Center |              |
| CCBF | Control Center-Backend für Frontend | Schnittstelle zur Umwandlung von Modellen und Aufrufen zwischen Frontend-                       | Control Center |              |

|      |                               |                                                                                                                                                                                                            |                |  |
|------|-------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------|--|
|      |                               | Anwendung und Backend-Diensten, um Komponenten klar voneinander zu entkoppeln.                                                                                                                             |                |  |
| DB   | Datenbank                     | Datenbank, z. B. DynamoDB-Tabellen                                                                                                                                                                         | Control Center |  |
| APIG | API-Gateway                   | Zentrale Authentifizierung für externe Systeme                                                                                                                                                             | Control Center |  |
| CCE  | CC Eventbus                   | CC Eventbus                                                                                                                                                                                                | Control Center |  |
| VAS  | Fahrzeugadapterdienst         | Wandelt eingehende Nachrichten in ein internes Datenformat um                                                                                                                                              | Control Center |  |
| CFM  | Kunden-/Flottenmanagement     | Beziehung zwischen Kunden und Flotten.                                                                                                                                                                     | AWS Cloud      |  |
| CS   | Befehlsservice                | Stellt Schnittstellen zum Senden von Befehlen an die Lkw bereit.                                                                                                                                           | AWS Cloud      |  |
| TRK  | Lkw                           | Ein mit ADS ausgestatteter Lkw, der für den fahrerlosen Betrieb unter routinemäßigen/normalen Betriebsbedingungen während aller Fahrten innerhalb seines vorgegebenen Einsatzbereichs (ODD) ausgelegt ist. |                |  |
| EP   | Externe Partner               | Andere externe Partnersysteme, die für das Control Center relevant sind, z. B. für die Weiterleitung von Problemen.                                                                                        | AWS Cloud      |  |
| DRM  | Dynamisches Routenmanagement  | Verwaltet freigegebene Routen, auf denen autonome Lkw fahren dürfen.                                                                                                                                       | AWS Cloud      |  |
| TSE  | Technischer Supervisor Geräte | Geräte (Laptop oder Desktop-Client), über die ein technischer Supervisor mit dem Control Center Frontend interagiert.                                                                                      |                |  |
| C2   | C2 und Konnektivität          | C2: Stellt Positionsdaten für autonome Lkw bereit.<br><br>Konnektivität: Stellt Echtzeitdaten der autonomen Lkw bereit.                                                                                    | AWS Cloud      |  |
| CONE | Konnektivität Eventbus        | Konnektivität Eventbus                                                                                                                                                                                     | AWS Cloud      |  |
| AWS  | AWS Cloud                     | Amazon Web Services Cloud-Plattform                                                                                                                                                                        |                |  |

Tabelle 29: Kommunikationstechnologien des Control Centers

| ID | Name | Beschreibung |
|----|------|--------------|
|----|------|--------------|



|      |                                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|------|-------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| HTTP | Hypertext Transfer Protocol         | HTTP (Hypertext Transfer Protocol) ist seit seiner Einführung das Rückgrat des World Wide Web. Es folgt einem Anfrage-Antwort-Modell, bei dem ein Client eine Anfrage an einen Server sendet und der Server mit den angeforderten Daten antwortet. HTTP arbeitet auf der Anwendungsschicht und stützt sich in erster Linie auf Textnachrichten, wobei für die Datenserialisierung in der Regel JSON oder XML verwendet wird.                                  |
| gRPC | gRPC Remote Procedure Call          | gRPC ist ein modernes und leistungsstarkes Remote Procedure Call (RPC)-Framework. Es ermöglicht die sprachunabhängige Kommunikation zwischen Diensten, sodass Entwickler Dienstmethoden und deren Datenstrukturen mithilfe von Protocol Buffers (Protobufs) definieren können. gRPC unterstützt mehrere Programmiersprachen und verwendet HTTP/2 für den Transport, das Multiplexing, Header-Komprimierung und andere Verbesserungen gegenüber HTTP/1 bietet. |
| MQTT | Message Queuing Telemetry Transport | MQTT ist ein OASIS-Standard-Messaging-Protokoll für das Internet der Dinge (IoT). Es ist als extrem leichtgewichtiges Publish/Subscribe-Messaging-Transportprotokoll konzipiert, das sich ideal für die Verbindung von Remote-Geräten mit geringem Code-Footprint und minimaler Netzwerkbandbreite eignet. MQTT wird heute in einer Vielzahl von Branchen eingesetzt, darunter Automobilindustrie, Fertigung, Telekommunikation, Öl und Gas usw.              |

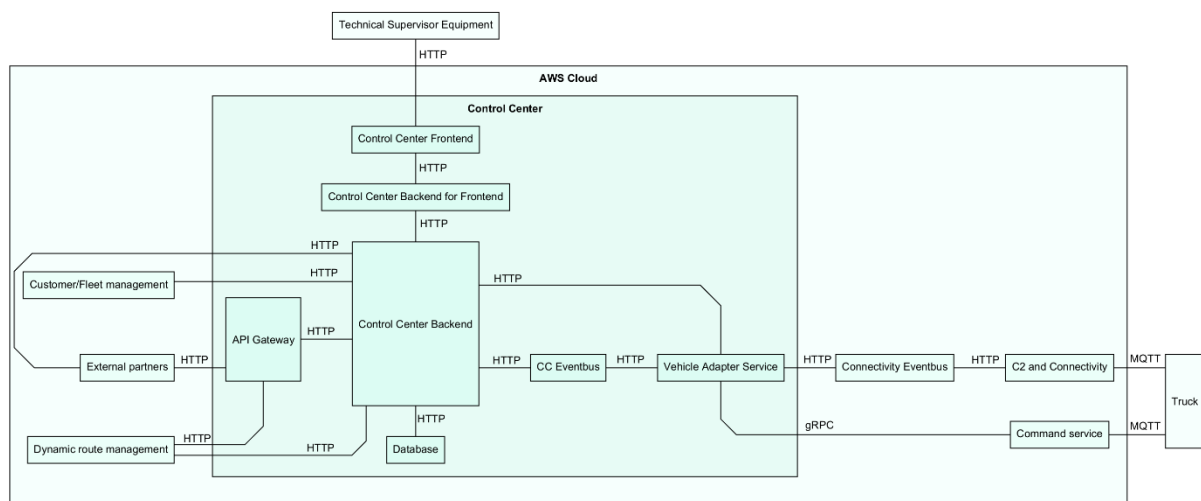


Abbildung 49: Control Center Diagramm, das die Komponenten und ihre Verbindungen zeigt.

Die Kommunikationsflüsse sind in Tabelle 30 aufgeführt und in Abbildung 50 dargestellt.

Tabelle 30: Kommunikationsflüsse des Control Centers

| ID | Sender                      | Empfänger                    | Datum                               | Datumsbeschreibung                                                                                                                   | Kommunikationstechnologie | Auslöser                                                          | Kommentar                                                                                                                                                                |
|----|-----------------------------|------------------------------|-------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------|---------------------------|-------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| N1 | Backend des Control Centers | Kunden-/Flottenmanagement    | D8 Anfrage für Flottendaten         | D8 Anfrage des Control Centers nach Flottendaten                                                                                     | HTTP                      | Anfängliche Systemintegration ODER kontinuierliche Aktualisierung | >> F1 Systemintegration                                                                                                                                                  |
| N2 | Kunden-/Flottenmanagement   | Backend des Control Centers  | D9 Kundendaten, D10 Hub-Daten       | D9 Informationen über die Fahrzeughalter, Beziehung zu Flotten, sonstige Kontaktdaten, D10 Informationen über die unterstützten Hubs | HTTP                      | N1                                                                |                                                                                                                                                                          |
| N3 | Backend des Control Centers | Datenbank                    | D9 Kundendaten, D10 Hub-Daten       | D9 Informationen über die Fahrzeughalter, Beziehung zu Flotten, sonstige Kontaktdaten, D10 Informationen über die unterstützten Hubs | HTTP                      | N2                                                                | Hinweis: Lesezugriffe aus der Datenbank werden in den Datenflüssen nicht berücksichtigt, da sie denselben Cybersicherheitsanforderungen unterliegen wie Schreibzugriffe. |
| N4 | Backend des Control Centers | Dynamisches Routenmanagement | D6 ODDs/Aktivierte Routen anfordern | D6 Anfrage des Control Centers für ODDs/aktivierte Routen                                                                            | HTTP                      | Anfängliche Systemintegration ODER kontinuierliche Aktualisierung |                                                                                                                                                                          |

|     |                                                |                                                |                                     |                                                            |      |                                               |                              |
|-----|------------------------------------------------|------------------------------------------------|-------------------------------------|------------------------------------------------------------|------|-----------------------------------------------|------------------------------|
| N5  | Dynami-<br>sches<br>Routen-<br>manage-<br>ment | API-Gate-<br>way                               | D7 ODDs/Ak-<br>tivierte Rou-<br>ten | D7 Routen, die autonome Lkw befahren dürfen                | HTTP | N4                                            |                              |
| N6  | API-Gate-<br>way                               | Backend<br>des Con-<br>trol Cen-<br>ters       | D7 ODDs/Ak-<br>tivierte Rou-<br>ten | D7 Routen, die autonome Lkw befahren dürfen                | HTTP | N5                                            |                              |
| N7  | Backend<br>des Con-<br>trol Cen-<br>ters       | Daten-<br>bank                                 | D7 ODDs/Ak-<br>tivierte Rou-<br>ten | D7 Routen, die autonome Lkw befahren dürfen                | HTTP | N6                                            |                              |
| N8  | Techni-<br>scher Su-<br>pervisor<br>Geräte     | Control<br>Center-<br>Frontend                 | D18 Aktivie-<br>rungsbefehl         | D18 Befehl des Control Centers zur Aktivierung<br>des Lkws | HTTP | Interaktion mit dem technischen<br>Supervisor | >> F2 Aktivierung des<br>Lkw |
| N9  | Control<br>Center-<br>Frontend                 | Control<br>Center-Ba-<br>ckend für<br>Frontend | D18 Aktivie-<br>rungsbefehl         | D18 Befehl des Control Centers zur Aktivierung<br>des Lkws | HTTP | N8                                            |                              |
| N10 | Control<br>Center-Ba-<br>ckend für<br>Frontend | Backend<br>des Con-<br>trol Cen-<br>ters       | D18 Aktivie-<br>rungsbefehl         | D18 Befehl des Control Centers zur Aktivierung<br>des Lkws | HTTP | N9                                            |                              |
| N11 | Backend<br>des                                 | Daten-<br>bank                                 | D18 Aktivie-<br>rungsbefehl         | D18 Befehl des Control Centers zur Aktivierung<br>des Lkws | HTTP | N10                                           |                              |

|     | Control Centers             |                         |                                 |                                                                                                                              |      |                                      |  |
|-----|-----------------------------|-------------------------|---------------------------------|------------------------------------------------------------------------------------------------------------------------------|------|--------------------------------------|--|
| N12 | Backend des Control Centers | Fahrzeug-adapter-dienst | D18 Aktivierungsbefehl          | D18 Befehl des Control Centers zur Aktivierung des Lkws                                                                      | HTTP | N10                                  |  |
| N13 | Fahrzeug-adapter-dienst     | Befehls-service         | D18 Aktivierungsbefehl          | D18 Befehl des Control Centers zur Aktivierung des Lkws                                                                      | gRPC | N12                                  |  |
| N14 | Befehls-service             | Lkw                     | D18 Aktivierungsbefehl          | D18 Befehl des Control Centers zur Aktivierung des Lkws                                                                      | MQTT | N13                                  |  |
| N15 | Lkw                         | C2 und Konnektivität    | D19 Aktivierungsbereiter Status | D19 Nachdem der Dispatcher die Betriebsbereitschaft des Lkw überprüft hat, wird dieser Befehl an das Control Center gesendet | MQTT | Interaktion des Disponenten nach N14 |  |
| N16 | C2 und Konnektivität        | Konnektivität Eventbus  | D19 Aktivierungsbereiter Status | D19 Nachdem der Dispatcher die Betriebsbereitschaft des Lkw überprüft hat, wird dieser Befehl an das Control Center gesendet | HTTP | N15                                  |  |
| N17 | Konnektivität Eventbus      | Fahrzeug-adapter-dienst | D19 Aktivierungsbereiter Status | D19 Nachdem der Dispatcher die Betriebsbereitschaft des Lkw überprüft hat, wird dieser Befehl an das Control Center gesendet | HTTP | N16                                  |  |
| N18 | Fahrzeug-adapter-dienst     | CC Eventbus             | D19 Aktivierungsbereiter Status | D19 Nachdem der Dispatcher die Betriebsbereitschaft des Lkw überprüft hat, wird dieser Befehl an das Control Center gesendet | HTTP | N17                                  |  |
| N19 | CC Eventbus                 | Backend des             | D19 Aktivierungsbereiter Status | D19 Nachdem der Dispatcher die Betriebsbereitschaft des Lkw überprüft hat, wird dieser Befehl an das Control Center gesendet | HTTP | N18                                  |  |

|     |                                     | Control Centers                     |                                                           |                                                                                                                                                                                  |      |                                                  |  |
|-----|-------------------------------------|-------------------------------------|-----------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|--------------------------------------------------|--|
| N20 | Backend des Control Centers         | Datenbank                           | D19 Aktivierungsbereiter Status                           | D19 Nachdem der Dispatcher die Betriebsbereitschaft des Lkw überprüft hat, wird dieser Befehl an das Control Center gesendet                                                     | HTTP | N19                                              |  |
| N21 | Backend des Control Centers         | Control Center-Backend für Frontend | D19 Aktivierungsbereiter Status                           | D19 Nachdem der Dispatcher die Betriebsbereitschaft des Lkw überprüft hat, wird dieser Befehl an das Control Center gesendet                                                     | HTTP | N19                                              |  |
| N22 | Control Center-Backend für Frontend | Control Center-Frontend             | D19 Aktivierungsbereiter Status                           | D19 Nachdem der Dispatcher die Betriebsbereitschaft des Lkw überprüft hat, wird dieser Befehl an das Control Center gesendet                                                     | HTTP | N21                                              |  |
| N23 | Control Center-Frontend             | Technischer Supervisor Geräte       | D19 Aktivierungsbereiter Status                           | D19 Nachdem der Dispatcher die Betriebsbereitschaft des Lkw überprüft hat, wird dieser Befehl an das Control Center gesendet                                                     | HTTP | N22                                              |  |
| N24 | Technischer Supervisor Geräte       | Control Center-Frontend             | D2 Startbefehl für Mission, D4 Missions- und Routen-daten | D2 Befehl zum Start einer Mission,<br>D4 Mission: Start und Ziel des Fahrzeugs einschließlich geschätzter Daten wie Ankunftszeit<br><br>Route: Die geplante Route dieser Mission | HTTP | Interaktion des technischen Supervisors nach N23 |  |
| N25 | Control Center-Frontend             | Control Center-Frontend             | D2 Startbefehl für Mission, D4 Missions-                  | D2 Befehl zum Start einer Mission,<br>D4 Mission: Start und Ziel des Fahrzeugs einschließlich geschätzter Daten wie Ankunftszeit                                                 | HTTP | N24                                              |  |

|     |                                                |                                                |                                                                               |                                                                                                                                                                                       |      |     |  |
|-----|------------------------------------------------|------------------------------------------------|-------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|-----|--|
|     |                                                | Backend<br>für Front-<br>end                   | und Routen-<br>daten                                                          | Route: Die geplante Route dieser Mission                                                                                                                                              |      |     |  |
| N26 | Control<br>Center-Ba-<br>ckend für<br>Frontend | Backend<br>des Con-<br>trol Cen-<br>ters       | D2 Startbe-<br>fehl für Mis-<br>sion,<br>D4 Missions-<br>und Routen-<br>daten | D2 Befehl zum Start einer Mission,<br>D4 Mission: Start und Ziel des Fahrzeugs ein-<br>schließlich geschätzter Daten wie Ankunftszeit<br><br>Route: Die geplante Route dieser Mission | HTTP | N25 |  |
| N27 | Backend<br>des Con-<br>trol Cen-<br>ters       | Daten-<br>bank                                 | D2 Startbe-<br>fehl für Mis-<br>sion,<br>D4 Missions-<br>und Routen-<br>daten | D2 Befehl zum Start einer Mission,<br>D4 Mission: Start und Ziel des Fahrzeugs ein-<br>schließlich geschätzter Daten wie Ankunftszeit<br><br>Route: Die geplante Route dieser Mission | HTTP | N26 |  |
| N28 | Backend<br>des Con-<br>trol Cen-<br>ters       | Dynami-<br>sches<br>Routen-<br>manage-<br>ment | D4 Missions-<br>und Routen-<br>daten                                          | D4 Mission: Startpunkt und Zielort des Fahrzeugs<br>einschließlich geschätzter Daten wie Ankunftszeit<br><br>Route: Die geplante Route dieser Mission                                 | HTTP | N26 |  |
| N29 | Backend<br>des Con-<br>trol Cen-<br>ters       | Fahrzeug-<br>adapter-<br>dienst                | D2 Startbe-<br>fehl für Mis-<br>sion,<br>D4 Missions-<br>und Routen-<br>daten | D2 Befehl zum Start einer Mission,<br>D4 Mission: Start und Ziel des Fahrzeugs ein-<br>schließlich geschätzter Daten wie Ankunftszeit<br><br>Route: Die geplante Route dieser Mission | HTTP | N26 |  |

|     |                         |                         |                                                                  |                                                                                                                                                                                                                                                                                      |      |     |                           |
|-----|-------------------------|-------------------------|------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|-----|---------------------------|
| N30 | Fahrzeug-adapter-dienst | Befehls-service         | D2 Startbefehl für Mission,<br>D4 Missions- und Routen-<br>daten | D2 Befehl zum Start einer Mission,<br>D4 Mission: Start und Ziel des Fahrzeugs einschließlich geschätzter Daten wie Ankunftszeit<br><br>Route: Die geplante Route dieser Mission                                                                                                     | gRPC | N29 |                           |
| N31 | Befehls-service         | Lkw                     | D2 Startbefehl für Mission,<br>D4 Missions- und Routen-<br>daten | D2 Befehl zum Start einer Mission,<br>D4 Mission: Start und Ziel des Fahrzeugs einschließlich geschätzter Daten wie Ankunftszeit<br><br>Route: Die geplante Route dieser Mission                                                                                                     | MQTT | N30 |                           |
| N32 | Lkw                     | C2 und Konnektivität    | D3 Lkw-Daten,<br>D23 Lkw-Zustand                                 | D3 Lkw-Daten wie Position, Geschwindigkeit, Ausrichtung, Telemetriedaten und statische Informationen,<br>D23 Die aktuelle Fähigkeit des Lkw, seine Funktionen auszuführen.                                                                                                           | MQTT | N31 | >> F3 Überwachung des Lkw |
| N33 | C2 und Konnektivität    | Konnektivität Eventbus  | D3 Lkw-Daten,<br>D23 Lkw-Zustand,<br>D24 CC-Zustand              | D3 Lkw-Daten wie Position, Geschwindigkeit, Ausrichtung, Telemetriedaten und statische Informationen,<br>D23 Die aktuelle Fähigkeit des Lkw, seine Funktionen auszuführen,<br>D24 Die aktuelle Fähigkeit der einzelnen Komponenten des Control Centers, ihre Funktionen auszuführen. | HTTP | N32 |                           |
| N34 | Konnektivität Eventbus  | Fahrzeug-adapter-dienst | D3 Lkw-Daten,<br>D23 Lkw-                                        | D3 Lkw-Daten wie Position, Geschwindigkeit, Ausrichtung, Telemetriedaten und statische Informationen,                                                                                                                                                                                | HTTP | N33 |                           |



|     |                                          |                                          |                                                                    |                                                                                                                                                                                                                                                                                                               |      |     |  |
|-----|------------------------------------------|------------------------------------------|--------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|-----|--|
|     |                                          |                                          | Zustand,<br>D24 CC-Zu-<br>stand                                    | D23 Die aktuelle Fähigkeit des Lkw, seine Funktio-<br>nen auszuführen,<br>D24 Die aktuelle Fähigkeit der einzelnen Kompo-<br>nenten des Control Centers, ihre Funktionen aus-<br>zuführen.                                                                                                                    |      |     |  |
| N35 | Fahrzeug-<br>adapter-<br>dienst          | CC Event-<br>bus                         | D3 Lkw-Da-<br>ten,<br>D23 Lkw-Zu-<br>stand,<br>D24 CC-Zu-<br>stand | D3 Lkw-Daten wie Position, Geschwindigkeit, Aus-<br>richtung, Telemetriedaten und statische Informati-<br>onen,<br>D23 Die aktuelle Fähigkeit des Lkw, seine Funktio-<br>nen auszuführen,<br>D24 Die aktuelle Fähigkeit der einzelnen Kompo-<br>nenten des Control Centers, ihre Funktionen aus-<br>zuführen. | HTTP | N34 |  |
| N36 | CC Event-<br>bus                         | Backend<br>des Con-<br>trol Cen-<br>ters | D3 Lkw-Da-<br>ten,<br>D23 Lkw-Zu-<br>stand,<br>D24 CC-Zu-<br>stand | D3 Lkw-Daten wie Position, Geschwindigkeit, Aus-<br>richtung, Telemetriedaten und statische Informati-<br>onen,<br>D23 Die aktuelle Fähigkeit des Lkw, seine Funktio-<br>nen auszuführen,<br>D24 Die aktuelle Fähigkeit der einzelnen Kompo-<br>nenten des Control Centers, ihre Funktionen aus-<br>zuführen. | HTTP | N35 |  |
| N37 | Backend<br>des Con-<br>trol Cen-<br>ters | Daten-<br>bank                           | D3 Lkw-Da-<br>ten,<br>D23 Lkw-Zu-<br>stand,<br>D24 CC-Zu-<br>stand | D3 Lkw-Daten wie Position, Geschwindigkeit, Aus-<br>richtung, Telemetriedaten und statische Informati-<br>onen,<br>D23 Die aktuelle Fähigkeit des Lkw, seine Funktio-<br>nen auszuführen,<br>D24 Die aktuelle Fähigkeit der einzelnen Kompo-<br>nenten des Control Centers, ihre Funktionen aus-<br>zuführen. | HTTP | N36 |  |

|     |                                     |                                     |                                                     |                                                                                                                                                                                                                                                                                      |      |     |  |
|-----|-------------------------------------|-------------------------------------|-----------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|-----|--|
| N38 | Backend des Control Centers         | Dynamisches Routenmanagement        | D3 Lkw-Daten,<br>D23 Lkw-Zustand,<br>D24 CC-Zustand | D3 Lkw-Daten wie Position, Geschwindigkeit, Ausrichtung, Telemetriedaten und statische Informationen,<br>D23 Die aktuelle Fähigkeit des Lkw, seine Funktionen auszuführen,<br>D24 Die aktuelle Fähigkeit der einzelnen Komponenten des Control Centers, ihre Funktionen auszuführen. | HTTP | N36 |  |
| N39 | Backend des Control Centers         | Control Center-Backend für Frontend | D3 Lkw-Daten,<br>D23 Lkw-Zustand,<br>D24 CC-Zustand | D3 Lkw-Daten wie Position, Geschwindigkeit, Ausrichtung, Telemetriedaten und statische Informationen,<br>D23 Die aktuelle Fähigkeit des Lkw, seine Funktionen auszuführen,<br>D24 Die aktuelle Fähigkeit der einzelnen Komponenten des Control Centers, ihre Funktionen auszuführen. | HTTP | N36 |  |
| N40 | Control Center-Backend für Frontend | Control Center-Frontend             | D3 Lkw-Daten,<br>D23 Lkw-Zustand,<br>D24 CC-Zustand | D3 Lkw-Daten wie Position, Geschwindigkeit, Ausrichtung, Telemetriedaten und statische Informationen,<br>D23 Die aktuelle Fähigkeit des Lkw, seine Funktionen auszuführen,<br>D24 Die aktuelle Fähigkeit der einzelnen Komponenten des Control Centers, ihre Funktionen auszuführen. | HTTP | N39 |  |
| N41 | Control Center-Frontend             | Technischer Supervisor Geräte       | D3 Lkw-Daten,<br>D23 Lkw-Zustand,                   | D3 Lkw-Daten wie Position, Geschwindigkeit, Ausrichtung, Telemetriedaten und statische Informationen,<br>D23 Die aktuelle Fähigkeit des Lkw, seine Funktionen auszuführen,                                                                                                           | HTTP | N40 |  |

|     |                                     |                                     |                                                                                    |                                                                                                                                                                                            |      |                                                                     |                          |
|-----|-------------------------------------|-------------------------------------|------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|---------------------------------------------------------------------|--------------------------|
|     |                                     |                                     | D24 CC-Zustand                                                                     | D24 Die aktuelle Fähigkeit der einzelnen Komponenten des Control Centers, ihre Funktionen auszuführen.                                                                                     |      |                                                                     |                          |
| N42 | Technischer Supervisor<br>Geräte    | Control Center-Frontend             | D13 Anfrage weiterer Umgebungsdaten,<br>D20 Anfrage detaillierter Fahrzeugzustände | D13 Anfrage des Control Centers nach weiteren Umgebungsdaten, die über Kameras als Bilder oder Videos erfasst wurden,<br>D20 Anfrage des Control Centers nach detailliertem Fahrzeugstatus | HTTP | Interaktion mit dem technischen Supervisor, möglicherweise nach N41 | >> F4 Problembeseitigung |
| N43 | Control Center-Frontend             | Control Center-Backend für Frontend | D13 Anfrage weiterer Umgebungsdaten,<br>D20 Anfrage detaillierter Fahrzeugzustände | D13 Anfrage des Control Centers nach weiteren Umgebungsdaten, die über Kameras als Bilder oder Videos erfasst wurden,<br>D20 Anfrage des Control Centers nach detailliertem Fahrzeugstatus | HTTP | N42                                                                 |                          |
| N44 | Control Center-Backend für Frontend | Backend des Control Centers         | D13 Anfrage weiterer Umgebungsdaten,<br>D20 Anfrage detaillierter Fahrzeugzustände | D13 Anfrage des Control Centers nach weiteren Umgebungsdaten, die über Kameras als Bilder oder Videos erfasst wurden,<br>D20 Anfrage des Control Centers nach detailliertem Fahrzeugstatus | HTTP | N43                                                                 |                          |

|     |                             |                              |                                                                                    |                                                                                                                                                                                            |      |     |  |
|-----|-----------------------------|------------------------------|------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|-----|--|
| N45 | Backend des Control Centers | Datenbank                    | D13 Anfrage weiterer Umgebungsdaten,<br>D20 Anfrage detaillierter Fahrzeugzustände | D13 Anfrage des Control Centers nach weiteren Umgebungsdaten, die über Kameras als Bilder oder Videos erfasst wurden,<br>D20 Anfrage des Control Centers nach detailliertem Fahrzeugstatus | HTTP | N44 |  |
| N46 | Backend des Control Centers | Dynamisches Routenmanagement | D13 Anfrage weiterer Umgebungsdaten,<br>D20 Anfrage detaillierter Fahrzeugzustände | D13 Anfrage des Control Centers nach weiteren Umgebungsdaten, die über Kameras als Bilder oder Videos erfasst wurden,<br>D20 Anfrage des Control Centers nach detailliertem Fahrzeugstatus | HTTP | N44 |  |
| N47 | Backend des Control Centers | Fahrzeugadapterdienst        | D13 Anfrage weiterer Umgebungsdaten,<br>D20 Anfrage detaillierter Fahrzeugzustände | D13 Anfrage des Control Centers nach weiteren Umgebungsdaten, die über Kameras als Bilder oder Videos erfasst wurden,<br>D20 Anfrage des Control Centers nach detailliertem Fahrzeugstatus | HTTP | N46 |  |
| N48 | Fahrzeugadapterdienst       | Befehlsservice               | D13 Anfrage weiterer Umgebungsdaten,<br>D20 Anfrage                                | D13 Anfrage des Control Centers nach weiteren Umgebungsdaten, die über Kameras als Bilder oder Videos erfasst wurden,<br>D20 Anfrage des Control Centers nach detailliertem Fahrzeugstatus | gRPC | N47 |  |

|     |                      |                        |                                                                                             |                                                                                                                                                                                                          |      |     |  |
|-----|----------------------|------------------------|---------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|-----|--|
|     |                      |                        | detaillierter Fahrzeugzustände                                                              |                                                                                                                                                                                                          |      |     |  |
| N49 | Befehlsservice       | Lkw                    | D13 Anfrage weiterer Umgebungsdaten,<br>D20 Anfrage detaillierter Fahrzeugzustände          | D13 Anfrage des Control Centers nach weiteren Umgebungsdaten, die über Kameras als Bilder oder Videos erfasst wurden,<br>D20 Anfrage des Control Centers nach detailliertem Fahrzeugstatus               | MQTT | N48 |  |
| N50 | Lkw                  | C2 und Konnektivität   | D14 Weitere Umgebungsdaten,<br>D21 Detaillierter Fahrzeugzustand,<br>D11 Verschlechterungen | D14 Weitere Umgebungsdaten, die über Kameras als Bilder oder Videos erfasst werden,<br>D21 Detaillierter Fahrzeugzustand und Fehlerprotokolle von ADS,<br>D11 Verschlechterungen aus Sicht des Fahrzeugs | MQTT | N49 |  |
| N51 | C2 und Konnektivität | Konnektivität Eventbus | D14 Weitere Umgebungsdaten,<br>D21 Detaillierter Fahrzeugzustand,<br>D11 Verschlechterungen | D14 Weitere Umgebungsdaten, die über Kameras als Bilder oder Videos erfasst werden,<br>D21 Detaillierter Fahrzeugzustand und Fehlerprotokolle von ADS,<br>D11 Verschlechterungen aus Sicht des Fahrzeugs | HTTP | N50 |  |

|     |                                 |                                   |                                                                                             |                                                                                                                                                                                                          |      |     |  |
|-----|---------------------------------|-----------------------------------|---------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|-----|--|
| N52 | Konnektivität<br>Eventbus       | Fahrzeug-<br>adapter-<br>dienst   | D14 Weitere Umgebungsdaten,<br>D21 Detaillierter Fahrzeugzustand,<br>D11 Verschlechterungen | D14 Weitere Umgebungsdaten, die über Kameras als Bilder oder Videos erfasst werden,<br>D21 Detaillierter Fahrzeugzustand und Fehlerprotokolle von ADS,<br>D11 Verschlechterungen aus Sicht des Fahrzeugs | HTTP | N51 |  |
| N53 | Fahrzeug-<br>adapter-<br>dienst | CC Event-<br>bus                  | D14 Weitere Umgebungsdaten,<br>D21 Detaillierter Fahrzeugzustand,<br>D11 Verschlechterungen | D14 Weitere Umgebungsdaten, die über Kameras als Bilder oder Videos erfasst werden,<br>D21 Detaillierter Fahrzeugzustand und Fehlerprotokolle von ADS,<br>D11 Verschlechterungen aus Sicht des Fahrzeugs | HTTP | N52 |  |
| N54 | CC Event-<br>bus                | Backend<br>des Control<br>Centers | D14 Weitere Umgebungsdaten,<br>D21 Detaillierter Fahrzeugzustand,<br>D11 Verschlechterungen | D14 Weitere Umgebungsdaten, die über Kameras als Bilder oder Videos erfasst werden,<br>D21 Detaillierter Fahrzeugzustand und Fehlerprotokolle von ADS,<br>D11 Verschlechterungen aus Sicht des Fahrzeugs | HTTP | N53 |  |

|     |                                     |                                     |                                                                                             |                                                                                                                                                                                                          |      |     |  |
|-----|-------------------------------------|-------------------------------------|---------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|-----|--|
| N55 | Backend des Control Centers         | Datenbank                           | D14 Weitere Umgebungsdaten,<br>D21 Detaillierter Fahrzeugzustand,<br>D11 Verschlechterungen | D14 Weitere Umgebungsdaten, die über Kameras als Bilder oder Videos erfasst werden,<br>D21 Detaillierter Fahrzeugzustand und Fehlerprotokolle von ADS,<br>D11 Verschlechterungen aus Sicht des Fahrzeugs | HTTP | N54 |  |
| N56 | Backend des Control Centers         | Control Center-Backend für Frontend | D14 Weitere Umgebungsdaten,<br>D21 Detaillierter Fahrzeugzustand,<br>D11 Verschlechterungen | D14 Weitere Umgebungsdaten, die über Kameras als Bilder oder Videos erfasst werden,<br>D21 Detaillierter Fahrzeugzustand und Fehlerprotokolle von ADS,<br>D11 Verschlechterungen aus Sicht des Fahrzeugs | HTTP | N54 |  |
| N57 | Control Center-Backend für Frontend | Control Center-Frontend             | D14 Weitere Umgebungsdaten,<br>D21 Detaillierter Fahrzeugzustand,<br>D11 Verschlechterungen | D14 Weitere Umgebungsdaten, die über Kameras als Bilder oder Videos erfasst werden,<br>D21 Detaillierter Fahrzeugzustand und Fehlerprotokolle von ADS,<br>D11 Verschlechterungen aus Sicht des Fahrzeugs | HTTP | N56 |  |



|     |                             |                               |                                                                                       |                                                                                                                                                                                                    |      |                                                                                                                                        |  |
|-----|-----------------------------|-------------------------------|---------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|----------------------------------------------------------------------------------------------------------------------------------------|--|
| N58 | Control Center-Frontend     | Technischer Supervisor Geräte | D14 Weitere Umgebungsdaten, D21 Detaillierter Fahrzeugzustand, D11 Verschlechterungen | D14 Weitere Umgebungsdaten, die über Kameras als Bilder oder Videos erfasst werden, D21 Detaillierter Fahrzeugzustand und Fehlerprotokolle von ADS, D11 Verschlechterungen aus Sicht des Fahrzeugs | HTTP | N57                                                                                                                                    |  |
| N59 | Backend des Control Centers | Externe Partner               | D11 Verschlechterungen                                                                | D11 Verschlechterungen aus Sicht des Fahrzeugs                                                                                                                                                     | HTTP | N54                                                                                                                                    |  |
| N60 | Externe Partner             | API-Gateway                   | D12 Anfrage für Lkw-Daten                                                             | D12 Anfrage externer Partner für Lkw-Daten                                                                                                                                                         | HTTP | N59                                                                                                                                    |  |
| N61 | API-Gateway                 | Backend des Control Centers   | D12 Anfrage für Lkw-Daten                                                             | D12 Anfrage externer Partner für Lkw-Daten                                                                                                                                                         | HTTP | N60                                                                                                                                    |  |
| N62 | Backend des Control Centers | Externe Partner               | D3-Lkw-Daten                                                                          | D3-Lkw-Daten wie Position, Geschwindigkeit, Ausrichtung, Telemetriedaten und statische Informationen                                                                                               | HTTP | N61                                                                                                                                    |  |
| N63 | Lkw                         | C2 und Konnektivität          | D15 Vorschlag für eine zu                                                             | D15 Dies kann auch ein Kamerabild sein, das eine durchgezogene Linie und die Umgebung des Lkw anstelle einer Trajektorie zeigt. Nachdem der                                                        | MQTT | Situation, in der das Fahrzeug Hilfe oder Genehmigung vom Control Center benötigt, z. B. wenn sich das Fahrzeug in einer Baustelle mit |  |

|     |                             |                             | genehmigende Trajektorie                           | Technischer Supervisor das Bild genehmigt hat, würde die Trajektorie dann im Lkw geplant werden.                                                                                                                                            |      | einer durchgehenden Linie befindet und das Control Center fragt, ob es die durchgehende Linie überqueren darf. |  |
|-----|-----------------------------|-----------------------------|----------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|----------------------------------------------------------------------------------------------------------------|--|
| N64 | C2 und Konnektivität        | Konnektivität Eventbus      | D15 Vorschlag für eine zu genehmigende Trajektorie | D15 Dies kann auch ein Kamerabild sein, das eine durchgezogene Linie und die Umgebung des Lkw anstelle einer Trajektorie zeigt. Nachdem der Technische Supervisor das Bild genehmigt hat, würde die Trajektorie dann im Lkw geplant werden. | HTTP | N63                                                                                                            |  |
| N65 | Konnektivität Eventbus      | Fahrzeugadapterdienst       | D15 Vorschlag für eine zu genehmigende Trajektorie | D15 Dies kann auch ein Kamerabild sein, das eine durchgezogene Linie und die Umgebung des Lkw anstelle einer Trajektorie zeigt. Nachdem der Technische Supervisor das Bild genehmigt hat, würde die Trajektorie dann im Lkw geplant werden. | HTTP | N64                                                                                                            |  |
| N66 | Fahrzeugadapterdienst       | CC Eventbus                 | D15 Vorschlag für eine zu genehmigende Trajektorie | D15 Dies kann auch ein Kamerabild sein, das eine durchgezogene Linie und die Umgebung des Lkw anstelle einer Trajektorie zeigt. Nachdem der Technische Supervisor das Bild genehmigt hat, würde die Trajektorie dann im Lkw geplant werden. | HTTP | N65                                                                                                            |  |
| N67 | CC Eventbus                 | Backend des Control Centers | D15 Vorschlag für eine zu genehmigende Trajektorie | D15 Dies kann auch ein Kamerabild sein, das eine durchgezogene Linie und die Umgebung des Lkw anstelle einer Trajektorie zeigt. Nachdem der Technische Supervisor das Bild genehmigt hat, würde die Trajektorie dann im Lkw geplant werden. | HTTP | N66                                                                                                            |  |
| N68 | Backend des Control Centers | Datenbank                   | D15 Vorschlag für eine zu                          | D15 Dies kann auch ein Kamerabild sein, das eine durchgezogene Linie und die Umgebung des Lkw anstelle einer Trajektorie zeigt. Nachdem der                                                                                                 | HTTP | N67                                                                                                            |  |

|     |                                     |                                     |                                                    |                                                                                                                                                                                                                                             |      |     |  |
|-----|-------------------------------------|-------------------------------------|----------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|-----|--|
|     |                                     |                                     | genehmigende Trajektorie                           | Technischer Supervisor das Bild genehmigt hat, würde die Trajektorie dann im Lkw geplant werden.                                                                                                                                            |      |     |  |
| N69 | Backend des Control Centers         | Control Center-Backend für Frontend | D15 Vorschlag für eine zu genehmigende Trajektorie | D15 Dies kann auch ein Kamerabild sein, das eine durchgezogene Linie und die Umgebung des Lkw anstelle einer Trajektorie zeigt. Nachdem der Technische Supervisor das Bild genehmigt hat, würde die Trajektorie dann im Lkw geplant werden. | HTTP | N68 |  |
| N70 | Control Center-Backend für Frontend | Control Center-Frontend             | D15 Vorschlag für eine zu genehmigende Trajektorie | D15 Dies kann auch ein Kamerabild sein, das eine durchgezogene Linie und die Umgebung des Lkw anstelle einer Trajektorie zeigt. Nachdem der Technische Supervisor das Bild genehmigt hat, würde die Trajektorie dann im Lkw geplant werden. | HTTP | N69 |  |
| N71 | Control Center-Frontend             | Technischer Supervisor Geräte       | D15 Vorschlag für eine zu genehmigende Trajektorie | D15 Dies kann auch ein Kamerabild sein, das eine durchgezogene Linie und die Umgebung des Lkw anstelle einer Trajektorie zeigt. Nachdem der Technische Supervisor das Bild genehmigt hat, würde die Trajektorie dann im Lkw geplant werden. | HTTP | N70 |  |
| N72 | Technischer Supervisor Geräte       | Control Center-Frontend             | D16 Genehmigung der zu genehmigenden Fahrstrecke   | D16 Genehmigung durch einen Technischer Supervisor, dass die Trajektorie oder die vorgeschlagene Aufgabe vom Lkw ausgeführt werden kann.                                                                                                    | HTTP | N71 |  |
| N73 | Control Center-Frontend             | Control Center-Backend für Frontend | D16 Genehmigung der zu genehmigenden Fahrstrecke   | D16 Genehmigung durch einen Technischer Supervisor, dass die Trajektorie oder die vorgeschlagene Aufgabe vom Lkw ausgeführt werden kann.                                                                                                    | HTTP | N72 |  |

|     |                                     |                              |                                                  |                                                                                                                                          |      |     |  |
|-----|-------------------------------------|------------------------------|--------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------|------|-----|--|
| N74 | Control Center-Backend für Frontend | Backend des Control Centers  | D16 Genehmigung der zu genehmigenden Fahrstrecke | D16 Genehmigung durch einen Technischer Supervisor, dass die Trajektorie oder die vorgeschlagene Aufgabe vom Lkw ausgeführt werden kann. | HTTP | N73 |  |
| N75 | Backend des Control Centers         | Datenbank                    | D16 Genehmigung der zu genehmigenden Fahrstrecke | D16 Genehmigung durch einen Technischer Supervisor, dass die Trajektorie oder die vorgeschlagene Aufgabe vom Lkw ausgeführt werden kann. | HTTP | N74 |  |
| N76 | Backend des Control Centers         | Dynamisches Routenmanagement | D16 Genehmigung der zu genehmigenden Fahrstrecke | D16 Genehmigung durch einen Technischer Supervisor, dass die Trajektorie oder die vorgeschlagene Aufgabe vom Lkw ausgeführt werden kann. | HTTP | N75 |  |
| N77 | Backend des Control Centers         | Fahrzeugadapterdienst        | D16 Genehmigung der zu genehmigenden Fahrstrecke | D16 Genehmigung durch einen Technischer Supervisor, dass die Trajektorie oder die vorgeschlagene Aufgabe vom Lkw ausgeführt werden kann. | HTTP | N76 |  |
| N78 | Fahrzeugadapterdienst               | Befehlsservice               | D16 Genehmigung der zu genehmigenden Fahrstrecke | D16 Genehmigung durch einen Technischer Supervisor, dass die Trajektorie oder die vorgeschlagene Aufgabe vom Lkw ausgeführt werden kann. | gRPC | N77 |  |
| N79 | Befehlsservice                      | Lkw                          | D16 Genehmigung der zu genehmigenden Fahrstrecke | D16 Genehmigung durch einen Technischer Supervisor, dass die Trajektorie oder die vorgeschlagene Aufgabe vom Lkw ausgeführt werden kann. | MQTT | N78 |  |

|     |                                                |                                                | genehmigen-<br>den Fahrstre-<br>cke |                                         |      |                                                                       |                                          |
|-----|------------------------------------------------|------------------------------------------------|-------------------------------------|-----------------------------------------|------|-----------------------------------------------------------------------|------------------------------------------|
| N80 | Techni-<br>scher Su-<br>pervisor<br>Geräte     | Control<br>Center-<br>Frontend                 | D17 MRM ini-<br>tieren              | D17 Auslöser zur Durchführung eines MRM | HTTP | Interaktion des technischen Super-<br>visors, möglicherweise nach N58 | >> F5 Minimales Risiko-<br>manöver (MRM) |
| N81 | Control<br>Center-<br>Frontend                 | Control<br>Center-Ba-<br>ckend für<br>Frontend | D17 MRM ini-<br>tieren              | D17 Auslöser zur Durchführung eines MRM | HTTP | N80                                                                   |                                          |
| N82 | Control<br>Center-Ba-<br>ckend für<br>Frontend | Backend<br>des Con-<br>trol Cen-<br>ters       | D17 MRM ini-<br>tieren              | D17 Auslöser zur Durchführung eines MRM | HTTP | N81                                                                   |                                          |
| N83 | Backend<br>des Con-<br>trol Cen-<br>ters       | Daten-<br>bank                                 | D17 MRM ini-<br>tieren              | D17 Auslöser zur Durchführung eines MRM | HTTP | N82                                                                   |                                          |
| N84 | Backend<br>des Con-<br>trol Cen-<br>ters       | Dynami-<br>sches<br>Routen-<br>manage-<br>ment | D17 MRM ini-<br>tieren              | D17 Auslöser zur Durchführung eines MRM | HTTP | N83                                                                   |                                          |
| N85 | Backend<br>des                                 | Fahrzeug-<br>adapter-<br>dienst                | D17 MRM ini-<br>tieren              | D17 Auslöser zur Durchführung eines MRM | HTTP | N84                                                                   |                                          |

|     |                                     |                                     |                       |                                                                |      |                                                                                                            |  |
|-----|-------------------------------------|-------------------------------------|-----------------------|----------------------------------------------------------------|------|------------------------------------------------------------------------------------------------------------|--|
|     | Control Centers                     |                                     |                       |                                                                |      |                                                                                                            |  |
| N86 | Fahrzeug-adapter-dienst             | Befehls-service                     | D17 MRM initiieren    | D17 Auslöser zur Durchführung eines MRM                        | gRPC | N85                                                                                                        |  |
| N87 | Befehls-service                     | Lkw                                 | D17 MRM initiieren    | D17 Auslöser zur Durchführung eines MRM                        | MQTT | N86                                                                                                        |  |
| N88 | Technischer Supervisor Geräte       | Control Center-Frontend             | D1 MRM-Befehl löschen | D1 Befehl zum Löschen/Aufheben einer bestehenden MRM-Bedingung | HTTP | Interaktion des technischen Supervisors nach Behebung der Situation unter Berücksichtigung von N41 und N58 |  |
| N89 | Control Center-Frontend             | Control Center-Backend für Frontend | D1 MRM-Befehl löschen | D1 Befehl zum Löschen/Aufheben einer bestehenden MRM-Bedingung | HTTP | N88                                                                                                        |  |
| N90 | Control Center-Backend für Frontend | Backend des Control Centers         | D1 MRM-Befehl löschen | D1 Befehl zum Löschen/Aufheben einer bestehenden MRM-Bedingung | HTTP | N89                                                                                                        |  |
| N91 | Backend des Control Centers         | Datenbank                           | D1 MRM-Befehl löschen | D1 Befehl zum Löschen/Aufheben einer bestehenden MRM-Bedingung | HTTP | N90                                                                                                        |  |
| N92 | Backend des Control Centers         | Dynamisches                         | D1 MRM-Befehl löschen | D1 Befehl zum Löschen/Aufheben einer bestehenden MRM-Bedingung | HTTP | N91                                                                                                        |  |

|     |                                                |                                                |                                    |                                                                     |      |                                                                                          |                                |
|-----|------------------------------------------------|------------------------------------------------|------------------------------------|---------------------------------------------------------------------|------|------------------------------------------------------------------------------------------|--------------------------------|
|     |                                                | Routen-<br>manage-<br>ment                     |                                    |                                                                     |      |                                                                                          |                                |
| N93 | Backend<br>des Con-<br>trol Cen-<br>ters       | Fahrzeug-<br>adapter-<br>dienst                | D1 MRM-Be-<br>fehl löschen         | D1 Befehl zum Löschen/Aufheben einer bestehen-<br>den MRM-Bedingung | HTTP | N92                                                                                      |                                |
| N94 | Fahrzeug-<br>adapter-<br>dienst                | Befehls-<br>service                            | D1 MRM-Be-<br>fehl löschen         | D1 Befehl zum Löschen/Aufheben einer bestehen-<br>den MRM-Bedingung | gRPC | N93                                                                                      |                                |
| N95 | Befehls-<br>service                            | Lkw                                            | D1 MRM-Be-<br>fehl löschen         | D1 Befehl zum Löschen/Aufheben einer bestehen-<br>den MRM-Bedingung | MQTT | N94                                                                                      |                                |
| N96 | Techni-<br>scher Su-<br>pervisor<br>Geräte     | Control<br>Center-<br>Frontend                 | D22 Deakti-<br>vierungsbe-<br>fehl | D22 Befehl zur Deaktivierung des Fahrzeugs                          | HTTP | Interaktion mit dem technischen<br>Supervisor, nachdem der Lkw sein<br>Ziel erreicht hat | >> F6 Deaktivierung des<br>Lkw |
| N97 | Control<br>Center-<br>Frontend                 | Control<br>Center-Ba-<br>ckend für<br>Frontend | D22 Deakti-<br>vierungsbe-<br>fehl | D22 Befehl zur Deaktivierung des Fahrzeugs                          | HTTP | N96                                                                                      |                                |
| N98 | Control<br>Center-Ba-<br>ckend für<br>Frontend | Backend<br>des Con-<br>trol Cen-<br>ters       | D22 Deakti-<br>vierungsbe-<br>fehl | D22 Befehl zur Deaktivierung des Fahrzeugs                          | HTTP | N97                                                                                      |                                |
| N99 | Backend<br>des                                 | Daten-<br>bank                                 | D22 Deakti-<br>vierungsbe-<br>fehl | D22 Befehl zur Deaktivierung des Fahrzeugs                          | HTTP | N98                                                                                      |                                |



|      | Control Centers             |                              |                           |                                            |      |      |  |
|------|-----------------------------|------------------------------|---------------------------|--------------------------------------------|------|------|--|
| N100 | Backend des Control Centers | Dynamisches Routenmanagement | D22 Deaktivierungsbe-fehl | D22 Befehl zur Deaktivierung des Fahrzeugs | HTTP | N99  |  |
| N101 | Backend des Control Centers | Fahrzeug-adapter-dienst      | D22 Deaktivierungsbe-fehl | D22 Befehl zur Deaktivierung des Fahrzeugs | HTTP | N100 |  |
| N102 | Fahrzeug-adapter-dienst     | Befehls-service              | D22 Deaktivierungsbe-fehl | D22 Befehl zur Deaktivierung des Fahrzeugs | gRPC | N101 |  |
| N103 | Befehls-service             | Lkw                          | D22 Deaktivierungsbe-fehl | D22 Befehl zur Deaktivierung des Fahrzeugs | MQTT | N102 |  |

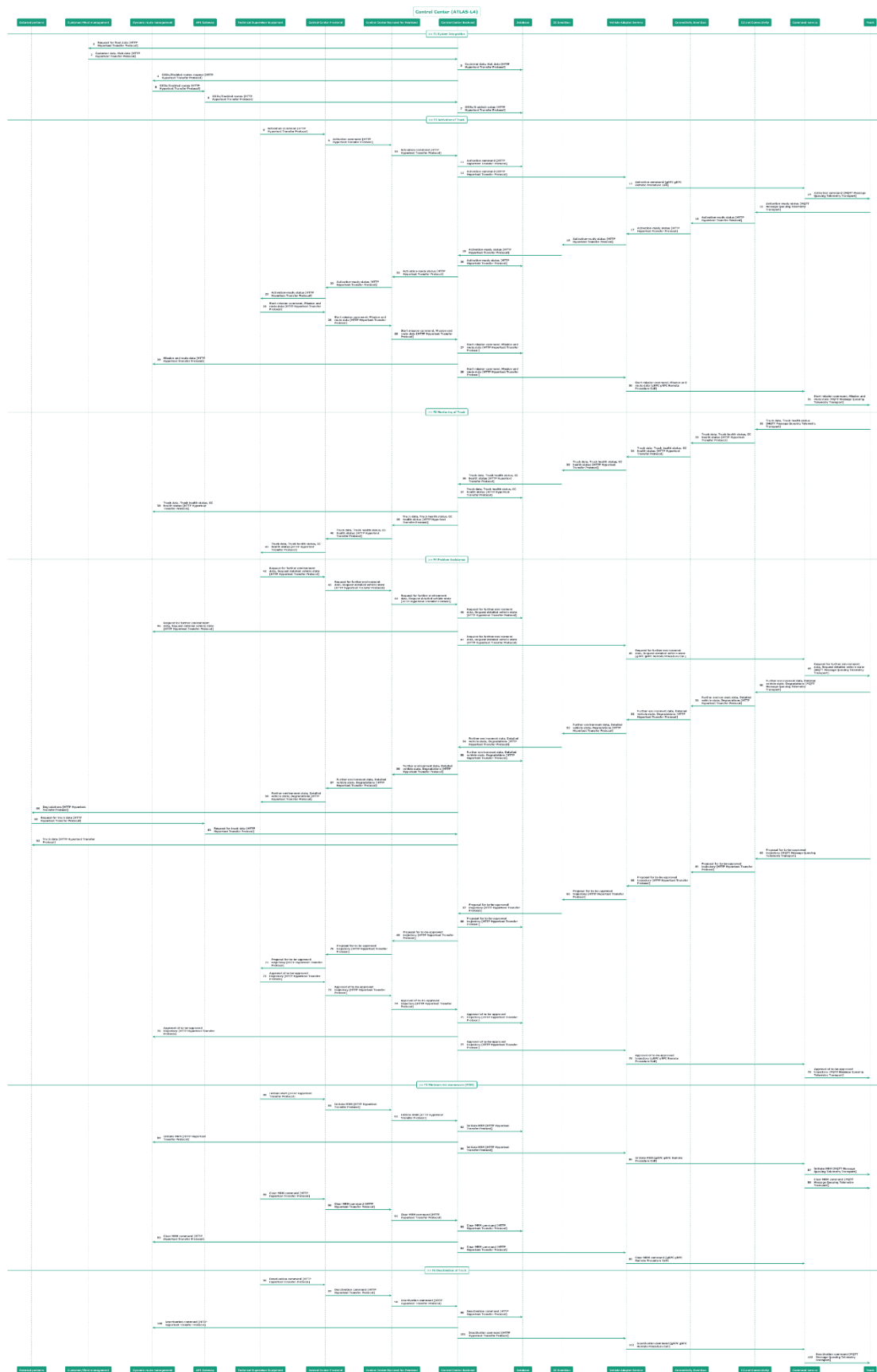


Abbildung 50: Sequenzdiagramm des Control Centers

## Schadensszenarien und Schutzziele

Wenn es einem Angreifer gelingt, die Sicherheitseigenschaften Vertraulichkeit, Integrität oder Verfügbarkeit von Teilen des TOE zu verletzen, kann dies zu einer Reihe von Schadensszenarien in den Auswirkungsklassen Sicherheit (S), Finanzen (F), Betrieb (O) und Datenschutz (P) mit Auswirkungsgraden auf einer Skala von 0 bis 3 führen, die in Tabelle 31 aufgeführt sind. Die Skalen und Bewertungsraster entsprechen denen der ADS-Analyse, um Risiken aus Fahrzeug und Control Center konsistent vergleichen zu können.

Tabelle 31: Schadensszenarien für das Control Center; Auswirkungsklassen: S-Sicherheit, F-Finanziell, O-Betrieb, P-Datenschutz; Auswirkungsgrade: 0-Vernachlässigbar, 1-Mäßig, 2-Erheblich, 3-Schwerwiegend.

| ID   | Name                                                                | Beschreibung und Begründung                                                                                                                                                                                                                    | Auswirkungsgrad |
|------|---------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|
| DS1  | Offenlegung von Videodaten                                          | P2: Mehrere Personen könnten erkennbar sein, Verstoß gegen die DSGVO                                                                                                                                                                           | Erheblich       |
| DS4  | Verlust des geistigen Eigentums am Code des Control Centers         | F2OEM: Es wird davon ausgegangen, dass das geistige Eigentum am Code des Control Centers für den OEM einen moderaten finanziellen Wert hat                                                                                                     | Erheblich       |
| DS5  | Verlust der ADS-Funktion im Ruhezustand                             | O2: Fahrzeugstart nicht möglich                                                                                                                                                                                                                | Erheblich       |
| DS6  | Verlust der ADS-Funktion während der Fahrt                          | S3: Kollisionen möglich, Verkehrsteilnehmer könnten lebensgefährliche Verletzungen erleiden<br><br>F2OEM: Der OEM muss möglicherweise finanzielle Entschädigungen an den Infrastrukturbetreiber für Schäden an der Straßeninfrastruktur zahlen | Schwerwiegend   |
| DS7  | Fehlauslösung eines MRM                                             | O2: Das Fahrzeug führt ein MRM durch, z. B. hält an einem definierten sicheren Ort an                                                                                                                                                          | Erheblich       |
| DS8  | Eingeschränkte ADS-Funktion oder Ausfall von Unterkomponenten       | O1: Wartung erforderlich, um die volle Funktionalität wiederherzustellen                                                                                                                                                                       | Mäßig           |
| DS9  | Betrieb der Fahrzeugflotte nicht möglich                            | O3: Regressansprüche wegen Schäden gegenüber OEM-Kunden/CC-Nutzern, Imageschaden                                                                                                                                                               | Schwerwiegend   |
| DS10 | Erhöhter Batterie- oder Kraftstoffverbrauch für Fahrzeugflotte      | F1OEM: Deaktivierung des Control Centers nicht für die gesamte Flotte verfügbar                                                                                                                                                                | Mäßig           |
| DS11 | Fahrzeug kann im Ruhezustand nicht ferngesteuert deaktiviert werden | O1: Lokale Deaktivierung durch Servicepersonal erforderlich                                                                                                                                                                                    | Mäßig           |
| DS12 | Gefährliche Fahrmanöver                                             | S3: Manipulierte ADS-Funktionalität könnte zu Kollisionen führen, Verkehrsteilnehmer könnten lebensgefährliche Verletzungen erleiden                                                                                                           | Schwerwiegend   |

|      |                                                            |                                                                                                                                                                        |                  |
|------|------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------|
|      |                                                            | F2OEM: Der OEM muss möglicherweise finanzielle Entschädigungen an den Infrastrukturbetreiber für Schäden an der Straßeninfrastruktur zahlen                            |                  |
| DS13 | Aktivierung außerhalb von s ODD (Sicherheit)               | S3: Unsichere Fahrbedingungen auf bestimmten Straßenabschnitten, auf denen automatisiertes Fahren nicht erlaubt ist, könnten zu lebensbedrohlichen Verletzungen führen | Schwerwiegend    |
| DS14 | Falsche Routenplanung für ein einzelnes Fahrzeug           | F0RU: Erhöhter Batterieverbrauch, unzufriedene Kunden                                                                                                                  | Vernachlässigbar |
| DS15 | Falsche Routenplanung für Fahrzeugflotte                   | F2OEM: Ein Angreifer leitet die Fahrzeugflotte zu einem Ort, an dem er die Ladung stiehlt. Es ist zu erwarten, dass der Kunde den OEM für die Verluste verklagt        | Erheblich        |
| DS16 | Offenlegung der Bewegungsprofile der Fahrzeugflotte        | F2OEM: Ein Angreifer kennt die Routen einer Fahrzeugflotte und stiehlt die Fracht unterwegs. Es ist zu erwarten, dass der Kunde den OEM für die Verluste verklagt.     | Erheblich        |
| DS17 | Vorübergehende Störung                                     | O0: Vorübergehende Störung ohne weitere Auswirkungen                                                                                                                   | Vernachlässigbar |
| DS18 | Offenlegung des Bewegungsprofils eines einzelnen Fahrzeugs | F1RU: Ein Angreifer kennt die Route eines einzelnen Fahrzeugs und stiehlt die Fracht unterwegs.                                                                        | Mäßig            |
| DS19 | Offenlegung von Kundendaten                                | P2: Offenlegung von Kundenkontaktdaten, Verstoß gegen die DSGVO                                                                                                        | Erheblich        |
| DS21 | Falsche Auslösung eines MRM für Fahrzeugflotte             | O2: Fahrzeugflotte führt ein MRM durch, z. B. Anhalten an einem definierten sicheren Ort                                                                               | Schwerwiegend    |
| DS13 | Aktivierung außerhalb von f ODD (finanziell)               | F3OEM: Gesetzesverstöße können zu erheblichen finanziellen Schäden führen                                                                                              | Schwerwiegend    |

Tabelle 32 zeigt auf, welche Schadensszenarien bei einem Asset (Daten, Komponenten) entstehen können, wenn deren Sicherheitseigenschaften Vertraulichkeit, Integrität, oder Verfügbarkeit verletzt werden. Dies wird als Schutzziel bezeichnet. Hier werden die Auswirkungen von Annahmen und Schutzmaßnahmen noch nicht berücksichtigt.

Tabelle 32: Schutzziele für das Control Center; Auswirkungsklassen: S-Sicherheit, F-Finanziell, O-Betrieb, P-Datenschutz; Auswirkungsgrade: 0-Vernachlässigbar, 1-Mäßig, 2-Erheblich, 3-Schwerwiegend.

| ID     | Name                                  | Schadensszenarien         | Auswirkungsgrad | Kommentar     |
|--------|---------------------------------------|---------------------------|-----------------|---------------|
|        | Vertraulichkeit des Clear MRM-Befehls |                           |                 | Keine Schäden |
| AVA.D1 | Verfügbarkeit des Clear-MRM-Befehls   | DS9 [O3]                  | Schwerwiegend   |               |
| INT.D1 | Integrität des Clear-MRM-Befehls      | DS9 [O3], DS12 [S3 F2OEM] | Schwerwiegend   |               |

|        |                                                       |                                                                                                               |               |                                                                                                                                                                                                                                                                                                                                        |
|--------|-------------------------------------------------------|---------------------------------------------------------------------------------------------------------------|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|        | Vertraulichkeit des Befehls „Mission starten“         |                                                                                                               |               | Keine Schäden                                                                                                                                                                                                                                                                                                                          |
| AVA.D2 | Verfügbarkeit des Befehls „Mission starten“           | DS9 [O3]                                                                                                      | Schwerwiegend |                                                                                                                                                                                                                                                                                                                                        |
| INT.D2 | Integrität des Befehls „Mission starten“              | DS9 [O3]                                                                                                      | Schwerwiegend |                                                                                                                                                                                                                                                                                                                                        |
| CNF.D3 | Vertraulichkeit der Lkw-Daten                         | DS16 [F2OEM]                                                                                                  | Erheblich     |                                                                                                                                                                                                                                                                                                                                        |
| AVA.D3 | Verfügbarkeit von Lkw-Daten                           | DS9 [O3], DS21 [O3], DS8 [O1]                                                                                 | Schwerwiegend |                                                                                                                                                                                                                                                                                                                                        |
| INT.D3 | Integrität der Lkw-Daten                              | DS9 [O3], DS21 [O3], DS8 [O1]                                                                                 | Schwerwiegend |                                                                                                                                                                                                                                                                                                                                        |
| CNF.D4 | Vertraulichkeit von Missions- und Routendaten         | DS16 [F2OEM]                                                                                                  | Erheblich     |                                                                                                                                                                                                                                                                                                                                        |
| AVA.D4 | Verfügbarkeit von Missions- und Routendaten           | DS9 [O3], DS13s [S3], DS13f [F3OEM]                                                                           | Schwerwiegend | DS13 kann auftreten, wenn während einer langen Lkw-Fahrt ein Teil der Strecke als nicht mehr zum ODD gehörig deklariert wird und die Streckenaktualisierung durch einen Angreifer gestört wird.                                                                                                                                        |
| INT.D4 | Integrität von Missions- und Routendaten              | DS9 [O3], DS13s [S3], DS13f [F3OEM], DS15 [F2OEM]                                                             | Schwerwiegend |                                                                                                                                                                                                                                                                                                                                        |
|        | Vertraulichkeit von ODDs/freigegebenen Routenanfragen |                                                                                                               |               | Keine Schäden                                                                                                                                                                                                                                                                                                                          |
| AVA.D6 | Verfügbarkeit von ODDs/Aktivierten Routen Anfrage     | DS13s-Aktivierung außerhalb von ODD (Sicherheit) [S3], DS13f-Aktivierung außerhalb von ODD (Finanzen) [F3OEM] | Schwerwiegend | <p>DS13 kann auftreten, wenn während einer langen Lkw-Fahrt ein Teil der Route als nicht mehr zum ODD gehörig deklariert wird und die Routenaktualisierung durch einen Angreifer gestört wird.</p> <p>DS9 wird nicht zugewiesen, da es nur während der anfänglichen Systeminitialisierung und nicht danach verursacht werden kann.</p> |

|        |                                                    |                                                                                                               |               |                                                                                                                                                                                                                                                                                                                                        |
|--------|----------------------------------------------------|---------------------------------------------------------------------------------------------------------------|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| INT.D6 | Integrität von ODDs/Anforderung aktivierter Routen | DS9 [O3], DS13s [S3], DS13f [F3OEM]                                                                           | Schwerwiegend |                                                                                                                                                                                                                                                                                                                                        |
|        | Vertraulichkeit von ODDs/freigegebenen Routen      |                                                                                                               |               | Keine Schäden                                                                                                                                                                                                                                                                                                                          |
| AVA.D7 | Verfügbarkeit von ODDs/freigegebenen Routen        | DS13s-Aktivierung außerhalb von ODD (Sicherheit) [S3], DS13f-Aktivierung außerhalb von ODD (Finanzen) [F3OEM] | Schwerwiegend | <p>DS13 kann auftreten, wenn während einer langen Lkw-Fahrt ein Teil der Route als nicht mehr zum ODD gehörig deklariert wird und die Routenaktualisierung durch einen Angreifer gestört wird.</p> <p>DS9 wird nicht zugewiesen, da es nur während der anfänglichen Systeminitialisierung und nicht danach verursacht werden kann.</p> |
| INT.D7 | Integrität von ODDs/freigegebenen Routen           | DS9 [O3], DS13s [S3], DS13f [F3OEM]                                                                           | Schwerwiegend |                                                                                                                                                                                                                                                                                                                                        |
|        | Vertraulichkeit der Anfrage nach Flottendaten      |                                                                                                               |               |                                                                                                                                                                                                                                                                                                                                        |
| AVA.D8 | Verfügbarkeit von Anfragen zu Flottendaten         | DS9 [O3]                                                                                                      | Schwerwiegend |                                                                                                                                                                                                                                                                                                                                        |
| INT.D8 | Integrität der Anfrage nach Flottendaten           | DS9 [O3]                                                                                                      | Schwerwiegend |                                                                                                                                                                                                                                                                                                                                        |
| CNF.D9 | Vertraulichkeit von Kundendaten                    | DS19 [P2]                                                                                                     | Erheblich     |                                                                                                                                                                                                                                                                                                                                        |
| AVA.D9 | Verfügbarkeit von Kundendaten                      | DS9 [O3]                                                                                                      | Schwerwiegend |                                                                                                                                                                                                                                                                                                                                        |
| INT.D9 | Integrität von Kundendaten                         | DS9 [O3], DS15 [F2OEM]                                                                                        | Schwerwiegend | DS15, wenn es einem Angreifer gelingt, die Kundendaten, d. h. die Informationen zum Fahrzeughalter, zu ändern und anschließend einen technischen Supervisor auffordert, die Fahrzeugflotte an einen Ort seiner Wahl zu schicken.                                                                                                       |
|        | Vertraulichkeit der Hub-Daten                      |                                                                                                               |               | Keine Schäden                                                                                                                                                                                                                                                                                                                          |

|         |                                                                    |                                                              |               |               |
|---------|--------------------------------------------------------------------|--------------------------------------------------------------|---------------|---------------|
| AVA.D10 | Verfügbarkeit von Hub-Daten                                        | DS9 [O3]                                                     | Schwerwiegend |               |
| INT.D10 | Integrität der Hub-Daten                                           | DS9 [O3]                                                     | Schwerwiegend |               |
|         | Vertraulichkeit von Verschlechterungen                             |                                                              |               | Keine Schäden |
| AVA.D11 | Verfügbarkeit von Degradationen                                    | DS21 [O3], DS8 [O1]                                          | Schwerwiegend |               |
| INT.D11 | Integrität von Beeinträchtigungen                                  | DS21 [O3], DS8 [O1]                                          | Schwerwiegend |               |
|         | Vertraulichkeit der Anforderung von Lkw-Daten                      |                                                              |               | Keine Schäden |
| AVA.D12 | Verfügbarkeit der Anfrage nach Lkw-Daten                           | DS8 [O1]                                                     | Mäßig         |               |
| INT.D12 | Integrität der Anfrage nach Lkw-Daten                              | DS8 [O1]                                                     | Mäßig         |               |
|         | Vertraulichkeit der Anfrage für weitere Umgebungsdaten             |                                                              |               | Keine Schäden |
| AVA.D13 | Verfügbarkeit von Anfragen nach weiteren Umweltdaten               | DS8 [O1]                                                     | Mäßig         |               |
| INT.D13 | Integrität der Anforderung weiterer Umgebungsdaten                 | DS8 [O1]                                                     | Mäßig         |               |
| CNF.D14 | Vertraulichkeit weiterer Umgebungsdaten                            | DS1 [P2]                                                     | Erheblich     |               |
| AVA.D14 | Verfügbarkeit weiterer Umgebungsdaten                              | DS21 [O3], DS8 [O1]                                          | Schwerwiegend |               |
| INT.D14 | Integrität weiterer Umgebungsdaten                                 | DS21 [O3], DS8 [O1], DS9 [O3]                                | Schwerwiegend |               |
| CNF.D15 | Vertraulichkeit des Vorschlags für die zu genehmigende Trajektorie | DS1 [P2]                                                     | Erheblich     |               |
| AVA.D15 | Verfügbarkeit des Vorschlags für die zu genehmigende Trajektorie   | DS9 [O3], DS8 [O1]                                           | Schwerwiegend |               |
| INT.D15 | Integrität des Vorschlags für die zu genehmigende Trajektorie      | DS21 [O3], DS8 [O1], DS9 [O3], DS12 [S3 F2OEM], DS15 [F2OEM] | Schwerwiegend |               |



|         |                                                                  |                           |               |               |
|---------|------------------------------------------------------------------|---------------------------|---------------|---------------|
|         | Vertraulichkeit der Genehmigung der zu genehmigenden Trajektorie |                           |               | Keine Schäden |
| AVA.D16 | Verfügbarkeit der Genehmigung der zu genehmigenden Trajektorie   | DS9 [O3], DS8 [O1]        | Schwerwiegend |               |
| INT.D16 | Integrität der Genehmigung der zu genehmigenden Trajektorie      | DS9 [O3], DS8 [O1]        | Schwerwiegend |               |
|         | Vertraulichkeit der Initiierung von MRM                          |                           |               | Keine Schäden |
| AVA.D17 | Verfügbarkeit von Initiate MRM                                   | DS6 [S3 F2OEM]            | Schwerwiegend |               |
| INT.D17 | Integrität von Initiate MRM                                      | DS6 [S3 F2OEM], DS21 [O3] | Schwerwiegend |               |
|         | Vertraulichkeit des Aktivierungsbefehls                          |                           |               | Keine Schäden |
| AVA.D18 | Verfügbarkeit des Aktivierungsbefehls                            | DS9 [O3]                  | Schwerwiegend |               |
| INT.D18 | Integrität des Aktivierungsbefehls                               | DS9 [O3], DS10 [F1OEM]    | Schwerwiegend |               |
|         | Vertraulichkeit des Aktivierungsstatus                           |                           |               | Keine Schäden |
| AVA.D19 | Verfügbarkeit des Status „Aktivierungsbereit“                    | DS9 [O3]                  | Schwerwiegend |               |
| INT.D19 | Integrität des Aktivierungsstatus                                | DS9 [O3]                  | Schwerwiegend |               |
|         | Vertraulichkeit der Anfrage zum detaillierten Fahrzeugstatus     |                           |               | Keine Schäden |
| AVA.D20 | Verfügbarkeit von detaillierten Fahrzeugzustandsanfragen         | DS21 [O3], DS8 [O1]       | Schwerwiegend |               |
| INT.D20 | Integrität der Anfrage zum detaillierten Fahrzeugstatus          | DS21 [O3], DS8 [O1]       | Schwerwiegend |               |
|         | Vertraulichkeit detaillierter Fahrzeugzustände                   |                           |               | Keine Schäden |
| AVA.D21 | Verfügbarkeit detaillierter Fahrzeugzustandsdaten                | DS21 [O3], DS8 [O1]       | Schwerwiegend |               |
| INT.D21 | Integrität des detaillierten Fahrzeugzustands                    | DS21 [O3], DS8 [O1]       | Schwerwiegend |               |

|         |                                              |                                                                                                                                  |                  |                                                                                                                                                                                                                                                                                          |
|---------|----------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|         | Vertraulichkeit des Deaktivierungsbefehls    |                                                                                                                                  |                  | Keine Schäden                                                                                                                                                                                                                                                                            |
| AVA.D22 | Verfügbarkeit des Deaktivierungsbefehls      | DS10 [F1OEM]                                                                                                                     | Mäßig            |                                                                                                                                                                                                                                                                                          |
| INT.D22 | Integrität des Deaktivierungsbefehls         | DS9 [O3], DS10 [F1OEM]                                                                                                           | Schwerwiegend    |                                                                                                                                                                                                                                                                                          |
|         | Vertraulichkeit des Fahrzeugzustands         |                                                                                                                                  |                  | Keine Schäden                                                                                                                                                                                                                                                                            |
| AVA.D23 | Verfügbarkeit des Fahrzeugzustands           | DS9 [O3], DS21 [O3], DS8 [O1]                                                                                                    | Schwerwiegend    |                                                                                                                                                                                                                                                                                          |
| INT.D23 | Integrität des Fahrzeugzustands              | DS9 [O3], DS21 [O3], DS8 [O1]                                                                                                    | Schwerwiegend    | Beachten Sie, dass im Gegensatz zu der Security-Risikoanalyse des automatisierten Fahrsystems DS12 hier nicht zugewiesen wird, da es nur verursacht werden kann, wenn ein Angreifer den Gesundheitszustand der Gesundheitsüberwachungskomponente im Lkw (System Management) manipuliert. |
|         | Vertraulichkeit des CC-Zustands              |                                                                                                                                  |                  | Keine Schäden                                                                                                                                                                                                                                                                            |
| AVA.D24 | Verfügbarkeit des Gesundheitszustands von CC | DS17 [O0]                                                                                                                        | Vernachlässigbar |                                                                                                                                                                                                                                                                                          |
| INT.D24 | Integrität des CC-Gesundheitsstatus          | DS17 [O0]                                                                                                                        | Vernachlässigbar |                                                                                                                                                                                                                                                                                          |
| CNF.CC  | Vertraulichkeit des Control Centers          | DS1 [P2], DS4 [F2OEM], DS16 [F2OEM], DS19 [P2]                                                                                   | Erheblich        |                                                                                                                                                                                                                                                                                          |
| AVA.CC  | Verfügbarkeit des Control Centers            | DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS13s [S3], DS13f [F3OEM], DS17 [O0], DS21 [O3]                                | Schwerwiegend    |                                                                                                                                                                                                                                                                                          |
| INT.CC  | Integrität des Control Centers               | DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS12 [S3 F2OEM], DS13s [S3], DS13f [F3OEM], DS15 [F2OEM], DS17 [O0], DS21 [O3] | Schwerwiegend    |                                                                                                                                                                                                                                                                                          |

|          |                                                                   |                                                                                                                                  |               |  |
|----------|-------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------|---------------|--|
| CNF.CCB  | Vertraulichkeit des Backends des Control Centers                  | DS1 [P2], DS4 [F2OEM], DS16 [F2OEM], DS19 [P2]                                                                                   | Erheblich     |  |
| AVA.CCB  | Verfügbarkeit des Backends des Control Centers                    | DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS13s [S3], DS13f [F3OEM], DS17 [O0], DS21 [O3]                                | Schwerwiegend |  |
| INT.CCB  | Integrität des Backends des Control Centers                       | DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS12 [S3 F2OEM], DS13s [S3], DS13f [F3OEM], DS15 [F2OEM], DS17 [O0], DS21 [O3] | Schwerwiegend |  |
| CNF.CCF  | Vertraulichkeit des Control Center Frontends                      | DS1 [P2], DS16 [F2OEM]                                                                                                           | Erheblich     |  |
| AVA.CCF  | Verfügbarkeit des Control Center Frontend                         | DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS13s [S3], DS13f [F3OEM], DS17 [O0], DS21 [O3]                                | Schwerwiegend |  |
| INT.CCF  | Integrität des Frontends des Control Centers                      | DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS12 [S3 F2OEM], DS13s [S3], DS13f [F3OEM], DS15 [F2OEM], DS17 [O0], DS21 [O3] | Schwerwiegend |  |
| CNF.CCBF | Vertraulichkeit des Backends des Control Centers für das Frontend | DS1 [P2], DS16 [F2OEM]                                                                                                           | Erheblich     |  |
| AVA.CCBF | Verfügbarkeit des Backends des Control Centers für das Frontend   | DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS13s [S3], DS13f [F3OEM], DS17 [O0], DS21 [O3]                                | Schwerwiegend |  |
| INT.CCBF | Integrität des Backends des Control Centers für das Frontend      | DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS12 [S3 F2OEM], DS13s [S3], DS13f [F3OEM], DS15 [F2OEM], DS17 [O0], DS21 [O3] | Schwerwiegend |  |
| CNF.DB   | Vertraulichkeit der Datenbank                                     | DS1 [P2], DS16 [F2OEM], DS19 [P2]                                                                                                | Erheblich     |  |

|          |                                             |                                                                                                                                  |               |               |
|----------|---------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------|---------------|---------------|
| AVA.DB   | Verfügbarkeit der Datenbank                 | DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS13s [S3], DS13f [F3OEM], DS17 [O0], DS21 [O3]                                | Schwerwiegend |               |
| INT.DB   | Integrität der Datenbank                    | DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS12 [S3 F2OEM], DS13s [S3], DS13f [F3OEM], DS15 [F2OEM], DS17 [O0], DS21 [O3] | Schwerwiegend |               |
|          | Vertraulichkeit des API-Gateways            |                                                                                                                                  |               | Keine Schäden |
| AVA.APIG | Verfügbarkeit des API-Gateways              | DS8 [O1], DS9 [O3], DS13s [S3], DS13f [F3OEM], DS21 [O3]                                                                         | Schwerwiegend |               |
| INT.APIG | Integrität des API-Gateways                 | DS8 [O1], DS9 [O3], DS13s [S3], DS13f [F3OEM], DS21 [O3]                                                                         | Schwerwiegend |               |
| CNF.CCE  | Vertraulichkeit des CC-Ereignisbusses       | DS1 [P2], DS16 [F2OEM]                                                                                                           | Erheblich     |               |
| AVA.CCE  | Verfügbarkeit von CC Eventbus               | DS8 [O1], DS9 [O3], DS17 [O0], DS21 [O3]                                                                                         | Schwerwiegend |               |
| INT.CCE  | Integrität des CC-Eventbusses               | DS8 [O1], DS9 [O3], DS12 [S3 F2OEM], DS15 [F2OEM], DS17 [O0], DS21 [O3]                                                          | Schwerwiegend |               |
| CNF.VAS  | Vertraulichkeit des Fahrzeugadapterdienstes | DS1 [P2], DS16 [F2OEM]                                                                                                           | Erheblich     |               |
| AVA.VAS  | Verfügbarkeit des Fahrzeugadapterdienstes   | DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS13s [S3], DS13f [F3OEM], DS17 [O0], DS21 [O3]                                | Schwerwiegend |               |
| INT.VAS  | Integrität des Fahrzeugadapterdienstes      | DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS12 [S3 F2OEM], DS13s [S3], DS13f [F3OEM], DS15 [F2OEM], DS17 [O0], DS21 [O3] | Schwerwiegend |               |

|         |                                               |                                                                                                                                                                                                                            |               |  |
|---------|-----------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------|--|
| CNF.CFM | Vertraulichkeit von Kunden-/Flottenmanagement | DS19 [P2]                                                                                                                                                                                                                  | Erheblich     |  |
| AVA.CFM | Verfügbarkeit von Kunden-/Flottenmanagement   | DS9 [O3]                                                                                                                                                                                                                   | Schwerwiegend |  |
| INT.CFM | Integrität des Kunden-/Flottenmanagements     | DS9 [O3], DS15 [F2OEM]                                                                                                                                                                                                     | Schwerwiegend |  |
| CNF.CS  | Vertraulichkeit des Befehlsdienstes           | DS16 [F2OEM]                                                                                                                                                                                                               | Erheblich     |  |
| AVA.CS  | Verfügbarkeit des Befehlsdienstes             | DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS13s [S3], DS13f [F3OEM], DS21 [O3]                                                                                                                                     | Schwerwiegend |  |
| INT.CS  | Integrität des Befehlsdienstes                | DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS12 [S3 F2OEM], DS13s [S3], DS13f [F3OEM], DS15 [F2OEM], DS21 [O3]                                                                                                      | Schwerwiegend |  |
| CNF.TRK | Vertraulichkeit von Lkw                       | DS1 [P2], DS18 Offenlegung des Bewegungsprofils einzelner Fahrzeuge [F1RU]                                                                                                                                                 | Erheblich     |  |
| AVA.TRK | Verfügbarkeit von Lkw                         | DS6 [S3 F2OEM], DS8 [O1], DS5 Verlust der ADS-Funktion im Stillstand [O2], DS11 Fahrzeug kann im Stillstand nicht ferngesteuert deaktiviert werden [O1], DS13s [S3], DS13f [F3OEM], DS7 [O2]                               | Schwerwiegend |  |
| INT.TRK | Integrität des Fahrzeugs                      | DS6 [S3 F2OEM], DS8 [O1], DS5 Verlust der ADS-Funktion im Stillstand [O2], DS11 Fahrzeug kann im Stillstand nicht ferngesteuert deaktiviert werden [O1], DS12 [S3 F2OEM], DS13s [S3], DS13f [F3OEM], DS14 [F0RU], DS7 [O2] | Schwerwiegend |  |
| CNF.EP  | Vertraulichkeit externer Partner              | DS16 [F2OEM]                                                                                                                                                                                                               | Erheblich     |  |
| AVA.EP  | Verfügbarkeit externer Partner                | DS8 [O1], DS9 [O3], DS21 [O3]                                                                                                                                                                                              | Schwerwiegend |  |

|          |                                                            |                                                                                                                                  |               |  |
|----------|------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------|---------------|--|
| INT.EP   | Integrität externer Partner                                | DS8 [O1], DS9 [O3], DS21 [O3]                                                                                                    | Schwerwiegend |  |
| CNF.DRM  | Vertraulichkeit des dynamischen Routenmanagements          | DS16 [F2OEM]                                                                                                                     | Erheblich     |  |
| AVA.DRM  | Verfügbarkeit der dynamischen Routenverwaltung             | DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS13s [S3], DS13f [F3OEM], DS17 [O0], DS21 [O3]                                | Schwerwiegend |  |
| INT.DRM  | Integrität des dynamischen Routenmanagements               | DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS12 [S3 F2OEM], DS13s [S3], DS13f [F3OEM], DS15 [F2OEM], DS17 [O0], DS21 [O3] | Schwerwiegend |  |
| CNF.TSE  | Vertraulichkeit der Ausrüstung des technischen Supervisors | DS1 [P2], DS16 [F2OEM]                                                                                                           | Erheblich     |  |
| AVA.TSE  | Verfügbarkeit der technischen Überwachungs-ausrüstung      | DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS13s [S3], DS13f [F3OEM], DS17 [O0], DS21 [O3]                                | Schwerwiegend |  |
| INT.TSE  | Integrität der technischen Überwachungs-ausrüstung         | DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS12 [S3 F2OEM], DS13s [S3], DS13f [F3OEM], DS15 [F2OEM], DS17 [O0], DS21 [O3] | Schwerwiegend |  |
| CNF.C2   | Vertraulichkeit von C2 und Konnektivität                   | DS1 [P2], DS16 [F2OEM]                                                                                                           | Erheblich     |  |
| AVA.C2   | Verfügbarkeit von C2 und Konnektivität                     | DS8 [O1], DS9 [O3], DS17 [O0], DS21 [O3]                                                                                         | Schwerwiegend |  |
| INT.C2   | Integrität von C2 und Konnektivität                        | DS8 [O1], DS9 [O3], DS12 [S3 F2OEM], DS15 [F2OEM], DS17 [O0], DS21 [O3]                                                          | Schwerwiegend |  |
| CNF.CONE | Vertraulichkeit des Connectivity Eventbus                  | DS1 [P2], DS16 [F2OEM]                                                                                                           | Erheblich     |  |
| AVA.CONE | Verfügbarkeit des Konnektivitäts-Ereignisbusses            | DS8 [O1], DS9 [O3], DS17 [O0], DS21 [O3]                                                                                         | Schwerwiegend |  |

|          |                                              |                                                                                                                                  |               |  |
|----------|----------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------|---------------|--|
| INT.CONE | Integrität des Konnektivitäts-Ereignisbusses | DS8 [O1], DS9 [O3], DS12 [S3 F2OEM], DS15 [F2OEM], DS17 [O0], DS21 [O3]                                                          | Schwerwiegend |  |
| CNF.AWS  | Vertraulichkeit der AWS Cloud                | DS1 [P2], DS4 [F2OEM], DS16 [F2OEM], DS19 [P2]                                                                                   | Erheblich     |  |
| AVA.AWS  | Verfügbarkeit der AWS Cloud                  | DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS13s [S3], DS13f [F3OEM], DS17 [O0], DS21 [O3]                                | Schwerwiegend |  |
| INT.AWS  | Integrität der AWS-Cloud                     | DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS12 [S3 F2OEM], DS13s [S3], DS13f [F3OEM], DS15 [F2OEM], DS17 [O0], DS21 [O3] | Schwerwiegend |  |

### Annahmen und Schutzmaßnahmen

Die Bedrohungsszenarien werden durch Annahmen behandelt, die entweder Schadensszenarien mindern oder transformieren oder sich auf die Bewertung der Durchführbarkeit von Angriffen auswirken. Annahmen beziehen sich auf den Umfang der Analyse, z. B. „Angriffe auf den Lkw fallen nicht in den Umfang dieser Risikoanalyse“, oder auf das Angreifer-Modell, z. B. „Begrenzte Störung des Mobilfunks“. Darüber hinaus wird beispielsweise die Verantwortlichkeitsverteilung gegenüber AWS aufgeführt. Die Annahmen sind in Tabelle 33 aufgeführt.

Tabelle 33: Annahmen für das Control Center

| ID | Name                                                                                | Beschreibung                                                                                                                                                                                                                                                                                  | Auswirkungsminde-<br>rung | Maxi-<br>ma-<br>ler<br>Risi-<br>ko-<br>wert | Bedrohungen | Kom-<br>mentar<br>/ ver-<br>ant-<br>wortli-<br>che<br>Stelle |
|----|-------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------|---------------------------------------------|-------------|--------------------------------------------------------------|
| A0 | Änderungen im Vergleich zu Security-Risikoanalyse eines automatisierten Fahrsystems | „Sendet Daten“ des Control Centers entfernt:<br>*D3 Virtuelle Sensordaten -> Kartenaktualisierungen über das Control Center sind nicht mehr geplant.<br>*D25 Navigationsziel -> aufgeteilt in Missionsdaten und Routendaten.<br>*D19 Fahrbefehl -> ersetzt durch Start-/Stopp-Missionsbefehl. |                           |                                             |             | Doku-<br>menta-<br>tion                                      |



|    |                                                                      |                                                                                                                                                                                                                                                                                                  |                                                                                                                                                                                                                                                                                                                                                                     |   |                                                                          |                  |
|----|----------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|--------------------------------------------------------------------------|------------------|
|    |                                                                      | <p>*D23 EDR-Daten anfordern -&gt; nicht mehr geplant.</p> <p>*D26 Fahrzeugentriegelungsbefehl -&gt; nicht mehr geplant.</p> <p>„Empfängt Daten“ des Control Centers entfernt:</p> <p>*D20 Betriebsinformationen -&gt; ersetzt durch Lkw-Daten</p> <p>*D24 EDR-Daten -&gt; nicht mehr geplant</p> |                                                                                                                                                                                                                                                                                                                                                                     |   |                                                                          |                  |
| A1 | Angriffe auf den Lkw fallen nicht in den Umfang dieser Risikoanalyse | Der Lkw ist gegen Angriffe von internen und externen Quellen geschützt.                                                                                                                                                                                                                          |                                                                                                                                                                                                                                                                                                                                                                     | 2 | T91 Angriffe auf oder von Lkw ausgehend                                  | OEM              |
| A4 | Begrenzte Störung des Mobilfunks                                     | Ein Angreifer kann Mobilfunkverbindungen nur vorübergehend und in der Nähe der Lkw stören. Störangriffe auf stehende Lkw können erkannt und weitere Maßnahmen ergriffen werden.                                                                                                                  | <p>Transformationen:</p> <p>DS7 [O2]<br/>-----&gt; DS17</p> <p>[O0]<br/>DS8 [O1]<br/>-----&gt; DS17</p> <p>[O0]<br/>DS9 [O3]<br/>-----&gt; DS17</p> <p>[O0]<br/>DS10<br/>[F1OEM]<br/>-----&gt; DS21</p> <p>[O3]<br/>DS13s [S3]<br/>-----&gt; DS21</p> <p>[O3]<br/>DS13f<br/>[F3OEM]<br/>-----&gt; DS21</p> <p>[O3]<br/>DS21 [O3]<br/>-----&gt; DS17</p> <p>[O0]</p> |   | P18 Störung einer Mobilfunkverbindung                                    | Angreifer-Modell |
| A8 | Vertrauliche Daten werden nur während der                            | Angriffe auf Komponenten, auf die diese Annahme zutrifft, können nicht zur Offenlegung von Videodaten oder                                                                                                                                                                                       | <p>Entfernt:</p> <p>DS1 [P2]<br/>DS16</p>                                                                                                                                                                                                                                                                                                                           |   | P1ec Unbefugter physischer Zugang zur AWS Cloud (Extraktionskomponente), | OEM              |

|     |                                                        |                                                                                                                                                                                                                                                                                                                             |                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |     |
|-----|--------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|
|     | Übertragung verarbeitet und nicht gespeichert.         | Fahrzeugbewegungsprofilen führen, da diese Daten nur während der Fahrt verarbeitet und nicht gespeichert werden.<br><br>Während der Entwicklungs- und Testphase des vollständig autonomen Lkw können Videodaten in anonymisierter Form gespeichert werden (d. h. Gesichter unkenntlich gemacht, Kennzeichen entfernt usw.). | [F2OEM]<br>DS18 [F1RU]         | P3ec Unbefugter physischer Zugang zum Control Center (Extraktionskomponente, die nicht sensible Daten speichert)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |     |
| A10 | Durch CC ausgelöste MRM sind nicht sicherheitskritisch | MRM, die vom Control Center ausgelöst werden, sind nicht sicherheitskritisch. Zusammenfassend lässt sich sagen, dass keine Sicherheitsschäden auftreten können, wenn ein Angreifer die Übertragung dieses Signals stört.                                                                                                    | Entfernt:<br>DS6<br>[S3 F2OEM] | T5 Störung von MQTT zwischen Lkw und Befehlsservice,<br>T6 Spoofing/Manipulation von MQTT zwischen Lkw und Befehlsservice,<br>T14 Störung von gRPC zwischen Fahrzeugadapterdienst und Befehlsservice,<br>T15 Spoofing/Manipulation von gRPC zwischen Fahrzeugadapterdienst und Befehlsservice,<br>T20 Störung von HTTP zwischen Fahrzeugadapterdienst und CC-Backend,<br>T21 Spoofing/Manipulation von HTTP zwischen Fahrzeugadapterdienst und CC-Backend,<br>T26 Störung von HTTP zwischen CC-Backend und Datenbank,<br>T27 Spoofing/Manipulation von HTTP zwischen CC-Backend und Datenbank,<br>T32 Störung von HTTP zwischen CC-Backend und CC-Backend für Frontend,<br>T33 | OEM |

|  |  |  |  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|--|--|--|--|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  |  |  |  | <p>Spoofing/Manipulation von HTTP zwischen CC-Backend und CC-Backend für Frontend,</p> <p>T35 Störung von HTTP zwischen technischer Überwachungs-ausrüstung und CC-Backend für Frontend,</p> <p>T36 Spoofing/Manipulation von HTTP zwischen technischen Überwachungsgeräten und CC-Backend für Frontend,</p> <p>T47 Störung von HTTP zwischen CC-Backend und dynamischer Routenverwaltung,</p> <p>T48 Spoofing/Manipulation von HTTP zwischen CC-Backend und dynamischer Routenverwaltung,</p> <p>T56 Denial-of-Service-Angriff auf CC-Backend,</p> <p>T57 Manipulation von Daten, Parametern oder Software des CC-Backends,</p> <p>T59 Denial-of-Service-Angriff auf CC-Frontend,</p> <p>T60 Manipulation von Daten, Parametern oder Software des CC-Frontends,</p> <p>T62 Denial-of-Service-Angriff auf CC-Backend für Frontend,</p> <p>T63 Manipulation von Daten, Parametern oder Software des CC-Backends für Frontend,</p> <p>T65 Denial-of-Service-Angriff auf Datenbank,</p> <p>T66 Manipulation von Daten, Parametern oder Software der Datenbank,</p> |
|--|--|--|--|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|     |                                                       |                                                                                                                                                                                                                                                                                              |  |   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |                |
|-----|-------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|---|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------|
|     |                                                       |                                                                                                                                                                                                                                                                                              |  |   | <p>T74 Denial-of-Service-Angriff auf den Fahrzeugadapterdienst,</p> <p>T75 Manipulation von Daten, Parametern oder Software des Fahrzeugadapterdienstes,</p> <p>T78 Denial-of-Service-Angriff auf den Befehlsdienst,</p> <p>T79 Manipulation von Daten, Parametern oder Software des Befehlsdienstes,</p> <p>T81 Angriffe auf die dynamische Routenverwaltung,</p> <p>T83 Denial-of-Service-Angriff auf technische Überwachungsgeräte,</p> <p>T84 Manipulation von Daten, Parametern oder Software von technischen Überwachungsgeräten,</p> <p>T92 Angriffe auf die AWS-Cloud</p> |                |
| A12 | AWS schützt die Verfügbarkeit der Cloud-Infrastruktur | AWS ist für den Schutz der Verfügbarkeit der Infrastruktur verantwortlich, auf der alle in der AWS Cloud angebotenen Dienste ausgeführt werden. Diese Infrastruktur besteht aus der Hardware, Software, den Netzwerken und Einrichtungen, auf denen die AWS Cloud-Dienste ausgeführt werden. |  | 2 | <p>P1dd Unbefugter physischer Zugriff auf die AWS Cloud (Unterbrechung des Datenflusses),</p> <p>P1dc Unbefugter physischer Zugriff auf die AWS Cloud (Unterbrechung von Komponenten),</p> <p>P3dd Unbefugter physischer Zugang zum Control Center (Unterbrechung des Datenflusses),</p> <p>P3dc Unbefugter physischer Zugang zum Control Center (Unterbrechung von Komponenten),</p> <p>P13 Physische Bedrohungen,</p>                                                                                                                                                           | AWS, OEM Legal |

|     |                                                                                               |                                                                                                                                             |  |   |                                                                                                                             |                                               |
|-----|-----------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------|--|---|-----------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------|
|     |                                                                                               |                                                                                                                                             |  |   | P14 Natürliche Bedrohungen,<br>P15 Ausfälle der Infrastruktur,<br>P16 Technische Ausfälle                                   |                                               |
| A13 | Angriffe auf das Kunden-/Flottenmanagement fallen nicht in den Umfang dieser Risikoanalyse    | Das Kunden-/Flottenmanagement ist gegen Angriffe aus internen und externen Quellen geschützt.                                               |  | 2 | T76 Angriffe auf Kunden-/Flottenmanagement,<br>P9 Ausnutzen von Software-Schwachstellen des Kunden-/Flottenmanagements      | Kunden-/Flottenmanagement,<br>OEM<br>Legal    |
| A14 | Angriffe auf externe Partner fallen nicht in den Umfang dieser Risikoanalyse.                 | Die Systeme externer Partner sind gegen Angriffe aus internen und externen Quellen geschützt.                                               |  | 2 | T80 Angriffe auf externe Partner,<br>P10 Ausnutzen von Software-Schwachstellen externer Partner                             | Externe Partner,<br>OEM<br>Legal              |
| A15 | Angriffe auf das dynamische Routenmanagement fallen nicht in den Umfang dieser Risikoanalyse. | Das dynamische Routenmanagement ist gegen Angriffe aus internen und externen Quellen geschützt.                                             |  | 2 | T81 Angriffe auf dynamisches Routenmanagement,<br>P11 Ausnutzen von Software-Schwachstellen im dynamischen Routenmanagement | Dynamisches Routenmanagement,<br>OEM<br>Legal |
| A16 | Vorbereitende Schritte verursachen bereits gleiche oder höhere Schäden                        | Bestimmte Risiken sind nicht relevant, wenn bereits durch die vorbereitenden Schritte gleiche oder höhere Schäden verursacht werden können. |  | 2 | P20 Flag für A16                                                                                                            | Schadensplausibilität                         |

Die Bedrohungsszenarien werden auch durch Schutzmaßnahmen behandelt, die sich auf Schadensszenarien oder die Bewertung der Durchführbarkeit von Angriffen auswirken. Sie adressieren sowohl klassische Automotive-Controls als auch IT-/Cloud-Controls. Die Schutzmaßnahmen sind in Tabelle 34 aufgeführt.

Tabelle 34: Schutzmaßnahmen für das Control Center

| ID      | Name                                                   | Beschreibung                                                                                                                                                                                                                                                                                                                                                                                                                                                   | Maßnahmen-<br>gruppe | Geschützte<br>Cybersi-<br>cherheitsei-<br>genschaft | Geminderte Bedrohungen                                                                                                                                                                                                                                                                                                                                                                                         | Auswir-<br>kungsmin-<br>derung                                                                            | Angriffs-<br>mach-<br>barkeit |
|---------|--------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------|-----------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------|-------------------------------|
| C2      | mTLS zwischen Control Center und Mission Control (Lkw) | Die mobile Verbindung zwischen Control Center und Mission Control wird durch gegenseitig authentifizierte Transport Layer Security in Version 1.3 oder höher gesichert. Es werden sichere, vertrauenswürdige Zertifizierungsstellen verwendet. Die Zertifikate werden validiert. Es werden vertrauenswürdige, eingeschränkte Vertrauensspeicher verwendet. Private Schlüssel werden sicher behandelt.                                                          | Security-CC          | CNF Vertraulichkeit,<br>INT Integrität              | T1 Abhören von MQTT zwischen Lkw und C2 und Konnektivität,<br>T3 Spoofing/Manipulation von MQTT zwischen Lkw und C2 und Konnektivität,<br>T4 Abhören von MQTT zwischen Lkw und Befehlsdienst,<br>T6 Spoofing/Manipulation von MQTT zwischen Lkw und Befehlsdienst                                                                                                                                              |                                                                                                           | Sehr gering                   |
| C5<br>A | Eigensicherheit des Lkw (gegen Störungen)              | Selbst wenn während einer langen Lkw-Fahrt ein Abschnitt der Route nicht mehr als Teil des ODD gilt und ein Angreifer die Routenaktualisierung stört, bleibt der Lkw intrinsisch sicher. Infolgedessen gibt es keine Sicherheitsschäden, aber die Lkw können MRMs durchführen. Dies wird jedoch nicht als Problem angesehen, da die Durchführung eines MRM und das Warten auf eine Missionsaktualisierung in diesem Szenario, in dem die Route nicht mehr Teil | Safety-Lkw           | AVA Verfügbarkeit                                   | T5 Unterbrechung von MQTT zwischen Lkw und Befehlsservice,<br>T14 Unterbrechung von gRPC zwischen Fahrzeugadapterdienst und Befehlsservice,<br>T20 Unterbrechung von HTTP zwischen Fahrzeugadapterdienst und CC-Backend,<br>T26 Unterbrechung von HTTP zwischen CC-Backend und Datenbank,<br>T29 Unterbrechung von HTTP zwischen CC-Backend und API-Gateway,<br>T32 Unterbrechung von HTTP zwischen CC-Backend | Entfernt:<br>DS13s-Aktivierung außerhalb von ODD (Sicherheit) [S3]<br>DS13f-Aktivierung außerhalb von ODD | Hoch                          |

|     |                                                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |            |                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                                                                               |      |
|-----|-------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------|------|
|     |                                                       | <p>des ODD ist, der gewünschte Zustand ist.</p> <p>Dadurch werden auch die finanziellen Schäden gemindert, da bei einer plötzlichen Aufhebung von für autonomes Fahren genehmigten Routen die derzeit auf diesen Routen fahrenden Lkw nicht gegen das Gesetz verstoßen.</p>                                                                                                                                                                                                  |            |                | <p>und CC-Backend für Frontend,</p> <p>T35 Unterbrechung von HTTP zwischen technischer Überwachungsausrüstung und CC-Backend für Frontend,</p> <p>T47 Unterbrechung von HTTP zwischen CC-Backend und dynamischer Routenverwaltung,</p> <p>T53 Unterbrechung von HTTP zwischen API-Gateway und dynamischer Routenverwaltung,</p> <p>T56 Denial-of-Service-Angriff auf CC-Backend,</p> <p>T59 Denial-of-Service-Angriff auf CC-Frontend,</p> <p>T62 Denial-of-Service-Angriff auf CC-Backend für Frontend,</p> <p>T65 Denial-of-Service-Angriff auf Datenbank,</p> <p>T68 Denial-of-Service-Angriff auf API-Gateway,</p> <p>T74 Denial-of-Service-Angriff auf Fahrzeugadapterdienst,</p> <p>T78 Denial-of-Service-Angriff auf Befehlsdienst,</p> <p>T83 Denial-of-Service-Angriff auf technische Überwachungsausrüstung</p> | <p>(Finanzen)</p> <p>[F3OEM]</p>                                              |      |
| C5I | Eigensicherheit des Lkw (gegen Spoofing/Manipulation) | <p>Wenn es einem Angreifer gelingt, eine Strecke, die nicht für autonomes Fahren zugelassen ist, als Teil des ODD zu deklarieren, beispielsweise durch Manipulation von D7 „ODDs/Aktivierte Strecken“, ist der Lkw dennoch intrinsisch sicher. Daher treten keine Sicherheitsschäden auf, aber der Lkw führt möglicherweise ein MRM durch. Dies wird jedoch nicht als Problem angesehen, da die Durchführung eines MRM und das Warten auf eine Missionsaktualisierung in</p> | Safety-Lkw | INT Integrität | <p>T6 Spoofing/Manipulation auf MQTT zwischen Lkw und Befehlsservice,</p> <p>T15 Spoofing/Manipulation auf gRPC zwischen Fahrzeugadapter-Service und Befehlsservice,</p> <p>T21 Spoofing/Manipulation auf HTTP zwischen Fahrzeugadapter-Service und CC-Backend,</p> <p>T27 Spoofing/Manipulation auf HTTP zwischen CC-Backend und Datenbank,</p> <p>T30 Spoofing/Manipulation auf HTTP zwischen CC-Backend und API-Gateway,</p> <p>T33 Spoofing/Manipulation auf HTTP zwischen CC-</p>                                                                                                                                                                                                                                                                                                                                    | <p>Entfernt:</p> <p>DS13s-Aktivierung außerhalb von ODD (Sicherheit) [S3]</p> | Hoch |



diesem Szenario, in dem die Strecke nicht mehr Teil des ODD ist, der gewünschte Zustand ist.

Dies mindert jedoch nicht den finanziellen Schaden, da das Befahren einer nicht genehmigten Strecke einen Verstoß gegen Gesetze darstellt.

Backend und CC-Backend für Frontend,  
T36 Spoofing/Manipulation auf HTTP zwischen technischer Überwachungs-ausrüstung und CC-Backend für Frontend,  
T48 Spoofing/Manipulation auf HTTP zwischen CC-Backend und dynamischer Routenverwaltung,  
T54 Spoofing/Manipulation von HTTP zwischen API-Gateway und dynamischer Routenverwaltung,  
T57 Manipulation von Daten, Parametern oder Software des CC-Backends,  
T60 Manipulation von Daten, Parametern oder Software des CC-Frontends,  
T63 Manipulation von Daten, Parametern oder Software des CC-Backends für das Frontend,  
T66 Manipulation von Daten, Parametern oder Software der Datenbank,  
T69 Manipulation von Daten, Parametern oder Software des API-Gateways,  
T72 Manipulation von Daten, Parametern oder Software des CC-Eventbusses,  
T75 Manipulation von Daten, Parametern oder Software des Fahrzeugadapterdienstes,  
T79 Manipulation von Daten, Parametern oder Software des Befehlsdienstes,  
T81 Angriffe auf die dynamische Routenverwaltung,  
T84 Manipulation von Daten, Parametern oder Software der technischen Überwachungs-ausrüstung,  
T87 Manipulation von Daten, Parametern oder Software von C2 und Konnektivität,  
T90 Manipulation von Daten, Parametern oder

|     |                                                                                  |                                                                                                                                                                                                                                                                                         |             |                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |  |         |
|-----|----------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|---------|
|     |                                                                                  |                                                                                                                                                                                                                                                                                         |             |                | Software des Konnektivitäts-Eventbusses,<br>T92 Angriffe auf die AWS Cloud                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |  |         |
| C18 | Absicherung von Komponenten mit Internetverbindung gegen Software-Schwachstellen | Robuste Implementierung von Software unter Befolgung sicherer Codierungsrichtlinien, Sicherheits- (Penetrations-)Tests, Codeüberprüfungen und Schwachstellenmanagement, um die Wahrscheinlichkeit von Software-Schwachstellen zu verringern. Entfernung aller unnötigen Internet-Ports. | Security-CC | INT Integrität | <p>P2e Ausnutzen von Software-Schwachstellen von C2 und Konnektivität (Abhören),</p> <p>P2d Ausnutzen von Software-Schwachstellen von C2 und Konnektivität (Stören),</p> <p>P2m Ausnutzen von Software-Schwachstellen von C2 und Konnektivität (Manipulieren),</p> <p>P4e Ausnutzen von Software-Schwachstellen des Fahrzeugadapterdienstes (Abhören),</p> <p>P4d Ausnutzen von Software-Schwachstellen des Fahrzeugadapterdienstes (Störung),</p> <p>P4m Ausnutzen von Software-Schwachstellen des Fahrzeugadapterdienstes (Manipulation),</p> <p>P6e Ausnutzen von Software-Schwachstellen des Backends des Control Centers für das Frontend (Abhören),</p> <p>P6d Ausnutzen von Software-Schwachstellen des Control Center Backend for Frontend (Störung),</p> <p>P6m Ausnutzen von Software-Schwachstellen des Control Center Backend for Frontend (Manipulation),</p> <p>P7e Ausnutzen von Software-Schwachstellen des API Gateway (Abhören),</p> <p>P7d Ausnutzen von Software-Schwachstellen des API-Gateways (Störung),</p> <p>P7m Ausnutzen von Software-Schwachstellen des API-Gateways (Manipulation),</p> <p>P12e Ausnutzen von Software-Schwachstellen des Befehlsdienstes (Abhören),</p> <p>P12d Ausnutzen von Software-Schwachstellen des</p> |  | Niedrig |

|     |                                                                                        |                                                                                                                                                                                                                                                                                                                                               |                |                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                                 |      |
|-----|----------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------|------|
|     |                                                                                        |                                                                                                                                                                                                                                                                                                                                               |                |                | Befehlsdienstes (Störung),<br>P12m Ausnutzen von Software-Schwachstellen des<br>Befehlsdienstes (Manipulation)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |                                 |      |
| C20 | ADS-Sicherheits-<br>validierungen<br>nach Entschei-<br>dungen des Con-<br>trol Centers | <p>Nachdem das Control Center die (manipulierte) Trajektorie (D15, D16) genehmigt hat, überprüft das ADS weiterhin, ob die Trajektorie sicher ausgeführt werden kann.</p> <p>Ebenso überprüft das ADS nach dem Senden eines Clear-MRM-Befehls durch das Control Center weiterhin, ob die Situation sicher ist, um die Fahrt fortzusetzen.</p> | Safety-<br>Lkw | INT Integrität | <p>T3 Spoofing/Manipulation auf MQTT zwischen Lkw und C2 und Konnektivität,</p> <p>T6 Spoofing/Manipulation auf MQTT zwischen Lkw und Befehlsservice,</p> <p>T9 Spoofing/Manipulation auf HTTP zwischen C2 und Konnektivität und Konnektivitäts-Eventbus,</p> <p>T12 Spoofing/Manipulation auf HTTP zwischen Konnektivitäts-Eventbus und Fahrzeugadapterdienst,</p> <p>T15 Spoofing/Manipulation auf gRPC zwischen Fahrzeugadapterdienst und Befehlsdienst,</p> <p>T18 Spoofing/Manipulation auf HTTP zwischen Fahrzeugadapterdienst und CC-Eventbus,</p> <p>T21 Spoofing/Manipulation auf HTTP zwischen Fahrzeugadapterdienst und CC-Backend,</p> <p>T24 Spoofing/Manipulation auf HTTP zwischen CC-Backend und CC-Eventbus,</p> <p>T27 Spoofing/Manipulation auf HTTP zwischen CC-Backend und Datenbank,</p> <p>T33 Spoofing/Manipulation auf HTTP zwischen CC-Backend und CC-Backend für Frontend,</p> <p>T36 Spoofing/Manipulation auf HTTP zwischen technischer Überwachungsausrüstung und CC-Backend für Frontend,</p> <p>T48 Spoofing/Manipulation auf HTTP zwischen CC-Backend und dynamischer Routenverwaltung,</p> <p>T57 Manipulation von Daten, Parametern oder Software des CC-Backends,</p> | Entfernt:<br>DS12<br>[S3 F2OEM] | Hoch |

|     |                                                               |                                                                                                                                                                                                                                                                                                                                |             |                                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |  |             |
|-----|---------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|----------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|-------------|
|     |                                                               |                                                                                                                                                                                                                                                                                                                                |             |                                        | <p>T60 Manipulation von Daten, Parametern oder Software des CC-Frontends,</p> <p>T63 Manipulation von Daten, Parametern oder Software des CC-Backends für das Frontend,</p> <p>T66 Manipulation von Daten, Parametern oder Software der Datenbank,</p> <p>T72 Manipulation von Daten, Parametern oder Software des CC-Eventbusses,</p> <p>T75 Manipulation von Daten, Parametern oder Software des Fahrzeugadapterdienstes,</p> <p>T79 Manipulation von Daten, Parametern oder Software des Befehlsdienstes,</p> <p>T81 Angriffe auf das dynamische Routenmanagement,</p> <p>T84 Manipulation von Daten, Parametern oder Software der technischen Überwachungs-ausrüstung,</p> <p>T87 Manipulation von Daten, Parametern oder Software von C2 und Konnektivität,</p> <p>T90 Manipulation von Daten, Parametern oder Software des Konnektivitäts-Eventbusses,</p> <p>T92 Angriffe auf die AWS Cloud</p> |  |             |
| C22 | Verschlüsselte und authentifizierte AWS-interne Kommunikation | <p>Die AWS-interne Kommunikation ist verschlüsselt und authentifiziert, sodass nur zugelassene Komponenten miteinander kommunizieren können.</p> <p>Dies kann beispielsweise durch die Verwendung von gegenseitig authentifizierter Transport Layer Security in Version 1.3 oder höher mit sicheren und vertrauenswürdigen</p> | Security-CC | CNF Vertraulichkeit,<br>INT Integrität | <p>T7 Abhören von HTTP zwischen C2 und Konnektivität und Konnektivitäts-Eventbus,</p> <p>T9 Spoofing/Manipulation von HTTP zwischen C2 und Konnektivität und Konnektivitäts-Eventbus,</p> <p>T10 Abhören von HTTP zwischen Konnektivitäts-Eventbus und Fahrzeugadapterdienst,</p> <p>T12 Spoofing/Manipulation von HTTP zwischen Konnektivitäts-Eventbus und Fahrzeugadapterdienst,</p> <p>T13 Abhören von gRPC zwischen</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |  | Sehr gering |

Zertifizierungsstellen erfolgen. Die Zertifikate werden validiert. Es werden vertrauenswürdige, eingeschränkte Trust Stores verwendet. Private Schlüssel werden sicher behandelt.

Alternativ ist auch serverseitiges TLS in Kombination mit AWS Security Groups zulässig, wodurch sichergestellt wird, dass nur zugelassene Clients auf den Server zugreifen können.

Fahrzeugadapterdienst und Befehlsdienst,  
T15 Spoofing/Manipulation von gRPC zwischen Fahrzeugadapterdienst und Befehlsdienst,  
T16 Abhören von HTTP zwischen Fahrzeugadapterdienst und CC Eventbus,  
T18 Spoofing/Manipulation von HTTP zwischen Fahrzeugadapterdienst und CC Eventbus,  
T19 Abhören von HTTP zwischen Fahrzeugadapterdienst und CC-Backend,  
T21 Spoofing/Manipulation von HTTP zwischen Fahrzeugadapterdienst und CC-Backend,  
T22 Abhören von HTTP zwischen CC-Backend und CC-Eventbus,  
T24 Spoofing/Manipulation von HTTP zwischen CC-Backend und CC-Eventbus,  
T25 Abhören von HTTP zwischen CC-Backend und Datenbank,  
T27 Spoofing/Manipulation von HTTP zwischen CC-Backend und Datenbank,  
T28 Abhören von HTTP zwischen CC-Backend und API-Gateway,  
T30 Spoofing/Manipulation von HTTP zwischen CC-Backend und API-Gateway,  
T31 Abhören von HTTP zwischen CC-Backend und CC-Backend für Frontend,  
T33 Spoofing/Manipulation von HTTP zwischen CC-Backend und CC-Backend für Frontend,  
T40 Abhören von HTTP zwischen CC-Backend und Kunden-/Flottenmanagement,  
T42 Spoofing/Manipulation von HTTP zwischen CC-

|     |                                                                                          |                                                                                                                                                                                                   |             |                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |  |             |
|-----|------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|-------------|
|     |                                                                                          |                                                                                                                                                                                                   |             |                             | Backend und Kunden-/Flottenmanagement,<br>T43 Abhören von HTTP zwischen CC-Backend und externen Partnern,<br>T45 Spoofing/Manipulation von HTTP zwischen CC-Backend und externen Partnern,<br>T46 Abhören von HTTP zwischen CC-Backend und dynamischem Routenmanagement,<br>T48 Spoofing/Manipulation von HTTP zwischen CC-Backend und dynamischem Routenmanagement,<br>T49 Abhören von HTTP zwischen API-Gateway und externen Partnern,<br>T51 Spoofing/Manipulation von HTTP zwischen API-Gateway und externen Partnern,<br>T52 Abhören von HTTP zwischen API-Gateway und dynamischer Routenverwaltung,<br>T54 Spoofing/Manipulation von HTTP zwischen API-Gateway und dynamischer Routenverwaltung |  |             |
| C23 | Schutz vor Distributed-Denial-of-Service-Angriffen (DDoS) für internetfähige Komponenten | Internet-kompatible Komponenten auf Netzwerk- und Transportschicht (Schichten 3 und 4) sowie auf Anwendungsschicht (Schicht 7) sind vor Distributed-Denial-of-Service-Angriffen (DDoS) geschützt. | Security-CC | AVA Verfügbarkeit           | T62 Denial-of-Service-Angriff auf CC-Backend für Frontend,<br>T68 Denial-of-Service-Angriff auf API-Gateway,<br>T74 Denial-of-Service-Angriff auf Fahrzeugadapterdienst,<br>T78 Denial-of-Service-Angriff auf Befehlsdienst,<br>T86 Denial-of-Service-Angriff auf C2 und Konnektivität                                                                                                                                                                                                                                                                                                                                                                                                                |  | Sehr gering |
| C24 | Absicherung der technischen Überwachungsgeräte                                           | Als technische Überwachungsgeräte werden dedizierte Geräte verwendet. Das bedeutet, dass nur die für den Betrieb des Control Centers erforderliche Software                                       | Security-CC | CNF Vertraulichkeit,<br>AVA | T82 Extrahieren von Daten aus der technischen Überwachungsausrüstung,<br>T83 Denial-of-Service-Angriff auf die technische Überwachungsausrüstung,                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |  | Sehr gering |

|     |                                                                                                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |             |                                                |                                                                                                                                                                                                                 |  |                    |
|-----|---------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|--------------------|
|     |                                                                                                               | <p>installiert ist, um die Angriffsfläche zu minimieren.</p> <p>Darüber hinaus werden die folgenden Schutzmaßnahmen (unvollständige Liste) implementiert:</p> <ul style="list-style-type: none"> <li>*Regelmäßiges Patch-Management</li> <li>*Sicherer Start</li> <li>*Speicherverschlüsselung</li> <li>*Whitelisting nur der erforderlichen Netzwerkverbindungen</li> </ul>                                                                                                                                                                                                                                                                                         |             | <p>Verfügbarkeit,<br/>INT Integrität</p>       | <p>T84 Manipulieren von Daten, Parametern oder Software der technischen Überwachungsausrüstung, P8 Ausnutzen von Software-Schwachstellen der technischen Überwachungsausrüstung</p>                             |  |                    |
| C25 | <p>mTLS zwischen dem Backend des Control Centers für das Frontend und den technischen Überwachungsgeräten</p> | <p>Die Verbindung zwischen dem Backend des Control Centers für das Frontend und den technischen Überwachungsgeräten wird durch gegenseitig authentifizierte Transport Layer Security in Version 1.3 oder höher gesichert.</p> <p>Die technischen Überwachungsgeräte führen eine Multi-Faktor-Authentifizierung durch, während das Backend des Control Centers für das Frontend über ein digitales Zertifikat authentifziert wird.</p> <p>Es werden sichere, vertrauenswürdige Zertifizierungsstellen verwendet. Die Zertifikate werden validiert. Es werden vertrauenswürdige, eingeschränkte Trust Stores verwendet. Private Schlüssel werden sicher behandelt.</p> | Security-CC | <p>CNF Vertraulichkeit,<br/>INT Integrität</p> | <p>T34 Abhören von HTTP zwischen technischer Überwachungsausrüstung und CC-Backend für Frontend, T36 Spoofing/Manipulation von HTTP zwischen technischer Überwachungsausrüstung und CC-Backend für Frontend</p> |  | <p>Sehr gering</p> |

|     |                                                                                                                                                         |                                                                                                                                                                                                                                                        |                       |                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                           |  |             |
|-----|---------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|---------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|-------------|
| C26 | Redundanz gegen Ausfall/Störung der technischen Überwachungsgeräte                                                                                      | Wenn ein Lkw Unterstützung benötigt, ist er nicht von einem bestimmten technischen Supervisor abhängig, sondern kann von verschiedenen technischen Supervisoren bedient werden. Der Ausfall einzelner technischer Supervisoren ist daher beherrschbar. | Security-CC           | AVA Verfügbarkeit   | T35 Unterbrechung von HTTP zwischen technischer Überwachungs-ausrüstung und CC-Backend für Frontend,<br>T83 Denial-of-Service-Angriff auf technische Überwachungs-ausrüstung                                                                                                                                                                                                                                                                              |  | Sehr gering |
| C27 | End-to-End-verschlüsselte Übertragung sensibler Daten zwischen technischen Überwachungsgeräten, Lkw, externen Partnern und dynamischem Routenmanagement | Verschlüsselte Übertragung vertraulicher Daten zum Schutz der Privatsphäre von Verkehrsteilnehmern und der Navigationsziele von Lkw.<br><br>Beachten Sie, dass in Bezug auf Videodaten eine Anonymisierung auf den Lkw ebenso ausreichend wäre.        | Ende-zu-Ende-Security | CNF Vertraulichkeit | P2e Ausnutzen von Software-Schwachstellen von C2 und Konnektivität (Abhören),<br>P4e Ausnutzen von Software-Schwachstellen des Fahrzeugadapterdienstes (Abhören),<br>P6e Ausnutzen von Software-Schwachstellen des Backends des Control Centers für das Frontend (Abhören),<br>P7e Ausnutzen von Software-Schwachstellen des API Gateway (Abhören),<br>P12e Ausnutzen von Software-Schwachstellen des Command Service (Abhören)                           |  | Sehr gering |
| C28 | Durchgängig authentische Übertragung von Daten zwischen technischen Überwachungsgeräten, Lkw, Kunden-/Flottenmanagement, externen Partnern und          | Authentische Übertragung von Daten. Die Daten werden vom Absender signiert und die Signatur vom Empfänger überprüft.                                                                                                                                   | Ende-zu-Ende-Security | INT Integrität      | P2m Ausnutzen von Software-Schwachstellen von C2 und Konnektivität (Manipulieren),<br>P4m Ausnutzen von Software-Schwachstellen des Fahrzeugadapterdienstes (Manipulieren),<br>P6m Ausnutzen von Software-Schwachstellen des Backends des Control Centers für das Frontend (Manipulieren),<br>P7m Ausnutzen von Software-Schwachstellen des API-Gateways (Manipulieren),<br>P12m Ausnutzen von Software-Schwachstellen des Befehlsdienstes (Manipulation) |  | Sehr gering |



|     | dynamischem<br>Routenmanage-<br>ment |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |           |                |                                                                                                                                                                                                                                                                                                                                                                                                                                      |             |
|-----|--------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|
| C29 | Resilienz/Sicherheit durch Vielfalt  | <p>Resilienz oder „Sicherheit durch Vielfalt“ erhöht die Systemresilienz durch den Einsatz verschiedener Systeme, Komponenten und Sicherheitslösungen. Zu den wichtigsten Aspekten gehören:</p> <ul style="list-style-type: none"> <li>*Heterogene Umgebungen: Einsatz verschiedener Betriebssysteme, Softwareplattformen und Hardwarekomponenten.</li> <li>*Redundanz und Failover: Mehrere und unterschiedliche Konfigurationen kritischer Systeme.</li> <li>*Plausibilitätsprüfungen: Verschiedene Lösungen können gegenseitig überprüft werden.</li> <li>*Unterschiedliche Sicherheitsmechanismen: Verwendung verschiedener Sicherheitslösungen von unterschiedlichen Anbietern.</li> <li>*Variationen bei Softwareversionen: Verwendung verschiedener Versionen derselben Software.</li> <li>*Geografische Diversifizierung: Betrieb von Systemen an verschiedenen geografischen Standorten.</li> <li>*Teamvielfalt: Unterschiedliche Perspektiven und Ansätze in Sicherheitsteams.</li> </ul> | Resilienz | INT Integrität | <p>P2d Ausnutzen von Software-Schwachstellen von C2 und Konnektivität (Störung),<br/> P4d Ausnutzen von Software-Schwachstellen des Vehicle Adapter Service (Störung),<br/> P6d Ausnutzen von Software-Schwachstellen des Control Center Backend for Frontend (Störung),<br/> P7d Ausnutzen von Software-Schwachstellen des API Gateway (Störung),<br/> P12d Ausnutzen von Software-Schwachstellen des Command Service (Störung)</p> | Sehr gering |

|     |                                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |             |                |                                                                                                                                                                              |  |             |
|-----|---------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|-------------|
|     |                                             | <p>Dadurch wird die Wahrscheinlichkeit verringert, dass ein einzelner Exploit oder eine einzelne Schwachstelle das gesamte System gefährdet. Ein Exploit, der gegen eine Plattform wirksam ist, muss nicht unbedingt auch gegen eine andere Plattform wirksam sein. Wenn ein System ausfällt oder kompromittiert wird, kann ein anderes diversifiziertes System die Aufgaben übernehmen. Dadurch wird die Widerstandsfähigkeit des Systems gegen Angriffe erhöht, da es für Angreifer schwieriger wird, alle verschiedenen Komponenten gleichzeitig zu kompromittieren.</p> <p>Diese Schutzmaßnahme sollte für internetfähige Komponenten mit einem höheren Schadenspotenzial wie dem Vehicle Adapter Service priorisiert werden. Im Gegensatz dazu ist ein Ausfall des API-Gateways, das für die Kommunikation mit externen AWS-Systemen verwendet wird, nicht so kritisch.</p> |             |                |                                                                                                                                                                              |  |             |
| C30 | Befolgung der AWS-Sicherheitsbest Practices | <p>Das Control Center wurde unter Berücksichtigung der Sicherheitssäule des AWS Well-Architected Framework entwickelt, darunter:</p> <ul style="list-style-type: none"> <li>*Sicherheitsgrundlagen</li> <li>*Identitäts- und Zugriffsverwaltung</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | Security-CC | INT Integrität | P1mc Unbefugter physischer Zugriff auf AWS Cloud (Manipulation von Komponenten),<br>P3mc Unbefugter physischer Zugriff auf das Control Center (Manipulation von Komponenten) |  | Sehr gering |

|     |                                                                                                       |                                                                                                                                                                                                                                                                                                                                                                                                  |             |                     |                                                                                           |                                                                                   |      |
|-----|-------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|---------------------|-------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------|------|
|     |                                                                                                       | *Erkennung<br>*Infrastrukturschutz<br>*Datenschutz<br>*Reaktion auf Vorfälle<br>*Anwendungssicherheit<br><br>Dadurch wird die Angriffsfläche der AWS-Instanz gegen physische Angriffe reduziert.                                                                                                                                                                                                 |             |                     |                                                                                           |                                                                                   |      |
| C31 | Verschlüsselte Speicherung sensibler Lkw- und Kundendaten                                             | Komponenten, die sensible Lkw- oder Kundendaten speichern, speichern diese nur in verschlüsselter Form.                                                                                                                                                                                                                                                                                          | Security-CC | CNF Vertraulichkeit | T55 Extrahieren von Daten aus dem CC-Backend, T64 Extrahieren von Daten aus der Datenbank | Entfernt: DS1 [P2] DS16 [F2OEM] DS19 [P2]                                         | Hoch |
| C32 | Schutz vor Piraterie und Reverse Engineering, um die Offenlegung von geistigem Eigentum zu verhindern | Es werden Tools wie ProGuard oder Obfuscator-LLVM eingesetzt, die das unbefugte Kopieren, Verbreiten und Verändern proprietärer Software verhindern. Dazu können Verschlüsselung, Verschleierungstechniken, Lizenzverwaltungssysteme und Manipulationsschutzmechanismen gehören, um sicherzustellen, dass das geistige Eigentum geschützt bleibt und nur autorisierten Benutzern zugänglich ist. | Security-CC | CNF Vertraulichkeit | T55 Extrahieren von Daten aus dem CC-Backend                                              | Entfernt: DS4 Verlust des geistigen Eigentums am Code des Control Centers [F2OEM] | Hoch |

### Bedrohungsszenarien und Risiken

Die Sicherheitseigenschaften des TOE werden durch insgesamt 208 Bedrohungsszenarien gefährdet, die sich aus einer Kombination von 89 Hauptangriffsschritten und 40 Vorbereitungsschritten zusammensetzen. Die Hauptangriffsschritte gefährden systematisch die Vertraulichkeit, Verfügbarkeit und Integrität der Datenflüsse und Komponenten des TOE, während die Vorbereitungsschritte bestimmen, wie auf sie zugegriffen wird (z. B. physisch oder aus der Ferne) und durch welche Art von Angreifer (z. B. Fahrzeugbesitzer/Tuner oder externer Angreifer). Die Bewertung

der Angriffsmachbarkeiten wurde anhand eines auf dem Angriffspotenzial basierenden Ansatzes gemäß ISO/IEC 18045:2022 und gemäß des vertraulichen Bedrohungskatalogs des OEM geschätzt, der nicht in diesem Abschlussbericht enthalten ist. Die Bewertung der Angriffsmachbarkeiten für die meisten Bedrohungen wird mit „hoch“ eingeschätzt, um Risiken nicht zu unterschätzen. Die 208 Bedrohungsszenarien sowie die Anwendung der Annahmen und Schutzmaßnahmen auf die Bedrohungsszenarien und ihre Auswirkungen auf Schadensszenarien, Angriffsmachbarkeiten und Risikowerte sind in Tabelle 35 dargestellt. Unter Berücksichtigung der Annahmen und Schutzmaßnahmen führt die Realisierung dieser Bedrohungsszenarien nur zu Risiken mit max. Wert 2.

Tabelle 35: Bedrohungsszenarien und Risiken für das Control Center; SZ<sub>v</sub>/SZ<sub>n</sub>-Schadensszenarien vor/nach Schutzmaßnahmen; AG<sub>v</sub>/AG<sub>n</sub>-Auswirkungsgrad vor/nach Schutzmaßnahmen, V-Vernachlässigbar, M-Mäßig, E-Erheblich, S-Schwerwiegend; AM<sub>v</sub>/AM<sub>n</sub>-Angriffsmachbarkeit vor/nach Schutzmaßnahmen, SG-Sehr gering, G-Gering, M-Mittel, H-Hoch; R<sub>v</sub>/R<sub>n</sub>-Risikowert vor/nach Schutzmaßnahmen; Hinweis: Wenn in den Spalten SZ<sub>v</sub>/SZ<sub>n</sub> zwei durchgezogene Linien vorhanden sind, ist dies so zu interpretieren, dass oberhalb der ersten Linie die Schadensszenarien ohne Berücksichtigung von Annahmen, darunter die durch Annahmen entfernten oder transformierten Schadensszenarien und ganz unten die Schadensszenarien unter Berücksichtigung von Annahmen aufgeführt sind.

| ID+Name                                                                                                                                                        | Schutzmaßnahmen und Annahmen                                                                                                                                                                             | SZ <sub>v</sub>        | AG <sub>v</sub> | AM <sub>v</sub> | R <sub>v</sub> | SZ <sub>n</sub>        | AG <sub>n</sub> | AM <sub>n</sub> | R <sub>n</sub> |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------|-----------------|-----------------|----------------|------------------------|-----------------|-----------------|----------------|
| R1: T1 Abhören von MQTT zwischen Lkw und C2 und Konnektivität                                                                                                  | C2 mTLS zwischen Control Center und Mission Control (Lkw)                                                                                                                                                | DS1 [P2], DS16 [F2OEM] | E               | H               | 4              | DS1 [P2], DS16 [F2OEM] | E               | SG              | 2              |
| R2: T1 Abhören von MQTT zwischen Lkw und C2 und Konnektivätsvorbereitung durch P1ed Unbefugter physischer Zugriff auf die AWS-Cloud (Abhören des Datenflusses) | C2 mTLS zwischen Control Center und Mission Control (Lkw)                                                                                                                                                | DS1 [P2], DS16 [F2OEM] | E               | H               | 4              | DS1 [P2], DS16 [F2OEM] | E               | SG              | 2              |
| R3: T1 Abhören von MQTT zwischen Lkw und C2 und Konnektivätsvorbereitung durch P2e Ausnutzen von Software-Schwachstellen von C2 und Konnektivität (Abhören)    | C18 Absicherung von Komponenten mit Internetanschluss gegen Software-Schwachstellen<br>C27 End-to-End-verschlüsselte Übertragung sensibler Daten zwischen technischen Überwachungsgeräten, Lkw, externen | DS1 [P2], DS16 [F2OEM] | E               | H               | 4              | DS1 [P2], DS16 [F2OEM] | E               | SG              | 2              |

|                                                                                                                                                                            | Partnern und dynamischem Routenmanagement                                                                                       |                                                                                                                                  |   |   |   |                                                                                                                                  |   |    |   |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------|---|---|---|----------------------------------------------------------------------------------------------------------------------------------|---|----|---|
| R4: T2 Unterbrechung von MQTT zwischen Lkw und C2 und Konnektivätsvorbereitung durch P1dd Unbefugter physischer Zugriff auf die AWS Cloud (Unterbrechung des Datenflusses) | A12 AWS schützt die Verfügbarkeit der Cloud-Infrastruktur                                                                       | DS8 [O1], DS9 [O3], DS21 [O3]                                                                                                    | S | H | 2 | DS8 [O1], DS9 [O3], DS21 [O3]                                                                                                    | S | H  | 2 |
| R5: T2 Störung des MQTT zwischen Lkw und C2 und Vorbereitung der Konnektivität durch P2d Ausnutzung von Software-Schwachstellen von C2 und Konnektivität (Störung)         | C18 Absicherung von Komponenten mit Internetverbindung gegen Software-Schwachstellen<br>C29 Resilienz/Sicherheit durch Vielfalt | DS8 [O1], DS9 [O3], DS21 [O3]                                                                                                    | S | H | 5 | DS8 [O1], DS9 [O3], DS21 [O3]                                                                                                    | S | SG | 2 |
| R6: T2 Unterbrechung der MQTT-Verbindung zwischen Lkw und C2 und Vorbereitung der Konnektivität durch P18 Unterbrechung einer Mobilfunkverbindung                          | A4 Begrenzte Störung des Mobilfunks                                                                                             | DS8 [O1], DS9 [O3], DS21 [O3]<br><br>DS7>DS17, DS8>DS17, DS9>DS17, DS10>DS21, DS13s>DS21, DS13f>DS21, DS21>DS17<br><br>DS17 [O0] | V | H | 2 | DS8 [O1], DS9 [O3], DS21 [O3]<br><br>DS7>DS17, DS8>DS17, DS9>DS17, DS10>DS21, DS13s>DS21, DS13f>DS21, DS21>DS17<br><br>DS17 [O0] | V | H  | 2 |
| R7: T3 Spoofing/Manipulation von MQTT zwischen Lkw und C2 und Konnektivität                                                                                                | C2 mTLS zwischen Control Center und Mission Control (Lkw)<br>C20 ADS-                                                           | DS8 [O1], DS9 [O3], DS12 [S3 F2OEM], DS15 [F2OEM], DS21 [O3]                                                                     | S | H | 5 | DS8 [O1], DS9 [O3], DS12 [S3 F2OEM], DS15 [F2OEM], DS21 [O3]                                                                     | S | SG | 2 |

|                                                                                                                                                                                   |                                                                                                                                                                                                                                                                                                                                                |                                                              |   |   |   |                                                                                                                     |   |    |   |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------|---|---|---|---------------------------------------------------------------------------------------------------------------------|---|----|---|
|                                                                                                                                                                                   | Sicherheitsüberprüfungen nach Entscheidungen des Control Centers                                                                                                                                                                                                                                                                               |                                                              |   |   |   | DS12<br>DS8 [O1], DS9 [O3], DS15 [F2OEM], DS21 [O3]                                                                 |   |    |   |
| R8: T3 Spoofing/Manipulation auf MQTT zwischen Lkw und C2 und Konnektivätsvorbereitung durch P1md Unbefugter physischer Zugriff auf die AWS Cloud (Manipulation des Datenflusses) | C2 mTLS zwischen Control Center und Mission Control (Lkw)<br>C20 ADS-Sicherheitsüberprüfungen nach Entscheidungen des Control Centers                                                                                                                                                                                                          | DS8 [O1], DS9 [O3], DS12 [S3 F2OEM], DS15 [F2OEM], DS21 [O3] | S | H | 5 | DS8 [O1], DS9 [O3], DS12 [S3 F2OEM], DS15 [F2OEM], DS21 [O3]<br>DS12<br>DS8 [O1], DS9 [O3], DS15 [F2OEM], DS21 [O3] | S | SG | 2 |
| R9: T3 Spoofing/Manipulation auf MQTT zwischen Lkw und C2 und Konnektivätsvorbereitung durch P2m Ausnutzung von Software-Schwachstellen von C2 und Konnektivität (Manipulation)   | C20 ADS-Sicherheitsvalidierungen nach Entscheidungen des Control Centers<br>C18 Absicherung von Komponenten mit Internetanschluss gegen Software-Schwachstellen<br>C28 Durchgängige authentische Datenübertragung zwischen technischer Überwachungsausrüstung, Lkw, Kunden-/Flottenmanagement, externen Partnern, dynamischem Routenmanagement | DS8 [O1], DS9 [O3], DS12 [S3 F2OEM], DS15 [F2OEM], DS21 [O3] | S | H | 5 | DS8 [O1], DS9 [O3], DS12 [S3 F2OEM], DS15 [F2OEM], DS21 [O3]<br>DS12<br>DS8 [O1], DS9 [O3], DS15 [F2OEM], DS21 [O3] | S | SG | 2 |

|                                                                                                                                                                         |                                                                                                                                                                                                                                                    |                                                                                                                                                                         |   |   |   |                                                                                                                                                            |   |    |   |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|---|---|------------------------------------------------------------------------------------------------------------------------------------------------------------|---|----|---|
| R10: T4 Abhören von MQTT zwischen Lkw und Befehlsservice                                                                                                                | C2 mTLS zwischen Control Center und Mission Control (Lkw)                                                                                                                                                                                          | DS16 [F2OEM]                                                                                                                                                            | E | H | 4 | DS16 [F2OEM]                                                                                                                                               | E | SG | 2 |
| R11: T4 Abhören von MQTT zwischen Lkw und Befehlsdienst, vorbereitet von P1ed Unbefugter physischer Zugriff auf die AWS Cloud (Abhören des Datenflusses)                | C2 mTLS zwischen Control Center und Mission Control (Lkw)                                                                                                                                                                                          | DS16 [F2OEM]                                                                                                                                                            | E | H | 4 | DS16 [F2OEM]                                                                                                                                               | E | SG | 2 |
| R12: T4 Abhören von MQTT zwischen Lkw und Befehlsservice, vorbereitet durch P12e Ausnutzen von Software-Schwachstellen des Befehlsservices (Abhören)                    | C18 Absicherung von Komponenten mit Internetanschluss gegen Software-Schwachstellen<br>C27 End-to-End-verschlüsselte Übertragung sensibler Daten zwischen technischen Überwachungsgeräten, Lkw, externen Partnern und dynamischem Routenmanagement | DS16 [F2OEM]                                                                                                                                                            | E | H | 4 | DS16 [F2OEM]                                                                                                                                               | E | SG | 2 |
| R13: T5 Unterbrechung von MQTT zwischen Lkw und Befehlsservice, vorbereitet durch P1dd Unbefugter physischer Zugriff auf die AWS Cloud (Unterbrechung des Datenflusses) | C5A Eigensicherheit des Lkw (gegen Störungen)<br>A10 Durch CC ausgelöste MRM sind nicht sicherheitskritisch<br>A12 AWS schützt die Verfügbarkeit der Cloud-Infrastruktur                                                                           | DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS13s [S3], DS21 [O3], DS13f [F3OEM]<br>DS6<br>DS8 [O1], DS9 [O3], DS10 [F1OEM], DS13s [S3], DS21 [O3], DS13f [F3OEM] | S | H | 2 | DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS13s [S3], DS21 [O3], DS13f [F3OEM]<br>DS13s, DS13f, DS6<br>DS8 [O1], DS9 [O3], DS10 [F1OEM], DS21 [O3] | S | H  | 2 |

|                                                                                                                                                      |                                                                                                                                                                                                                                                                          |                                                                                                                                                                                                                            |   |   |   |                                                                                                                                                                                                                                          |   |    |   |
|------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|---|---|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|----|---|
| R14: T5 Störung des MQTT zwischen Lkw und Befehlsdienst, vorbereitet durch P12d Ausnutzung von Software-Schwachstellen des Befehlsdienstes (Störung) | <p>C5A Intrinsische Sicherheit des Lkw (gegen Störungen)</p> <p>C18 Absicherung von Komponenten mit Internetanbindung gegen Software-Schwachstellen</p> <p>C29 Resilienz/Sicherheit durch Vielfalt</p> <p>A10 Durch CC ausgelöste MRM sind nicht sicherheitskritisch</p> | <p>DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS13s [S3], DS21 [O3], DS13f [F3OEM]</p> <p>DS6</p> <p>DS8 [O1], DS9 [O3], DS10 [F1OEM], DS13s [S3], DS21 [O3], DS13f [F3OEM]</p>                                     | S | H | 5 | <p>DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS13s [S3], DS21 [O3], DS13f [F3OEM]</p> <p>DS13s, DS13f, DS6</p> <p>DS8 [O1], DS9 [O3], DS10 [F1OEM], DS21 [O3]</p>                                                                | S | SG | 2 |
| R15: T5 Störung des MQTT zwischen Lkw und Befehlsservice Vorbereitung durch P18 Störung einer Mobilfunkverbindung                                    | <p>C5A Eigensicherheit des Lkw (gegen Störungen)</p> <p>A10 Durch CC ausgelöste MRM sind nicht sicherheitskritisch</p> <p>A4 Begrenzte Störung des Mobilfunks</p>                                                                                                        | <p>DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS13s [S3], DS21 [O3], DS13f [F3OEM]</p> <p>DS6, DS7&gt;DS17, DS8&gt;DS17, DS9&gt;DS17, DS10&gt;DS21, DS13s&gt;DS21, DS13f&gt;DS21, DS21&gt;DS17</p> <p>DS17 [O0]</p> | V | H | 2 | <p>DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS13s [S3], DS21 [O3], DS13f [F3OEM]</p> <p>DS13s, DS13f, DS6, DS7&gt;DS17, DS8&gt;DS17, DS9&gt;DS17, DS10&gt;DS21, DS13s&gt;DS21, DS13f&gt;DS21, DS21&gt;DS17</p> <p>DS17 [O0]</p> | V | H  | 2 |
| R16: T6 Spoofing/Manipulation von MQTT zwischen Lkw und Kommandodienst                                                                               | C2 mTLS zwischen Control Center und Mission Control                                                                                                                                                                                                                      | DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10                                                                                                                                                                                   | S | H | 5 | DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10                                                                                                                                                                                                 | S | SG | 2 |



|                                                                                                                                                                                |                                                                                                                                                                                                                                                                              |                                                                                                                                                                                                                                               |   |   |   |                                                                                                                                                                                                                               |   |    |   |  |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|---|---|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|----|---|--|
|                                                                                                                                                                                | (Lkw)<br>C5I Intrinsische Sicherheit des Lkw (gegen Spoofing/Manipulation)<br>C20 ADS-Sicherheitsvalidierungen nach Entscheidungen des Control Centers<br><br>A10 Durch CC ausgelöste MRM sind nicht sicherheitskritisch                                                     | [F1OEM], DS12<br>[S3 F2OEM], DS13s<br>[S3], DS15 [F2OEM], DS21 [O3], DS13f<br>[F3OEM]<br><br>DS6<br><br>DS8 [O1], DS9 [O3], DS10 [F1OEM], DS12 [S3 F2OEM], DS13s [S3], DS15 [F2OEM], DS21 [O3], DS13f [F3OEM]                                 |   |   |   | [F1OEM], DS12<br>[S3 F2OEM], DS13s<br>[S3], DS15 [F2OEM], DS21 [O3], DS13f [F3OEM]<br><br>DS13s, DS12, DS6<br><br>DS8 [O1], DS9 [O3], DS10 [F1OEM], DS15 [F2OEM], DS21 [O3], DS13f [F3OEM]                                    |   |    |   |  |
| R17: T6 Spoofing/Manipulation auf MQTT zwischen Lkw und Befehlsservice, vorbereitet durch P1md Unbefugter physischer Zugriff auf die AWS Cloud (Manipulation des Datenflusses) | C2 mTLS zwischen Control Center und Mission Control (Lkw)<br>C5I Intrinsische Sicherheit des Lkw (gegen Spoofing/Manipulation)<br>C20 ADS-Sicherheitsvalidierungen nach Entscheidungen des Control Centers<br><br>A10 Durch CC ausgelöste MRM sind nicht sicherheitskritisch | DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS12 [S3 F2OEM], DS13s [S3], DS15 [F2OEM], DS21 [O3], DS13f [F3OEM]<br><br>DS6<br><br>DS8 [O1], DS9 [O3], DS10 [F1OEM], DS12 [S3 F2OEM], DS13s [S3], DS15 [F2OEM], DS21 [O3], DS13f [F3OEM] | S | H | 5 | DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS12 [S3 F2OEM], DS13s [S3], DS15 [F2OEM], DS21 [O3], DS13f [F3OEM]<br><br>DS13s, DS12, DS6<br><br>DS8 [O1], DS9 [O3], DS10 [F1OEM], DS15 [F2OEM], DS21 [O3], DS13f [F3OEM] | S | SG | 2 |  |

|                                                                                                                                                                                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                                                                                                                                                                                                                                                      |   |   |   |                                                                                                                                                                                                                                      |   |    |   |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|---|---|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|----|---|
| R18: T6 Spoofing/Manipulation auf MQTT zwischen Lkw und Befehlsservice, vorbereitet durch P12m Ausnutzen von Software-Schwachstellen des Befehlsservices (Manipulation)               | <p>C5I Intrinsische Sicherheit des Lkw (gegen Spoofing/Manipulation)</p> <p>C20 ADS-Sicherheitsvalidierungen nach Entscheidungen des Control Centers</p> <p>C18 Absicherung von Komponenten mit Internetanbindung gegen Software-Schwachstellen</p> <p>C28 End-to-End-Authentifizierung der Datenübertragung zwischen technischer Überwachungsausrüstung, Lkw, Kunden-/Flottenmanagement, externen Partnern, dynamischem Routenmanagement</p> <p>A10 Durch CC ausgelöste MRM sind nicht sicherheitskritisch</p> | <p>DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS12 [S3 F2OEM], DS13s [S3], DS15 [F2OEM], DS21 [O3], DS13f [F3OEM]</p> <p>DS6</p> <p>DS8 [O1], DS9 [O3], DS10 [F1OEM], DS12 [S3 F2OEM], DS13s [S3], DS15 [F2OEM], DS21 [O3], DS13f [F3OEM]</p> | S | H | 5 | <p>DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS12 [S3 F2OEM], DS13s [S3], DS15 [F2OEM], DS21 [O3], DS13f [F3OEM]</p> <p>DS13s, DS12, DS6</p> <p>DS8 [O1], DS9 [O3], DS10 [F1OEM], DS15 [F2OEM], DS21 [O3], DS13f [F3OEM]</p> | S | SG | 2 |
| R19: T7 Abhören von HTTP zwischen C2 und Konnektivität und Konnektivitäts-Eventbus Vorbereitung durch P1ed Unbefugter physischer Zugriff auf die AWS Cloud (Abhören des Datenflusses) | C22 Verschlüsselte und authentifizierte AWS-interne Kommunikation                                                                                                                                                                                                                                                                                                                                                                                                                                               | DS1 [P2], DS16 [F2OEM]                                                                                                                                                                                                                               | E | H | 4 | DS1 [P2], DS16 [F2OEM]                                                                                                                                                                                                               | E | SG | 2 |
| R20: T7 Abhören von HTTP zwischen C2 und Konnektivität und Konnektivitäts-Eventbus Vorbereitung durch P2e Ausnutzen von Software-Schwachstellen von C2 und Konnektivität (Abhören)    | <p>C18 Absicherung von Komponenten mit Internetanschluss gegen Software-Schwachstellen</p> <p>C27 End-to-End-verschlüsselte</p>                                                                                                                                                                                                                                                                                                                                                                                 | DS1 [P2], DS16 [F2OEM]                                                                                                                                                                                                                               | E | H | 4 | DS1 [P2], DS16 [F2OEM]                                                                                                                                                                                                               | E | SG | 2 |

|                                                                                                                                                                                                          |                                                                                                                                               |                                                                         |   |   |   |                                                                                                                                                   |   |    |   |  |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------|---|---|---|---------------------------------------------------------------------------------------------------------------------------------------------------|---|----|---|--|
|                                                                                                                                                                                                          | Übertragung sensibler Daten zwischen technischen Überwachungsgeräten, Lkw, externen Partnern und dynamischem Routenmanagement                 |                                                                         |   |   |   |                                                                                                                                                   |   |    |   |  |
| R21: T8 Unterbrechung von HTTP zwischen C2 und Konnektivität und Konnektivitäts-Eventbus Vorbereitung durch P1dd Unbefugter physischer Zugriff auf die AWS Cloud (Unterbrechung des Datenflusses)        | A12 AWS schützt die Verfügbarkeit der Cloud-Infrastruktur                                                                                     | DS8 [O1], DS9 [O3], DS17 [O0], DS21 [O3]                                | S | H | 2 | DS8 [O1], DS9 [O3], DS17 [O0], DS21 [O3]                                                                                                          | S | H  | 2 |  |
| R22: T8 Unterbrechung von HTTP zwischen C2 und Konnektivität und Vorbereitung des Konnektivitäts-Eventbusses durch P2d Ausnutzung von Software-Schwachstellen von C2 und Konnektivität (Unterbrechung)   | C18 Absicherung von Komponenten mit Internetverbindung gegen Software-Schwachstellen<br>C29 Resilienz/Sicherheit durch Vielfalt               | DS8 [O1], DS9 [O3], DS17 [O0], DS21 [O3]                                | S | H | 5 | DS8 [O1], DS9 [O3], DS17 [O0], DS21 [O3]                                                                                                          | S | SG | 2 |  |
| R23: T9 Spoofing/Manipulation auf HTTP zwischen C2 und Konnektivität und Konnektivitäts-Eventbus-Vorbereitung durch P1md Unbefugter physischer Zugriff auf die AWS Cloud (Manipulation des Datenflusses) | C20 ADS-Sicherheitsvalidierungen nach Entscheidungen des Control Centers<br>C22 Verschlüsselte und authentifizierte AWS-interne Kommunikation | DS8 [O1], DS9 [O3], DS12 [S3 F2OEM], DS15 [F2OEM], DS17 [O0], DS21 [O3] | S | H | 5 | DS8 [O1], DS9 [O3], DS12 [S3 F2OEM], DS15 [F2OEM], DS17 [O0], DS21 [O3]<br><br>DS12<br><br>DS8 [O1], DS9 [O3], DS15 [F2OEM], DS17 [O0], DS21 [O3] | S | SG | 2 |  |
| R24: T9 Spoofing/Manipulation auf HTTP zwischen C2 und Konnektivität und Konnektivitäts-Eventbus                                                                                                         | C20 ADS-Sicherheitsvalidierungen nach Entscheidungen des Control Centers                                                                      | DS8 [O1], DS9 [O3], DS12 [S3 F2OEM],                                    | S | H | 5 | DS8 [O1], DS9 [O3], DS12 [S3 F2OEM], DS15 [F2OEM], DS17                                                                                           | S | SG | 2 |  |

|                                                                                                                                                                                         |                                                                                                                                                                                                                                                                    |                                    |   |   |   |                                                                                   |   |    |   |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------|---|---|---|-----------------------------------------------------------------------------------|---|----|---|
| Vorbereitung durch P2m Ausnutzen von Software-Schwachstellen von C2 und Konnektivität (Manipulation)                                                                                    | C18 Absicherung von Komponenten mit Internetanschluss gegen Software-Schwachstellen<br>C28 Durchgängige authentische Datenübertragung zwischen technischer Überwachungsausrüstung, Lkw, Kunden-/Flottenmanagement, externen Partnern, dynamischem Routenmanagement | DS15 [F2OEM], DS17 [O0], DS21 [O3] |   |   |   | [O0], DS21 [O3]<br>DS12<br>DS8 [O1], DS9 [O3], DS15 [F2OEM], DS17 [O0], DS21 [O3] |   |    |   |
| R25: T10 Abhören von HTTP zwischen Connectivity Eventbus und Vehicle Adapter Service, vorbereitet von P1ed Unbefugter physischer Zugriff auf die AWS Cloud (Abhören des Datenflusses)   | C22 Verschlüsselte und authentifizierte AWS-interne Kommunikation                                                                                                                                                                                                  | DS1 [P2], DS16 [F2OEM]             | E | H | 4 | DS1 [P2], DS16 [F2OEM]                                                            | E | SG | 2 |
| R26: T10 Abhören von HTTP zwischen Connectivity Eventbus und Vehicle Adapter Service, vorbereitet durch P3ed Unbefugter physischer Zugang zum Control Center (Abhören des Datenflusses) | C22 Verschlüsselte und authentifizierte AWS-interne Kommunikation                                                                                                                                                                                                  | DS1 [P2], DS16 [F2OEM]             | E | H | 4 | DS1 [P2], DS16 [F2OEM]                                                            | E | SG | 2 |
| R27: T10 Abhören von HTTP zwischen Connectivity Eventbus und Vehicle Adapter Service Vorbereitung durch P4e Ausnutzen von Software-Schwachstellen des Vehicle Adapter Service (Abhören) | C18 Absicherung von Komponenten mit Internetanschluss gegen Software-Schwachstellen<br>C27 End-to-End-verschlüsselte Übertragung sensibler Daten zwischen technischen Überwachungsgeräten, Lkw, externen Partnern und dynamischem Routenmanagement                 | DS1 [P2], DS16 [F2OEM]             | E | H | 4 | DS1 [P2], DS16 [F2OEM]                                                            | E | SG | 2 |

|                                                                                                                                                                                                              |                                                                                                                                               |                                                                         |   |   |   |                                                                                                                                                   |   |    |   |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------|---|---|---|---------------------------------------------------------------------------------------------------------------------------------------------------|---|----|---|
| R28: T11 Unterbrechung von HTTP zwischen Connectivity Eventbus und Vehicle Adapter Service prep. durch P1dd Unbefugter physischer Zugriff auf die AWS Cloud (Unterbrechung des Datenflusses)                 | A12 AWS schützt die Verfügbarkeit der Cloud-Infrastruktur                                                                                     | DS8 [O1], DS9 [O3], DS17 [O0], DS21 [O3]                                | S | H | 2 | DS8 [O1], DS9 [O3], DS17 [O0], DS21 [O3]                                                                                                          | S | H  | 2 |
| R29: T11 Unterbrechung des HTTP-Verkehrs zwischen Connectivity Eventbus und Vehicle Adapter Service, vorbereitet durch P3dd Unbefugter physischer Zugang zum Control Center (Unterbrechung des Datenflusses) | A12 AWS schützt die Verfügbarkeit der Cloud-Infrastruktur                                                                                     | DS8 [O1], DS9 [O3], DS17 [O0], DS21 [O3]                                | S | H | 2 | DS8 [O1], DS9 [O3], DS17 [O0], DS21 [O3]                                                                                                          | S | H  | 2 |
| R30: T11 Unterbrechung des HTTP-Verkehrs zwischen Connectivity Eventbus und Vehicle Adapter Service, vorbereitet von P4d Ausnutzen von Software-Schwachstellen des Vehicle Adapter Service (Unterbrechung)   | C18 Absicherung von Komponenten mit Internetverbindung gegen Software-Schwachstellen<br>C29 Resilienz/Sicherheit durch Vielfalt               | DS8 [O1], DS9 [O3], DS17 [O0], DS21 [O3]                                | S | H | 5 | DS8 [O1], DS9 [O3], DS17 [O0], DS21 [O3]                                                                                                          | S | SG | 2 |
| R31: T12 Spoofing/Manipulation auf HTTP zwischen Connectivity Eventbus und Vehicle Adapter Service, vorbereitet durch P1md Unbefugter physischer Zugriff auf die AWS Cloud (Manipulation des Datenflusses)   | C20 ADS-Sicherheitsvalidierungen nach Entscheidungen des Control Centers<br>C22 Verschlüsselte und authentifizierte AWS-interne Kommunikation | DS8 [O1], DS9 [O3], DS12 [S3 F2OEM], DS15 [F2OEM], DS17 [O0], DS21 [O3] | S | H | 5 | DS8 [O1], DS9 [O3], DS12 [S3 F2OEM], DS15 [F2OEM], DS17 [O0], DS21 [O3]<br><br>DS12<br><br>DS8 [O1], DS9 [O3], DS15 [F2OEM], DS17 [O0], DS21 [O3] | S | SG | 2 |
| R32: T12 Spoofing/Manipulation auf HTTP zwischen Connectivity Eventbus und Vehicle Adapter Service, vorbereitet von P3md Unbefugter physischer Zugang zum Control Center (Manipulation des Datenflusses)     | C20 ADS-Sicherheitsvalidierungen nach Entscheidungen des Control Centers<br>C22 Verschlüsselte und                                            | DS8 [O1], DS9 [O3], DS12 [S3 F2OEM], DS15 [F2OEM], DS17 [O0], DS21 [O3] | S | H | 5 | DS8 [O1], DS9 [O3], DS12 [S3 F2OEM], DS15 [F2OEM], DS17 [O0], DS21 [O3]                                                                           | S | SG | 2 |

|                                                                                                                                                                                                            |                                                                                                                                                                                                                                                                                                                                                |                                                                         |   |   |   |                                                                                                                                           |   |    |   |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------|---|---|---|-------------------------------------------------------------------------------------------------------------------------------------------|---|----|---|
|                                                                                                                                                                                                            | authentifizierte AWS-interne Kommunikation                                                                                                                                                                                                                                                                                                     |                                                                         |   |   |   | DS12<br>DS8 [O1], DS9 [O3], DS15 [F2OEM], DS17 [O0], DS21 [O3]                                                                            |   |    |   |
| R33: T12 Spoofing/Manipulation auf HTTP zwischen Connectivity Eventbus und Vehicle Adapter Service Vorbereitung durch P4m Ausnutzen von Software-Schwachstellen des Vehicle Adapter Service (Manipulation) | C20 ADS-Sicherheitsvalidierungen nach Entscheidungen des Control Centers<br>C18 Absicherung von Komponenten mit Internetanschluss gegen Software-Schwachstellen<br>C28 Durchgängige authentische Datenübertragung zwischen technischer Überwachungsausrüstung, Lkw, Kunden-/Flottenmanagement, externen Partnern, dynamischem Routenmanagement | DS8 [O1], DS9 [O3], DS12 [S3 F2OEM], DS15 [F2OEM], DS17 [O0], DS21 [O3] | S | H | 5 | DS8 [O1], DS9 [O3], DS12 [S3 F2OEM], DS15 [F2OEM], DS17 [O0], DS21 [O3]<br>DS12<br>DS8 [O1], DS9 [O3], DS15 [F2OEM], DS17 [O0], DS21 [O3] | S | SG | 2 |
| R34: T13 Abhören von gRPC zwischen Fahrzeugadapterdienst und Befehlsdienst, vorbereitet durch P1ed Unbefugter physischer Zugriff auf die AWS Cloud (Abhören des Datenflusses)                              | C22 Verschlüsselte und authentifizierte AWS-interne Kommunikation                                                                                                                                                                                                                                                                              | DS16 [F2OEM]                                                            | E | H | 4 | DS16 [F2OEM]                                                                                                                              | E | SG | 2 |
| R35: T13 Abhören von gRPC zwischen Fahrzeugadapterdienst und Befehlsdienst, vorbereitet durch P3ed Unbefugter physischer Zugang zum Control Center (Abhören des Datenflusses)                              | C22 Verschlüsselte und authentifizierte AWS-interne Kommunikation                                                                                                                                                                                                                                                                              | DS16 [F2OEM]                                                            | E | H | 4 | DS16 [F2OEM]                                                                                                                              | E | SG | 2 |

|                                                                                                                                                                                           |                                                                                                                                                                                                                                                    |                                                                                                                      |   |   |   |                                                                                                                                    |   |    |   |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------|---|---|---|------------------------------------------------------------------------------------------------------------------------------------|---|----|---|
| R36: T13 Abhören von gRPC zwischen Fahrzeugadapterdienst und Befehlsdienst, vorbereitet von P4e Ausnutzen von Software-Schwachstellen des Fahrzeugadapterdienstes (Abhören)               | C18 Absicherung von Komponenten mit Internetanschluss gegen Software-Schwachstellen<br>C27 End-to-End-verschlüsselte Übertragung sensibler Daten zwischen technischen Überwachungsgeräten, Lkw, externen Partnern und dynamischem Routenmanagement | DS16 [F2OEM]                                                                                                         | E | H | 4 | DS16 [F2OEM]                                                                                                                       | E | SG | 2 |
| R37: T13 Abhören von gRPC zwischen Fahrzeugadapterdienst und Befehlsdienst, vorbereitet durch P12e Ausnutzen von Software-Schwachstellen des Befehlsdienstes (Abhören)                    | C18 Absicherung von Komponenten mit Internetanschluss gegen Software-Schwachstellen<br>C27 End-to-End-verschlüsselte Übertragung sensibler Daten zwischen technischen Überwachungsgeräten, Lkw, externen Partnern und dynamischem Routenmanagement | DS16 [F2OEM]                                                                                                         | E | H | 4 | DS16 [F2OEM]                                                                                                                       | E | SG | 2 |
| R38: T14 Unterbrechung von gRPC zwischen Fahrzeugadapterdienst und Befehlsdienst, vorbereitet durch P1dd Unbefugter physischer Zugriff auf die AWS Cloud (Unterbrechung des Datenflusses) | C5A Eigensicherheit des Lkw (gegen Störungen)<br>A10 Durch CC ausgelöste MRM sind nicht sicherheitskritisch<br>A12 AWS schützt die Verfügbarkeit der Cloud-Infrastruktur                                                                           | DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS13s [S3], DS21 [O3], DS13f [F3OEM]<br>DS6<br>DS8 [O1], DS9 [O3], | S | H | 2 | DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS13s [S3], DS21 [O3], DS13f [F3OEM]<br>DS13s, DS13f, DS6<br>DS8 [O1], DS9 [O3], | S | H  | 2 |

|                                                                                                                                                                              |                                                                                                                                                                                                                                                                          |                                                                                                                                                                                        |   |   |   |                                                                                                                                                                           |   |    |   |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|---|---|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|----|---|
|                                                                                                                                                                              |                                                                                                                                                                                                                                                                          | DS10 [F1OEM], DS13s [S3], DS21 [O3], DS13f [F3OEM]                                                                                                                                     |   |   |   | DS10 [F1OEM], DS21 [O3]                                                                                                                                                   |   |    |   |
| R39: T14 Störung von gRPC zwischen Fahrzeugadapterdienst und Befehlsdienstvorbereitung durch P3dd Unbefugter physischer Zugang zum Control Center (Störung des Datenflusses) | <p>C5A Eigensicherheit des Lkw (gegen Störungen)</p> <p>A10 Durch CC ausgelöste MRM sind nicht sicherheitskritisch</p> <p>A12 AWS schützt die Verfügbarkeit der Cloud-Infrastruktur</p>                                                                                  | <p>DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS13s [S3], DS21 [O3], DS13f [F3OEM]</p> <p>DS6</p> <p>DS8 [O1], DS9 [O3], DS10 [F1OEM], DS13s [S3], DS21 [O3], DS13f [F3OEM]</p> | S | H | 2 | <p>DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS13s [S3], DS21 [O3], DS13f [F3OEM]</p> <p>DS13s, DS13f, DS6</p> <p>DS8 [O1], DS9 [O3], DS10 [F1OEM], DS21 [O3]</p> | S | H  | 2 |
| R40: T14 Störung von gRPC zwischen Fahrzeugadapterdienst und Befehlsdienst, vorbereitet von P4d Ausnutzen von Software-Schwachstellen des Fahrzeugadapterdienstes (Störung)  | <p>C5A Intrinsische Sicherheit des Lkw (gegen Störungen)</p> <p>C18 Absicherung von Komponenten mit Internetanbindung gegen Software-Schwachstellen</p> <p>C29 Resilienz/Sicherheit durch Vielfalt</p> <p>A10 Durch CC ausgelöste MRM sind nicht sicherheitskritisch</p> | <p>DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS13s [S3], DS21 [O3], DS13f [F3OEM]</p> <p>DS6</p> <p>DS8 [O1], DS9 [O3], DS10 [F1OEM], DS13s [S3], DS21 [O3], DS13f [F3OEM]</p> | S | H | 5 | <p>DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS13s [S3], DS21 [O3], DS13f [F3OEM]</p> <p>DS13s, DS13f, DS6</p> <p>DS8 [O1], DS9 [O3], DS10 [F1OEM], DS21 [O3]</p> | S | SG | 2 |
| R41: T14 Störung von gRPC zwischen Fahrzeugadapterdienst und Befehlsdienst durch P12d Ausnutzung von                                                                         | C5A Intrinsische Sicherheit des Lkw (gegen Störungen)                                                                                                                                                                                                                    | DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10                                                                                                                                               | S | H | 5 | DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10                                                                                                                                  | S | SG | 2 |



|                                                                                                                                                                                                  |                                                                                                                                                                                                                                                                                                |                                                                                                                                                                                                                                                      |   |   |   |                                                                                                                                                                                                                                      |   |    |   |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|---|---|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|----|---|
| Software-Schwachstellen des Befehlsdienstes (Störung)                                                                                                                                            | <p>C18 Absicherung von Komponenten mit Internetanbindung gegen Software-Schwachstellen</p> <p>C29 Resilienz/Sicherheit durch Vielfalt</p> <p>A10 Durch CC ausgelöste MRM sind nicht sicherheitskritisch</p>                                                                                    | <p>[F1OEM], DS13s [S3], DS21 [O3], DS13f [F3OEM]</p> <p>DS6</p> <p>DS8 [O1], DS9 [O3], DS10 [F1OEM], DS13s [S3], DS21 [O3], DS13f [F3OEM]</p>                                                                                                        |   |   |   | <p>[F1OEM], DS13s [S3], DS21 [O3], DS13f [F3OEM]</p> <p>DS13s, DS13f, DS6</p> <p>DS8 [O1], DS9 [O3], DS10 [F1OEM], DS21 [O3]</p>                                                                                                     |   |    |   |
| R42: T15 Spoofing/Manipulation auf gRPC zwischen Fahrzeugadapterdienst und Befehlsdienst, vorbereitet durch P1md Unbefugter physischer Zugriff auf die AWS Cloud (Manipulation des Datenflusses) | <p>C5I Eigensicherheit des Trucks (gegen Spoofing/Manipulation)</p> <p>C20 ADS-Sicherheitsvalidierungen nach Entscheidungen des Control Centers</p> <p>C22 Verschlüsselte und authentifizierte AWS-interne Kommunikation</p> <p>A10 Durch CC ausgelöste MRM sind nicht sicherheitskritisch</p> | <p>DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS12 [S3 F2OEM], DS13s [S3], DS15 [F2OEM], DS21 [O3], DS13f [F3OEM]</p> <p>DS6</p> <p>DS8 [O1], DS9 [O3], DS10 [F1OEM], DS12 [S3 F2OEM], DS13s [S3], DS15 [F2OEM], DS21 [O3], DS13f [F3OEM]</p> | S | H | 5 | <p>DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS12 [S3 F2OEM], DS13s [S3], DS15 [F2OEM], DS21 [O3], DS13f [F3OEM]</p> <p>DS13s, DS12, DS6</p> <p>DS8 [O1], DS9 [O3], DS10 [F1OEM], DS15 [F2OEM], DS21 [O3], DS13f [F3OEM]</p> | S | SG | 2 |
| R43: T15 Spoofing/Manipulation auf gRPC zwischen Fahrzeugadapterdienst und Befehlsdienst, vorbereitet                                                                                            | <p>C5I Eigensicherheit des Trucks (gegen Spoofing/Manipulation)</p> <p>C20 ADS-</p>                                                                                                                                                                                                            | <p>DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS12</p>                                                                                                                                                                                        | S | H | 5 | <p>DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS12</p>                                                                                                                                                                        | S | SG | 2 |

|                                                                                                                                                                                                  |                                                                                                                                                                                                                                                                                                                                                                                                                                               |                                                                                                                                                                                                                                                      |   |   |   |                                                                                                                                                                                                                                      |   |    |   |  |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|---|---|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|----|---|--|
| durch P3md Unbefugter physischer Zugang zum Control Center (Manipulation des Datenflusses)                                                                                                       | <p>Sicherheitsvalidierungen nach Entscheidungen des Control Centers</p> <p>C22 Verschlüsselte und authentifizierte AWS-interne Kommunikation</p> <p>A10 Durch CC ausgelöste MRM sind nicht sicherheitskritisch</p>                                                                                                                                                                                                                            | <p>[S3 F2OEM], DS13s [S3], DS15 [F2OEM], DS21 [O3], DS13f [F3OEM]</p> <p>DS6</p> <p>DS8 [O1], DS9 [O3], DS10 [F1OEM], DS12 [S3 F2OEM], DS13s [S3], DS15 [F2OEM], DS21 [O3], DS13f [F3OEM]</p>                                                        |   |   |   | <p>[S3 F2OEM], DS13s [S3], DS15 [F2OEM], DS21 [O3], DS13f [F3OEM]</p> <p>DS13s, DS12, DS6</p> <p>DS8 [O1], DS9 [O3], DS10 [F1OEM], DS15 [F2OEM], DS21 [O3], DS13f [F3OEM]</p>                                                        |   |    |   |  |
| R44: T15 Spoofing/Manipulation auf gRPC zwischen Fahrzeugadapterdienst und Befehlsdienst Vorbereitung durch P4m Ausnutzen von Software-Schwachstellen des Fahrzeugadapterdienstes (Manipulation) | <p>C5I Intrinsische Sicherheit des Lkw (gegen Spoofing/Manipulation)</p> <p>C20 ADS-Sicherheitsvalidierungen nach Entscheidungen des Control Centers</p> <p>C18 Absicherung von Komponenten mit Internetanbindung gegen Software-Schwachstellen</p> <p>C28 End-to-End-Authentifizierung der Datenübertragung zwischen technischer Überwachungsausrüstung, Lkw, Kunden-/Flottenmanagement, externen Partnern, dynamischem Routenmanagement</p> | <p>DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS12 [S3 F2OEM], DS13s [S3], DS15 [F2OEM], DS21 [O3], DS13f [F3OEM]</p> <p>DS6</p> <p>DS8 [O1], DS9 [O3], DS10 [F1OEM], DS12 [S3 F2OEM], DS13s [S3], DS15 [F2OEM], DS21 [O3], DS13f [F3OEM]</p> | S | H | 5 | <p>DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS12 [S3 F2OEM], DS13s [S3], DS15 [F2OEM], DS21 [O3], DS13f [F3OEM]</p> <p>DS13s, DS12, DS6</p> <p>DS8 [O1], DS9 [O3], DS10 [F1OEM], DS15 [F2OEM], DS21 [O3], DS13f [F3OEM]</p> | S | SG | 2 |  |

|                                                                                                                                                                                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                                                                                                                                                                                                                                                      |   |   |   |                                                                                                                                                                                                                                      |   |    |   |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|---|---|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|----|---|
|                                                                                                                                                                                           | A10 Durch CC ausgelöste MRM sind nicht sicherheitskritisch                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                                                                                                                                                                                                                                                      |   |   |   |                                                                                                                                                                                                                                      |   |    |   |
| R45: T15 Spoofing/Manipulation auf gRPC zwischen Fahrzeugadapterdienst und Befehlsdienst, vorbereitet durch P12m Ausnutzen von Software-Schwachstellen des Befehlsdienstes (Manipulation) | <p>C5I Intrinsische Sicherheit des Lkw (gegen Spoofing/Manipulation)</p> <p>C20 ADS-Sicherheitsvalidierungen nach Entscheidungen des Control Centers</p> <p>C18 Absicherung von Komponenten mit Internetanbindung gegen Software-Schwachstellen</p> <p>C28 End-to-End-Authentifizierung der Datenübertragung zwischen technischer Überwachungsausrüstung, Lkw, Kunden-/Flottenmanagement, externen Partnern, dynamischem Routenmanagement</p> <p>A10 Durch CC ausgelöste MRM sind nicht sicherheitskritisch</p> | <p>DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS12 [S3 F2OEM], DS13s [S3], DS15 [F2OEM], DS21 [O3], DS13f [F3OEM]</p> <p>DS6</p> <p>DS8 [O1], DS9 [O3], DS10 [F1OEM], DS12 [S3 F2OEM], DS13s [S3], DS15 [F2OEM], DS21 [O3], DS13f [F3OEM]</p> | S | H | 5 | <p>DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS12 [S3 F2OEM], DS13s [S3], DS15 [F2OEM], DS21 [O3], DS13f [F3OEM]</p> <p>DS13s, DS12, DS6</p> <p>DS8 [O1], DS9 [O3], DS10 [F1OEM], DS15 [F2OEM], DS21 [O3], DS13f [F3OEM]</p> | S | SG | 2 |
| R46: T16 Abhören von HTTP zwischen Fahrzeugadapterdienst und CC Eventbus Vorbereitung durch P3ed Unbefugter physischer Zugang zum Control Center (Abhören des Datenflusses)               | C22 Verschlüsselte und authentifizierte AWS-interne Kommunikation                                                                                                                                                                                                                                                                                                                                                                                                                                               | DS1 [P2], DS16 [F2OEM]                                                                                                                                                                                                                               | E | H | 4 | DS1 [P2], DS16 [F2OEM]                                                                                                                                                                                                               | E | SG | 2 |
| R47: T16 Abhören von HTTP zwischen Fahrzeugadapterdienst und CC Eventbus Vorbereitung durch P4e                                                                                           | C18 Absicherung von Komponenten mit Internetanschluss                                                                                                                                                                                                                                                                                                                                                                                                                                                           | DS1 [P2], DS16 [F2OEM]                                                                                                                                                                                                                               | E | H | 4 | DS1 [P2], DS16 [F2OEM]                                                                                                                                                                                                               | E | SG | 2 |

|                                                                                                                                                                                                |                                                                                                                                                                                              |                                                                         |   |   |   |                                                                                                                                                   |   |    |   |  |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------|---|---|---|---------------------------------------------------------------------------------------------------------------------------------------------------|---|----|---|--|
| Ausnutzen von Software-Schwachstellen des Fahrzeugadapterdienstes (Abhören)                                                                                                                    | gegen Software-Schwachstellen<br>C27 End-to-End-verschlüsselte Übertragung sensibler Daten zwischen technischen Überwachungsgeräten, Lkw, externen Partnern und dynamischem Routenmanagement |                                                                         |   |   |   |                                                                                                                                                   |   |    |   |  |
| R48: T17 Unterbrechung von HTTP zwischen Fahrzeugadapterdienst und CC Eventbus Vorbereitung durch P3dd Unbefugter physischer Zugang zum Control Center (Unterbrechung des Datenflusses)        | A12 AWS schützt die Verfügbarkeit der Cloud-Infrastruktur                                                                                                                                    | DS8 [O1], DS9 [O3], DS17 [O0], DS21 [O3]                                | S | H | 2 | DS8 [O1], DS9 [O3], DS17 [O0], DS21 [O3]                                                                                                          | S | H  | 2 |  |
| R49: T17 Unterbrechung des HTTP-Verkehrs zwischen Fahrzeugadapterdienst und CC-Eventbus, vorbereitet von P4d Ausnutzen von Software-Schwachstellen des Fahrzeugadapterdienstes (Unterbrechung) | C18 Absicherung von Komponenten mit Internetverbindung gegen Software-Schwachstellen<br>C29 Resilienz/Sicherheit durch Vielfalt                                                              | DS8 [O1], DS9 [O3], DS17 [O0], DS21 [O3]                                | S | H | 5 | DS8 [O1], DS9 [O3], DS17 [O0], DS21 [O3]                                                                                                          | S | SG | 2 |  |
| R50: T18 Spoofing/Manipulation auf HTTP zwischen Fahrzeugadapterdienst und CC Eventbus Vorbereitung durch P3md Unbefugter physischer Zugang zum Control Center (Manipulation des Datenflusses) | C20 ADS-Sicherheitsvalidierungen nach Entscheidungen des Control Centers<br>C22 Verschlüsselte und authentifizierte AWS-interne Kommunikation                                                | DS8 [O1], DS9 [O3], DS12 [S3 F2OEM], DS15 [F2OEM], DS17 [O0], DS21 [O3] | S | H | 5 | DS8 [O1], DS9 [O3], DS12 [S3 F2OEM], DS15 [F2OEM], DS17 [O0], DS21 [O3]<br><br>DS12<br><br>DS8 [O1], DS9 [O3], DS15 [F2OEM], DS17 [O0], DS21 [O3] | S | SG | 2 |  |

|                                                                                                                                                                                                |                                                                                                                                                                                                                                                                                                                                                               |                                                                         |   |   |   |                                                                                                                                                                      |   |    |   |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------|---|---|---|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|----|---|
| R51: T18 Spoofing/Manipulation auf HTTP zwischen Fahrzeugadapterdienst und CC Eventbus Vorbereitung durch P4m Ausnutzen von Software-Schwachstellen des Fahrzeugadapterdienstes (Manipulation) | <p>C20 ADS-Sicherheitsvalidierungen nach Entscheidungen des Control Centers</p> <p>C18 Absicherung von Komponenten mit Internetanschluss gegen Software-Schwachstellen</p> <p>C28 Durchgängige authentische Datenübertragung zwischen technischer Überwachungsausrüstung, Lkw, Kunden-/Flottenmanagement, externen Partnern, dynamischem Routenmanagement</p> | DS8 [O1], DS9 [O3], DS12 [S3 F2OEM], DS15 [F2OEM], DS17 [O0], DS21 [O3] | S | H | 5 | <p>DS8 [O1], DS9 [O3], DS12 [S3 F2OEM], DS15 [F2OEM], DS17 [O0], DS21 [O3]</p> <hr/> <p>DS12</p> <hr/> <p>DS8 [O1], DS9 [O3], DS15 [F2OEM], DS17 [O0], DS21 [O3]</p> | S | SG | 2 |
| R52: T19 Abhören von HTTP zwischen Fahrzeugadapterdienst und CC-Backend, vorbereitet durch P3ed Unbefugter physischer Zugang zum Control Center (Abhören des Datenflusses)                     | C22 Verschlüsselte und authentifizierte AWS-interne Kommunikation                                                                                                                                                                                                                                                                                             | DS16 [F2OEM]                                                            | E | H | 4 | DS16 [F2OEM]                                                                                                                                                         | E | SG | 2 |
| R53: T19 Abhören von HTTP zwischen Fahrzeugadapterdienst und CC-Backend, vorbereitet durch P4e Ausnutzen von Software-Schwachstellen des Fahrzeugadapterdienstes (Abhören)                     | <p>C18 Absicherung von Komponenten mit Internetanschluss gegen Software-Schwachstellen</p> <p>C27 End-to-End-verschlüsselte Übertragung sensibler Daten zwischen technischen Überwachungsgeräten, Lkw, externen Partnern und dynamischem Routenmanagement</p>                                                                                                 | DS16 [F2OEM]                                                            | E | H | 4 | DS16 [F2OEM]                                                                                                                                                         | E | SG | 2 |

|                                                                                                                                                                                                 |                                                                                                                                                                                                                                                                          |                                                                                                                                                                                        |   |   |   |                                                                                                                                                                           |   |    |   |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|---|---|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|----|---|
| R54: T20 Unterbrechung des HTTP-Verkehrs zwischen Fahrzeugadapterdienst und CC-Backend, vorbereitet durch P3dd Unbefugter physischer Zugang zum Control Center (Unterbrechung des Datenflusses) | <p>C5A Eigensicherheit des Lkw (gegen Störungen)</p> <p>A10 Durch CC ausgelöste MRM sind nicht sicherheitskritisch</p> <p>A12 AWS schützt die Verfügbarkeit der Cloud-Infrastruktur</p>                                                                                  | <p>DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS13s [S3], DS21 [O3], DS13f [F3OEM]</p> <p>DS6</p> <p>DS8 [O1], DS9 [O3], DS10 [F1OEM], DS13s [S3], DS21 [O3], DS13f [F3OEM]</p> | S | H | 2 | <p>DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS13s [S3], DS21 [O3], DS13f [F3OEM]</p> <p>DS13s, DS13f, DS6</p> <p>DS8 [O1], DS9 [O3], DS10 [F1OEM], DS21 [O3]</p> | S | H  | 2 |
| R55: T20 Unterbrechung des HTTP-Verkehrs zwischen Fahrzeugadapterdienst und CC-Backend, vorbereitet von P4d Ausnutzen von Software-Schwachstellen des Fahrzeugadapterdienstes (Unterbrechung)   | <p>C5A Intrinsische Sicherheit des Lkw (gegen Störungen)</p> <p>C18 Absicherung von Komponenten mit Internetanbindung gegen Software-Schwachstellen</p> <p>C29 Resilienz/Sicherheit durch Vielfalt</p> <p>A10 Durch CC ausgelöste MRM sind nicht sicherheitskritisch</p> | <p>DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS13s [S3], DS21 [O3], DS13f [F3OEM]</p> <p>DS6</p> <p>DS8 [O1], DS9 [O3], DS10 [F1OEM], DS13s [S3], DS21 [O3], DS13f [F3OEM]</p> | S | H | 5 | <p>DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS13s [S3], DS21 [O3], DS13f [F3OEM]</p> <p>DS13s, DS13f, DS6</p> <p>DS8 [O1], DS9 [O3], DS10 [F1OEM], DS21 [O3]</p> | S | SG | 2 |
| R56: T21 Spoofing/Manipulation auf HTTP zwischen Fahrzeugadapterdienst und CC-Backend, vorbereitet von P3md Unbefugter physischer Zugang zum Control Center (Manipulation des Datenflusses)     | <p>C5I Eigensicherheit des Trucks (gegen Spoofing/Manipulation)</p> <p>C20 ADS-Sicherheitsvalidierungen nach Entscheidungen des Control Centers</p>                                                                                                                      | <p>DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS12 [S3 F2OEM], DS13s [S3], DS15 [F2OEM],</p>                                                                                    | S | H | 5 | <p>DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS12 [S3 F2OEM], DS13s [S3], DS15 [F2OEM],</p>                                                                       | S | SG | 2 |

|                                                                                                                                                                                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                               |                                                                                                                                                                                                                                                      |   |   |   |                                                                                                                                                                                                                                      |   |    |   |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|---|---|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|----|---|
|                                                                                                                                                                                                      | <p>C22 Verschlüsselte und authentifizierte AWS-interne Kommunikation</p> <p>A10 Durch CC ausgelöste MRM sind nicht sicherheitskritisch</p>                                                                                                                                                                                                                                                                                                    | <p>DS21 [O3], DS13f [F3OEM]</p> <p>DS6</p> <p>DS8 [O1], DS9 [O3], DS10 [F1OEM], DS12 [S3 F2OEM], DS13s [S3], DS15 [F2OEM], DS21 [O3], DS13f [F3OEM]</p>                                                                                              |   |   |   | <p>DS21 [O3], DS13f [F3OEM]</p> <p>DS13s, DS12, DS6</p> <p>DS8 [O1], DS9 [O3], DS10 [F1OEM], DS15 [F2OEM], DS21 [O3], DS13f [F3OEM]</p>                                                                                              |   |    |   |
| <p>R57: T21 Spoofing/Manipulation auf HTTP zwischen Fahrzeugadapterdienst und CC-Backend Vorbereitung durch P4m Ausnutzen von Software-Schwachstellen des Fahrzeugadapterdienstes (Manipulation)</p> | <p>C5I Intrinsische Sicherheit des Lkw (gegen Spoofing/Manipulation)</p> <p>C20 ADS-Sicherheitsvalidierungen nach Entscheidungen des Control Centers</p> <p>C18 Absicherung von Komponenten mit Internetanbindung gegen Software-Schwachstellen</p> <p>C28 End-to-End-Authentifizierung der Datenübertragung zwischen technischer Überwachungsausrüstung, Lkw, Kunden-/Flottenmanagement, externen Partnern, dynamischem Routenmanagement</p> | <p>DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS12 [S3 F2OEM], DS13s [S3], DS15 [F2OEM], DS21 [O3], DS13f [F3OEM]</p> <p>DS6</p> <p>DS8 [O1], DS9 [O3], DS10 [F1OEM], DS12 [S3 F2OEM], DS13s [S3], DS15 [F2OEM], DS21 [O3], DS13f [F3OEM]</p> | S | H | 5 | <p>DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS12 [S3 F2OEM], DS13s [S3], DS15 [F2OEM], DS21 [O3], DS13f [F3OEM]</p> <p>DS13s, DS12, DS6</p> <p>DS8 [O1], DS9 [O3], DS10 [F1OEM], DS15 [F2OEM], DS21 [O3], DS13f [F3OEM]</p> | S | SG | 2 |

|                                                                                                                                                                                   |                                                                                                                                               |                                                                                     |   |   |   |                                                                                                                                                   |   |    |   |  |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|---|---|---|---------------------------------------------------------------------------------------------------------------------------------------------------|---|----|---|--|
|                                                                                                                                                                                   | A10 Durch CC ausgelöste MRM sind nicht sicherheitskritisch                                                                                    |                                                                                     |   |   |   |                                                                                                                                                   |   |    |   |  |
| R58: T22 Abhören von HTTP zwischen CC-Backend und CC-Eventbus Vorbereitung durch P3ed Unbefugter physischer Zugang zum Control Center (Abhören des Datenflusses)                  | C22 Verschlüsselte und authentifizierte AWS-interne Kommunikation                                                                             | DS1 [P2], DS16 [F2OEM]                                                              | E | H | 4 | DS1 [P2], DS16 [F2OEM]                                                                                                                            | E | SG | 2 |  |
| R59: T23 Unterbrechung von HTTP zwischen CC-Backend und CC-Eventbus Vorbereitung durch P3dd Unbefugter physischer Zugang zum Control Center (Unterbrechung des Datenflusses)      | A12 AWS schützt die Verfügbarkeit der Cloud-Infrastruktur                                                                                     | DS8 [O1], DS9 [O3], DS17 [O0], DS21 [O3]                                            | S | H | 2 | DS8 [O1], DS9 [O3], DS17 [O0], DS21 [O3]                                                                                                          | S | H  | 2 |  |
| R60: T24 Spoofing/Manipulation von HTTP zwischen CC-Backend und CC-Eventbus, vorbereitet von P3md Unbefugter physischer Zugang zum Control Center (Manipulation des Datenflusses) | C20 ADS-Sicherheitsvalidierungen nach Entscheidungen des Control Centers<br>C22 Verschlüsselte und authentifizierte AWS-interne Kommunikation | DS8 [O1], DS9 [O3], DS12 [S3 F2OEM], DS15 [F2OEM], DS17 [O0], DS21 [O3]             | S | H | 5 | DS8 [O1], DS9 [O3], DS12 [S3 F2OEM], DS15 [F2OEM], DS17 [O0], DS21 [O3]<br><br>DS12<br><br>DS8 [O1], DS9 [O3], DS15 [F2OEM], DS17 [O0], DS21 [O3] | S | SG | 2 |  |
| R61: T25 Abhören von HTTP zwischen CC-Backend und Datenbank Vorbereitung durch P3ed Unbefugter physischer Zugang zum Control Center (Abhören des Datenflusses)                    | C22 Verschlüsselte und authentifizierte AWS-interne Kommunikation                                                                             | DS1 [P2], DS16 [F2OEM], DS19 [P2]                                                   | E | H | 4 | DS1 [P2], DS16 [F2OEM], DS19 [P2]                                                                                                                 | E | SG | 2 |  |
| R62: T26 Unterbrechung von HTTP zwischen CC-Backend und Datenbankvorbereitung durch P3dd Unbefugter physischer Zugang zum Control Center (Unterbrechung des Datenflusses)         | C5A Eigensicherheit des Lkw (gegen Störungen)<br><br>A10 Durch CC ausgelöste MRM                                                              | DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS13s [S3], DS17 [O0], DS21 [O3], | S | H | 2 | DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS13s [S3], DS17 [O0], DS21 [O3],                                                               | S | H  | 2 |  |



|                                                                                                                                                                                 |                                                                                                                                                                                                                                                                                      |                                                                                                                                                                                                                                                                               |   |   |   |                                                                                                                                                                                                                                                               |   |    |   |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|---|---|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|----|---|
|                                                                                                                                                                                 | sind nicht sicherheitskritisch<br>A12 AWS schützt die Verfügbarkeit der Cloud-Infrastruktur                                                                                                                                                                                          | DS13f [F3OEM]<br>_____<br>DS6<br>_____<br>DS8 [O1], DS9 [O3],<br>DS10 [F1OEM], DS13s<br>[S3], DS17 [O0], DS21<br>[O3], DS13f [F3OEM]                                                                                                                                          |   |   |   | DS13f [F3OEM]<br>_____<br>DS13s, DS13f, DS6<br>_____<br>DS8 [O1], DS9 [O3],<br>DS10 [F1OEM], DS17<br>[O0], DS21 [O3]                                                                                                                                          |   |    |   |
| R63: T27 Spoofing/Manipulation von HTTP zwischen CC-Backend und Datenbank, vorbereitet von P3md Unbefugter physischer Zugang zum Control Center (Manipulation des Datenflusses) | C5I Eigensicherheit des Trucks (gegen Spoofing/Manipulation)<br>C20 ADS-Sicherheitsvalidierungen nach Entscheidungen des Control Centers<br>C22 Verschlüsselte und authentifizierte AWS-interne Kommunikation<br>_____<br>A10 Durch CC ausgelöste MRM sind nicht sicherheitskritisch | DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS12 [S3 F2OEM], DS13s [S3], DS15 [F2OEM], DS17 [O0], DS21 [O3], DS13f [F3OEM]<br>_____<br>DS6<br>_____<br>DS8 [O1], DS9 [O3], DS10 [F1OEM], DS12 [S3 F2OEM], DS13s [S3], DS15 [F2OEM], DS17 [O0], DS21 [O3], DS13f [F3OEM] | S | H | 5 | DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS12 [S3 F2OEM], DS13s [S3], DS15 [F2OEM], DS17 [O0], DS21 [O3], DS13f [F3OEM]<br>_____<br>DS13s, DS12, DS6<br>_____<br>DS8 [O1], DS9 [O3], DS10 [F1OEM], DS15 [F2OEM], DS17 [O0], DS21 [O3], DS13f [F3OEM] | S | SG | 2 |
| R64: T28 Abhören von HTTP zwischen CC-Backend und API-Gateway Vorbereitung durch P3ed Unbefugter physischer Zugang zum Control Center (Abhören des Datenflusses)                | C22 Verschlüsselte und authentifizierte AWS-interne Kommunikation                                                                                                                                                                                                                    |                                                                                                                                                                                                                                                                               |   | H | 1 |                                                                                                                                                                                                                                                               |   | SG | 1 |

|                                                                                                                                                                                     |                                                                                                                                                                                                                                                    |                                               |   |   |   |                                                                 |   |    |   |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------|---|---|---|-----------------------------------------------------------------|---|----|---|
| R65: T28 Abhören von HTTP zwischen CC-Backend und API-Gateway, vorbereitet von P7e Ausnutzen von Software-Schwachstellen des API-Gateways (Abhören)                                 | C18 Absicherung von Komponenten mit Internetanschluss gegen Software-Schwachstellen<br>C27 End-to-End-verschlüsselte Übertragung sensibler Daten zwischen technischen Überwachungsgeräten, Lkw, externen Partnern und dynamischem Routenmanagement |                                               |   | H | 1 |                                                                 |   | SG | 1 |
| R66: T29 Störung von HTTP zwischen CC-Backend und API-Gateway Vorbereitung durch P3dd Unbefugter physischer Zugang zum Control Center (Störung des Datenflusses)                    | C5A Eigensicherheit des Trucks (gegen Störungen)<br>A12 AWS schützt die Verfügbarkeit der Cloud-Infrastruktur                                                                                                                                      | DS8 [O1], DS13s [S3], DS13f [F3OEM]           | S | H | 2 | DS8 [O1], DS13s [S3], DS13f [F3OEM]<br>DS13s, DS13f<br>DS8 [O1] | M | H  | 2 |
| R67: T29 Unterbrechung des HTTP-Verkehrs zwischen CC-Backend und API-Gateway, vorbereitet durch P7d Ausnutzen von Software-Schwachstellen des API-Gateways (Unterbrechung)          | C5A Eigensicherheit des Lkw (gegen Störungen)<br>C18 Absicherung von Komponenten mit Internetanbindung gegen Software-Schwachstellen<br>C29 Resilienz/Sicherheit durch Vielfalt                                                                    | DS8 [O1], DS13s [S3], DS13f [F3OEM]           | S | H | 5 | DS8 [O1], DS13s [S3], DS13f [F3OEM]<br>DS13s, DS13f<br>DS8 [O1] | M | SG | 1 |
| R68: T30 Spoofing/Manipulation auf HTTP zwischen CC-Backend und API-Gateway, vorbereitet durch P3md Unbefugter physischer Zugang zum Control Center (Manipulation des Datenflusses) | C5I Intrinsische Sicherheit des Lkw (gegen Spoofing/Manipulation)<br>C22 Verschlüsselte und                                                                                                                                                        | DS8 [O1], DS9 [O3], DS13s [S3], DS13f [F3OEM] | S | H | 5 | DS8 [O1], DS9 [O3], DS13s [S3], DS13f [F3OEM]<br>DS13s          | S | SG | 2 |

|                                                                                                                                                                                           | authentifizierte AWS-interne Kommunikation                                                                                                                                                                                                                                                                                                     |                                               |   |   |   | DS8 [O1], DS9 [O3], DS13f [F3OEM]                                                                   |   |    |   |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------|---|---|---|-----------------------------------------------------------------------------------------------------|---|----|---|
| R69: T30 Spoofing/Manipulation auf HTTP zwischen CC-Backend und API-Gateway, vorbereitet durch P7m Ausnutzen von Software-Schwachstellen des API-Gateways (Manipulation)                  | C5I Intrinsische Sicherheit des Lkw (gegen Spoofing/Manipulation)<br>C18 Absicherung von Komponenten mit Internetanbindung gegen Software-Schwachstellen<br>C28 End-to-End-Authentifizierung der Datenübertragung zwischen technischer Überwachungsausrüstung, Lkw, Kunden-/Flottenmanagement, externen Partnern, dynamischem Routenmanagement | DS8 [O1], DS9 [O3], DS13s [S3], DS13f [F3OEM] | S | H | 5 | DS8 [O1], DS9 [O3], DS13s [S3], DS13f [F3OEM]<br><br>DS13s<br><br>DS8 [O1], DS9 [O3], DS13f [F3OEM] | S | SG | 2 |
| R70: T31 Abhören von HTTP zwischen CC-Backend und CC-Backend für Frontend-Vorbereitung durch P3ed Unbefugter physischer Zugang zum Control Center (Abhören des Datenflusses)              | C22 Verschlüsselte und authentifizierte AWS-interne Kommunikation                                                                                                                                                                                                                                                                              | DS1 [P2], DS16 [F2OEM]                        | E | H | 4 | DS1 [P2], DS16 [F2OEM]                                                                              | E | SG | 2 |
| R71: T31 Abhören von HTTP zwischen CC-Backend und CC-Backend für Frontend-Vorbereitung durch P6e Ausnutzen von Software-Schwachstellen des Control Center-Backends für Frontend (Abhören) | C18 Absicherung von Komponenten mit Internetanschluss gegen Software-Schwachstellen<br>C27 End-to-End-verschlüsselte Übertragung sensibler Daten zwischen technischen Überwachungsgeräten, Lkw, externen                                                                                                                                       | DS1 [P2], DS16 [F2OEM]                        | E | H | 4 | DS1 [P2], DS16 [F2OEM]                                                                              | E | SG | 2 |

|                                                                                                                                                                                                                    | Partnern und dynamischem Routenmanagement                                                                                                                                                                                                                                  |                                                                                                                                                                                                              |   |   |   |                                                                                                                                                                                                 |   |    |   |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|---|---|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|----|---|
| R72: T32 Unterbrechung von HTTP zwischen CC-Ba-ckend und CC-Backend für Frontend-Vorbereitung durch P3dd Unbefugter physischer Zugang zum Control Center (Unterbrechung des Datenflusses)                          | <p>C5A Eigensicherheit des Lkw (gegen Störungen)</p> <p>A10 Durch CC ausgelöste MRM sind nicht sicherheitskritisch</p> <p>A12 AWS schützt die Verfügbar-keit der Cloud-Infrastruktur</p>                                                                                   | <p>DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS13s [S3], DS17 [O0], DS21 [O3], DS13f [F3OEM]</p> <p>DS6</p> <p>DS8 [O1], DS9 [O3], DS10 [F1OEM], DS13s [S3], DS17 [O0], DS21 [O3], DS13f [F3OEM]</p> | S | H | 2 | <p>DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS13s [S3], DS17 [O0], DS21 [O3], DS13f [F3OEM]</p> <p>DS13s, DS13f, DS6</p> <p>DS8 [O1], DS9 [O3], DS10 [F1OEM], DS17 [O0], DS21 [O3]</p> | S | H  | 2 |
| R73: T32 Unterbrechung des HTTP-Verkehrs zwischen CC-Backend und CC-Backend für Frontend-Vorberei-tung durch P6d Ausnutzung von Software-Schwach-stellen des Control Center-Backends für Frontend (Un-terbrechung) | <p>C5A Intrinsische Sicherheit des Lkw (gegen Störungen)</p> <p>C18 Absicherung von Kompo-nenten mit Internetanbindung gegen Software-Schwachstel-len</p> <p>C29 Resilienz/Sicherheit durch Vielfalt</p> <p>A10 Durch CC ausgelöste MRM sind nicht sicherheitskritisch</p> | <p>DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS13s [S3], DS17 [O0], DS21 [O3], DS13f [F3OEM]</p> <p>DS6</p> <p>DS8 [O1], DS9 [O3], DS10 [F1OEM], DS13s [S3], DS17 [O0], DS21 [O3], DS13f [F3OEM]</p> | S | H | 5 | <p>DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS13s [S3], DS17 [O0], DS21 [O3], DS13f [F3OEM]</p> <p>DS13s, DS13f, DS6</p> <p>DS8 [O1], DS9 [O3], DS10 [F1OEM], DS17 [O0], DS21 [O3]</p> | S | SG | 2 |
| R74: T33 Spoofing/Manipulation auf HTTP zwischen CC-Backend und CC-Backend für Frontend-                                                                                                                           | <p>C5I Eigensicherheit des Trucks (gegen Spoofing/Manipulation)</p> <p>C20 ADS-</p>                                                                                                                                                                                        | <p>DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS12</p>                                                                                                                                                | S | H | 5 | <p>DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS12</p>                                                                                                                                   | S | SG | 2 |

|                                                                                                                                                                                                              |                                                                                                                                                                                                                                                                                                                                                                                                                            |                                                                                                                                                                                                                                                                                                      |   |   |   |                                                                                                                                                                                                                                                                                   |   |    |   |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|---|---|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|----|---|
| Vorbereitung durch P3md Unbefugter physischer Zugang zum Control Center (Manipulation des Datenflusses)                                                                                                      | Sicherheitsvalidierungen nach Entscheidungen des Control Centers<br>C22 Verschlüsselte und authentifizierte AWS-interne Kommunikation                                                                                                                                                                                                                                                                                      | [S3 F2OEM], DS13s<br>[S3], DS15 [F2OEM],<br>DS17 [O0], DS21 [O3],<br>DS13f [F3OEM]<br><br>DS6                                                                                                                                                                                                        |   |   |   | [S3 F2OEM], DS13s<br>[S3], DS15 [F2OEM],<br>DS17 [O0], DS21 [O3],<br>DS13f [F3OEM]<br><br>DS13s, DS12, DS6                                                                                                                                                                        |   |    |   |
|                                                                                                                                                                                                              | A10 Durch CC ausgelöste MRM sind nicht sicherheitskritisch                                                                                                                                                                                                                                                                                                                                                                 | DS8 [O1], DS9 [O3],<br>DS10 [F1OEM], DS12<br>[S3 F2OEM], DS13s<br>[S3], DS15 [F2OEM],<br>DS17 [O0], DS21 [O3],<br>DS13f [F3OEM]                                                                                                                                                                      |   |   |   | DS8 [O1], DS9 [O3],<br>DS10 [F1OEM], DS15<br>[F2OEM], DS17 [O0],<br>DS21 [O3], DS13f<br>[F3OEM]                                                                                                                                                                                   |   |    |   |
| R75: T33 Spoofing/Manipulation auf HTTP zwischen CC-Backend und CC-Backend für Frontend-Vorbereitung durch P6m Ausnutzen von Software-Schwachstellen des Control Center-Backends für Frontend (Manipulation) | C5I Intrinsische Sicherheit des Lkw (gegen Spoofing/Manipulation)<br>C20 ADS-Sicherheitsvalidierungen nach Entscheidungen des Control Centers<br>C18 Absicherung von Komponenten mit Internetanbindung gegen Software-Schwachstellen<br>C28 End-to-End-Authentifizierung der Datenübertragung zwischen technischer Überwachungsausrüstung, Lkw, Kunden-/Flottenmanagement, externen Partnern, dynamischem Routenmanagement | DS6 [S3 F2OEM], DS8<br>[O1], DS9 [O3], DS10<br>[F1OEM], DS12<br>[S3 F2OEM], DS13s<br>[S3], DS15 [F2OEM],<br>DS17 [O0], DS21 [O3],<br>DS13f [F3OEM]<br><br>DS6<br><br>DS8 [O1], DS9 [O3],<br>DS10 [F1OEM], DS12<br>[S3 F2OEM], DS13s<br>[S3], DS15 [F2OEM],<br>DS17 [O0], DS21 [O3],<br>DS13f [F3OEM] | S | H | 5 | DS6 [S3 F2OEM], DS8<br>[O1], DS9 [O3], DS10<br>[F1OEM], DS12<br>[S3 F2OEM], DS13s<br>[S3], DS15 [F2OEM],<br>DS17 [O0], DS21 [O3],<br>DS13f [F3OEM]<br><br>DS13s, DS12, DS6<br><br>DS8 [O1], DS9 [O3],<br>DS10 [F1OEM], DS15<br>[F2OEM], DS17 [O0],<br>DS21 [O3], DS13f<br>[F3OEM] | S | SG | 2 |

|                                                                                                                                                                                                                     |                                                                                                                                                                                                                                                                                                                                                                  |                        |   |   |   |                        |   |    |   |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------|---|---|---|------------------------|---|----|---|
|                                                                                                                                                                                                                     | A10 Durch CC ausgelöste MRM sind nicht sicherheitskritisch                                                                                                                                                                                                                                                                                                       |                        |   |   |   |                        |   |    |   |
| R76: T34 Abhören von HTTP zwischen technischer Überwachungs-ausrüstung und CC-Backend für Front-end                                                                                                                 | C25 mTLS zwischen dem Backend des Control Centers für das Frontend und den technischen Überwachungsgeräten                                                                                                                                                                                                                                                       | DS1 [P2], DS16 [F2OEM] | E | H | 4 | DS1 [P2], DS16 [F2OEM] | E | SG | 2 |
| R77: T34 Abhören von HTTP zwischen technischer Überwachungs-ausrüstung und CC-Backend für Front-end Vorbereitung durch P3ed Unbefugter physischer Zugang zum Control Center (Abhören des Datenflusses)              | C25 mTLS zwischen dem Backend des Control Centers für das Frontend und den technischen Überwachungsgeräten                                                                                                                                                                                                                                                       | DS1 [P2], DS16 [F2OEM] | E | H | 4 | DS1 [P2], DS16 [F2OEM] | E | SG | 2 |
| R78: T34 Abhören von HTTP zwischen technischer Überwachungs-ausrüstung und CC-Backend für Front-end Vorbereitung durch P6e Ausnutzen von Software-Schwachstellen des Control Center-Backends für Frontend (Abhören) | C25 mTLS zwischen dem Backend des Control Centers für das Frontend und den technischen Überwachungsgeräten<br>C18 Absicherung von Komponenten mit Internetanbindung gegen Software-Schwachstellen<br>C27 End-to-End-verschlüsselte Übertragung sensibler Daten zwischen technischen Überwachungsgeräten, Lkw, externen Partnern und dynamischem Routenmanagement | DS1 [P2], DS16 [F2OEM] | E | H | 4 | DS1 [P2], DS16 [F2OEM] | E | SG | 2 |
| R79: T34 Abhören von HTTP zwischen technischer Überwachungs-ausrüstung und CC-Backend für                                                                                                                           | C24 Absicherung technischer Überwachungsgeräte                                                                                                                                                                                                                                                                                                                   | DS1 [P2], DS16 [F2OEM] | E | H | 4 | DS1 [P2], DS16 [F2OEM] | E | SG | 2 |

|                                                                                                                                                                                                                                      |                                                                                                                                                                                                                                                                                                                                             |                                                                                                                                                                                                       |   |   |   |                                                                                                                                                                                          |   |    |   |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|---|---|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|----|---|
| Frontend-Vorbereitung durch P8 Ausnutzen von Software-Schwachstellen der technischen Überwachungs-ausrüstung                                                                                                                         |                                                                                                                                                                                                                                                                                                                                             |                                                                                                                                                                                                       |   |   |   |                                                                                                                                                                                          |   |    |   |
| R80: T35 Unterbrechung von HTTP zwischen technischer Überwachungs-ausrüstung und CC-Backend für Frontend-Vorbereitung durch P3dd Unbefugter physischer Zugang zum Control Center (Unterbrechung des Datenflusses)                    | C5A Eigensicherheit des Trucks (gegen Störungen)<br>C26 Redundanz gegen Ausfall/Störung der technischen Überwachungs-ausrüstung<br><br>A10 Durch CC ausgelöste MRM sind nicht sicherheitskritisch<br>A12 AWS schützt die Verfügbarkeit der Cloud-Infrastruktur                                                                              | DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS13s [S3], DS17 [O0], DS21 [O3], DS13f [F3OEM]<br><br>DS6<br><br>DS8 [O1], DS9 [O3], DS10 [F1OEM], DS13s [S3], DS17 [O0], DS21 [O3], DS13f [F3OEM] | S | H | 2 | DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS13s [S3], DS17 [O0], DS21 [O3], DS13f [F3OEM]<br><br>DS13s, DS13f, DS6<br><br>DS8 [O1], DS9 [O3], DS10 [F1OEM], DS17 [O0], DS21 [O3] | S | SG | 2 |
| R81: T35 Unterbrechung des HTTP-Verkehrs zwischen technischen Überwachungsgeräten und CC-Backend für Frontend-Vorbereitung durch P6d Ausnutzung von Software-Schwachstellen des Control Center-Backends für Frontend (Unterbrechung) | C5A Eigensicherheit des Trucks (gegen Störungen)<br>C26 Redundanz gegen Ausfall/Störung der technischen Überwachungs-ausrüstung<br>C18 Absicherung von Komponenten mit Internetanbindung gegen Software-Schwachstellen<br>C29 Ausfallsicherheit/Sicherheit durch Vielfalt<br><br>A10 Durch CC ausgelöste MRM sind nicht sicherheitskritisch | DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS13s [S3], DS17 [O0], DS21 [O3], DS13f [F3OEM]<br><br>DS6<br><br>DS8 [O1], DS9 [O3], DS10 [F1OEM], DS13s [S3], DS17 [O0], DS21 [O3], DS13f [F3OEM] | S | H | 5 | DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS13s [S3], DS17 [O0], DS21 [O3], DS13f [F3OEM]<br><br>DS13s, DS13f, DS6<br><br>DS8 [O1], DS9 [O3], DS10 [F1OEM], DS17 [O0], DS21 [O3] | S | SG | 2 |

|                                                                                                                                                                                                                                                    |                                                                                                                                                                                                                                                                         |                                                                                                                                                                                                              |   |   |   |                                                                                                                                                                                                 |   |    |   |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|---|---|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|----|---|
| R82: T35 Unterbrechung des HTTP-Verkehrs zwischen der technischen Überwachungs-ausrüstung und dem CC-Backend zur Vorbereitung des Frontends durch P8 Ausnutzung von Software-Schwachstellen der technischen Überwachungs-ausrüstung                | <p>C5A Eigensicherheit des Trucks (gegen Störungen)</p> <p>C26 Redundanz gegen Ausfall/Störung der technischen Überwachungs-ausrüstung</p> <p>C24 Härtung der technischen Überwachungs-ausrüstung</p> <p>A10 Durch CC ausgelöste MRM sind nicht sicherheitskritisch</p> | <p>DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS13s [S3], DS17 [O0], DS21 [O3], DS13f [F3OEM]</p> <p>DS6</p> <p>DS8 [O1], DS9 [O3], DS10 [F1OEM], DS13s [S3], DS17 [O0], DS21 [O3], DS13f [F3OEM]</p> | S | H | 5 | <p>DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS13s [S3], DS17 [O0], DS21 [O3], DS13f [F3OEM]</p> <p>DS13s, DS13f, DS6</p> <p>DS8 [O1], DS9 [O3], DS10 [F1OEM], DS17 [O0], DS21 [O3]</p> | S | SG | 2 |
| R83: T35 Unterbrechung von HTTP zwischen technischer Überwachungs-ausrüstung und CC-Backend für Frontend-Vorbereitung durch P19 Unterbrechung der Internetverbindung zwischen technischer Überwachungs-ausrüstung und Frontend des Control Centers | <p>C5A Eigensicherheit des Trucks (gegen Störungen)</p> <p>C26 Redundanz gegen Ausfall/Störung der technischen Überwachungs-ausrüstung</p> <p>A10 Durch CC ausgelöste MRM sind nicht sicherheitskritisch</p>                                                            | <p>DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS13s [S3], DS17 [O0], DS21 [O3], DS13f [F3OEM]</p> <p>DS6</p> <p>DS8 [O1], DS9 [O3], DS10 [F1OEM], DS13s [S3], DS17 [O0], DS21 [O3], DS13f [F3OEM]</p> | S | G | 3 | <p>DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS13s [S3], DS17 [O0], DS21 [O3], DS13f [F3OEM]</p> <p>DS13s, DS13f, DS6</p> <p>DS8 [O1], DS9 [O3], DS10 [F1OEM], DS17 [O0], DS21 [O3]</p> | S | SG | 2 |
| R84: T36 Spoofing/Manipulation auf HTTP zwischen technischer Überwachungs-ausrüstung und CC-Backend für Frontend                                                                                                                                   | <p>C5I Eigensicherheit des Trucks (gegen Spoofing/Manipulation)</p> <p>C20 ADS-Sicherheitsvalidierungen nach Entscheidungen des Control Centers</p>                                                                                                                     | <p>DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS12 [S3 F2OEM], DS13s [S3], DS15 [F2OEM],</p>                                                                                                          | S | H | 5 | <p>DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS12 [S3 F2OEM], DS13s [S3], DS15 [F2OEM],</p>                                                                                             | S | SG | 2 |



|                                                                                                                                                                                                                        |                                                                                                                                                                                                                                                                                                                                                             |                                                                                                                                                                                                                                                                            |   |   |   |                                                                                                                                                                                                                                                            |   |    |   |  |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|---|---|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|----|---|--|
|                                                                                                                                                                                                                        | <p>C25 mTLS zwischen dem Backend des Control Centers für das Frontend und der technischen Überwachungs-ausrüstung</p> <p>A10 Durch das Control Center ausgelöste MRM sind nicht sicherheitskritisch</p>                                                                                                                                                     | <p>DS17 [O0], DS21 [O3], DS13f [F3OEM]</p> <p>DS6</p> <p>DS8 [O1], DS9 [O3], DS10 [F1OEM], DS12 [S3 F2OEM], DS13s [S3], DS15 [F2OEM], DS17 [O0], DS21 [O3], DS13f [F3OEM]</p>                                                                                              |   |   |   | <p>DS17 [O0], DS21 [O3], DS13f [F3OEM]</p> <p>DS13s, DS12, DS6</p> <p>DS8 [O1], DS9 [O3], DS10 [F1OEM], DS15 [F2OEM], DS17 [O0], DS21 [O3], DS13f [F3OEM]</p>                                                                                              |   |    |   |  |
| R85: T36 Spoofing/Manipulation auf HTTP zwischen technischer Überwachungs-ausrüstung und CC-Backend für Frontend, vorbereitet von P3md Unbefugter physischer Zugang zum Control Center (Manipulation des Datenflusses) | <p>C5I Eigensicherheit des Trucks (gegen Spoofing/Manipulation)</p> <p>C20 ADS-Sicherheitsvalidierungen nach Entscheidungen des Control Centers</p> <p>C25 mTLS zwischen dem Backend des Control Centers für das Frontend und der technischen Überwachungs-ausrüstung</p> <p>A10 Durch das Control Center ausgelöste MRM sind nicht sicherheitskritisch</p> | <p>DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS12 [S3 F2OEM], DS13s [S3], DS15 [F2OEM], DS17 [O0], DS21 [O3], DS13f [F3OEM]</p> <p>DS6</p> <p>DS8 [O1], DS9 [O3], DS10 [F1OEM], DS12 [S3 F2OEM], DS13s [S3], DS15 [F2OEM], DS17 [O0], DS21 [O3], DS13f [F3OEM]</p> | S | H | 5 | <p>DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS12 [S3 F2OEM], DS13s [S3], DS15 [F2OEM], DS17 [O0], DS21 [O3], DS13f [F3OEM]</p> <p>DS13s, DS12, DS6</p> <p>DS8 [O1], DS9 [O3], DS10 [F1OEM], DS15 [F2OEM], DS17 [O0], DS21 [O3], DS13f [F3OEM]</p> | S | SG | 2 |  |
| R86: T36 Spoofing/Manipulation auf HTTP zwischen technischer Überwachungs-ausrüstung und CC-                                                                                                                           | C5I Intrinsische Sicherheit des Trucks (gegen                                                                                                                                                                                                                                                                                                               | <p>DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10</p>                                                                                                                                                                                                                            | S | H | 5 | <p>DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10</p>                                                                                                                                                                                                            | S | SG | 2 |  |

|                                                                                                                                                                                                                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |                                                                                                                                                                                                                                                 |   |   |   |                                                                                                                                                                                                                                 |   |    |   |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|---|---|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|----|---|
| Backend für Frontend Vorbereitung durch P6m Ausnutzen von Software-Schwachstellen des Control Center-Backends für Frontend (Manipulation)                                                                             | <p>Spoofing/Manipulation)</p> <p>C20 ADS-Sicherheitsvalidierungen nach Entscheidungen des Control Centers</p> <p>C25 mTLS zwischen dem Backend des Control Centers für das Frontend und der technischen Überwachungs-ausrüstung</p> <p>C18 Absicherung von Komponenten mit Internetanschluss gegen Software-Schwachstellen</p> <p>C28 End-to-End-Authentifizierung der Datenübertragung zwischen technischer Überwachungs-ausrüstung, Lkw, Kunden-/Flottenmanagement, externen Partnern, dynamischem Routenmanagement</p> <p>A10 Durch das Control Center ausgelöste MRM sind nicht sicherheitskritisch</p> | <p>[F1OEM], DS12</p> <p>[S3 F2OEM], DS13s</p> <p>[S3], DS15 [F2OEM], DS17 [O0], DS21 [O3], DS13f [F3OEM]</p> <p>DS6</p> <p>DS8 [O1], DS9 [O3], DS10 [F1OEM], DS12 [S3 F2OEM], DS13s [S3], DS15 [F2OEM], DS17 [O0], DS21 [O3], DS13f [F3OEM]</p> |   |   |   | <p>[F1OEM], DS12</p> <p>[S3 F2OEM], DS13s</p> <p>[S3], DS15 [F2OEM], DS17 [O0], DS21 [O3], DS13f [F3OEM]</p> <p>DS13s, DS12, DS6</p> <p>DS8 [O1], DS9 [O3], DS10 [F1OEM], DS15 [F2OEM], DS17 [O0], DS21 [O3], DS13f [F3OEM]</p> |   |    |   |
| R87: T36 Spoofing/Manipulation auf HTTP zwischen technischer Überwachungs-ausrüstung und CC-Backend für Frontend-Vorbereitung durch P8 Ausnutzung von Software-Schwachstellen der technischen Überwachungs-ausrüstung | <p>C5I Eigensicherheit des Trucks (gegen Spoofing/Manipulation)</p> <p>C20 ADS-Sicherheitsvalidierungen nach Entscheidungen des Control Centers</p> <p>C24 Härtung der technischen</p>                                                                                                                                                                                                                                                                                                                                                                                                                      | <p>DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS12 [S3 F2OEM], DS13s [S3], DS15 [F2OEM], DS17 [O0], DS21 [O3],</p>                                                                                                                       | S | H | 5 | <p>DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS12 [S3 F2OEM], DS13s [S3], DS15 [F2OEM], DS17 [O0], DS21 [O3],</p>                                                                                                       | S | SG | 2 |

|                                                                                                                                                                                | Überwachungsausrüstung                                                                         | DS13f [F3OEM]                                                                                                           |   |   |   | DS13f [F3OEM]                                                                                           |   |    |   |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------|---|---|---|---------------------------------------------------------------------------------------------------------|---|----|---|
|                                                                                                                                                                                | A10 Durch CC ausgelöste MRM sind nicht sicherheitskritisch                                     | DS6<br>DS8 [O1], DS9 [O3], DS10 [F1OEM], DS12 [S3 F2OEM], DS13s [S3], DS15 [F2OEM], DS17 [O0], DS21 [O3], DS13f [F3OEM] |   |   |   | DS13s, DS12, DS6<br>DS8 [O1], DS9 [O3], DS10 [F1OEM], DS15 [F2OEM], DS17 [O0], DS21 [O3], DS13f [F3OEM] |   |    |   |
| R88: T40 Abhören von HTTP zwischen CC-Backend und Kunden-/Flottenmanagement, vorbereitet durch P1ed Unbefugter physischer Zugriff auf AWS Cloud (Abhören des Datenflusses)     | C22 Verschlüsselte und authentifizierte AWS-interne Kommunikation                              | DS19 [P2]                                                                                                               | E | H | 4 | DS19 [P2]                                                                                               | E | SG | 2 |
| R89: T40 Abhören von HTTP zwischen CC-Backend und Kunden-/Flottenmanagement, vorbereitet durch P3ed Unbefugter physischer Zugang zum Control Center (Abhören des Datenflusses) | C22 Verschlüsselte und authentifizierte AWS-interne Kommunikation                              | DS19 [P2]                                                                                                               | E | H | 4 | DS19 [P2]                                                                                               | E | SG | 2 |
| R90: T40 Abhören von HTTP zwischen CC-Backend und Kunden-/Flottenmanagement Vorbereitung durch P9 Ausnutzen von Software-Schwachstellen des Kunden-/Flottenmanagements         | A13 Angriffe auf das Kunden-/Flottenmanagement fallen nicht in den Umfang dieser Risikoanalyse | DS19 [P2]                                                                                                               | E | H | 2 | DS19 [P2]                                                                                               | E | H  | 2 |
| R91: T41 Störung von HTTP zwischen CC-Backend und Kunden-/Flottenmanagement, vorbereitet durch P1dd Unbefugter physischer Zugriff auf AWS Cloud (Störung des Datenflusses)     | A12 AWS schützt die Verfügbarkeit der Cloud-Infrastruktur                                      | DS9 [O3]                                                                                                                | S | H | 2 | DS9 [O3]                                                                                                | S | H  | 2 |
| R92: T41 Unterbrechung des HTTP-Verkehrs zwischen CC-Backend und Kunden-/Flottenmanagement,                                                                                    | A12 AWS schützt die Verfügbarkeit der Cloud-Infrastruktur                                      | DS9 [O3]                                                                                                                | S | H | 2 | DS9 [O3]                                                                                                | S | H  | 2 |

|                                                                                                                                                                                                   |                                                                                                |                        |   |   |   |                        |   |    |   |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------|------------------------|---|---|---|------------------------|---|----|---|
| vorbereitet durch P3dd Unbefugter physischer Zugang zum Control Center (Unterbrechung des Datenflusses)                                                                                           |                                                                                                |                        |   |   |   |                        |   |    |   |
| R93: T41 Unterbrechung der HTTP-Verbindung zwischen CC-Backend und Kunden-/Flottenmanagement, vorbereitet durch P9 Ausnutzen von Software-Schwachstellen des Kunden-/Flottenmanagements           | A13 Angriffe auf das Kunden-/Flottenmanagement fallen nicht in den Umfang dieser Risikoanalyse | DS9 [O3]               | S | H | 2 | DS9 [O3]               | S | H  | 2 |
| R94: T42 Spoofing/Manipulation von HTTP zwischen CC-Backend und Kunden-/Flottenmanagement, vorbereitet durch P1md Unbefugter physischer Zugriff auf die AWS Cloud (Manipulation des Datenflusses) | C22 Verschlüsselte und authentifizierte AWS-interne Kommunikation                              | DS9 [O3], DS15 [F2OEM] | S | H | 5 | DS9 [O3], DS15 [F2OEM] | S | SG | 2 |
| R95: T42 Spoofing/Manipulation auf HTTP zwischen CC-Backend und Kunden-/Flottenmanagement, vorbereitet durch P3md Unbefugter physischer Zugang zum Control Center (Manipulation des Datenflusses) | C22 Verschlüsselte und authentifizierte AWS-interne Kommunikation                              | DS9 [O3], DS15 [F2OEM] | S | H | 5 | DS9 [O3], DS15 [F2OEM] | S | SG | 2 |
| R96: T42 Spoofing/Manipulation auf HTTP zwischen CC-Backend und Kunden-/Flottenmanagement Vorbereitung durch P9 Ausnutzung von Software-Schwachstellen des Kunden-/Flottenmanagements             | A13 Angriffe auf das Kunden-/Flottenmanagement fallen nicht in den Umfang dieser Risikoanalyse | DS9 [O3], DS15 [F2OEM] | S | H | 2 | DS9 [O3], DS15 [F2OEM] | S | H  | 2 |
| R97: T43 Abhören von HTTP zwischen CC-Backend und externen Partnern, vorbereitet durch P1ed Unbefugter physischer Zugriff auf die AWS Cloud (Abhören des Datenflusses)                            | C22 Verschlüsselte und authentifizierte AWS-interne Kommunikation                              | DS16 [F2OEM]           | E | H | 4 | DS16 [F2OEM]           | E | SG | 2 |
| R98: T43 Abhören von HTTP zwischen CC-Backend und externen Partnern, vorbereitet durch P3ed Unbefugter physischer Zugang zum Control Center (Abhören des Datenflusses)                            | C22 Verschlüsselte und authentifizierte AWS-interne Kommunikation                              | DS16 [F2OEM]           | E | H | 4 | DS16 [F2OEM]           | E | SG | 2 |

|                                                                                                                                                                                            |                                                                                  |                               |   |   |   |                               |   |    |   |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------|-------------------------------|---|---|---|-------------------------------|---|----|---|
| R99: T43 Abhören von HTTP zwischen CC-Backend und externen Partnern Vorbereitung durch P10 Ausnutzen von Software-Schwachstellen externer Partner                                          | A14 Angriffe auf externe Partner fallen nicht in den Umfang dieser Risikoanalyse | DS16 [F2OEM]                  | E | H | 2 | DS16 [F2OEM]                  | E | H  | 2 |
| R100: T44 Störung von HTTP zwischen CC-Backend und externen Partnern Vorbereitung durch P1dd Unbefugter physischer Zugriff auf AWS Cloud (Störung des Datenflusses)                        | A12 AWS schützt die Verfügbarkeit der Cloud-Infrastruktur                        | DS8 [O1], DS9 [O3], DS21 [O3] | S | H | 2 | DS8 [O1], DS9 [O3], DS21 [O3] | S | H  | 2 |
| R101: T44 Störung des HTTP-Verkehrs zwischen CC-Backend und externen Partnern, vorbereitet von P3dd Unbefugter physischer Zugang zum Control Center (Störung des Datenflusses)             | A12 AWS schützt die Verfügbarkeit der Cloud-Infrastruktur                        | DS8 [O1], DS9 [O3], DS21 [O3] | S | H | 2 | DS8 [O1], DS9 [O3], DS21 [O3] | S | H  | 2 |
| R102: T44 Störung des HTTP-Verkehrs zwischen CC-Backend und externen Partnern, vorbereitet durch P10 Ausnutzung von Software-Schwachstellen externer Partner                               | A14 Angriffe auf externe Partner fallen nicht in den Umfang dieser Risikoanalyse | DS8 [O1], DS9 [O3], DS21 [O3] | S | H | 2 | DS8 [O1], DS9 [O3], DS21 [O3] | S | H  | 2 |
| R103: T45 Spoofing/Manipulation von HTTP zwischen CC-Backend und externen Partnern, vorbereitet durch P1md Unbefugter physischer Zugriff auf die AWS Cloud (Manipulation des Datenflusses) | C22 Verschlüsselte und authentifizierte AWS-interne Kommunikation                | DS8 [O1], DS9 [O3], DS21 [O3] | S | H | 5 | DS8 [O1], DS9 [O3], DS21 [O3] | S | SG | 2 |
| R104: T45 Spoofing/Manipulation auf HTTP zwischen CC-Backend und externen Partnern, vorbereitet durch P3md Unbefugter physischer Zugang zum Control Center (Manipulation des Datenflusses) | C22 Verschlüsselte und authentifizierte AWS-interne Kommunikation                | DS8 [O1], DS9 [O3], DS21 [O3] | S | H | 5 | DS8 [O1], DS9 [O3], DS21 [O3] | S | SG | 2 |
| R105: T45 Spoofing/Manipulation auf HTTP zwischen CC-Backend und externen Partnern, vorbereitet durch P10 Ausnutzen von Software-Schwachstellen externer Partner                           | A14 Angriffe auf externe Partner fallen nicht in den Umfang dieser Risikoanalyse | DS8 [O1], DS9 [O3], DS21 [O3] | S | H | 2 | DS8 [O1], DS9 [O3], DS21 [O3] | S | H  | 2 |

|                                                                                                                                                                                                         |                                                                                                                                                                          |                                                                                                                                                                                               |   |   |   |                                                                                                                                                                                  |   |    |   |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|---|---|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|----|---|
| R106: T46 Abhören von HTTP zwischen CC-Backend und dynamischer Routenverwaltung, vorbereitet durch P1ed Unbefugter physischer Zugriff auf die AWS Cloud (Abhören des Datenflusses)                      | C22 Verschlüsselte und authentifizierte AWS-interne Kommunikation                                                                                                        | DS16 [F2OEM]                                                                                                                                                                                  | E | H | 4 | DS16 [F2OEM]                                                                                                                                                                     | E | SG | 2 |
| R107: T46 Abhören von HTTP zwischen CC-Backend und dynamischer Routenverwaltung, vorbereitet durch P3ed Unbefugter physischer Zugang zum Control Center (Abhören des Datenflusses)                      | C22 Verschlüsselte und authentifizierte AWS-interne Kommunikation                                                                                                        | DS16 [F2OEM]                                                                                                                                                                                  | E | H | 4 | DS16 [F2OEM]                                                                                                                                                                     | E | SG | 2 |
| R108: T46 Abhören von HTTP zwischen CC-Backend und dynamischer Routenverwaltung Vorbereitung durch P11 Ausnutzen von Software-Schwachstellen der dynamischen Routenverwaltung                           | A15 Angriffe auf das dynamische Routenmanagement fallen nicht in den Umfang dieser Risikoanalyse                                                                         | DS16 [F2OEM]                                                                                                                                                                                  | E | H | 2 | DS16 [F2OEM]                                                                                                                                                                     | E | H  | 2 |
| R109: T47 Störung von HTTP zwischen CC-Backend und dynamischer Routenverwaltung, vorbereitet durch P1dd Unbefugter physischer Zugriff auf die AWS Cloud (Störung des Datenflusses)                      | C5A Eigensicherheit des Lkw (gegen Störungen)<br>A10 Durch CC ausgelöste MRM sind nicht sicherheitskritisch<br>A12 AWS schützt die Verfügbarkeit der Cloud-Infrastruktur | DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS13s [S3], DS17 [O0], DS21 [O3], DS13f [F3OEM]<br>DS6<br>DS8 [O1], DS9 [O3], DS10 [F1OEM], DS13s [S3], DS17 [O0], DS21 [O3], DS13f [F3OEM] | S | H | 2 | DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS13s [S3], DS17 [O0], DS21 [O3], DS13f [F3OEM]<br>DS13s, DS13f, DS6<br>DS8 [O1], DS9 [O3], DS10 [F1OEM], DS17 [O0], DS21 [O3] | S | H  | 2 |
| R110: T47 Unterbrechung des HTTP-Verkehrs zwischen CC-Backend und dynamischer Routenverwaltung, vorbereitet durch P3dd Unbefugter physischer Zugang zum Control Center (Unterbrechung des Datenflusses) | C5A Eigensicherheit des Lkw (gegen Störungen)<br>A10 Durch CC ausgelöste MRM                                                                                             | DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS13s [S3], DS17 [O0], DS21 [O3],                                                                                                           | S | H | 2 | DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS13s [S3], DS17 [O0], DS21 [O3],                                                                                              | S | H  | 2 |

|                                                                                                                                                                                                     |                                                                                                                                                                                                                                    |                                                                                                                                                                                                                                      |   |   |   |                                                                                                                                                                                                                      |   |    |   |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|---|---|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|----|---|
|                                                                                                                                                                                                     | sind nicht sicherheitskritisch<br>A12 AWS schützt die Verfügbarkeit der Cloud-Infrastruktur                                                                                                                                        | DS13f [F3OEM]<br>_____<br>DS6<br>_____<br>DS8 [O1], DS9 [O3],<br>DS10 [F1OEM], DS13s<br>[S3], DS17 [O0], DS21<br>[O3], DS13f [F3OEM]                                                                                                 |   |   |   | DS13f [F3OEM]<br>_____<br>DS13s, DS13f, DS6<br>_____<br>DS8 [O1], DS9 [O3],<br>DS10 [F1OEM], DS17<br>[O0], DS21 [O3]                                                                                                 |   |    |   |
| R111: T47 Störung des HTTP-Verkehrs zwischen CC-Backend und dynamischer Routenverwaltung, vorbereitet durch P11 Ausnutzung von Software-Schwachstellen der dynamischen Routenverwaltung             | C5A Intrinsische Sicherheit des Lkw (gegen Störungen)<br>_____<br>A10 Durch CC ausgelöste MRM sind nicht sicherheitskritisch.<br>A15 Angriffe auf das dynamische Routenmanagement fallen nicht in den Umfang dieser Risikoanalyse. | DS6 [S3 F2OEM], DS8<br>[O1], DS9 [O3], DS10<br>[F1OEM], DS13s [S3],<br>DS17 [O0], DS21 [O3],<br>DS13f [F3OEM]<br>_____<br>DS6<br>_____<br>DS8 [O1], DS9 [O3],<br>DS10 [F1OEM], DS13s<br>[S3], DS17 [O0], DS21<br>[O3], DS13f [F3OEM] | S | H | 2 | DS6 [S3 F2OEM], DS8<br>[O1], DS9 [O3], DS10<br>[F1OEM], DS13s [S3],<br>DS17 [O0], DS21 [O3],<br>DS13f [F3OEM]<br>_____<br>DS13s, DS13f, DS6<br>_____<br>DS8 [O1], DS9 [O3],<br>DS10 [F1OEM], DS17<br>[O0], DS21 [O3] | S | H  | 2 |
| R112: T48 Spoofing/Manipulation von HTTP zwischen CC-Backend und dynamischer Routenverwaltung, vorbereitet von P1md Unbefugter physischer Zugriff auf die AWS Cloud (Manipulation des Datenflusses) | C5I Eigensicherheit des Trucks (gegen Spoofing/Manipulation)<br>C20 ADS-Sicherheitsvalidierungen nach Entscheidungen des Control Centers<br>C22 Verschlüsselte und authentifizierte AWS-interne Kommunikation<br>_____             | DS6 [S3 F2OEM], DS8<br>[O1], DS9 [O3], DS10<br>[F1OEM], DS12<br>[S3 F2OEM], DS13s<br>[S3], DS15 [F2OEM],<br>DS17 [O0], DS21 [O3],<br>DS13f [F3OEM]<br>_____<br>DS6                                                                   | S | H | 5 | DS6 [S3 F2OEM], DS8<br>[O1], DS9 [O3], DS10<br>[F1OEM], DS12<br>[S3 F2OEM], DS13s<br>[S3], DS15 [F2OEM],<br>DS17 [O0], DS21 [O3],<br>DS13f [F3OEM]<br>_____<br>DS13s, DS12, DS6                                      | S | SG | 2 |

|                                                                                                                                                                                                     |                                                                                                                                                                                                                                                                                 |                                                                                                                                                                                                                                                                     |   |   |   |                                                                                                                                                                                                                                                     |   |    |   |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|---|---|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|----|---|
|                                                                                                                                                                                                     | A10 Durch CC ausgelöste MRM sind nicht sicherheitskritisch                                                                                                                                                                                                                      | DS8 [O1], DS9 [O3], DS10 [F1OEM], DS12 [S3 F2OEM], DS13s [S3], DS15 [F2OEM], DS17 [O0], DS21 [O3], DS13f [F3OEM]                                                                                                                                                    |   |   |   | DS8 [O1], DS9 [O3], DS10 [F1OEM], DS15 [F2OEM], DS17 [O0], DS21 [O3], DS13f [F3OEM]                                                                                                                                                                 |   |    |   |
| R113: T48 Spoofing/Manipulation auf HTTP zwischen CC-Backend und dynamischer Routenverwaltung, vorbereitet von P3md Unbefugter physischer Zugang zum Control Center (Manipulation des Datenflusses) | C5I Eigensicherheit des Trucks (gegen Spoofing/Manipulation)<br>C20 ADS-Sicherheitsvalidierungen nach Entscheidungen des Control Centers<br>C22 Verschlüsselte und authentifizierte AWS-interne Kommunikation<br><br>A10 Durch CC ausgelöste MRM sind nicht sicherheitskritisch | DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS12 [S3 F2OEM], DS13s [S3], DS15 [F2OEM], DS17 [O0], DS21 [O3], DS13f [F3OEM]<br><br>DS6<br><br>DS8 [O1], DS9 [O3], DS10 [F1OEM], DS12 [S3 F2OEM], DS13s [S3], DS15 [F2OEM], DS17 [O0], DS21 [O3], DS13f [F3OEM] | S | H | 5 | DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS12 [S3 F2OEM], DS13s [S3], DS15 [F2OEM], DS17 [O0], DS21 [O3], DS13f [F3OEM]<br><br>DS13s, DS12, DS6<br><br>DS8 [O1], DS9 [O3], DS10 [F1OEM], DS15 [F2OEM], DS17 [O0], DS21 [O3], DS13f [F3OEM] | S | SG | 2 |
| R114: T48 Spoofing/Manipulation auf HTTP zwischen CC-Backend und dynamischer Routenverwaltung Vorbereitung durch P11 Ausnutzung von Software-Schwachstellen der dynamischen Routenverwaltung        | C5I Intrinsische Sicherheit des Lkw (gegen Spoofing/Manipulation)<br>C20 ADS-Sicherheitsvalidierungen nach Entscheidungen des Control Centers                                                                                                                                   | DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS12 [S3 F2OEM], DS13s [S3], DS15 [F2OEM], DS17 [O0], DS21 [O3],                                                                                                                                                  | S | H | 2 | DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS12 [S3 F2OEM], DS13s [S3], DS15 [F2OEM], DS17 [O0], DS21 [O3],                                                                                                                                  | S | H  | 2 |



|                                                                                                                                                                          |                                                                                                                                                                                                                                                               |                                                                                                                                                         |  |   |   |                                                                                                                                         |  |    |   |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|--|---|---|-----------------------------------------------------------------------------------------------------------------------------------------|--|----|---|
|                                                                                                                                                                          | <p>A10 Durch das Control Center ausgelöste MRM sind nicht sicherheitskritisch.</p> <p>A15 Angriffe auf das dynamische Routenmanagement fallen nicht in den Geltungsbereich dieser Risikoanalyse.</p>                                                          | <p>DS13f [F3OEM]</p> <p>DS6</p> <p>DS8 [O1], DS9 [O3], DS10 [F1OEM], DS12 [S3 F2OEM], DS13s [S3], DS15 [F2OEM], DS17 [O0], DS21 [O3], DS13f [F3OEM]</p> |  |   |   | <p>DS13f [F3OEM]</p> <p>DS13s, DS12, DS6</p> <p>DS8 [O1], DS9 [O3], DS10 [F1OEM], DS15 [F2OEM], DS17 [O0], DS21 [O3], DS13f [F3OEM]</p> |  |    |   |
| R115: T49 Abhören von HTTP zwischen API-Gateway und externen Partnern Vorbereitung durch P1ed Unbefugter physischer Zugriff auf die AWS Cloud (Abhören des Datenflusses) | C22 Verschlüsselte und authentifizierte AWS-interne Kommunikation                                                                                                                                                                                             |                                                                                                                                                         |  | H | 1 |                                                                                                                                         |  | SG | 1 |
| R116: T49 Abhören von HTTP zwischen API-Gateway und externen Partnern, vorbereitet von P3ed Unbefugter physischer Zugang zum Control Center (Abhören des Datenflusses)   | C22 Verschlüsselte und authentifizierte AWS-interne Kommunikation                                                                                                                                                                                             |                                                                                                                                                         |  | H | 1 |                                                                                                                                         |  | SG | 1 |
| R117: T49 Abhören von HTTP zwischen API-Gateway und externen Partnern, vorbereitet von P7e Ausnutzen von Software-Schwachstellen des API-Gateways (Abhören)              | <p>C18 Absicherung von Komponenten mit Internetanschluss gegen Software-Schwachstellen</p> <p>C27 End-to-End-verschlüsselte Übertragung sensibler Daten zwischen technischen Überwachungsgeräten, Lkw, externen Partnern und dynamischem Routenmanagement</p> |                                                                                                                                                         |  | H | 1 |                                                                                                                                         |  | SG | 1 |

|                                                                                                                                                                                             |                                                                                                                                 |          |   |   |   |          |   |    |   |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------|----------|---|---|---|----------|---|----|---|
| R118: T49 Abhören von HTTP zwischen API-Gateway und externen Partnern, vorbereitet von P10 Ausnutzen von Software-Schwachstellen externer Partner                                           | A14 Angriffe auf externe Partner fallen nicht in den Umfang dieser Risikoanalyse                                                |          |   | H | 1 |          |   | H  | 1 |
| R119: T50 Störung von HTTP zwischen API-Gateway und externen Partnern Vorbereitung durch P1dd Unbefugter physischer Zugriff auf AWS Cloud (Störung des Datenflusses)                        | A12 AWS schützt die Verfügbarkeit der Cloud-Infrastruktur                                                                       | DS8 [O1] | M | H | 2 | DS8 [O1] | M | H  | 2 |
| R120: T50 Unterbrechung des HTTP-Verkehrs zwischen API-Gateway und externen Partnern, vorbereitet von P3dd Unbefugter physischer Zugang zum Control Center (Unterbrechung des Datenflusses) | A12 AWS schützt die Verfügbarkeit der Cloud-Infrastruktur                                                                       | DS8 [O1] | M | H | 2 | DS8 [O1] | M | H  | 2 |
| R121: T50 Unterbrechung des HTTP-Verkehrs zwischen API-Gateway und externen Partnern, vorbereitet von P7d Ausnutzen von Software-Schwachstellen des API-Gateways (Unterbrechung)            | C18 Absicherung von Komponenten mit Internetverbindung gegen Software-Schwachstellen<br>C29 Resilienz/Sicherheit durch Vielfalt | DS8 [O1] | M | H | 3 | DS8 [O1] | M | SG | 1 |
| R122: T50 Unterbrechung von HTTP zwischen API-Gateway und externen Partnern, vorbereitet durch P10 Ausnutzung von Software-Schwachstellen externer Partner                                  | A14 Angriffe auf externe Partner fallen nicht in den Umfang dieser Risikoanalyse                                                | DS8 [O1] | M | H | 2 | DS8 [O1] | M | H  | 2 |
| R123: T51 Spoofing/Manipulation von HTTP zwischen API-Gateway und externen Partnern, vorbereitet durch P1md Unbefugter physischer Zugriff auf die AWS Cloud (Manipulation des Datenflusses) | C22 Verschlüsselte und authentifizierte AWS-interne Kommunikation                                                               | DS8 [O1] | M | H | 3 | DS8 [O1] | M | SG | 1 |
| R124: T51 Spoofing/Manipulation auf HTTP zwischen API-Gateway und externen Partnern, vorbereitet von                                                                                        | C22 Verschlüsselte und authentifizierte AWS-interne Kommunikation                                                               | DS8 [O1] | M | H | 3 | DS8 [O1] | M | SG | 1 |

|                                                                                                                                                                                     |                                                                                                                                                                                                                                                                    |          |   |   |   |          |   |    |   |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|---|---|---|----------|---|----|---|
| P3md Unbefugter physischer Zugang zum Control Center (Manipulation des Datenflusses)                                                                                                |                                                                                                                                                                                                                                                                    |          |   |   |   |          |   |    |   |
| R125: T51 Spoofing/Manipulation auf HTTP zwischen API-Gateway und externen Partnern, vorbereitet durch P7m Ausnutzung von Software-Schwachstellen des API-Gateways (Manipulation)   | C18 Absicherung von Komponenten mit Internetanbindung gegen Software-Schwachstellen<br>C28 Durchgängige authentische Datenübertragung zwischen technischer Überwachungsausrüstung, Lkw, Kunden-/Flottenmanagement, externen Partnern, dynamischem Routenmanagement | DS8 [O1] | M | H | 3 | DS8 [O1] | M | SG | 1 |
| R126: T51 Spoofing/Manipulation auf HTTP zwischen API-Gateway und externen Partnern, vorbereitet durch P10 Ausnutzung von Software-Schwachstellen externer Partner                  | A14 Angriffe auf externe Partner fallen nicht in den Umfang dieser Risikoanalyse                                                                                                                                                                                   | DS8 [O1] | M | H | 2 | DS8 [O1] | M | H  | 2 |
| R127: T52 Abhören von HTTP zwischen API-Gateway und dynamischer Routenverwaltung, vorbereitet durch P1ed Unbefugter physischer Zugriff auf die AWS Cloud (Abhören des Datenflusses) | C22 Verschlüsselte und authentifizierte AWS-interne Kommunikation                                                                                                                                                                                                  |          |   | H | 1 |          |   | SG | 1 |
| R128: T52 Abhören von HTTP zwischen API-Gateway und dynamischer Routenverwaltung, vorbereitet von P3ed Unbefugter physischer Zugang zum Control Center (Abhören des Datenflusses)   | C22 Verschlüsselte und authentifizierte AWS-interne Kommunikation                                                                                                                                                                                                  |          |   | H | 1 |          |   | SG | 1 |
| R129: T52 Abhören von HTTP zwischen API-Gateway und dynamischer Routenverwaltung, vorbereitet von                                                                                   | C18 Absicherung von Komponenten mit Internetanschluss gegen Software-                                                                                                                                                                                              |          |   | H | 1 |          |   | SG | 1 |

|                                                                                                                                                                                                        |                                                                                                                                                                               |                           |   |   |   |                                           |  |    |   |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------|---|---|---|-------------------------------------------|--|----|---|
| P7e Ausnutzen von Software-Schwachstellen des API-Gateways (Abhören)                                                                                                                                   | Schwachstellen<br>C27 End-to-End-verschlüsselte Übertragung sensibler Daten zwischen technischen Überwachungsgeräten, Lkw, externen Partnern und dynamischem Routenmanagement |                           |   |   |   |                                           |  |    |   |
| R130: T52 Abhören von HTTP zwischen API-Gateway und dynamischer Routenverwaltung, vorbereitet von P11 Ausnutzen von Software-Schwachstellen der dynamischen Routenverwaltung                           | A15 Angriffe auf das dynamische Routenmanagement fallen nicht in den Umfang dieser Risikoanalyse                                                                              |                           |   | H | 1 |                                           |  | H  | 1 |
| R131: T53 Störung von HTTP zwischen API-Gateway und dynamischer Routenverwaltung, vorbereitet durch P1dd Unbefugter physischer Zugriff auf AWS Cloud (Störung des Datenflusses)                        | C5A Eigensicherheit des Trucks (gegen Störungen)<br>A12 AWS schützt die Verfügbarkeit der Cloud-Infrastruktur                                                                 | DS13s [S3], DS13f [F3OEM] | S | H | 2 | DS13s [S3], DS13f [F3OEM]<br>DS13s, DS13f |  | H  | 1 |
| R132: T53 Unterbrechung des HTTP-Verkehrs zwischen API-Gateway und dynamischer Routenverwaltung, vorbereitet von P3dd Unbefugter physischer Zugang zum Control Center (Unterbrechung des Datenflusses) | C5A Eigensicherheit des Trucks (gegen Störungen)<br>A12 AWS schützt die Verfügbarkeit der Cloud-Infrastruktur                                                                 | DS13s [S3], DS13f [F3OEM] | S | H | 2 | DS13s [S3], DS13f [F3OEM]<br>DS13s, DS13f |  | H  | 1 |
| R133: T53 Unterbrechung des HTTP-Verkehrs zwischen API Gateway und dynamischer Routenverwaltung, vorbereitet durch P7d Ausnutzen von Software-Schwachstellen des API Gateway (Unterbrechung)           | C5A Eigensicherheit des Lkw (gegen Störungen)<br>C18 Absicherung von Komponenten mit Internetanbindung gegen Software-Schwachstellen                                          | DS13s [S3], DS13f [F3OEM] | S | H | 5 | DS13s [S3], DS13f [F3OEM]<br>DS13s, DS13f |  | SG | 1 |

|                                                                                                                                                                                                        |                                                                                                                                                       |                                     |   |   |   |                                                                                 |   |    |   |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------|---|---|---|---------------------------------------------------------------------------------|---|----|---|
|                                                                                                                                                                                                        | C29 Resilienz/Sicherheit durch Vielfalt                                                                                                               |                                     |   |   |   |                                                                                 |   |    |   |
| R134: T53 Störung des HTTP zwischen API-Gateway und dynamischer Routenverwaltung, vorbereitet durch P11 Ausnutzung von Software-Schwachstellen der dynamischen Routenverwaltung                        | C5A Eigensicherheit des Lkw (gegen Störungen)<br><br>A15 Angriffe auf das dynamische Routenmanagement fallen nicht in den Umfang dieser Risikoanalyse | DS13s [S3], DS13f [F3OEM]           | S | H | 2 | DS13s [S3], DS13f [F3OEM]<br><br>DS13s, DS13f                                   |   | H  | 1 |
| R135: T54 Spoofing/Manipulation von HTTP zwischen API-Gateway und dynamischer Routenverwaltung, vorbereitet durch P1md Unbefugter physischer Zugriff auf die AWS Cloud (Manipulation des Datenflusses) | C5I Intrinsische Sicherheit des Lkw (gegen Spoofing/Manipulation)<br><br>C22 Verschlüsselte und authentifizierte AWS-interne Kommunikation            | DS9 [O3], DS13s [S3], DS13f [F3OEM] | S | H | 5 | DS9 [O3], DS13s [S3], DS13f [F3OEM]<br><br>DS13s<br><br>DS9 [O3], DS13f [F3OEM] | S | SG | 2 |
| R136: T54 Spoofing/Manipulation auf HTTP zwischen API-Gateway und dynamischer Routenverwaltung, vorbereitet durch P3md Unbefugter physischer Zugang zum Control Center (Manipulation des Datenflusses) | C5I Intrinsische Sicherheit des Lkw (gegen Spoofing/Manipulation)<br><br>C22 Verschlüsselte und authentifizierte AWS-interne Kommunikation            | DS9 [O3], DS13s [S3], DS13f [F3OEM] | S | H | 5 | DS9 [O3], DS13s [S3], DS13f [F3OEM]<br><br>DS13s<br><br>DS9 [O3], DS13f [F3OEM] | S | SG | 2 |
| R137: T54 Spoofing/Manipulation auf HTTP zwischen API-Gateway und dynamischer Routenverwaltung, vorbereitet durch P7m Ausnutzen von Software-Schwachstellen des API-Gateways (Manipulation)            | C5I Intrinsische Sicherheit des Lkw (gegen Spoofing/Manipulation)<br><br>C18 Absicherung von Komponenten mit Internetanbindung                        | DS9 [O3], DS13s [S3], DS13f [F3OEM] | S | H | 5 | DS9 [O3], DS13s [S3], DS13f [F3OEM]<br><br>DS13s                                | S | SG | 2 |

|                                                                                                                                                                                                |                                                                                                                                                                                                                     |                                                                                                             |   |   |   |                                                                                                                                    |   |   |   |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------|---|---|---|------------------------------------------------------------------------------------------------------------------------------------|---|---|---|
|                                                                                                                                                                                                | gegen Software-Schwachstellen<br>C28 End-to-End-Authentifizierung der Datenübertragung zwischen technischer Überwachungsausrüstung, Lkw, Kunden-/Flottenmanagement, externen Partnern, dynamischem Routenmanagement |                                                                                                             |   |   |   | DS9 [O3], DS13f [F3OEM]                                                                                                            |   |   |   |
| R138: T54 Spoofing/Manipulation auf HTTP zwischen API-Gateway und dynamischem Routenmanagement, vorbereitet durch P11 Ausnutzung von Software-Schwachstellen des dynamischen Routenmanagements | C51 Intrinsische Sicherheit des Trucks (gegen Spoofing/Manipulation)<br><br>A15 Angriffe auf das dynamische Routenmanagement fallen nicht in den Umfang dieser Risikoanalyse                                        | DS9 [O3], DS13s [S3], DS13f [F3OEM]                                                                         | S | H | 2 | DS9 [O3], DS13s [S3], DS13f [F3OEM]<br><br>DS13s<br><br>DS9 [O3], DS13f [F3OEM]                                                    | S | H | 2 |
| R139: T55 Extrahieren von Daten aus dem CC-Backend Vorbereitung durch P3ecs Unbefugter physischer Zugang zum Control Center (Extrahieren von Komponenten, die sensible Daten speichern)        | C31 Verschlüsselte Speicherung sensibler Lkw- und Kundendaten<br>C32 Schutz vor Piraterie und Reverse Engineering zur Verhinderung der Offenlegung von geistigem Eigentum                                           | DS1 [P2], DS4 Verlust von geistigem Eigentum des Codes des Control Centers [F2OEM], DS16 [F2OEM], DS19 [P2] | E | H | 4 | DS1 [P2], DS4 Verlust von geistigem Eigentum des Control Center-Codes [F2OEM], DS16 [F2OEM], DS19 [P2]<br><br>DS1, DS16, DS19, DS4 |   | H | 1 |
| R140: T56 Denial-of-Service-Angriff auf CC-Backend, vorbereitet durch P3dc Unbefugter physischer Zugang zum Control Center (Störung von Komponenten)                                           | C5A Eigensicherheit des Lkw (gegen Störungen)<br><br>A10 Durch CC ausgelöste MRM                                                                                                                                    | DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS13s [S3], DS17 [O0], DS21 [O3],                         | S | H | 2 | DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS13s [S3], DS17 [O0], DS21 [O3],                                                | S | H | 2 |

|                                                                                                                                                                        |                                                                                                                                                                                                                                                                |                                                                                                                                                                                                                 |   |   |   |                                                                                                                                                                                                    |   |    |   |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|---|---|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|----|---|
|                                                                                                                                                                        | sind nicht sicherheitskritisch<br>A12 AWS schützt die Verfügbarkeit der Cloud-Infrastruktur                                                                                                                                                                    | DS13f [F3OEM]<br>_____<br>DS6<br>_____<br>DS8 [O1], DS9 [O3],<br>DS10 [F1OEM], DS13s<br>[S3], DS17 [O0], DS21<br>[O3], DS13f [F3OEM]                                                                            |   |   |   | DS13f [F3OEM]<br>_____<br>DS13s, DS13f, DS6<br>_____<br>DS8 [O1], DS9 [O3],<br>DS10 [F1OEM], DS17<br>[O0], DS21 [O3]                                                                               |   |    |   |
| R141: T56 Denial-of-Service-Angriff auf CC-Backend, vorbereitet von P4d Ausnutzen von Software-Schwachstellen des Vehicle Adapter Service (Störung)                    | C5A Intrinsische Sicherheit des Lkw (gegen Störungen)<br>C18 Absicherung von Komponenten mit Internetanbindung gegen Software-Schwachstellen<br>C29 Resilienz/Sicherheit durch Vielfalt<br>_____<br>A10 Durch CC ausgelöste MRM sind nicht sicherheitskritisch | DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS13s [S3], DS17 [O0], DS21 [O3], DS13f [F3OEM]<br>_____<br>DS6<br>_____<br>DS8 [O1], DS9 [O3], DS10 [F1OEM], DS13s [S3], DS17 [O0], DS21 [O3], DS13f [F3OEM] | S | H | 5 | DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS13s [S3], DS17 [O0], DS21 [O3], DS13f [F3OEM]<br>_____<br>DS13s, DS13f, DS6<br>_____<br>DS8 [O1], DS9 [O3], DS10 [F1OEM], DS17 [O0], DS21 [O3] | S | SG | 2 |
| R142: T56 Denial-of-Service-Angriff auf CC-Backend, vorbereitet durch P6d Ausnutzen von Software-Schwachstellen des Control Center-Backends für das Frontend (Störung) | C5A Intrinsische Sicherheit des Lkw (gegen Störungen)<br>C18 Absicherung von Komponenten mit Internetanbindung gegen Software-Schwachstellen<br>C29 Resilienz/Sicherheit durch Vielfalt<br>_____                                                               | DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS13s [S3], DS17 [O0], DS21 [O3], DS13f [F3OEM]<br>_____<br>DS6<br>_____<br>DS8 [O1], DS9 [O3],                                                               | S | H | 5 | DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS13s [S3], DS17 [O0], DS21 [O3], DS13f [F3OEM]<br>_____<br>DS13s, DS13f, DS6<br>_____<br>DS8 [O1], DS9 [O3],                                    | S | SG | 2 |

|                                                                                                                                                                                   |                                                                                                                                                                                                                                                                                      |                                                                                                                                                                                                                                        |   |   |   |                                                                                                                                                                                                                                   |   |    |   |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|---|---|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|----|---|
|                                                                                                                                                                                   | A10 Durch CC ausgelöste MRM sind nicht sicherheitskritisch                                                                                                                                                                                                                           | DS10 [F1OEM], DS13s [S3], DS17 [O0], DS21 [O3], DS13f [F3OEM]                                                                                                                                                                          |   |   |   | DS10 [F1OEM], DS17 [O0], DS21 [O3]                                                                                                                                                                                                |   |    |   |
| R143: T56 Denial-of-Service-Angriff auf CC-Backend, vorbereitet durch P7d Ausnutzen von Software-Schwachstellen des API-Gateways (Störung)                                        | <p>C5A Intrinsische Sicherheit des Lkw (gegen Störungen)</p> <p>C18 Absicherung von Komponenten mit Internetanbindung gegen Software-Schwachstellen</p> <p>C29 Resilienz/Sicherheit durch Vielfalt</p> <p>A10 Durch CC ausgelöste MRM sind nicht sicherheitskritisch</p>             | <p>DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS13s [S3], DS17 [O0], DS21 [O3], DS13f [F3OEM]</p> <p>DS6</p> <p>DS8 [O1], DS9 [O3], DS10 [F1OEM], DS13s [S3], DS17 [O0], DS21 [O3], DS13f [F3OEM]</p>                           | S | H | 5 | <p>DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS13s [S3], DS17 [O0], DS21 [O3], DS13f [F3OEM]</p> <p>DS13s, DS13f, DS6</p> <p>DS8 [O1], DS9 [O3], DS10 [F1OEM], DS17 [O0], DS21 [O3]</p>                                   | S | SG | 2 |
| R144: T57 Manipulation von Daten, Parametern oder Software des CC-Backends Vorbereitung durch P3mc Unbefugter physischer Zugang zum Control Center (Manipulation von Komponenten) | <p>C5I Intrinsische Sicherheit des Trucks (gegen Spoofing/Manipulation)</p> <p>C20 ADS-Sicherheitsvalidierungen nach Entscheidungen des Control Centers</p> <p>C30 Befolgung der AWS-Sicherheitsbest Practices</p> <p>A10 Durch CC ausgelöste MRM sind nicht sicherheitskritisch</p> | <p>DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS12 [S3 F2OEM], DS13s [S3], DS15 [F2OEM], DS17 [O0], DS21 [O3], DS13f [F3OEM]</p> <p>DS6</p> <p>DS8 [O1], DS9 [O3], DS10 [F1OEM], DS12 [S3 F2OEM], DS13s [S3], DS15 [F2OEM],</p> | S | H | 5 | <p>DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS12 [S3 F2OEM], DS13s [S3], DS15 [F2OEM], DS17 [O0], DS21 [O3], DS13f [F3OEM]</p> <p>DS13s, DS12, DS6</p> <p>DS8 [O1], DS9 [O3], DS10 [F1OEM], DS15 [F2OEM], DS17 [O0],</p> | S | SG | 2 |



|                                                                                                                                                                                  |                                                                                                                                                                                                                                                    |                                                                                                                                                                                                                                      |   |   |   |                                                                                                                                                                                                                      |   |    |   |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|---|---|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|----|---|
|                                                                                                                                                                                  |                                                                                                                                                                                                                                                    | DS17 [O0], DS21 [O3],<br>DS13f [F3OEM]                                                                                                                                                                                               |   |   |   | DS21 [O3], DS13f<br>[F3OEM]                                                                                                                                                                                          |   |    |   |
| R145: T58 Extraktion von Daten aus CC Frontend prep. durch P3ec Unbefugter physischer Zugang zum Control Center (Extraktion von Komponenten, die nicht sensible Daten speichern) | A8 Vertrauliche Daten werden nur während der Übertragung verarbeitet und nicht gespeichert                                                                                                                                                         | DS1 [P2], DS16<br>[F2OEM]<br>_____<br>DS1, DS16, DS18<br>_____                                                                                                                                                                       |   | H | 1 | DS1 [P2], DS16<br>[F2OEM]<br>_____<br>DS1, DS16, DS18<br>_____                                                                                                                                                       |   | H  | 1 |
| R146: T58 Extrahieren von Daten aus CC Frontend prep. durch P6e Ausnutzen von Software-Schwachstellen des Control Center Backend für Frontend (Abhören)                          | C18 Absicherung von Komponenten mit Internetanschluss gegen Software-Schwachstellen<br>C27 End-to-End-verschlüsselte Übertragung sensibler Daten zwischen technischen Überwachungsgeräten, Lkw, externen Partnern und dynamischem Routenmanagement | DS1 [P2], DS16<br>[F2OEM]                                                                                                                                                                                                            | E | H | 4 | DS1 [P2], DS16<br>[F2OEM]                                                                                                                                                                                            | E | SG | 2 |
| R147: T59 Denial-of-Service-Angriff auf CC-Frontend, vorbereitet durch P3dc Unbefugter physischer Zugang zum Control Center (Störung von Komponenten)                            | C5A Eigensicherheit des Lkw (gegen Störungen)<br>_____<br>A10 Durch CC ausgelöste MRM sind nicht sicherheitskritisch<br>A12 AWS schützt die Verfügbarkeit der Cloud-Infrastruktur                                                                  | DS6 [S3 F2OEM], DS8<br>[O1], DS9 [O3], DS10<br>[F1OEM], DS13s [S3],<br>DS17 [O0], DS21 [O3],<br>DS13f [F3OEM]<br>_____<br>DS6<br>_____<br>DS8 [O1], DS9 [O3],<br>DS10 [F1OEM], DS13s<br>[S3], DS17 [O0], DS21<br>[O3], DS13f [F3OEM] | S | H | 2 | DS6 [S3 F2OEM], DS8<br>[O1], DS9 [O3], DS10<br>[F1OEM], DS13s [S3],<br>DS17 [O0], DS21 [O3],<br>DS13f [F3OEM]<br>_____<br>DS13s, DS13f, DS6<br>_____<br>DS8 [O1], DS9 [O3],<br>DS10 [F1OEM], DS17<br>[O0], DS21 [O3] | S | H  | 2 |

|                                                                                                                                                                                    |                                                                                                                                                                                                                                                                   |                                                                                                                                                                                                                                                             |   |   |   |                                                                                                                                                                                                                                             |   |    |   |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|---|---|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|----|---|
| R148: T59 Denial-of-Service-Angriff auf CC-Frontend, vorbereitet durch P6d Ausnutzen von Software-Schwachstellen des Control Center-Backends für das Frontend (Störung)            | C5A Intrinsische Sicherheit des Lkw (gegen Störungen)<br>C18 Absicherung von Komponenten mit Internetanbindung gegen Software-Schwachstellen<br>C29 Resilienz/Sicherheit durch Vielfalt<br>A10 Durch CC ausgelöste MRM sind nicht sicherheitskritisch             | DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS13s [S3], DS17 [O0], DS21 [O3], DS13f [F3OEM]<br>DS6<br>DS8 [O1], DS9 [O3], DS10 [F1OEM], DS13s [S3], DS17 [O0], DS21 [O3], DS13f [F3OEM]                                                               | S | H | 5 | DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS13s [S3], DS17 [O0], DS21 [O3], DS13f [F3OEM]<br>DS13s, DS13f, DS6<br>DS8 [O1], DS9 [O3], DS10 [F1OEM], DS17 [O0], DS21 [O3]                                                            | S | SG | 2 |
| R149: T60 Manipulation von Daten, Parametern oder Software des CC-Frontends Vorbereitung durch P3mc Unbefugter physischer Zugang zum Control Center (Manipulation von Komponenten) | C5I Intrinsische Sicherheit des Trucks (gegen Spoofing/Manipulation)<br>C20 ADS-Sicherheitsvalidierungen nach Entscheidungen des Control Centers<br>C30 Befolgung der AWS-Sicherheitsbest Practices<br>A10 Durch CC ausgelöste MRM sind nicht sicherheitskritisch | DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS12 [S3 F2OEM], DS13s [S3], DS15 [F2OEM], DS17 [O0], DS21 [O3], DS13f [F3OEM]<br>DS6<br>DS8 [O1], DS9 [O3], DS10 [F1OEM], DS12 [S3 F2OEM], DS13s [S3], DS15 [F2OEM], DS17 [O0], DS21 [O3], DS13f [F3OEM] | S | H | 5 | DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS12 [S3 F2OEM], DS13s [S3], DS15 [F2OEM], DS17 [O0], DS21 [O3], DS13f [F3OEM]<br>DS13s, DS12, DS6<br>DS8 [O1], DS9 [O3], DS10 [F1OEM], DS15 [F2OEM], DS17 [O0], DS21 [O3], DS13f [F3OEM] | S | SG | 2 |

|                                                                                                                                                                                                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                                                                                                                                                                                                                                                                            |   |   |   |                                                                                                                                                                                                                                                            |   |    |   |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|---|---|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|----|---|
| R150: T60 Manipulation von Daten, Parametern oder Software des CC-Frontends Vorbereitung durch P6m Ausnutzung von Software-Schwachstellen des Control Center-Backends für das Frontend (Manipulation)       | <p>C5I Intrinsische Sicherheit des Lkw (gegen Spoofing/Manipulation)</p> <p>C20 ADS-Sicherheitsvalidierungen nach Entscheidungen des Control Centers</p> <p>C18 Absicherung von Komponenten mit Internetanbindung gegen Software-Schwachstellen</p> <p>C28 End-to-End-Authentifizierung der Datenübertragung zwischen technischer Überwachungsausrüstung, Lkw, Kunden-/Flottenmanagement, externen Partnern, dynamischem Routenmanagement</p> <p>A10 Durch CC ausgelöste MRM sind nicht sicherheitskritisch</p> | <p>DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS12 [S3 F2OEM], DS13s [S3], DS15 [F2OEM], DS17 [O0], DS21 [O3], DS13f [F3OEM]</p> <p>DS6</p> <p>DS8 [O1], DS9 [O3], DS10 [F1OEM], DS12 [S3 F2OEM], DS13s [S3], DS15 [F2OEM], DS17 [O0], DS21 [O3], DS13f [F3OEM]</p> | S | H | 5 | <p>DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS12 [S3 F2OEM], DS13s [S3], DS15 [F2OEM], DS17 [O0], DS21 [O3], DS13f [F3OEM]</p> <p>DS13s, DS12, DS6</p> <p>DS8 [O1], DS9 [O3], DS10 [F1OEM], DS15 [F2OEM], DS17 [O0], DS21 [O3], DS13f [F3OEM]</p> | S | SG | 2 |
| R151: T61 Extraktion von Daten aus dem CC-Backend für die Frontend-Vorbereitung durch P3ec Unbefugter physischer Zugang zum Control Center (Extraktion von Komponenten, die nicht sensible Daten speichern) | A8 Vertrauliche Daten werden nur während der Übertragung verarbeitet und nicht gespeichert                                                                                                                                                                                                                                                                                                                                                                                                                      | <p>DS1 [P2], DS16 [F2OEM]</p> <p>DS1, DS16, DS18</p>                                                                                                                                                                                                                       |   | H | 1 | <p>DS1 [P2], DS16 [F2OEM]</p> <p>DS1, DS16, DS18</p>                                                                                                                                                                                                       |   | H  | 1 |
| R152: T61 Extrahieren von Daten aus dem CC-Backend für die Frontend-Vorbereitung durch P6e Ausnutzen von Software-Schwachstellen des Control Center-Backends für das Frontend (Abhören)                     | C18 Absicherung von Komponenten mit Internetanschluss gegen Software-Schwachstellen                                                                                                                                                                                                                                                                                                                                                                                                                             | DS1 [P2], DS16 [F2OEM]                                                                                                                                                                                                                                                     | E | H | 4 | DS1 [P2], DS16 [F2OEM]                                                                                                                                                                                                                                     | E | SG | 2 |

|                                                                                                                                                                        |                                                                                                                                                                                                                                                                                                  |                                                                                                                                                                                                              |   |   |   |                                                                                                                                                                                                 |   |    |   |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|---|---|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|----|---|
|                                                                                                                                                                        | C27 End-to-End-verschlüsselte Übertragung sensibler Daten zwischen technischen Überwachungsgeräten, Lkw, externen Partnern und dynamischem Routenmanagement                                                                                                                                      |                                                                                                                                                                                                              |   |   |   |                                                                                                                                                                                                 |   |    |   |
| R153: T62 Denial-of-Service-Angriff auf CC-Backend für Frontend                                                                                                        | <p>C5A Eigensicherheit des Trucks (gegen Störungen)</p> <p>C23 Schutz vor Distributed-Denial-of-Service-Angriffen (DDoS) für Komponenten mit Internetanbindung</p> <p>A10 Durch CC ausgelöste MRM sind nicht sicherheitskritisch</p>                                                             | <p>DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS13s [S3], DS17 [O0], DS21 [O3], DS13f [F3OEM]</p> <p>DS6</p> <p>DS8 [O1], DS9 [O3], DS10 [F1OEM], DS13s [S3], DS17 [O0], DS21 [O3], DS13f [F3OEM]</p> | S | H | 5 | <p>DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS13s [S3], DS17 [O0], DS21 [O3], DS13f [F3OEM]</p> <p>DS13s, DS13f, DS6</p> <p>DS8 [O1], DS9 [O3], DS10 [F1OEM], DS17 [O0], DS21 [O3]</p> | S | SG | 2 |
| R154: T62 Denial-of-Service-Angriff auf CC-Backend zur Vorbereitung des Frontends durch P3dc Unbefugter physischer Zugang zum Control Center (Störung von Komponenten) | <p>C5A Eigensicherheit des Trucks (gegen Störungen)</p> <p>C23 Schutz vor Distributed-Denial-of-Service-Angriffen (DDoS) für internetfähige Komponenten</p> <p>A10 Durch CC ausgelöste MRM sind nicht sicherheitskritisch.</p> <p>A12 AWS schützt die Verfügbarkeit der Cloud-Infrastruktur.</p> | <p>DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS13s [S3], DS17 [O0], DS21 [O3], DS13f [F3OEM]</p> <p>DS6</p> <p>DS8 [O1], DS9 [O3], DS10 [F1OEM], DS13s</p>                                           | S | H | 2 | <p>DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS13s [S3], DS17 [O0], DS21 [O3], DS13f [F3OEM]</p> <p>DS13s, DS13f, DS6</p> <p>DS8 [O1], DS9 [O3], DS10 [F1OEM], DS17 [O0], DS21 [O3]</p> | S | SG | 2 |

|                                                                                                                                                                                                    |                                                                                                                                                                                                                                                                                                                                                |                                                                                                                                                                                                                       |   |   |   |                                                                                                                                                                                                                                      |   |    |   |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|---|---|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|----|---|
|                                                                                                                                                                                                    |                                                                                                                                                                                                                                                                                                                                                | [S3], DS17 [O0], DS21 [O3], DS13f [F3OEM]                                                                                                                                                                             |   |   |   |                                                                                                                                                                                                                                      |   |    |   |
| R155: T62 Denial-of-Service-Angriff auf CC-Backend für Frontend-Vorbereitung durch P6d Ausnutzen von Software-Schwachstellen des Control Center-Backends für Frontend (Störung)                    | C5A Eigensicherheit des Trucks (gegen Störungen)<br>C23 Schutz vor Distributed-Denial-of-Service-Angriffen (DDoS) für internetfähige Komponenten<br>C18 Absicherung internetfähiger Komponenten gegen Software-Schwachstellen<br>C29 Ausfallsicherheit/Sicherheit durch Vielfalt<br>A10 Durch CC ausgelöste MRM sind nicht sicherheitskritisch | DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS13s [S3], DS17 [O0], DS21 [O3], DS13f [F3OEM]<br>_____<br>DS6<br>_____<br>DS8 [O1], DS9 [O3], DS10 [F1OEM], DS13s [S3], DS17 [O0], DS21 [O3], DS13f [F3OEM]       | S | H | 5 | DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS13s [S3], DS17 [O0], DS21 [O3], DS13f [F3OEM]<br>_____<br>DS13s, DS13f, DS6<br>_____<br>DS8 [O1], DS9 [O3], DS10 [F1OEM], DS17 [O0], DS21 [O3]                                   | S | SG | 2 |
| R156: T63 Manipulation von Daten, Parametern oder Software des CC-Backends für die Frontend-Vorbereitung durch P3mc Unbefugter physischer Zugang zum Control Center (Manipulation von Komponenten) | C5I Intrinsische Sicherheit des Trucks (gegen Spoofing/Manipulation)<br>C20 ADS-Sicherheitsvalidierungen nach Entscheidungen des Control Centers<br>C30 Befolgung der AWS-Sicherheitsbest Practices<br>A10 Durch CC ausgelöste MRM sind nicht sicherheitskritisch                                                                              | DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS12 [S3 F2OEM], DS13s [S3], DS15 [F2OEM], DS17 [O0], DS21 [O3], DS13f [F3OEM]<br>_____<br>DS6<br>_____<br>DS8 [O1], DS9 [O3], DS10 [F1OEM], DS12 [S3 F2OEM], DS13s | S | H | 5 | DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS12 [S3 F2OEM], DS13s [S3], DS15 [F2OEM], DS17 [O0], DS21 [O3], DS13f [F3OEM]<br>_____<br>DS13s, DS12, DS6<br>_____<br>DS8 [O1], DS9 [O3], DS10 [F1OEM], DS15 [F2OEM], DS17 [O0], | S | SG | 2 |

|                                                                                                                                                                                                                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |                                                                                                                                                                                                                                                                               |   |   |   |                                                                                                                                                                                                                                                               |   |    |   |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|---|---|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|----|---|
|                                                                                                                                                                                                                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | [S3], DS15 [F2OEM],<br>DS17 [O0], DS21 [O3],<br>DS13f [F3OEM]                                                                                                                                                                                                                 |   |   |   | DS21 [O3], DS13f<br>[F3OEM]                                                                                                                                                                                                                                   |   |    |   |
| R157: T63 Manipulation von Daten, Parametern oder Software des CC-Backends für die Frontend-Vorbereitung durch P6m Ausnutzung von Software-Schwachstellen des Control Center-Backends für das Frontend (Manipulation) | C5I Intrinsische Sicherheit des Lkw (gegen Spoofing/Manipulation)<br>C20 ADS-Sicherheitsvalidierungen nach Entscheidungen des Control Centers<br>C18 Absicherung von Komponenten mit Internetanbindung gegen Software-Schwachstellen<br>C28 End-to-End-Authentifizierung der Datenübertragung zwischen technischer Überwachungsausrüstung, Lkw, Kunden-/Flottenmanagement, externen Partnern, dynamischem Routenmanagement<br>A10 Durch CC ausgelöste MRM sind nicht sicherheitskritisch | DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS12 [S3 F2OEM], DS13s [S3], DS15 [F2OEM], DS17 [O0], DS21 [O3], DS13f [F3OEM]<br>_____<br>DS6<br>_____<br>DS8 [O1], DS9 [O3], DS10 [F1OEM], DS12 [S3 F2OEM], DS13s [S3], DS15 [F2OEM], DS17 [O0], DS21 [O3], DS13f [F3OEM] | S | H | 5 | DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS12 [S3 F2OEM], DS13s [S3], DS15 [F2OEM], DS17 [O0], DS21 [O3], DS13f [F3OEM]<br>_____<br>DS13s, DS12, DS6<br>_____<br>DS8 [O1], DS9 [O3], DS10 [F1OEM], DS15 [F2OEM], DS17 [O0], DS21 [O3], DS13f [F3OEM] | S | SG | 2 |
| R158: T64 Extraktion von Daten aus der Datenbankvorbereitung durch P3ecs Unbefugter physischer Zugang zum Control Center (Extraktion von Komponenten, die sensible Daten speichern)                                   | C31 Verschlüsselte Speicherung sensibler Lkw- und Kundendaten                                                                                                                                                                                                                                                                                                                                                                                                                            | DS1 [P2], DS16 [F2OEM], DS19 [P2]                                                                                                                                                                                                                                             | E | H | 4 | DS1 [P2], DS16 [F2OEM], DS19 [P2]<br>_____<br>DS1, DS16, DS19<br>_____                                                                                                                                                                                        |   | H  | 1 |

|                                                                                                                                                                                |                                                                                                                                                                                                                                                                       |                                                                                                                                                                                                                                                                     |   |   |   |                                                                                                                                                                                                                                                     |   |    |   |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|---|---|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|----|---|
| R159: T65 Denial-of-Service-Angriff auf Datenbankvorbereitung durch P3dc Unbefugter physischer Zugang zum Control Center (Störung von Komponenten)                             | C5A Eigensicherheit des Lkw (gegen Störungen)<br><br>A10 Durch CC ausgelöste MRM sind nicht sicherheitskritisch<br>A12 AWS schützt die Verfügbarkeit der Cloud-Infrastruktur                                                                                          | DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS13s [S3], DS17 [O0], DS21 [O3], DS13f [F3OEM]<br><br>DS6<br><br>DS8 [O1], DS9 [O3], DS10 [F1OEM], DS13s [S3], DS17 [O0], DS21 [O3], DS13f [F3OEM]                                                               | S | H | 2 | DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS13s [S3], DS17 [O0], DS21 [O3], DS13f [F3OEM]<br><br>DS13s, DS13f, DS6<br><br>DS8 [O1], DS9 [O3], DS10 [F1OEM], DS17 [O0], DS21 [O3]                                                            | S | H  | 2 |
| R160: T66 Manipulation von Daten, Parametern oder Software der Datenbankvorbereitung durch P3mc Unbefugter physischer Zugang zum Control Center (Manipulation von Komponenten) | C5I Intrinsische Sicherheit des Trucks (gegen Spoofing/Manipulation)<br>C20 ADS-Sicherheitsvalidierungen nach Entscheidungen des Control Centers<br>C30 Befolgung der AWS-Sicherheitsbest Practices<br><br>A10 Durch CC ausgelöste MRM sind nicht sicherheitskritisch | DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS12 [S3 F2OEM], DS13s [S3], DS15 [F2OEM], DS17 [O0], DS21 [O3], DS13f [F3OEM]<br><br>DS6<br><br>DS8 [O1], DS9 [O3], DS10 [F1OEM], DS12 [S3 F2OEM], DS13s [S3], DS15 [F2OEM], DS17 [O0], DS21 [O3], DS13f [F3OEM] | S | H | 5 | DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS12 [S3 F2OEM], DS13s [S3], DS15 [F2OEM], DS17 [O0], DS21 [O3], DS13f [F3OEM]<br><br>DS13s, DS12, DS6<br><br>DS8 [O1], DS9 [O3], DS10 [F1OEM], DS15 [F2OEM], DS17 [O0], DS21 [O3], DS13f [F3OEM] | S | SG | 2 |

|                                                                                                                                                                                  |                                                                                                                                                                                                                                                    |                                                          |   |   |   |                                                                                                           |   |    |   |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------|---|---|---|-----------------------------------------------------------------------------------------------------------|---|----|---|
| R161: T67 Extrahieren von Daten aus API Gateway prep. von P3ec Unbefugter physischer Zugang zum Control Center (Extrahieren von Komponenten, die nicht sensible Daten speichern) | A8 Vertrauliche Daten werden nur während der Übertragung verarbeitet und nicht gespeichert                                                                                                                                                         | DS1, DS16, DS18                                          |   | H | 1 | DS1, DS16, DS18                                                                                           |   | H  | 1 |
| R162: T67 Extrahieren von Daten aus dem API-Gateway, vorbereitet durch P7e Ausnutzen von Software-Schwachstellen des API-Gateways (Abhören)                                      | C18 Absicherung von Komponenten mit Internetanschluss gegen Software-Schwachstellen<br>C27 End-to-End-verschlüsselte Übertragung sensibler Daten zwischen technischen Überwachungsgeräten, Lkw, externen Partnern und dynamischem Routenmanagement |                                                          |   | H | 1 |                                                                                                           |   | SG | 1 |
| R163: T68 Denial-of-Service-Angriff auf API-Gateway                                                                                                                              | C5A Eigensicherheit des Lkw (gegen Störungen)<br>C23 Schutz vor Distributed-Denial-of-Service-Angriffen (DDoS) für internetfähige Komponenten                                                                                                      | DS8 [O1], DS9 [O3], DS13s [S3], DS21 [O3], DS13f [F3OEM] | S | H | 5 | DS8 [O1], DS9 [O3], DS13s [S3], DS21 [O3], DS13f [F3OEM]<br>DS13s, DS13f<br>DS8 [O1], DS9 [O3], DS21 [O3] | S | SG | 2 |
| R164: T68 Denial-of-Service-Angriff auf API-Gateway, vorbereitet durch P3dc Unbefugter physischer Zugang zum Control Center (Störung der Komponente)                             | C5A Eigensicherheit des Trucks (gegen Störungen)<br>C23 Schutz vor Distributed-Denial-of-Service-Angriffen (DDoS) für Komponenten mit Internetanbindung                                                                                            | DS8 [O1], DS9 [O3], DS13s [S3], DS21 [O3], DS13f [F3OEM] | S | H | 2 | DS8 [O1], DS9 [O3], DS13s [S3], DS21 [O3], DS13f [F3OEM]<br>DS13s, DS13f                                  | S | SG | 2 |



|                                                                                                                                                                                    |                                                                                                                                                                                                                                                                                  |                                                          |   |   |   |                                                                                                                                     |   |    |   |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------|---|---|---|-------------------------------------------------------------------------------------------------------------------------------------|---|----|---|
|                                                                                                                                                                                    | A12 AWS schützt die Verfügbarkeit der Cloud-Infrastruktur                                                                                                                                                                                                                        |                                                          |   |   |   | DS8 [O1], DS9 [O3], DS21 [O3]                                                                                                       |   |    |   |
| R165: T68 Denial-of-Service-Angriff auf API Gateway, vorbereitet durch P7d Ausnutzen von Software-Schwachstellen des API Gateway (Störung)                                         | C5A Eigensicherheit des Trucks (gegen Störungen)<br>C23 Schutz vor Distributed-Denial-of-Service-Angriffen (DDoS) für internetfähige Komponenten<br>C18 Absicherung internetfähiger Komponenten gegen Software-Schwachstellen<br>C29 Ausfallsicherheit/Sicherheit durch Vielfalt | DS8 [O1], DS9 [O3], DS13s [S3], DS21 [O3], DS13f [F3OEM] | S | H | 5 | DS8 [O1], DS9 [O3], DS13s [S3], DS21 [O3], DS13f [F3OEM]<br>_____<br>DS13s, DS13f<br>_____<br>DS8 [O1], DS9 [O3], DS21 [O3]         | S | SG | 2 |
| R166: T69 Manipulation von Daten, Parametern oder Software des API-Gateways Vorbereitung durch P3mc Unbefugter physischer Zugang zum Control Center (Manipulation von Komponenten) | C5I Intrinsische Sicherheit des Lkw (gegen Spoofing/Manipulation)<br>C30 Befolgung der AWS-Sicherheitsbestimmungen                                                                                                                                                               | DS8 [O1], DS9 [O3], DS13s [S3], DS21 [O3], DS13f [F3OEM] | S | H | 5 | DS8 [O1], DS9 [O3], DS13s [S3], DS21 [O3], DS13f [F3OEM]<br>_____<br>DS13s<br>_____<br>DS8 [O1], DS9 [O3], DS21 [O3], DS13f [F3OEM] | S | SG | 2 |
| R167: T69 Manipulation von Daten, Parametern oder Software des API-Gateways Vorbereitung durch P7m Ausnutzung von Software-Schwachstellen des API-Gateways (Manipulation)          | C5I Intrinsische Sicherheit des Lkw (gegen Spoofing/Manipulation)<br>C18 Absicherung von Komponenten mit Internetanbindung gegen Software-Schwachstellen                                                                                                                         | DS8 [O1], DS9 [O3], DS13s [S3], DS21 [O3], DS13f [F3OEM] | S | H | 5 | DS8 [O1], DS9 [O3], DS13s [S3], DS21 [O3], DS13f [F3OEM]<br>_____<br>DS13s<br>_____<br>DS8 [O1], DS9 [O3],                          | S | SG | 2 |

|                                                                                                                                                                                  |                                                                                                                                                                                                                         |                                                         |   |   |   |                                                         |   |    |   |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------|---|---|---|---------------------------------------------------------|---|----|---|
|                                                                                                                                                                                  | C28 End-to-End-Authentifizierung der Datenübertragung zwischen technischer Überwachungsausrüstung, Lkw, Kunden-/Flottenmanagement, externen Partnern, dynamischem Routenmanagement                                      |                                                         |   |   |   | DS21 [O3], DS13f [F3OEM]                                |   |    |   |
| R168: T70 Extraktion von Daten aus CC Eventbus prep. durch P3ec Unbefugter physischer Zugang zum Control Center (Extraktion von Komponenten, die nicht sensible Daten speichern) | A8 Vertrauliche Daten werden nur während der Übertragung verarbeitet und nicht gespeichert                                                                                                                              | DS1 [P2], DS16 [F2OEM]<br>DS1, DS16, DS18               |   | H | 1 | DS1 [P2], DS16 [F2OEM]<br>DS1, DS16, DS18               |   | H  | 1 |
| R169: T71 Denial-of-Service-Angriff auf CC Eventbus, vorbereitet von P3dc Unbefugter physischer Zugang zum Control Center (Störung der Komponente)                               | A12 AWS schützt die Verfügbarkeit der Cloud-Infrastruktur                                                                                                                                                               | DS8 [O1], DS9 [O3], DS17 [O0], DS21 [O3]                | S | H | 2 | DS8 [O1], DS9 [O3], DS17 [O0], DS21 [O3]                | S | H  | 2 |
| R170: T71 Denial-of-Service-Angriff auf CC Eventbus, vorbereitet von P4d Ausnutzen von Software-Schwachstellen des Vehicle Adapter Service (Störung)                             | C18 Absicherung von Komponenten mit Internetanschluss gegen Software-Schwachstellen<br>C29 Widerstandsfähigkeit/Sicherheit durch Vielfalt<br>A16 Vorbereitende Schritte verursachen bereits gleiche oder höhere Schäden | DS8 [O1], DS9 [O3], DS17 [O0], DS21 [O3]                | S | H | 2 | DS8 [O1], DS9 [O3], DS17 [O0], DS21 [O3]                | S | SG | 2 |
| R171: T72 Manipulation von Daten, Parametern oder Software des CC Eventbus durch P3mc Unbefugter                                                                                 | C5I Intrinsische Sicherheit des Lkw (gegen Spoofing/Manipulation)                                                                                                                                                       | DS8 [O1], DS9 [O3], DS12 [S3 F2OEM], DS15 [F2OEM], DS17 | S | H | 5 | DS8 [O1], DS9 [O3], DS12 [S3 F2OEM], DS15 [F2OEM], DS17 | S | SG | 2 |

|                                                                                                                                                                                                         |                                                                                                                                                                                                                                                    |                                                                                                          |   |   |   |                                                                                                                        |   |    |   |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------|---|---|---|------------------------------------------------------------------------------------------------------------------------|---|----|---|
| physischer Zugang zum Control Center (Manipulation von Komponenten)                                                                                                                                     | C20 ADS-Sicherheitsvalidierungen nach Entscheidungen des Control Centers<br>C30 Befolgung der AWS-Sicherheitsbest Practices                                                                                                                        | DS15 [F2OEM], DS17 [O0], DS21 [O3]                                                                       |   |   |   | [O0], DS21 [O3]<br>DS13s, DS12<br>DS8 [O1], DS9 [O3], DS15 [F2OEM], DS17 [O0], DS21 [O3]                               |   |    |   |
| R172: T73 Extrahieren von Daten aus dem Vehicle Adapter Service, vorbereitet von P3ec Unbefugter physischer Zugang zum Control Center (Extrahieren von Komponenten, die nicht sensible Daten speichern) | A8 Vertrauliche Daten werden nur während der Übertragung verarbeitet und nicht gespeichert                                                                                                                                                         | DS1 [P2], DS16 [F2OEM]<br>DS1, DS16, DS18                                                                |   | H | 1 | DS1 [P2], DS16 [F2OEM]<br>DS1, DS16, DS18                                                                              |   | H  | 1 |
| R173: T73 Extrahieren von Daten aus dem Vehicle Adapter Service, vorbereitet durch P4e Ausnutzen von Software-Schwachstellen des Vehicle Adapter Service (Abhören)                                      | C18 Absicherung von Komponenten mit Internetanschluss gegen Software-Schwachstellen<br>C27 End-to-End-verschlüsselte Übertragung sensibler Daten zwischen technischen Überwachungsgeräten, Lkw, externen Partnern und dynamischem Routenmanagement | DS1 [P2], DS16 [F2OEM]                                                                                   | E | H | 4 | DS1 [P2], DS16 [F2OEM]                                                                                                 | E | SG | 2 |
| R174: T74 Denial-of-Service-Angriff auf den Fahrzeugadapterdienst                                                                                                                                       | C5A Eigensicherheit des Trucks (gegen Störungen)<br>C23 Schutz vor Distributed-Denial-of-Service-Angriffen (DDoS) für Komponenten mit Internetanbindung                                                                                            | DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS13s [S3], DS17 [O0], DS21 [O3], DS13f [F3OEM]<br>DS6 | S | H | 5 | DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS13s [S3], DS17 [O0], DS21 [O3], DS13f [F3OEM]<br>DS13s, DS13f, DS6 | S | SG | 2 |

|                                                                                                                                                                      |                                                                                                                                                                                                                                                                                   |                                                                                                                                                                                                       |   |   |   |                                                                                                                                                                                          |   |    |   |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|---|---|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|----|---|
|                                                                                                                                                                      | A10 Durch CC ausgelöste MRM sind nicht sicherheitskritisch                                                                                                                                                                                                                        | DS8 [O1], DS9 [O3], DS10 [F1OEM], DS13s [S3], DS17 [O0], DS21 [O3], DS13f [F3OEM]                                                                                                                     |   |   |   | DS8 [O1], DS9 [O3], DS10 [F1OEM], DS17 [O0], DS21 [O3]                                                                                                                                   |   |    |   |
| R175: T74 Denial-of-Service-Angriff auf Fahrzeugadapterdienst, vorbereitet durch P3dc Unbefugter physischer Zugang zum Control Center (Störung der Komponente)       | C5A Eigensicherheit des Trucks (gegen Störungen)<br>C23 Schutz vor Distributed-Denial-of-Service-Angriffen (DDoS) für internetfähige Komponenten<br><br>A10 Durch CC ausgelöste MRM sind nicht sicherheitskritisch.<br>A12 AWS schützt die Verfügbarkeit der Cloud-Infrastruktur. | DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS13s [S3], DS17 [O0], DS21 [O3], DS13f [F3OEM]<br><br>DS6<br><br>DS8 [O1], DS9 [O3], DS10 [F1OEM], DS13s [S3], DS17 [O0], DS21 [O3], DS13f [F3OEM] | S | H | 2 | DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS13s [S3], DS17 [O0], DS21 [O3], DS13f [F3OEM]<br><br>DS13s, DS13f, DS6<br><br>DS8 [O1], DS9 [O3], DS10 [F1OEM], DS17 [O0], DS21 [O3] | S | SG | 2 |
| R176: T74 Denial-of-Service-Angriff auf den Fahrzeugadapterdienst, vorbereitet durch P4d Ausnutzen von Software-Schwachstellen des Fahrzeugadapterdienstes (Störung) | C5A Eigensicherheit des Trucks (gegen Störungen)<br>C23 Schutz vor Distributed-Denial-of-Service-Angriffen (DDoS) für internetfähige Komponenten<br>C18 Absicherung internetfähiger Komponenten gegen Software-Schwachstellen<br>C29 Ausfallsicherheit/Sicherheit durch Vielfalt  | DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS13s [S3], DS17 [O0], DS21 [O3], DS13f [F3OEM]<br><br>DS6<br><br>DS8 [O1], DS9 [O3], DS10 [F1OEM], DS13s [S3], DS17 [O0], DS21 [O3], DS13f [F3OEM] | S | H | 5 | DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS13s [S3], DS17 [O0], DS21 [O3], DS13f [F3OEM]<br><br>DS13s, DS13f, DS6<br><br>DS8 [O1], DS9 [O3], DS10 [F1OEM], DS17 [O0], DS21 [O3] | S | SG | 2 |

|                                                                                                                                                                                                 | A10 Durch CC ausgelöste MRM<br>sind nicht sicherheitskritisch                                                                                                                                                                                                                              |                                                                                                                                                                                                                                                                                        |   |   |   |                                                                                                                                                                                                                                                                        |   |    |   |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|---|---|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|----|---|
| R177: T75 Manipulation von Daten, Parametern oder Software des Fahrzeugadapterdienstes Vorbereitung durch P3mc Unbefugter physischer Zugang zum Control Center (Manipulation von Komponenten)   | <p>C5I Intrinsische Sicherheit des Trucks (gegen Spoofing/Manipulation)</p> <p>C20 ADS-Sicherheitsvalidierungen nach Entscheidungen des Control Centers</p> <p>C30 Befolgung der AWS-Sicherheitsbest Practices</p> <hr/> <p>A10 Durch CC ausgelöste MRM sind nicht sicherheitskritisch</p> | <p>DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS12 [S3 F2OEM], DS13s [S3], DS15 [F2OEM], DS17 [O0], DS21 [O3], DS13f [F3OEM]</p> <hr/> <p>DS6</p> <hr/> <p>DS8 [O1], DS9 [O3], DS10 [F1OEM], DS12 [S3 F2OEM], DS13s [S3], DS15 [F2OEM], DS17 [O0], DS21 [O3], DS13f [F3OEM]</p> | S | H | 5 | <p>DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS12 [S3 F2OEM], DS13s [S3], DS15 [F2OEM], DS17 [O0], DS21 [O3], DS13f [F3OEM]</p> <hr/> <p>DS13s, DS12, DS6</p> <hr/> <p>DS8 [O1], DS9 [O3], DS10 [F1OEM], DS15 [F2OEM], DS17 [O0], DS21 [O3], DS13f [F3OEM]</p> | S | SG | 2 |
| R178: T75 Manipulation von Daten, Parametern oder Software des Vehicle Adapter Service Vorbereitung durch P4m Ausnutzung von Software-Schwachstellen des Vehicle Adapter Service (Manipulation) | <p>C5I Intrinsische Sicherheit des Lkw (gegen Spoofing/Manipulation)</p> <p>C20 ADS-Sicherheitsvalidierungen nach Entscheidungen des Control Centers</p> <p>C18 Absicherung von Komponenten mit Internetanbindung gegen Software-Schwachstellen</p> <p>C28 End-to-End-</p>                 | <p>DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS12 [S3 F2OEM], DS13s [S3], DS15 [F2OEM], DS17 [O0], DS21 [O3], DS13f [F3OEM]</p> <hr/> <p>DS6</p> <hr/> <p>DS8 [O1], DS9 [O3],</p>                                                                                              | S | H | 5 | <p>DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS12 [S3 F2OEM], DS13s [S3], DS15 [F2OEM], DS17 [O0], DS21 [O3], DS13f [F3OEM]</p> <hr/> <p>DS13s, DS12, DS6</p> <hr/> <p>DS8 [O1], DS9 [O3],</p>                                                                 | S | SG | 2 |

|                                                                                                                                                                |                                                                                                                                                                                                                                                                                      |                                                                                                          |   |   |   |                                                                          |   |    |   |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------|---|---|---|--------------------------------------------------------------------------|---|----|---|
|                                                                                                                                                                | Authentifizierung der Daten-<br>übertragung zwischen techni-<br>scher Überwachungsäusrüs-<br>tung, Lkw, Kunden-/Flottenma-<br>nagement, externen Partnern,<br>dynamischem Routenmanage-<br>ment<br><br>A10 Durch CC ausgelöste MRM<br>sind nicht sicherheitskritisch                 | DS10 [F1OEM], DS12<br>[S3 F2OEM], DS13s<br>[S3], DS15 [F2OEM],<br>DS17 [O0], DS21 [O3],<br>DS13f [F3OEM] |   |   |   | DS10 [F1OEM], DS15<br>[F2OEM], DS17 [O0],<br>DS21 [O3], DS13f<br>[F3OEM] |   |    |   |
| R179: T76 Angriffe auf Kunden-/Flottenmanagement<br>vorbereitet durch P17 Ausfall der IT-Systeme von<br>Dienstleistern                                         | A13 Angriffe auf das Kunden-<br>/Flottenmanagement fallen<br>nicht in den Umfang dieser Ri-<br>sikoanalyse                                                                                                                                                                           | DS9 [O3], DS15<br>[F2OEM], DS19 [P2]                                                                     | S | H | 2 | DS9 [O3], DS15<br>[F2OEM], DS19 [P2]                                     | S | H  | 2 |
| R180: T77 Extraktion von Daten aus dem Befehlsdienst,<br>vorbereitet durch P1ec Unbefugter physischer Zugriff<br>auf die AWS Cloud (Extraktion der Komponente) | A8 Vertrauliche Daten werden<br>nur während der Übertragung<br>verarbeitet und nicht gespei-<br>chert                                                                                                                                                                                | DS16 [F2OEM]<br><br>DS1, DS16, DS18                                                                      |   | H | 1 | DS16 [F2OEM]<br><br>DS1, DS16, DS18                                      |   | H  | 1 |
| R181: T77 Extrahieren von Daten aus dem Befehls-<br>dienst, vorbereitet durch P12e Ausnutzen von Soft-<br>ware-Schwachstellen des Befehlsdienstes (Abhören)    | C18 Absicherung von Kompo-<br>nenten mit Internetanschluss<br>gegen Software-Schwachstel-<br>len<br><br>C27 End-to-End-verschlüsselte<br>Übertragung sensibler Daten<br>zwischen technischen Überwa-<br>chungsgeräten, Lkw, externen<br>Partnern und dynamischem<br>Routenmanagement | DS16 [F2OEM]                                                                                             | E | H | 4 | DS16 [F2OEM]                                                             | E | SG | 2 |

|                                                                                                                                               |                                                                                                                                                                                                                                                                                                  |                                                                                                                                                                                        |   |   |   |                                                                                                                                                                           |   |    |   |
|-----------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|---|---|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|----|---|
| R182: T78 Denial-of-Service-Angriff auf den Befehlsdienst                                                                                     | <p>C5A Eigensicherheit des Trucks (gegen Störungen)</p> <p>C23 Schutz vor Distributed-Denial-of-Service-Angriffen (DDoS) für Komponenten mit Internetanbindung</p> <p>A10 Durch CC ausgelöste MRM sind nicht sicherheitskritisch</p>                                                             | <p>DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS13s [S3], DS21 [O3], DS13f [F3OEM]</p> <p>DS6</p> <p>DS8 [O1], DS9 [O3], DS10 [F1OEM], DS13s [S3], DS21 [O3], DS13f [F3OEM]</p> | S | H | 5 | <p>DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS13s [S3], DS21 [O3], DS13f [F3OEM]</p> <p>DS13s, DS13f, DS6</p> <p>DS8 [O1], DS9 [O3], DS10 [F1OEM], DS21 [O3]</p> | S | SG | 2 |
| R183: T78 Denial-of-Service-Angriff auf Command Service Prep. durch P1dc Unbefugter physischer Zugriff auf AWS Cloud (Störung der Komponente) | <p>C5A Eigensicherheit des Trucks (gegen Störungen)</p> <p>C23 Schutz vor Distributed-Denial-of-Service-Angriffen (DDoS) für internetfähige Komponenten</p> <p>A10 Durch CC ausgelöste MRM sind nicht sicherheitskritisch.</p> <p>A12 AWS schützt die Verfügbarkeit der Cloud-Infrastruktur.</p> | <p>DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS13s [S3], DS21 [O3], DS13f [F3OEM]</p> <p>DS6</p> <p>DS8 [O1], DS9 [O3], DS10 [F1OEM], DS13s [S3], DS21 [O3], DS13f [F3OEM]</p> | S | H | 2 | <p>DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS13s [S3], DS21 [O3], DS13f [F3OEM]</p> <p>DS13s, DS13f, DS6</p> <p>DS8 [O1], DS9 [O3], DS10 [F1OEM], DS21 [O3]</p> | S | SG | 2 |
| R184: T78 Denial-of-Service-Angriff auf Command Service Prep. durch P12d Ausnutzen von Software-Schwachstellen des Command Service (Störung)  | <p>C5A Eigensicherheit des Trucks (gegen Störungen)</p> <p>C23 Schutz vor Distributed-Denial-of-Service-Angriffen (DDoS) für internetfähige</p>                                                                                                                                                  | <p>DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS13s [S3], DS21 [O3], DS13f [F3OEM]</p>                                                                                          | S | H | 5 | <p>DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS13s [S3], DS21 [O3], DS13f [F3OEM]</p>                                                                             | S | SG | 2 |

|                                                                                                                                                                                  |                                                                                                                                                                                                                                                                                      |                                                                                                                                                                                                                                                      |   |   |   |                                                                                                                                                                                                                                      |   |    |   |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|---|---|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|----|---|
|                                                                                                                                                                                  | <p>Komponenten</p> <p>C18 Absicherung internetfähiger Komponenten gegen Software-Schwachstellen</p> <p>C29 Ausfallsicherheit/Sicherheit durch Vielfalt</p> <p>A10 Durch CC ausgelöste MRM sind nicht sicherheitskritisch</p>                                                         | <p>DS6</p> <p>DS8 [O1], DS9 [O3], DS10 [F1OEM], DS13s [S3], DS21 [O3], DS13f [F3OEM]</p>                                                                                                                                                             |   |   |   | <p>DS13s, DS13f, DS6</p> <p>DS8 [O1], DS9 [O3], DS10 [F1OEM], DS21 [O3]</p>                                                                                                                                                          |   |    |   |
| R185: T79 Manipulation von Daten, Parametern oder Software des Befehlsdienstes durch P1mc Unbefugter physischer Zugriff auf die AWS Cloud (Manipulation von Komponenten)         | <p>C5I Intrinsische Sicherheit des Trucks (gegen Spoofing/Manipulation)</p> <p>C20 ADS-Sicherheitsvalidierungen nach Entscheidungen des Control Centers</p> <p>C30 Befolgung der AWS-Sicherheitsbest Practices</p> <p>A10 Durch CC ausgelöste MRM sind nicht sicherheitskritisch</p> | <p>DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS12 [S3 F2OEM], DS13s [S3], DS15 [F2OEM], DS21 [O3], DS13f [F3OEM]</p> <p>DS6</p> <p>DS8 [O1], DS9 [O3], DS10 [F1OEM], DS12 [S3 F2OEM], DS13s [S3], DS15 [F2OEM], DS21 [O3], DS13f [F3OEM]</p> | S | H | 5 | <p>DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS12 [S3 F2OEM], DS13s [S3], DS15 [F2OEM], DS21 [O3], DS13f [F3OEM]</p> <p>DS13s, DS12, DS6</p> <p>DS8 [O1], DS9 [O3], DS10 [F1OEM], DS15 [F2OEM], DS21 [O3], DS13f [F3OEM]</p> | S | SG | 2 |
| R186: T79 Manipulation von Daten, Parametern oder Software des Befehlsdienstes Vorbereitung durch P12m Ausnutzung von Software-Schwachstellen des Befehlsdienstes (Manipulation) | <p>C5I Intrinsische Sicherheit des Lkw (gegen Spoofing/Manipulation)</p> <p>C20 ADS-</p>                                                                                                                                                                                             | <p>DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS12 [S3 F2OEM], DS13s</p>                                                                                                                                                                      | S | H | 5 | <p>DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS12 [S3 F2OEM], DS13s</p>                                                                                                                                                      | S | SG | 2 |



|                                                                                                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                |                                                                                                                                                                             |   |   |   |                                                                                                                                                             |   |   |   |
|----------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|---|---|-------------------------------------------------------------------------------------------------------------------------------------------------------------|---|---|---|
|                                                                                                                      | <p>Sicherheitsvalidierungen nach Entscheidungen des Control Centers</p> <p>C18 Absicherung von Komponenten mit Internetanbindung gegen Software-Schwachstellen</p> <p>C28 End-to-End-Authentifizierung der Datenübertragung zwischen technischer Überwachungsausrüstung, Lkw, Kunden-/Flottenmanagement, externen Partnern, dynamischem Routenmanagement</p> <p>A10 Durch CC ausgelöste MRM sind nicht sicherheitskritisch</p> | <p>[S3], DS15 [F2OEM], DS21 [O3], DS13f [F3OEM]</p> <p>DS6</p> <p>DS8 [O1], DS9 [O3], DS10 [F1OEM], DS12 [S3 F2OEM], DS13s [S3], DS15 [F2OEM], DS21 [O3], DS13f [F3OEM]</p> |   |   |   | <p>[S3], DS15 [F2OEM], DS21 [O3], DS13f [F3OEM]</p> <p>DS13s, DS12, DS6</p> <p>DS8 [O1], DS9 [O3], DS10 [F1OEM], DS15 [F2OEM], DS21 [O3], DS13f [F3OEM]</p> |   |   |   |
| R187: T80 Angriffe auf externe Partner, vorbereitet durch P17 Ausfall der IT-Systeme von Dienstleistern              | A14 Angriffe auf externe Partner fallen nicht in den Umfang dieser Risikoanalyse                                                                                                                                                                                                                                                                                                                                               | DS8 [O1], DS9 [O3], DS16 [F2OEM], DS21 [O3]                                                                                                                                 | S | H | 2 | DS8 [O1], DS9 [O3], DS16 [F2OEM], DS21 [O3]                                                                                                                 | S | H | 2 |
| R188: T81 Angriffe auf dynamisches Routenmanagement, vorbereitet durch P17 Ausfall der IT-Systeme von Dienstleistern | <p>C5I Intrinsische Sicherheit des Lkw (gegen Spoofing/Manipulation)</p> <p>C20 ADS-Sicherheitsvalidierungen nach Entscheidungen des Control Centers</p> <p>A10 Durch das Control Center ausgelöste MRM sind nicht</p>                                                                                                                                                                                                         | <p>DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS12 [S3 F2OEM], DS13s [S3], DS15 [F2OEM], DS16 [F2OEM], DS17 [O0], DS21 [O3], DS13f [F3OEM]</p>                       | S | H | 2 | <p>DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS12 [S3 F2OEM], DS13s [S3], DS15 [F2OEM], DS16 [F2OEM], DS17 [O0], DS21 [O3], DS13f [F3OEM]</p>       | S | H | 2 |

|                                                                                                   |                                                                                                                                                                                                                                                        |                                                                                                                                                                                                       |   |   |   |                                                                                                                                                                                          |   |    |   |
|---------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|---|---|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|----|---|
|                                                                                                   | sicherheitskritisch.<br>A15 Angriffe auf das dynamische Routenmanagement fallen nicht in den Geltungsbereich dieser Risikoanalyse.                                                                                                                     | DS6<br><br>DS8 [O1], DS9 [O3], DS10 [F1OEM], DS12 [S3 F2OEM], DS13s [S3], DS15 [F2OEM], DS16 [F2OEM], DS17 [O0], DS21 [O3], DS13f [F3OEM]                                                             |   |   |   | DS13s, DS12, DS6<br><br>DS8 [O1], DS9 [O3], DS10 [F1OEM], DS15 [F2OEM], DS16 [F2OEM], DS17 [O0], DS21 [O3], DS13f [F3OEM]                                                                |   |    |   |
| R189: T82 Extraktion von Daten aus technischen Überwachungsgeräten                                | C24 Absicherung technischer Überwachungsgeräte                                                                                                                                                                                                         | DS1 [P2], DS16 [F2OEM]                                                                                                                                                                                | E | H | 4 | DS1 [P2], DS16 [F2OEM]                                                                                                                                                                   | E | SG | 2 |
| R190: T83 Denial-of-Service-Angriff auf technische Überwachungsausrüstung                         | C5A Eigensicherheit des Trucks (gegen Störungen)<br>C24 Härtung der technischen Überwachungsausrüstung<br>C26 Redundanz gegen Ausfall/Störung der technischen Überwachungsausrüstung<br><br>A10 Durch CC ausgelöste MRM sind nicht sicherheitskritisch | DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS13s [S3], DS17 [O0], DS21 [O3], DS13f [F3OEM]<br><br>DS6<br><br>DS8 [O1], DS9 [O3], DS10 [F1OEM], DS13s [S3], DS17 [O0], DS21 [O3], DS13f [F3OEM] | S | H | 5 | DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS13s [S3], DS17 [O0], DS21 [O3], DS13f [F3OEM]<br><br>DS13s, DS13f, DS6<br><br>DS8 [O1], DS9 [O3], DS10 [F1OEM], DS17 [O0], DS21 [O3] | S | SG | 2 |
| R191: T84 Manipulation von Daten, Parametern oder Software der technischen Überwachungsausrüstung | C5I Eigensicherheit des Trucks (gegen Spoofing/Manipulation)<br>C20 ADS-Sicherheitsvalidierungen nach Entscheidungen des Control Centers<br>C24 Härtung der technischen                                                                                | DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS12 [S3 F2OEM], DS13s [S3], DS15 [F2OEM], DS17 [O0], DS21 [O3],                                                                                    | S | H | 5 | DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS12 [S3 F2OEM], DS13s [S3], DS15 [F2OEM], DS17 [O0], DS21 [O3],                                                                       | S | SG | 2 |

|                                                                                                                                                                  |                                                                                                                                                                                                                                                    |                                                                                                                         |   |   |   |                                                                                                         |   |    |   |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------|---|---|---|---------------------------------------------------------------------------------------------------------|---|----|---|
|                                                                                                                                                                  | Überwachungsausrüstung                                                                                                                                                                                                                             | DS13f [F3OEM]                                                                                                           |   |   |   | DS13f [F3OEM]                                                                                           |   |    |   |
|                                                                                                                                                                  | A10 Durch CC ausgelöste MRM sind nicht sicherheitskritisch                                                                                                                                                                                         | DS6<br>DS8 [O1], DS9 [O3], DS10 [F1OEM], DS12 [S3 F2OEM], DS13s [S3], DS15 [F2OEM], DS17 [O0], DS21 [O3], DS13f [F3OEM] |   |   |   | DS13s, DS12, DS6<br>DS8 [O1], DS9 [O3], DS10 [F1OEM], DS15 [F2OEM], DS17 [O0], DS21 [O3], DS13f [F3OEM] |   |    |   |
| R192: T85 Extraktion von Daten aus C2 und Vorbereitung der Konnektivität durch P1ec Unbefugter physischer Zugriff auf die AWS-Cloud (Extraktion von Komponenten) | A8 Vertrauliche Daten werden nur während der Übertragung verarbeitet und nicht gespeichert                                                                                                                                                         | DS1 [P2], DS16 [F2OEM]<br>DS1, DS16, DS18                                                                               |   | H | 1 | DS1 [P2], DS16 [F2OEM]<br>DS1, DS16, DS18                                                               |   | H  | 1 |
| R193: T85 Extraktion von Daten aus C2 und Konnektivitätsvorbereitung durch P2e Ausnutzung von Software-Schwachstellen von C2 und Konnektivität (Abhören)         | C18 Absicherung von Komponenten mit Internetanschluss gegen Software-Schwachstellen<br>C27 End-to-End-verschlüsselte Übertragung sensibler Daten zwischen technischen Überwachungsgeräten, Lkw, externen Partnern und dynamischem Routenmanagement | DS1 [P2], DS16 [F2OEM]                                                                                                  | E | H | 4 | DS1 [P2], DS16 [F2OEM]                                                                                  | E | SG | 2 |
| R194: T86 Denial-of-Service-Angriff auf C2 und Konnektivität                                                                                                     | C23 Schutz vor Distributed-Denial-of-Service-Angriffen (DDoS) für Komponenten mit Internetanbindung                                                                                                                                                | DS8 [O1], DS9 [O3], DS17 [O0], DS21 [O3]                                                                                | S | H | 5 | DS8 [O1], DS9 [O3], DS17 [O0], DS21 [O3]                                                                | S | SG | 2 |

|                                                                                                                                                                                            |                                                                                                                                                                                                                                                 |                                                                         |   |   |   |                                                                                                                                                                 |   |    |   |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------|---|---|---|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|---|----|---|
| R195: T86 Denial-of-Service-Angriff auf C2 und Konnektivitätsvorbereitung durch P1dc Unbefugter physischer Zugriff auf die AWS Cloud (Störung der Komponente)                              | <p>C23 Schutz vor Distributed-Denial-of-Service-Angriffen (DDoS) für internetbasierte Komponenten</p> <p>A12 AWS schützt die Verfügbarkeit der Cloud-Infrastruktur</p>                                                                          | DS8 [O1], DS9 [O3], DS17 [O0], DS21 [O3]                                | S | H | 2 | DS8 [O1], DS9 [O3], DS17 [O0], DS21 [O3]                                                                                                                        | S | SG | 2 |
| R196: T86 Denial-of-Service-Angriff auf C2 und Konnektivitätsvorbereitung durch P2d Ausnutzen von Software-Schwachstellen von C2 und Konnektivität (Störung)                               | <p>C23 Schutz vor Distributed-Denial-of-Service-Angriffen (DDoS) für internetbasierte Komponenten</p> <p>C18 Absicherung internetbasierter Komponenten gegen Software-Schwachstellen</p> <p>C29 Ausfallsicherheit/Sicherheit durch Vielfalt</p> | DS8 [O1], DS9 [O3], DS17 [O0], DS21 [O3]                                | S | H | 5 | DS8 [O1], DS9 [O3], DS17 [O0], DS21 [O3]                                                                                                                        | S | SG | 2 |
| R197: T87 Manipulation von Daten, Parametern oder Software von C2 und Konnektivitätsvorbereitung durch P1mc Unbefugter physischer Zugriff auf die AWS Cloud (Manipulation von Komponenten) | <p>C5I Intrinsische Sicherheit des Lkw (gegen Spoofing/Manipulation)</p> <p>C20 ADS-Sicherheitsvalidierungen nach Entscheidungen des Control Centers</p> <p>C30 Befolgung der AWS-Sicherheitsbest Practices</p>                                 | DS8 [O1], DS9 [O3], DS12 [S3 F2OEM], DS15 [F2OEM], DS17 [O0], DS21 [O3] | S | H | 5 | <p>DS8 [O1], DS9 [O3], DS12 [S3 F2OEM], DS15 [F2OEM], DS17 [O0], DS21 [O3]</p> <p>DS13s, DS12</p> <p>DS8 [O1], DS9 [O3], DS15 [F2OEM], DS17 [O0], DS21 [O3]</p> | S | SG | 2 |
| R198: T87 Manipulation von Daten, Parametern oder Software von C2 und Konnektivitätsvorbereitung durch                                                                                     | C5I Intrinsische Sicherheit des Lkw (gegen Spoofing/Manipulation)                                                                                                                                                                               | DS8 [O1], DS9 [O3], DS12 [S3 F2OEM],                                    | S | H | 5 | DS8 [O1], DS9 [O3], DS12 [S3 F2OEM], DS15 [F2OEM], DS17                                                                                                         | S | SG | 2 |

|                                                                                                                                                                   |                                                                                                                                                                                                                                                                                                                                                |                                                             |   |   |   |                                                                                                            |   |    |   |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------|---|---|---|------------------------------------------------------------------------------------------------------------|---|----|---|
| P2m Ausnutzung von Software-Schwachstellen von C2 und Konnektivität (Manipulation)                                                                                | C20 ADS-Sicherheitsvalidierungen nach Entscheidungen des Control Centers<br>C18 Absicherung von Komponenten mit Internetanschluss gegen Software-Schwachstellen<br>C28 Durchgängige authentische Datenübertragung zwischen technischer Überwachungsausrüstung, Lkw, Kunden-/Flottenmanagement, externen Partnern, dynamischem Routenmanagement | DS15 [F2OEM], DS17 [O0], DS21 [O3]                          |   |   |   | [O0], DS21 [O3]<br>_____<br>DS13s, DS12<br>_____<br>DS8 [O1], DS9 [O3], DS15 [F2OEM], DS17 [O0], DS21 [O3] |   |    |   |
| R199: T88 Extraktion von Daten aus dem Connectivity Eventbus, vorbereitet durch P1ec Unbefugter physischer Zugriff auf die AWS Cloud (Extraktion von Komponenten) | A8 Vertrauliche Daten werden nur während der Übertragung verarbeitet und nicht gespeichert                                                                                                                                                                                                                                                     | DS1 [P2], DS16 [F2OEM]<br>_____<br>DS1, DS16, DS18<br>_____ |   | H | 1 | DS1 [P2], DS16 [F2OEM]<br>_____<br>DS1, DS16, DS18<br>_____                                                |   | H  | 1 |
| R200: T89 Denial-of-Service-Angriff auf Connectivity Eventbus, vorbereitet von P1dc Unbefugter physischer Zugriff auf die AWS Cloud (Störung der Komponente)      | A12 AWS schützt die Verfügbarkeit der Cloud-Infrastruktur                                                                                                                                                                                                                                                                                      | DS8 [O1], DS9 [O3], DS17 [O0], DS21 [O3]                    | S | H | 2 | DS8 [O1], DS9 [O3], DS17 [O0], DS21 [O3]                                                                   | S | H  | 2 |
| R201: T89 Denial-of-Service-Angriff auf Connectivity Eventbus, vorbereitet von P2d Ausnutzung von Software-Schwachstellen von C2 und Connectivity (Störung)       | C18 Absicherung von Komponenten mit Internetanschluss gegen Software-Schwachstellen<br>C29 Widerstandsfähigkeit/Sicherheit durch Vielfalt<br>_____                                                                                                                                                                                             | DS8 [O1], DS9 [O3], DS17 [O0], DS21 [O3]                    | S | H | 2 | DS8 [O1], DS9 [O3], DS17 [O0], DS21 [O3]                                                                   | S | SG | 2 |

|                                                                                                                                                                                  |                                                                                                                                                                                                                                        |                                                                                                      |   |   |   |                                                                                                                                                                 |   |    |   |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------|---|---|---|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|---|----|---|
|                                                                                                                                                                                  | A16 Vorbereitende Schritte verursachen bereits gleiche oder höhere Schäden                                                                                                                                                             |                                                                                                      |   |   |   |                                                                                                                                                                 |   |    |   |
| R202: T89 Denial-of-Service-Angriff auf Connectivity Eventbus, vorbereitet durch P4d Ausnutzung von Software-Schwachstellen des Vehicle Adapter Service (Störung),               | <p>C18 Absicherung von Komponenten mit Internetanschluss gegen Software-Schwachstellen</p> <p>C29 Widerstandsfähigkeit/Sicherheit durch Vielfalt</p> <p>A16 Vorbereitende Schritte verursachen bereits gleiche oder höhere Schäden</p> | DS8 [O1], DS9 [O3], DS17 [O0], DS21 [O3]                                                             | S | H | 2 | DS8 [O1], DS9 [O3], DS17 [O0], DS21 [O3]                                                                                                                        | S | SG | 2 |
| R203: T90 Manipulation von Daten, Parametern oder Software von Connectivity Eventbus prep. durch P1mc Unbefugter physischer Zugriff auf AWS Cloud (Manipulation von Komponenten) | <p>C5I Intrinsische Sicherheit des Lkw (gegen Spoofing/Manipulation)</p> <p>C20 ADS-Sicherheitsvalidierungen nach Entscheidungen des Control Centers</p> <p>C30 Befolgung der AWS-Sicherheitsbest Practices</p>                        | DS8 [O1], DS9 [O3], DS12 [S3 F2OEM], DS15 [F2OEM], DS17 [O0], DS21 [O3]                              | S | H | 5 | <p>DS8 [O1], DS9 [O3], DS12 [S3 F2OEM], DS15 [F2OEM], DS17 [O0], DS21 [O3]</p> <p>DS13s, DS12</p> <p>DS8 [O1], DS9 [O3], DS15 [F2OEM], DS17 [O0], DS21 [O3]</p> | S | SG | 2 |
| R204: T91 Angriffe auf oder von dem Lkw ausgehend                                                                                                                                | A1 Angriffe auf den Lkw fallen nicht in den Umfang dieser Risikoanalyse.                                                                                                                                                               | DS1 [P2], DS5 [O2], DS6 [S3 F2OEM], DS7 [O2], DS8 [O1], DS11 [O1], DS12 [S3 F2OEM], DS13s [S3], DS14 | S | H | 2 | DS1 [P2], DS5 [O2], DS6 [S3 F2OEM], DS7 [O2], DS8 [O1], DS11 [O1], DS12 [S3 F2OEM], DS13s [S3], DS14                                                            | S | H  | 2 |

|                                                                                    |                                                                                                                                                                                                                                                                               | [F0RU], DS18 [F1RU],<br>DS13f [F3OEM]                                                                                                                                                                                                                                                                                                                       |   |   |   | [F0RU], DS18 [F1RU],<br>DS13f [F3OEM]                                                                                                                                                                                                                                                                                                       |   |   |   |
|------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|---|---|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|---|---|
| R205: T92 Angriffe auf die AWS Cloud, vorbereitet durch P13 Physische Bedrohungen  | C5I Intrinsische Sicherheit des Trucks (gegen Spoofing/Manipulation)<br>C20 ADS-Sicherheitsvalidierungen nach Entscheidungen des Control Centers<br>A10 Durch CC ausgelöste MRM sind nicht sicherheitskritisch.<br>A12 AWS schützt die Verfügbarkeit der Cloud-Infrastruktur. | DS1 [P2], DS4 [F2OEM], DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS12 [S3 F2OEM], DS13s [S3], DS15 [F2OEM], DS16 [F2OEM], DS17 [O0], DS19 [P2], DS21 [O3], DS13f [F3OEM]<br>DS6<br>DS1 [P2], DS4 [F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS12 [S3 F2OEM], DS13s [S3], DS15 [F2OEM], DS16 [F2OEM], DS17 [O0], DS19 [P2], DS21 [O3], DS13f [F3OEM] | S | H | 2 | DS1 [P2], DS4 [F2OEM], DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS12 [S3 F2OEM], DS13s [S3], DS15 [F2OEM], DS16 [F2OEM], DS17 [O0], DS19 [P2], DS21 [O3], DS13f [F3OEM]<br>DS13s, DS12, DS6<br>DS1 [P2], DS4 [F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS15 [F2OEM], DS16 [F2OEM], DS17 [O0], DS19 [P2], DS21 [O3], DS13f [F3OEM] | S | H | 2 |
| R206: T92 Angriffe auf die AWS Cloud Vorbereitung durch P14 Natürliche Bedrohungen | C5I Intrinsische Sicherheit des Trucks (gegen Spoofing/Manipulation)<br>C20 ADS-Sicherheitsvalidierungen nach Entscheidungen des Control Centers                                                                                                                              | DS1 [P2], DS4 [F2OEM], DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS12 [S3 F2OEM], DS13s [S3], DS15 [F2OEM], DS16 [F2OEM], DS17                                                                                                                                                                                                                      | S | H | 2 | DS1 [P2], DS4 [F2OEM], DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS12 [S3 F2OEM], DS13s [S3], DS15 [F2OEM], DS16 [F2OEM], DS17                                                                                                                                                                                                      | S | H | 2 |

|                                                                                   |                                                                                                                                                                                                                                                                                                  |                                                                                                                                                                                                                                                                                                               |   |   |   |                                                                                                                                                                                                                                                                                                                        |   |   |   |
|-----------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|---|---|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|---|---|
|                                                                                   | <p>A10 Durch CC ausgelöste MRM sind nicht sicherheitskritisch.</p> <p>A12 AWS schützt die Verfügbarkeit der Cloud-Infrastruktur.</p>                                                                                                                                                             | <p>[O0], DS19 [P2], DS21 [O3], DS13f [F3OEM]</p> <p>DS6</p> <p>DS1 [P2], DS4 [F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS12 [S3 F2OEM], DS13s [S3], DS15 [F2OEM], DS16 [F2OEM], DS17 [O0], DS19 [P2], DS21 [O3], DS13f [F3OEM]</p>                                                                           |   |   |   | <p>[O0], DS19 [P2], DS21 [O3], DS13f [F3OEM]</p> <p>DS13s, DS12, DS6</p> <p>DS1 [P2], DS4 [F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS15 [F2OEM], DS16 [F2OEM], DS17 [O0], DS19 [P2], DS21 [O3], DS13f [F3OEM]</p>                                                                                                    |   |   |   |
| R207: T92 Angriffe auf die AWS Cloud Vorbereitung durch P15 Infrastrukturausfälle | <p>C5I Intrinsische Sicherheit des Trucks (gegen Spoofing/Manipulation)</p> <p>C20 ADS-Sicherheitsvalidierungen nach Entscheidungen des Control Centers</p> <p>A10 Durch CC ausgelöste MRM sind nicht sicherheitskritisch.</p> <p>A12 AWS schützt die Verfügbarkeit der Cloud-Infrastruktur.</p> | <p>DS1 [P2], DS4 [F2OEM], DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS12 [S3 F2OEM], DS13s [S3], DS15 [F2OEM], DS16 [F2OEM], DS17 [O0], DS19 [P2], DS21 [O3], DS13f [F3OEM]</p> <p>DS6</p> <p>DS1 [P2], DS4 [F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS12 [S3 F2OEM], DS13s [S3], DS15 [F2OEM],</p> | S | H | 2 | <p>DS1 [P2], DS4 [F2OEM], DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS12 [S3 F2OEM], DS13s [S3], DS15 [F2OEM], DS16 [F2OEM], DS17 [O0], DS19 [P2], DS21 [O3], DS13f [F3OEM]</p> <p>DS13s, DS12, DS6</p> <p>DS1 [P2], DS4 [F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS15 [F2OEM], DS16 [F2OEM], DS17 [O0],</p> | S | H | 2 |



|                                                                                 |                                                                                                                                                                                                                                                                                                  |                                                                                                                                                                                                                                                                                                                                                                            |   |   |   |                                                                                                                                                                                                                                                                                                                                                            |   |   |   |
|---------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|---|---|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|---|---|
|                                                                                 |                                                                                                                                                                                                                                                                                                  | DS16 [F2OEM], DS17 [O0], DS19 [P2], DS21 [O3], DS13f [F3OEM]                                                                                                                                                                                                                                                                                                               |   |   |   | DS19 [P2], DS21 [O3], DS13f [F3OEM]                                                                                                                                                                                                                                                                                                                        |   |   |   |
| R208: T92 Angriffe auf die AWS Cloud Vorbereitung durch P16 Technische Ausfälle | <p>C5I Intrinsische Sicherheit des Trucks (gegen Spoofing/Manipulation)</p> <p>C20 ADS-Sicherheitsvalidierungen nach Entscheidungen des Control Centers</p> <p>A10 Durch CC ausgelöste MRM sind nicht sicherheitskritisch.</p> <p>A12 AWS schützt die Verfügbarkeit der Cloud-Infrastruktur.</p> | <p>DS1 [P2], DS4 [F2OEM], DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS12 [S3 F2OEM], DS13s [S3], DS15 [F2OEM], DS16 [F2OEM], DS17 [O0], DS19 [P2], DS21 [O3], DS13f [F3OEM]</p> <p>DS6</p> <p>DS1 [P2], DS4 [F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS12 [S3 F2OEM], DS13s [S3], DS15 [F2OEM], DS16 [F2OEM], DS17 [O0], DS19 [P2], DS21 [O3], DS13f [F3OEM]</p> | S | H | 2 | <p>DS1 [P2], DS4 [F2OEM], DS6 [S3 F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS12 [S3 F2OEM], DS13s [S3], DS15 [F2OEM], DS16 [F2OEM], DS17 [O0], DS19 [P2], DS21 [O3], DS13f [F3OEM]</p> <p>DS13s, DS12, DS6</p> <p>DS1 [P2], DS4 [F2OEM], DS8 [O1], DS9 [O3], DS10 [F1OEM], DS15 [F2OEM], DS16 [F2OEM], DS17 [O0], DS19 [P2], DS21 [O3], DS13f [F3OEM]</p> | S | H | 2 |

## 2.2 Wichtige Positionen des zahlungsmäßigen Nachweises

Die bewilligten Mittel wurden im Wesentlichen für folgende Kostenarten eingesetzt:

- **Personalkosten (Pos. 0837):** größter Anteil der Zuwendung; Finanzierung des wissenschaftlichen Personals und studentischer Hilfskräfte, die die methodische Weiterentwicklung, die Risikoanalysen, die Entwicklung der Prototypen und die wissenschaftliche Verwertung durchgeführt haben.
- **Reise- und Tagungskosten (Pos. 0838):** vorgesehen waren u. a. mehrere Projekt- und Konsortialtreffen, Abstimmungen mit Partnern sowie Besuche nationaler und internationaler Fachkonferenzen. Im Projektverlauf wurden zahlreiche Veranstaltungen pandemiebedingt oder organisatorisch auf Online-/Hybridformate umgestellt; zusätzlich wurden Konsortial-, Steuerkreis- und AP-Meetings überwiegend als Videokonferenz durchgeführt. Dadurch blieb die Zahl physischer Dienstreisen deutlich hinter der ursprünglichen Planung zurück. Entsprechend liegen die tatsächlichen Reisekosten um mehr als 20 % unter dem in der Vorkalkulation angesetzten Betrag. Inhaltlich konnten alle geplanten Abstimmungen dennoch vollumfänglich durchgeführt werden.
- **Sonstige Kosten (Pos. 0850):** in der Vorkalkulation waren hierfür insbesondere der Erwerb einschlägiger Normen und Standards (z. B. ISO/SAE 21434, ISO 26262, IEC-62443-Reihe, ISO/IEC-27000-Familie), Lizenzen für Software-Entwicklungsumgebungen und -Tools (Enterprise Architect, SharePoint/Power-Automate) sowie anteilige Kosten für ein Projektbüro vorgesehen. Die tatsächlichen Ausgaben fielen aus mehreren Gründen niedriger aus:
  - ein Teil der benötigten Standards war institutsweit bereits vorhanden oder konnte zentral über Fraunhofer-Bibliothekslizenzen (Nautos) bezogen werden,
  - bei der Umsetzung des SharePoint-basierten Security-Management-Prototyps konnten überwiegend vorhandene Microsoft-365-Lizenzen genutzt werden, sodass keine zusätzlichen Enterprise-Architect-Lizenzen in der ursprünglich geplanten Anzahl notwendig waren.

Investive Ausgaben für langlebige, vorhabensspezifische Anlagen wurden nicht getätigt. Die Mittelverwendung entspricht damit der im Antrag vorgesehenen Kostenstruktur; Restmittel sind im zahlenmäßigen Verwendungsnachweis ausgewiesen und mit dem Projektträger abgestimmt.

## 2.3 Darstellung der Notwendigkeit und Angemessenheit der geleisteten Arbeit

Die geleisteten Arbeiten waren notwendig, um die ambitionierten Ziele des Verbundprojekts ATLAS-L4 im Bereich der Cybersicherheit zu erreichen. Die Entwicklung und Absicherung eines L4-fähigen Lkw mit cloudbasiertem Control Center und komplexer Vernetzung (Backend, Produktion, Infrastruktur) erfordert spezialisierte Methoden zur Security-Risikoanalyse, tiefgehende Standardanalysen sowie die Entwicklung geeigneter Test- und Managementwerkzeuge. Ohne diese Vorarbeiten wäre eine normkonforme, nachvollziehbare Umsetzung der Security-Anforderungen und eine spätere Integration in CSMS-/ISMS-/IACS-Programme der Partner nicht möglich gewesen.

Die eingesetzten Ressourcen (Personalkapazitäten, Reisen, Infrastruktur) standen in einem angemessenen Verhältnis zu Umfang und Komplexität der Aufgaben. Die Arbeiten wurden im Wesentlichen entlang der im Zuwendungsbescheid und der Vorhabenbeschreibung beschriebenen

Arbeitspakete umgesetzt; inhaltliche Vertiefungen und kleinere Anpassungen erfolgten im Rahmen der Projektziele und in Abstimmung mit dem Projektträger. Zusätzliche Mittel über die bewilligte Zuwendung hinaus wurden nicht benötigt. Effizienzgewinne ergaben sich durch enge Abstimmung mit anderen Projekten und Vorarbeiten (z. B. zu MoRA, gallia, Woodpecker), sodass Doppelarbeiten vermieden werden konnten.

## 2.4 Nutzen und Verwertbarkeit der Ergebnisse

Die im Teilvorhaben „Security-Umfänge“ erzielten Ergebnisse leisten einen direkten Beitrag zur sicheren Einführung hoch- und vollautomatisierter Nutzfahrzeuge und sind zugleich breit verwertbar. Kernnutzen sind (i) die an den ATLAS-L4-Kontext angepasste MoRA-Security-Risikoanalyse-Methode (AP 2.1), (ii) der übergreifende Vergleich und die Harmonisierung von Security-Standards über Fahrzeug, Backend und Produktion hinweg (AP 2.2) sowie (iii) das prototypische, bereichsübergreifende Security-Management-Werkzeug auf Basis von Microsoft 365 (AP 2.3). Ergänzend liefern die technischen Arbeiten (u. a. zu V2X-Security-Tests, gallia, Testsystemen für Ladekommunikation, Industrial-Ethernet-Security und Woodpecker für SAST) konkrete Bausteine für Security-Analysen und -Tests in der Automobilpraxis.

Das Teilvorhaben wurde ausschließlich im nicht-wirtschaftlichen Bereich durchgeführt. Der partnerspezifische Verwertungsplan des Fraunhofer AISEC bleibt weiterhin gültig; die dort beschriebenen anwendungsbezogenen Erfolgsaussichten werden durch die im Projekt erzielten wissenschaftlich-technischen Ergebnisse untermauert. Die im Vorhaben weiterentwickelte Security-Risikoanalyse-Methode (AP 2.1) sowie die Arbeiten zu Security-Standards und bereichsübergreifendem Security-Management (AP 2.2 und 2.3) wurden im Rahmen von ATLAS-L4 als methodische Bausteine, Konzeptstudien und Prototypen erarbeitet. Parallel laufende, eigen- bzw. auftragsfinanzierte Unterstützungsprojekte mit Automobilherstellern konnten auf diesen allgemeinen Kompetenzaufbau zurückgreifen, wurden jedoch organisatorisch und finanziell strikt getrennt vom ATLAS-L4-Vorhaben abgewickelt und nicht über die Zuwendung abgerechnet.

Mittelfristig können die weiterentwickelte MoRA-Methode und die im Projekt aufgebauten Kataloge (Annahmen, Bedrohungen, Maßnahmen) regulär in weiteren Risiko- und IT-Sicherheitsanalysen von OEMs und Zulieferern eingesetzt werden, insbesondere in vorwettbewerblichen Forschungs- und Transferprojekten sowie Standardisierungsgremien. Das prototypische, SharePoint basierte Security Management Werkzeug dient als Grundlage für interne und kundenspezifische Weiterentwicklungen hin zu vollwertigen CSMS-/ISMS nahen Lösungen (z. B. Integration in bestehende Tool Landschaften, Erweiterung der Workflows, Individualisierung der Sichten). Hieraus ergeben sich weitere Potenziale in Form von Beratungs-, Integrations- und Schulungsleistungen außerhalb des geförderten nicht-wirtschaftlichen Vorhabens.

Die entwickelten Test- und Analysewerkzeuge – etwa das C-ITS/V2X-Testframework, das Testsystem für Ladekommunikation, die Erweiterungen von gallia für Diagnose-Security-Tests sowie der modulare SAST-Baukasten Woodpecker – können in Folgeprojekten und industriefinanzierten Dienstleistungen für Security-Tests von Fahrzeugen, Ladeinfrastruktur, Backend-Systemen und OT-Netzen eingesetzt werden. Durch die (geplante bzw. teilweise bereits erfolgte) Open-Source-Bereitstellung ausgewählter Komponenten wird zugleich eine breite externe Nutzung ermöglicht und die Position des Fraunhofer AISEC als Ansprechpartner für Automotive-Security-Werkzeuge gestärkt.

Wissenschaftlich wurden und werden die Ergebnisse in Form von begutachteten Konferenz- und Journalbeiträgen (u. a. zu Privacy-Enhancing Technologies im Fahrzeug, zu Resilienzmessung in Ethernet-/TSN-Netzen, zu Group-Key-Agreement-Protokollen für CPS-Busse sowie zu bereichsübergreifendem Cybersicherheits-Risikomanagement) verwertet und fließen in Dissertationen und studentische Abschlussarbeiten ein. Über die enge Kooperation mit der Technischen Universität München und weiteren Hochschulen werden Methoden und Werkzeuge in Lehrveranstaltungen und Praktika genutzt und tragen damit zur Ausbildung zukünftiger Cybersicherheitsexpertinnen und -experten bei.

Die im Projekt aufgebauten Kompetenzen sind darüber hinaus auf andere Domänen übertragbar. Die Ergebnisse der Standardanalyse und des bereichsübergreifenden Security-Managements können in Industrie-4.0-/OT-Projekten, im Bereich kritischer Infrastrukturen und in weiteren CPS-Anwendungen genutzt werden. Insgesamt schafft das Teilvorhaben damit sowohl die Grundlage für weitere Forschungs- und Industrieprojekte als auch für eine nachhaltige Nutzung der entwickelten Methoden, Werkzeuge und Referenzlösungen über die Laufzeit von ATLAS-L4 hinaus. Etwaige wirtschaftliche Nutzungen erfolgen – im Einklang mit der Gemeinnützigkeit der Fraunhofer-Gesellschaft – außerhalb des geförderten nicht-wirtschaftlichen Vorhabens und dienen der weiteren Erfüllung des satzungsgemäßen Forschungs- und Transferauftrags.

## **2.5 Bekannt gewordener Fortschritt auf dem Gebiet des Vorhabens bei anderen Stellen**

Während der Projektlaufzeit wurde der nationale und internationale Forschungs- und Entwicklungsstand fortlaufend beobachtet. Hierzu wurden regelmäßig einschlägige Literatur- und Patentdatenbanken (u. a. Scopus, Web of Science, IEEE Xplore, ACM Digital Library, SpringerLink, Google Scholar) sowie relevante Normungs- und Regulierungsvorhaben (ISO/SAE, ISO/IEC, IEC, UNECE, EU) ausgewertet.

Die identifizierten Arbeiten betrafen insbesondere:

- Weiterentwicklungen im Bereich Automotive- und Backend-Security,
- neue Ansätze für Risiko- und Compliance-Management,
- Fortschritte bei Privacy-Enhancing Technologies und Post-Quantum-Kryptographie,
- neue Test- und Analysewerkzeuge (z. B. für V2X, Ladekommunikation, mobile Applikationen) sowie
- die Entstehung neuer Regulierungsrahmen (EU AI Act, Cyber Resilience Act, Data Act, nationale Datenschutzgesetze).

Wesentliche Ergebnisse Dritter machten keine grundlegende Änderung des Arbeitsprogramms erforderlich, wurden aber bei der Ausgestaltung der eigenen Methoden, Risikoanalysen und Empfehlungen berücksichtigt. Dadurch konnte das Teilvorhaben jederzeit am aktuellen Stand von Wissenschaft und Technik anknüpfen.

## **2.6 Erfolgte oder geplante Veröffentlichungen**

Die im Teilvorhaben erzielten Ergebnisse werden wissenschaftlich und praktisch verwertet. Wesentliche Veröffentlichungs- und Transferaktivitäten sind:

- P. Wagner, N. Puch und D. Emeis, „Cybersecurity risk analysis of an automated driving system,“ in 21th escar Europe: The World’s Leading Automotive Cyber Security Conference, Hamburg, 15.–16.11.2023, 2023.
- P. Wagner, „Cross-Divisional Cybersecurity Risk Management in Automotive: Requirements and Current Practices,“ in Proceedings of the 2025 IEEE 30th International Conference on Emerging Technologies and Factory Automation (ETFA), 2025.
- **Group Key Agreement (GRACYBUS):** Das entwickelte GKA-Protokoll wurde bereits als Pre-print publiziert; eine vertiefte Ausarbeitung für ein Fachjournal oder eine Top-Konferenz ist für Q1 2026 vorgesehen: S. N. Peters, L. Lautenschlager, D. Emeis, and J. Lochert, „Secure Group Key Agreement on Cyber-Physical System Buses,“ *arXiv preprint*, Jan. 2026.
- **Privacy-Enhancing Technologies:** Die Inhalte der Unterkapitel zu „Technologien zum Schutz der Privatsphäre für vernetzte Automobilumgebungen“ sollen in Form eines Systematization-of-Knowledge-Papers auf einer einschlägigen Konferenz (z. B. ACM WiSec 2026) publiziert werden.
- **Testen von Resilienzeigenschaften in Ethernet-/TSN-Netzen:** Die in den Abschnitten zu Testen von Resilienzeigenschaften in Ethernet-Netzwerken dargelegten Methoden und Ergebnisse sollen zusätzlich in einem wissenschaftlichen Konferenzpapier veröffentlicht werden.
- **C-ITS Testing Framework:** Zurzeit wird die Veröffentlichung (von Teilen) des C-ITS Testing Framework geprüft. Dabei ist die sensible Natur derartiger Werkzeuge zu beachten, um auszuschließen, dass damit böartigen Angreifern neue, potente Werkzeuge an die Hand gegeben werden. Begleitend wird eine Vorstellung auf technischen Fachkonferenzen erwogen.
- **Open-Source-Veröffentlichungen:** Erweiterungen von gallia werden sukzessive als Open Source bereitgestellt bzw. in das bestehende Repositorium zurückgespielt. Für den Woodpecker-Baukasten und das SARIF-Editor-Plugin für VS Code ist eine Open-Source-Veröffentlichung geplant. Diese Bereitstellung unterstützt die Nachnutzbarkeit der im Projekt erzielten Ergebnisse in der Automotive-Domäne.
  - Teile der Erweiterungen von gallia wurden zudem in folgender Dissertation aufgenommen: S. Tatschner, „Towards a more sustainable and secure software tooling in free/libre open source software environments,“ Ph.D. dissertation, University of Limerick, Limerick, Ireland, 2025.
- **Dissertationen und Abschlussarbeiten:** Inhalte des Teilvorhabens fließen in mehrere laufende und geplante Dissertationen der beteiligten wissenschaftlichen Mitarbeitenden ein sowie in studentische Abschlussarbeiten (Bachelor/Master), die an den Partnerhochschulen betreut werden.

Damit ist sichergestellt, dass die erzielten Ergebnisse sowohl in der wissenschaftlichen Gemeinschaft als auch in der industriellen Praxis nachhaltig sichtbar und nutzbar werden.