

Schlussbericht

zum Vorhaben

Datenbasierte EntwurfsUNterstützung durch kontinuierliches
MOnitoring Von SichERheitsvorfällen (UNCOVER)



FÖRDERKENNZEICHEN 16KIS1410K



FZI Forschungszentrum Informatik

Haid-und-Neu-Str. 10-14

76131 Karlsruhe

Autoren: Victor Pazmino Betancourt, Laurenz Adolph, Maximilian Kirschner, Carl Philipp Hohl,
Daniel Vonderau

Telefon: +49 721 9654-190

E-Mail: pazmino@fzi.de

Inhaltsverzeichnis

Schlussbericht.....	1
1 Thema und Zielsetzung des Vorhabens	5
1.1 Zielsetzung des Teilvorhabens.....	7
1.2 Voraussetzungen der Vorhabensdurchführung	8
1.3 Planung und Ablauf des Vorhabens.....	10
1.4 Stand der Wissenschaft und Technik zu Beginn des Vorhabens	11
1.5 Angaben bekannter Konstruktionen, Verfahren und Schutzrechte, die für die Durchführung des Vorhabens benutzt wurden	12
1.6 Zusammenarbeit mit anderen Stellen	12
2 Ergebnisse	13
2.1 AP1: Use Case Definition und Anforderungen an die Daten und Sicherheitsanalysen	13
2.1.1 Motivation und Gesamtprozess	13
2.1.2 Szenarien für kontinuierliche Entwicklung	14
2.1.3 Daten und Sicherheitsanalyse	15
2.2 AP2: Methoden und Werkzeug für kontinuierliche Security- und Safety-Analysen basierend auf den Erkenntnissen aus Security- und Safety-Vorfällen	15
2.2.1 Überblick über den Analyseprozess	16
2.2.2 Festlegung von Daten, Modellen und Schnittstellen	18
2.2.3 Automatische Analyse.....	18
2.2.4 Händische Analyse	19
2.3 AP3: Monitoring-Plattform zur Erkennung von Security- und Safety-Vorfällen	20
2.3.1 Überblick über die Monitoring Plattform	20
2.3.2 Kontinuierliche Entwicklung von HW/SW Systemen für E/E-Architekturen.....	21
2.3.3 Überführung von Änderungen und Analysen auf HW/SW Systeme und Monitoring Plattform	23
2.3.4 Framework für kontinuierliche Entwicklung und Deployment von HW/SW-Systemen ...	24
2.4 AP4: Methoden für datengetriebene Unterstützung der Entwurfsphase	27
2.4.1 Konzept und Methodik für datengetriebene Entwurfsunterstützung – Analysemethoden, Taxonomie und Metadaten.....	28
2.4.2 Ansätze zur Integration in eine modellbasierte Entwicklungsumgebung	29
2.4.3 Ansätze zur Integration in einen modellbasierten Entwurf.....	30

2.5	AP5: Datenschutzrechtliche Betrachtung.....	33
2.5.1	Rechtswissenschaftliche Analyse und Sachverhaltsmodellierung.....	33
2.5.2	Konzeption/Modellierung Überführung der Anforderungen.....	36
2.5.3	Handlungsempfehlungen.....	38
2.6	AP6: Evaluation und Demonstration	39
2.6.1	UNCOVER Prozess.....	39
2.6.2	Simulation und CAN Bridge	40
2.6.3	Monitoring Plattform	40
2.6.4	Manuelle Analyse.....	41
3	Nutzen und Verwertbarkeit der Ergebnisse und Erfahrungen	42
4	Fortschritt auf dem Gebiet an anderer Stelle	43
5	Veröffentlichung der Ergebnisse und Publikationen.....	44

Abbildungsverzeichnis

Abbildung 1: Big Picture des Projekts	6
Abbildung 2: Arbeitspaketübersicht und Informationsfluss.....	10
Abbildung 3: Gesamtprozess	13
Abbildung 4: Fahrscenarien	14
Abbildung 5: Gesamter Analyseprozess.....	16
Abbildung 6: Automatisierter Analyseprozess	19
Abbildung 7: Händische Analyse.....	19
Abbildung 8: Schematische Darstellung der Integration einer Monitoring Plattform	20
Abbildung 9: DevOps Prozess mit relevanten Phasen für kontinuierliche Entwicklung.....	21
Abbildung 10: Transitionen zwischen Entwurf und Betrieb.....	23
Abbildung 11: Aufbau des Entwicklungsframeworks.....	25
Abbildung 12: Schematischer Aufbau von Hypervisor und Container Virtualisierung	26
Abbildung 13: Schematischer Aufbau des Edge Frameworks	27
Abbildung 14: Definitionen von Anomalien	29
Abbildung 15: Struktureller Aufbau des Neuronalen Netzes	30
Abbildung 16: Ergebnis des Neuronalen Netzes	30
Abbildung 17: Systemmodell der Fahrfunktion	31
Abbildung 18: Detaillierter Ablauf des Analyseprozesses für die Entwurfsunterstützung	32
Abbildung 19: Mapping Rollen StVG-Datenschutz.....	33
Abbildung 20: Datenarten und -formate nach § 1g StVG	34
Abbildung 21: Anonymitätslevel	35
Abbildung 22: Sachverhaltsspezifische Abbildung der Normenhierarchie (Datenschutz und IT-Sicherheit beim autonomen Fahren)	36
Abbildung 23: Modellierung der Normenhierarchie.....	37
Abbildung 24: Auszug Überführung in Coodex-Tool I	38
Abbildung 25: Auszug Überführung in Coodex-Tool II	38
Abbildung 26: Prozess zur Rückführung von Daten in die Monitoring Plattform	39
Abbildung 27: Aufbau des Demonstrators.....	40
Abbildung 28: GUI des Demonstrators	41

1 Thema und Zielsetzung des Vorhabens

Für die Realisierung und Einführung autonom agierender Fahrzeuge ist das sichere Zusammenspiel von Funktionen, Systemen und Diensten sowie deren Überwachung über den kompletten Produktlebenszyklus unerlässlich. Diese Kooperation findet sowohl innerhalb des Fahrzeugs, in Form von Kommunikation zwischen Steuergeräten, als auch mit der Umwelt im Sinne von mobilen Endgeräten und Infrastruktur statt. Dabei spielen neben interagierenden Fahrzeugen auch übergreifende Informationsdienste wie Navigations- oder Wetterdienste eine zentrale Rolle. Diese Informationen fließen im autonom agierenden Fahrzeug zusammen, um Entscheidungen über Navigation, Spurführung und Stabilisierung auf unterschiedlichen Funktionsebenen im Fahrzeug treffen zu können. Da diese Informationen bei Fehlern oder Manipulation zu Fehlverhalten des Fahrzeugs bis hin zu Gefahrensituationen führen können, müssen sie besonders geschützt werden. Dadurch gewinnt die IT-Sicherheit in den vernetzten Systemen und Anwendungen sowie der Einsatz von sicheren und vertrauenswürdigen Informations- und Kommunikationstechnologien (IKT) immer mehr an Bedeutung bei der Entwicklung und dem Betrieb solcher Systeme.

Zur sicheren Entwicklung und Auslegung der Fahrzeuge werden im Rahmen eines Security-by-Design Maßnahmen getroffen, um möglichst viele Risiken bereits zur Entwurfszeit abzudecken. Jedoch können sich während der Betriebszeit zusätzliche Schwachstellen und Sicherheitslücken ergeben, die zur Entwurfszeit nicht bekannt waren. Diese Änderungen können sowohl das System selbst, als auch seine Umwelt betreffen:

- Selbstlernende Systeme basierend auf KI-Anteilen, die sich durch Lernen eigenständig weiterentwickeln.
- Änderungen an der Umwelt (neue Kommunikationsmöglichkeiten, neue Verkehrsteilnehmer wie z.B. E-Scooter, veränderte Rahmenbedingungen, Gesetzgebung, ...).
- Änderungen/Updates von bestehenden Funktionen im Fahrzeug, neue Kommunikationspfade entstehen

Die kontinuierlichen Veränderungen bergen potenzielle Risiken in Bezug auf die Cyber-Sicherheit, die zugleich durch ihre Auswirkung auf die funktionale Sicherheit und insbesondere auf die Erfüllung der Sollfunktion (SOTIF) zu erheblichen Gefährdungen für Verkehrsteilnehmer führen können. So besteht erhebliches Potenzial für wirtschaftliche Schäden, die bspw. durch Datenmissbrauch und Datenmanipulation entstehen können. Zudem ist es durch die Veränderungen der Umwelt sowie des Systems zwingend notwendig, über den gesamten Produktlebenszyklus der Fahrzeuge und Systeme bis hin zur Außerbetriebnahme kontinuierlich die Sicherheit zu gewährleisten. Eine ausschließliche entwicklungsbegleitende Unterstützung im Rahmen eines Security-by-Design ist nicht mehr ausreichend und muss durch die Rückführung von Erfahrungen aus dem Betrieb kontinuierlich unterstützt werden.

Dies führt zu Herausforderungen bei der Entwicklung und dem Betrieb von sicheren autonomen Fahrfunktionen, die in diesem Projekt bewältigt werden sollen. Die etablierten Ansätze im Bereich Security-by-Design wurden durch eine systematische Rückführung von Erkenntnissen aus Sicherheitsvorfällen in die Entwicklungs- bzw. Updatephase ergänzt. Sicherheitsvorfälle im Feld, welche sich bspw. durch Änderungen im System oder neue Angriffspfade während des Betriebs ergeben,

können so identifiziert und analysiert werden. Hierfür ist eine systematische und strukturierte Zusammenführung unterschiedlicher Methoden zur Erkennung von Sicherheitsvorfällen auf unterschiedlichen Systemebenen notwendig. Im Anschluss wurde untersucht, inwiefern sich diese Sicherheitsvorfälle auf das Design und die Entwicklungs- bzw. Updatephase auswirken. Hierzu wurden die erkannten Vorfälle mit den Sicherheitsanalysen, -anforderungen, Modellen und Maßnahmen aus der Entwurfsphase verknüpft. Dies ermöglichte eine Anpassung von Sicherheitsanalysen sowie die Erarbeitung von neuen Sicherheitsmaßnahmen. So können kontinuierlich Fehlfunktionen behandelt, Sicherheitslücken geschlossen, sowie sichere Updates von Funktionen (auch KI-Funktionen) ermöglicht werden. Hierbei ist es essentiell, Security stets gemeinsam mit der Sicherheit der Sollfunktion (SOTIF) zu betrachten.

Die **Ziele dieses Vorhaben** waren:

- Erforschung von Verfahren und Werkzeugen zur systematischen und strukturierten Erfassung von Sicherheitsvorfällen (Security und Safety/SOTIF) auf verschiedenen Systemebenen bei autonomen Fahrfunktionen. Dabei wurden die Felddaten zur Identifizierung der Sicherheitsvorfälle genutzt, um eine kontinuierliche datenbasierte Unterstützung des Entwurfs sowie von Updates zu ermöglichen.
- Rückführung der Sicherheitsvorfälle und Erkenntnisse aus dem Feld in die Entwicklungswerkzeuge, Verknüpfung mit Anforderungen, Architekturmodellen, Security/Safety-Maßnahmen im Design.
- Entwicklung einer Monitoring-Plattform für sichere und vertrauenswürdige IKT-Systeme und Technologien, um sicherheitsrelevante Ereignisse in vernetzten Systemen und Anwendungen identifizieren und lokalisieren zu können.
- Berücksichtigung von datenschutzrechtlichen Aspekten im gesamten Produktlebenszyklus.

Um dies zu realisieren, war eine Zusammenarbeit der folgenden Teilbereiche zwingend erforderlich, wie im Big Picture des Vorhabens dargestellt (Abbildung 1, Schwerpunkte grün hervorgehoben). Dabei basiert das Vorhaben auf der iterativen Verknüpfung von der Datengeneration/-aufnahme im Betrieb, der Datenanalyse für die datengetriebene Unterstützung der Entwurfsphase, der Datenintegration mit zuvor erstellten Entwurfsmodellen für die kontinuierliche Security- und Safety-Analysen, dem Re-Design und der Entwicklung einer Monitoring-Plattform.

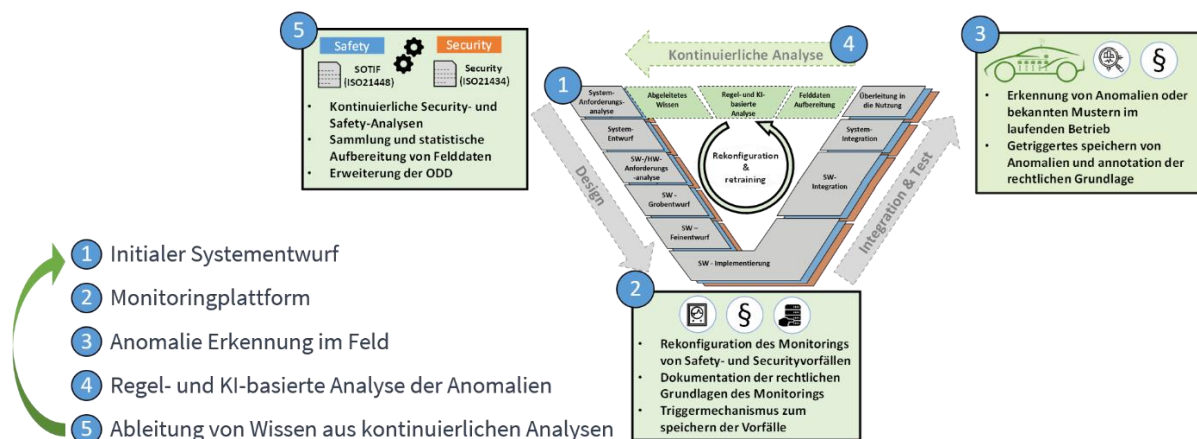


Abbildung 1: Big Picture des Projekts

1.1 Zielsetzung des Teilvorhabens

Ziel des Teilvorhabens des FZI im Projekt UNCOVER war die Konzeption, das Design und die Umsetzung von Entwicklungsmethoden und Werkzeugunterstützung für die Analyse von Security Vorfällen im Automotive Umfeld. Der Fokus lag dabei auf der Gewinnung und Rückführung von Erkenntnissen aus Security Vorfällen aus der Betriebsphase zurück in die Entwurfsphase. Folgende Aspekte bilden den Schwerpunkt der Arbeit des FZI.

Methoden für datengetriebene Unterstützung der Entwurfsphase: Um anfallende Daten über die Sicherheit betreffende Ereignisse für die Identifizierung von Fehlern und für unterstützende Mechanismen in der Entwurfsphase nutzen zu können, müssen die Informationen aufbereitet, analysiert und das nötige Wissen für den Entwurf extrahiert werden. Methoden zur Analyse von Daten und Auffälligkeiten wurden angepasst, um aus den Daten von Fahrzeugen oder Fahrzeugflotten Sicherheitsvorfälle und andere Anomalien zu identifizieren. Hierfür wurden unter anderem regel- und KI-basierte Ansätze betrachtet.

Methoden und Werkzeuge für die kontinuierliche Safety- und Security-Analysen basierend auf den Erkenntnissen aus Security- und Safety-Vorfällen: Die aus den Daten abstrahierten und gewonnenen Informationen unterstützen bei der Fehlerbehebung. Das Vorgehen und die Methoden und Werkzeuge, die für den kompletten Automobil-Entwicklungsupdatezyklus anfallen gilt es zu evaluieren, um ein kontinuierliches Safety- und Security-Monitoring zu erreichen. Dafür wurden Methoden für eine systematische Zusammenführung der Informationen aus dem Betrieb dieser Systeme in die Entwicklungsphase angewandt, um diese mit Anforderungen, Modellen und Sicherheitskonzepten im Entwurf zu verknüpfen. Hierfür wurden Metamodelle und Schnittstellen angepasst, die zur Beschreibung der Veränderungen in Bezug auf Safety/Security, E/E-Architekturen und Angriffsvektoren verwendet werden. Basierend auf der modellbasierten Beschreibung wurden Konzepte für das Re-Design der Systeme unter Berücksichtigung der identifizierten Schwachstellen und deren Auswirkungen auf die E/E-Architektur erarbeitet.

Monitoring-Plattform zur Erkennung von Security- und Safety-Vorfällen: Ein essentieller Baustein des Vorhabens ist die Entwicklung einer flexiblen Monitoring-Plattform zur Erkennung sicherheitsrelevanter Ereignisse im laufenden Betrieb. Sie stellt die technische Basis für die Integration von konfigurierbaren Monitoring-Mechanismen und einem Redeployment-Prozess in eine E/E-Architektur dar. Zu diesem Zweck wurden auch ein zugehöriger kontinuierlicher Entwicklungsprozess und ein HW/SW-Framework für das Deployment erarbeitet.

Datenschutzrechtliche Fragestellungen: Im Rahmen der Entwicklungsmethoden müssen auch nicht-funktionale Aspekte aus dem Bereich des Datenschutzrechts in bewertbare technische Sicherheitsmechanismen überführt werden. Die Einbeziehung dieser Aspekte hat bereits aufgrund des "Privacy by Design"-Grundsatzes nach Art. 25 DSGVO im Entwurfsstadium zu erfolgen, da bereits bei der Festlegung der Mittel die technischen und organisatorischen Maßnahmen getroffen werden müssen, um die Datenschutzgrundsätze umzusetzen und die Rechte und Freiheiten der betroffenen Personen zu schützen. Rechtliche Aspekte wurden sowohl bei der Datenanalyse als auch bei dem Redesign berücksichtigt und für die Entwurfsunterstützung implementiert.

1.2 Voraussetzungen der Vorhabensdurchführung

Das Projekt UnCOVER - Datenbasierte EntwurfsUNterstützung durch kontinuierliches MONitoring Von SichERheitsvorfällen (Förderkennzeichen 16KIS1410K) wurde im Rahmen einer Förderung durch das Programm „KMU Innovativ IKT“ des BMBF durchgeführt. Das Projekt wurde vom FZI Forschungszentrum Informatik unter Einbeziehung der Projektpartner bearbeitet. Projektpartner waren:

Karlsruher Institut für Technologie (KIT):	Das Karlsruher Institut für Technologie (KIT) ist eine Universität des Landes Baden-Württemberg und ein nationales Forschungszentrum in der Helmholtz-Gemeinschaft mit ungefähr 9.300 Beschäftigten und ca. 25.000 Studierenden. Das jährliche Budget beträgt etwa 881 Millionen Euro. Das Institut für Technik der Informationsverarbeitung (ITIV) beschäftigt sich seit vielen Jahren mit dem Entwurf und der Anwendung rekonfigurierbarer Hardware. Die Forschungsschwerpunkte liegen insbesondere im Bereich des Architekturentwurfs für eingebettete elektronische Systeme, inklusive der zugehörigen Methoden, Tools, Design-Prozesse. Der Fokus der Forschungsarbeiten liegt auf echtzeitfähigen Architekturen, der Betrachtung von Safety und Security, der Integration in existierende E/E-Architekturen, Methodiken und Tools hinsichtlich ISO 26262, IT-Sicherheit und Softwareschutz.
EnCo GmbH	EnCo Software GmbH wurde 2008 in Hamburg gegründet als Dienstleister im Bereich funktionale Sicherheit. Das Angebot umfasste Training, Beratung und operative Projektunterstützung in funktionaler Sicherheit, insbesondere nach ISO 26262. Seit 2012 wurde der Schwerpunkt des Geschäfts zunehmend auf die Entwicklung eines integrierten Werkzeugs zur Unterstützung der funktionalen Sicherheit gelegt. Das resultierende Werkzeug Safety Office X2 (SOX2) hat sich seitdem in enger Zusammenarbeit mit Partnern und Kunden (z.B. Bosch, Continental, Magna Powertrain, Volkswagen) zu einer umfassenden Plattform für Safety Engineering entwickelt, die den gesamten Entwicklungsprozess abdeckt. Dies umfasst die Anforderungen, das Systemdesign und die verschiedenen Sicherheitsanalysen. Im Jahr 2016 wurde SOX2 bei Bosch weltweit in das Portfolio der Standardwerkzeuge aufgenommen. EnCo ist an mehreren Forschungsprojekten beteiligt, u.a. mit den Partnern Fraunhofer, TU München, RWTH Aachen, Bosch, Schaeffler, ZF, Continental. Weiterhin befasst sich EnCo mit der Umsetzung der Security-Engineering Prozesse und Analysen auf der Plattform.
RISA Sicherheitsanalysen GmbH	Im Jahr 1990 ist die RISA Sicherheitsanalysen GmbH aus der Arbeitsgruppe „Sicherheit und Zuverlässigkeit technischer Anlagen“ der TU Berlin hervorgegangen. Neben probabilistischen Sicherheitsanalysen in der Kraftwerkstechnik sind in mehr als 25 Jahren ebenso Analysen zur Sicherheit und Zuverlässigkeit straßen-, schienen- und luftgebundener Verkehrssysteme durchgeführt worden. Seit 1993 beschäftigt sich der Bereich Umwelt der Firma RISA mit der Entwicklung von

	Umweltinformationssystemen und seit Ende der 90er Jahre mit der Erfassung, Qualitätssicherung, Aufbereitung und der Übermittlung von Umweltdaten im Rahmen europäischer Richtlinien. Das Personal der RISA ist mit Forschung, Entwicklung und Anwendung sicherheitstechnischer Methoden befasst. Aufgrund der neben dem Bereich „Automotive“ bisher bearbeiteten Schwerpunkte in der Kerntechnik und der Luft- und Raumfahrt sieht sich die Firma hinreichend breit aufgestellt, um zu einem sicherheitstechnischen Konzept für autonomes Fahren substantiell beizutragen. Für einen deutschen Automobilhersteller hat RISA neben anderen Projekten zudem ein Projektlösungsteam bei der Analyse eines Fehlers unterstützt, um eine Rückrufaktion zu vermeiden.
ERNW	ERNW Research GmbH ist ein Tochterunternehmen für die Forschungsaktivitäten der ERNW Enno Rey Netzwerke (kurz ERNW). ERNW ist ein herstellerunabhängiges IT-Security Beratungs- und Prüfungshaus. Zu den Kunden zählen insbesondere Banken, Versicherungen, Telekommunikationsanbieter und Industrie-konzerne. ERNW-Mitarbeiter vermitteln ihr Fachwissen regelmäßig auf internationalen Sicherheitskonferenzen und publizieren eine Vielzahl von Büchern, Fachartikeln und White Papers. Mit verschiedenen Hochschulen werden jährlich mehrere Abschlussarbeiten zu aktuellen Themen der Informationssicherheit wissenschaftlich bearbeitet. Die auf Forschung ausgerichtete Firmenkultur prägt die Tätigkeit des Unternehmens und hat zur Aufdeckung vieler kritischer Schwachstellen geführt.

Das FZI Forschungszentrum Informatik ist eine gemeinnützige Einrichtung für Informatik-Anwendungsforschung und Technologietransfer und fungiert als Innovationsdrehscheibe für Informations- und Kommunikationstechnologien des KIT. Ca. 250 wissenschaftliche Mitarbeitende aus den Fakultäten Informatik, Elektrotechnik, Wirtschaftsingenieurwesen und Maschinenbau forschen und entwickeln gemeinsam mit Geschäfts- und Forschungspartner*Innen an Ansätzen und Konzepten für innovative Lösungen, Dienstleistungen und Prozessen. Durch seine breite und interdisziplinäre Ausrichtung und einem Forschungsschwerpunkt auf Sicherheit ist das FZI ein idealer Forschungspartner für die Querschnittstechnologie IT-Sicherheit. Im Bereich Mobilität stehen autonome Fahrzeuge, Elektromobilität und intermodale, vernetzte Mobilität sowie deren Absicherung im Vordergrund der Forschung am FZI.

Der Forschungsbereich Embedded Systems and Sensors Engineering (ESS) erforscht und entwickelt innovative Funktionen, Technologien und Entwurfsmethoden für interagierende eingebettete Systeme. Dazu gehören HW-Plattformen und Prozessorarchitekturen, Kommunikationsschnittstellen, Sensorik, Signal- und Informationsverarbeitung, Steuerungs- und Regelungstechnik, Cloud- und App-Anwendungen, Safety und Security, modellbasierte Entwicklung und Rapid Prototyping, E/E- und Funktionsarchitekturen sowie Simulation und Testing. Der Forschungsbereich ESS besitzt langjährige Erfahrung in der Analyse und Entwicklung von Entwicklungsmethoden und Werkzeugen für eingebettete Systeme. Der Tätigkeitsbereich reicht von modellbasierten Entwurfsmethoden und -

werkzeugen über technologieorientierte Forschung bis hin zu anwendungsorientierten Forschungs- und Entwicklungsprojekten.

Im Kompetenzzentrum IT-Sicherheit ist auch die rechtliche Forschungsgruppe vertreten, welche auf langjährige Erfahrung in der prospektiven informationsrechtlichen Analyse neuer IKT-Systeme und -Anwendungen sowie in der Erarbeitung von Vorschlägen zur rechtlich konsistenten Fortentwicklung des jeweils relevanten Rechts- und Regulierungsrahmens zurückgreifen kann. Die mit diesem Vorhaben angesprochenen Fragestellungen können auf vielfältige Vorarbeiten aufbauen, die insbesondere in den Projekten SINQ (BMBF), PaKoS (BMBF), EDV (BMW), DeFEND (BMBF), Heike (Ministerium für Wirtschaft, Arbeit und Wohnungsbau Baden-Württemberg (WM)) sowie der Smart Data Begleitforschung gewonnen werden konnten. Auch im Testfeld Autonomes Fahren (TAF) Baden-Württemberg (Land Baden-Württemberg, Ministerium für Verkehr) werden die rechtlichen Aspekte betrachtet und evaluiert.

1.3 Planung und Ablauf des Vorhabens

Das Vorhaben folgte dem untenstehenden Arbeits- und Zeitplan zur Erreichung der Projektziele.



Abbildung 2 Arbeitspaketübersicht und Informationsfluss

AP	Projektjahr 1				Projektjahr 2				Projektjahr 3	
	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2
AP 1										
AP 2										
AP 3										
AP 4										
AP 5										
AP 6										
Meilensteine			♦ M1			♦ M2			♦ M3	

- ♦ M1: Beschreibungen der Szenarien vorhanden und Anforderungen abgeleitet.
- ♦ M2: Erste Konzeptbeschreibungen und Methoden verfügbar. Erste Umsetzungen von Tools und Technologien durchgeführt.
- ♦ M3: Konzepte und Methoden verfügbar. Erste prototypische Version der Demonstratoren verfügbar.

1.4 Stand der Wissenschaft und Technik zu Beginn des Vorhabens

Kontinuierlichen modellbasierten Analyse von Safety und Security: Zur Einordnung des Stands der Technik ist grundsätzlich zwischen Verhaltens- und Architekturmodellen zu unterscheiden. Bei damaligen Safety und Security Analysen kamen Architekturmodelle zum Einsatz. So gab es Werkzeuge, die eine Safety Analyse mit der zugehörigen Systemarchitektur verknüpfen. Für Safety sind das beispielsweise SOX von ENCO, PREEvision von Vector Informatik und Medini Analyse von Ansys. Werkzeuge wie SOX oder PREEvision boten zusätzlich erste Lösungsansätze zur Durchführung von Security Risiko-Assessments. Mit Werkzeugen wie zum Beispiel Matlab Simulink von Mathworks oder ACET von ETAS lassen sich Verhaltensmodelle entwerfen und analysieren. Dadurch ist ein Rapid Prototyping von Funktionen möglich. Bis zur Verwendung der entwickelten Funktionen werden zahlreiche Tests wie beispielsweise Hardware-in-the-Loop (HiL) oder Penetrationstests zur Absicherung der entwickelten Funktionen und Systeme durchgeführt. Entdeckte Fehler, Fehlverhalten und Schwachstellen werden so bis zur Anwendung im Feld auf ein verträgliches Risiko reduziert. Treten beim Testen Fehler auf, die eine Änderung an einer Funktion oder einer Komponente zur Folge haben, wird dies über einen Change-Management Prozess mit entsprechender Werkzeugunterstützung realisiert. Eine Methodik wie Daten aus dem Feld aufbereitet und direkt im Architekturwerkzeug mit den Entwurfsvarianten verknüpft werden können, um eine kontinuierliche Safety- und Securitybewertung durchführen zu können, war uns nicht bekannt.

Mechanismen zum Monitoring von Safety und Security: Um die mit der stetigen Zunahme an Elektronikfunktionen im Fahrzeug einhergehenden Safetyanforderungen erfüllen zu können, haben sich Monitoringverfahren wie der Einsatz von Lockstep-Prozessoren oder Watchdog-Timern etabliert. Die zunehmende Vernetzung innerhalb von und über die Grenzen von Fahrzeugen hinweg führt darüber hinaus zu Anforderungen an die IT-Sicherheit, die z. B. durch die intensive Erforschung von Methoden zur Anomalieerkennung beherrscht werden sollten. Diese Mechanismen wurden derzeit jedoch weitgehend isoliert betrachtet und bereits in frühen Schritten des Entwicklungsprozesses auf ihren speziellen Betrachtungsrahmen ausgerichtet. Sie waren für den kontinuierlichen Bezug und die Rückführung von Felddaten daher nur unzureichend geeignet. Durch das hochautomatisierte Fahren ist darüber hinaus ein Trend hin zu mehr Dynamik und einer Zentralisierung der E/E-Architektur entstanden. Ein geeigneter Monitoringansatz muss Safety- und Securityaspekte gemeinsam berücksichtigen und bei einer hohen Flexibilität selbst hinreichend abgesichert sein. Hierbei handelte es sich um eine bisher ungelöste Problemstellung.

Datenbasierte Unterstützung der Entwurfsphase: Daten für die iterative Fortführung des Entwicklungsprozesses wurden manuell von den Entwicklern erfasst. Solche Datenakquirierungen sind aufwändig und z.T. unzuverlässig. Die bereits über den Fehlerspeicher zur Verfügung stehenden Daten waren für viele Zwecke des Entwicklungsprozesses nicht ausreichend, z.B. die Ermittlung von Ausfallraten und Ausfallwahrscheinlichkeiten. Felddaten flossen manuell zurück in den Entwicklungsprozess, zum Teil wurden generische Daten ergänzt. Die Ermittlung von Fehlerursachen kann durch eine Abbildung der anfallenden Daten auf die bekannten Strukturen in den Modellen der Fahrzeugarchitektur verbessert werden. Darüber hinaus sind die Randbedingungen eines Ausfalls für die Ursachenermittlung zu berücksichtigen. Eine automatische KI-unterstützte Analyse und Klassifizierung von Felddaten kann für die Identifizierung von Sicherheitsvorfällen genutzt werden, um Sicherheitsanalysen und Entwurfsentscheidungen zu unterstützen.

Rechtliche Fragestellungen und Datenschutz: Die juristische Diskussion im Zusammenhang mit autonomen Fahrzeugen erschöpft sich überwiegend im Umgang mit haftungsrechtlichen Fragestellungen, insbesondere wird hierbei diskutiert wer bei der Nutzung von autonomen Fahrzeugen zur Verantwortung gezogen werden muss. Ferner wird beleuchtet, ob ein Eigentum an Daten begründet werden kann. Auch datenschutzrechtliche Aspekte finden nur mit Bezug zu bereits eingesetzter Technik Einzug in die juristische Diskussion. Hierbei geht es primär um die Umsetzung der datenschutzrechtlichen Anforderungen. Arbeiten im Hinblick auf eine Felddatennutzung der OEM, die datenschutzrechtliche Aspekte als nicht funktionale Anforderungen in eine serviceorientierte Infrastruktur direkt in der Entwicklungsphase und damit im Rahmen der Konzeption mitberücksichtigen, waren nicht bekannt.

1.5 Angaben bekannter Konstruktionen, Verfahren und Schutzrechte, die für die Durchführung des Vorhabens benutzt wurden

Es konnten keine Patente identifiziert werden, die diesem Vorhaben entgegengestanden oder die Ausübungsfreiheit eingeschränkt hätten.

1.6 Zusammenarbeit mit anderen Stellen

Das Vorhaben erforderte keine weitere Zusammenarbeit mit anderen Stellen außerhalb des Projekts.

2 Ergebnisse

2.1 AP1: Use Case Definition und Anforderungen an die Daten und Sicherheitsanalysen

2.1.1 Motivation und Gesamtprozess

Mit der zunehmenden Digitalisierung und Automatisierung von Kraftfahrzeugen werden immer mehr sicherheitskritische Aufgaben durch Software übernommen. Daraus ergeben sich neue Anforderungen und Herausforderungen an die Entwicklung und Wartung von Softwarekomponenten. Die durchschnittliche Lebensdauer von Fahrzeugen ist deutlich länger, als die Zyklen innerhalb derer neue Erkenntnisse und Erfordernisse an sichere Software zu Tage treten. In Bezug auf den sicheren Betrieb gibt es zwei Kategorien von Gefahren, die die Sicherheit von Kraftfahrzeugen bedrohen:

- **Safety-Vorfälle:** Bei Ausfall einer Komponente, sei es Soft- oder Hardware, fallen auch die durch diese Komponente ausgeführten Funktionen aus. Ist die Funktionalität für die Sicherheit des Fahrzeugs relevant, handelt es sich um einen Safety-Vorfall.
- **Security-Vorfälle:** Gelingt es Dritten willentlich, die Ausführung einer Software-Komponente zu unterbrechen, zu beeinflussen oder zu beenden, stellt dies einen Security-Vorfall dar. Ist die betroffene Komponente an einer sicherheitskritischen Funktion beteiligt, so handelt es sich gleichzeitig auch um einen Safety-Vorfall.

Um den sicheren Betrieb zu gewährleisten, müssen sowohl Safety- als auch Security-Vorfälle verhindert werden. Dies wird durch die Umsetzung entsprechender Normen (ISO 21434, ISO 26262, ISO 21448) im Entwicklungsprozess berücksichtigt. Nach Abschluss der Entwicklung ergeben sich jedoch neue Herausforderungen. So finden einerseits Alterungsprozesse von Hardwarekomponenten statt, andererseits werden durch Fortschritte in der Informationstechnik neue Angriffe auf informationstechnische Systeme möglich. Es müssen also Maßnahmen ergriffen werden, die im laufenden Betrieb Systeme auf Safety- und Security-Vorfälle überwachen, diese melden und geeignete Reaktionen ermöglichen. Auf diese Weise lässt sich die Lücke zwischen Betrieb und Entwicklung schließen und ein kontinuierlicher Prozess zur Weiterentwicklung von Systemen aufbauen. Dieser Prozess ist in der untenstehenden Abbildung schematische gezeigt.

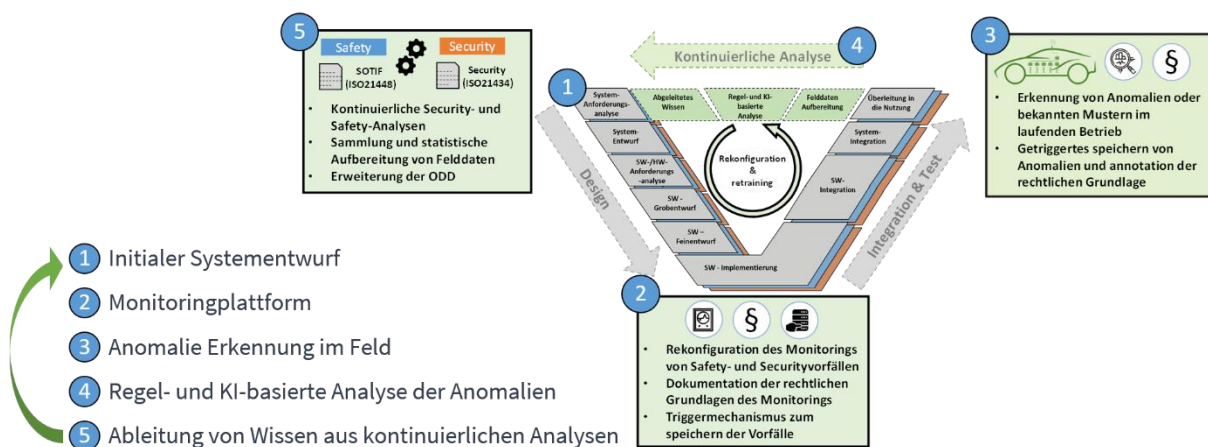


Abbildung 3: Gesamtprozess

Um die im Projekt erarbeiteten Methoden anwenden und zeigen zu können, wurden im Arbeitspaket 1 Use Cases erarbeitet, die sowohl Safety- als auch Security-Vorfälle darstellen können. Dabei wurden, strukturiert anhand der geplanten Prozesse, Anforderungen und Artefakte aus den Teilprozessen erhoben. Die Anforderungen an die Use Cases wurden gesammelt und aufbereitet an die Partner verteilt. Dabei wurde klar, dass es unterschiedlicher Use Cases bedarf, um die Anforderungen des Gesamtprozesses abzudecken. Die Szenarien wurden in folgender Form konkretisiert.

2.1.2 Szenarien für kontinuierliche Entwicklung

Aufdecken von Sicherheitsvorfällen:

Während des Betriebs des Fahrzeugs wird der Sicherheitszustand kontinuierlich überwacht. Bei Entdecken eines Sicherheitsvorfalls werden Monitore eingeschaltet, die den Fahrzeugzustand aufzeichnen. Die Daten, die dabei gesammelt werden enthalten die internen Zustände der Steuergeräte sowie Kommunikation innerhalb des Netzwerks. Beim Design der Monitore ist zu berücksichtigen, welche Daten später im Betrieb notwendig sind, um spätere Sicherheitsanalysen zu ermöglichen. Die Informationen die im Falle eines Sicherheitsvorfalls im Fahrzeug aufgezeichnet werden, werden anschließend an eine zentrale Stelle übermittelt, an welcher Sicherheitsanalysen durchgeführt werden können. Die Daten sollen dabei anhand der rechtlichen Rahmenbedingungen erhoben und gespeichert werden.

Die Szenarien für die Fahrzeuge wurden so gewählt, dass es bekannte gute Szenarien gab sowie unbekannte Szenarien. Das bekannte Szenario stellt ein Überholvorgang durch einen anderen Verkehrsteilnehmer dar, während das unbekannte Szenario entweder ein Überholvorgang *rechts* des Fahrzeugs ist oder die Injektion von falschen Sensorsignalen. Die untenstehenden Bilder zeigen die jeweils abgebildeten Fahrszenarien:

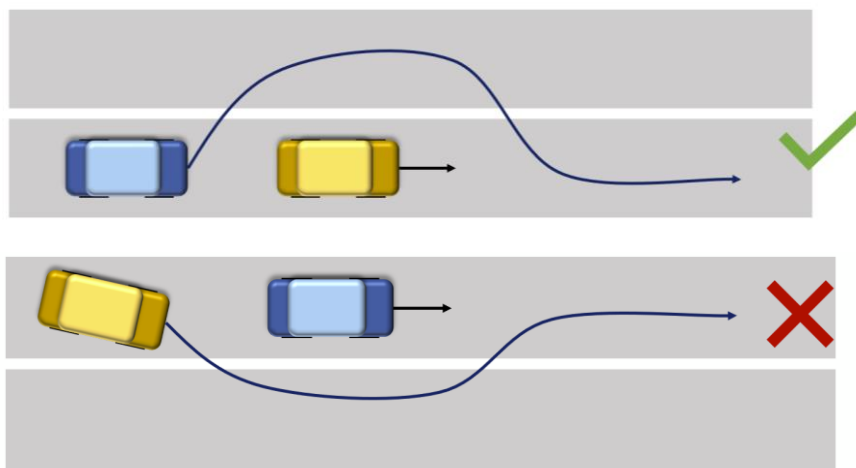


Abbildung 4: Fahrszenarien

Angriffsszenario:

Innerhalb des Projektes stellt sich die Frage, welche Angriffsszenarien betrachtet werden. Dabei wurde entschieden, dass der initiale Angriffspfad, also wie der Angreifer Zugriff auf eine Komponente des Fahrzeugs erlangt hat, eine untergeordnete Rolle spielt. Primäres Ziel ist es, schadhaftes Verhalten, das

sich innerhalb des Systems abspielt, zu erkennen, zu isolieren und zu verhindern. Dies lässt sich durch die Monitoring-Verfahren abbilden und mit geeigneten Isolationsverfahren vermeiden. Entscheidend für den Erfolg eines Angriffs, ist es, dass der Angreifer die Möglichkeit erlangt, Kommunikation innerhalb des Systems abzuhören und zu reproduzieren. Diese Kommunikation kann erkannt und unterbunden werden. Ziel des Projekts ist es entsprechend, durch Beobachtung des CAN-Busses, bösartige Aktionen zu detektieren und in Zukunft verhindern zu können.

2.1.3 Daten und Sicherheitsanalyse

Anhand der erhobenen Daten können nun Analysen zur Ursache bzw. des Ursprungs des Vorfalls ermittelt werden. Dazu gehört die Identifikation relevanter Signale, die Gruppierung von Vorfällen anhand von Ähnlichkeitsmaßen und die Analyse einzelner Signale auf Auffälligkeiten. Dadurch sollen Muster in den Angriffen identifiziert werden, um dieselben Muster später im Fahrzeug zu erkennen und ihnen vorbeugen zu können. Außerdem ermöglicht dieses Vorgehen Aussagen über die Systemarchitektur, die zu einer besseren Kapselung besonders gefährdeter Bereiche genutzt werden können.

Sicherheitsanalyse anhand der analysierten Daten: Die Daten sowie die Analyseergebnisse können nun in ein geeignetes Werkzeug für das System- und Architekturdesign überführt werden. Durch die Verknüpfung des Systemmodells mit den erhobenen Daten können systemspezifische Verhaltensweisen analysiert und reproduziert werden. Dies erlaubt die oben genannten Schlüsse in Bezug auf besonders gefährdete Zonen, die durch Schnittstellen nach außen exponiert sind. Treten Anomalien in bestimmten Zonen auf, können diese vom Gesamtsystem isoliert werden und Angriffe bleiben so auf unkritische Bereiche begrenzt.

Betroffene Komponenten aktualisieren: Anhand der Sicherheitsanalyse können die Komponenten identifiziert werden, die durch Sicherheitslücken die Systemsicherheit gefährden. Diese können jetzt gezielt für ein Update markiert und Entwicklern entsprechende Informationen für ein Update bereitgestellt werden. Die aktualisierten Sicherheitsvorgaben können in Form von Anforderungen an Implementierung und Verifizierung weitergegeben werden. Nach der Implementierung muss durch intensives und gezieltes Testen die Erfüllung der Anforderungen überprüft werden. Anschließend kann das Update freigegeben und an die Zielsysteme verteilt werden.

Automatisiertes Deployment von aktualisierten Komponenten: Mithilfe von Container-Technologien können Software-Module flexibel auf dem Zielsystem ausgetauscht werden. Dabei muss berücksichtigt werden, dass sowohl die Funktionsbestandteile als auch aktualisierte Monitore für die kontinuierliche Sicherheitsüberwachung aktualisiert werden müssen.

2.2 AP2: Methoden und Werkzeug für kontinuierliche Security- und Safety-Analysen basierend auf den Erkenntnissen aus Security- und Safety-Vorfällen

In Arbeitspaket 2 wurden Methoden und Werkzeuge entwickelt, um kontinuierliche Security- und Safety Analysen basierend auf Felddaten zu ermöglichen. Die Herausforderung bestand in der Trennung von verschiedenen Vorfällen in die Kategorien kritisch, unkritisch, bekannt, unbekannt sowie Safety und

Security. Je nach Kategorie eines Vorfalls sind unterschiedliche Reaktionen in der weiteren Entwicklung nötig. Bekannte, unkritische Vorfälle können in eine Verfeinerung der Monitoring-Funktionalität einfließen. Bekannte, kritische Vorfälle werden zur weiteren Analyse von Vorfällen sowie deren statistischer Einordnung verwendet. Unbekannte, unkritische Vorfälle können in der Entwicklung dabei helfen, eventuell nicht betrachtete Betriebsbedingungen aufzudecken.

In diesem Kapitel wird zum besseren Verständnis der gesamte Analyseprozess aus Abbildung 5 beschrieben, einschließlich der in AP3 (Monitoring-Plattform) und AP4 (datengestützte Unterstützung der Entwurfsphase) verwendeten Komponenten.

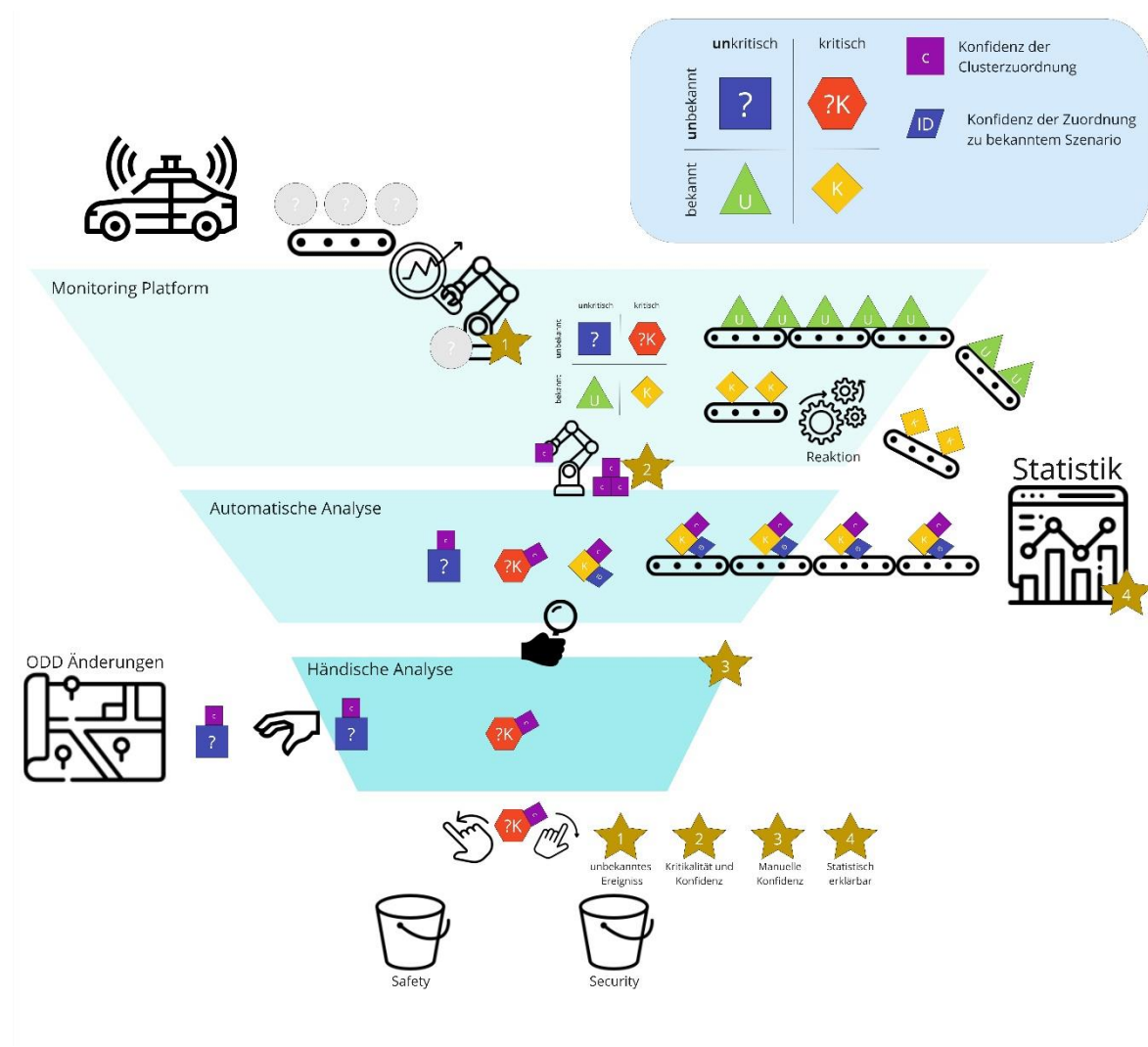


Abbildung 5: Gesamter Analyseprozess

2.2.1 Überblick über den Analyseprozess

In AP 2.1 wurden Methoden zur automatisierten und händischen Analyse von gemeldeten Sicherheitsvorfällen anhand des Systemmodells und anhand der vorliegenden Daten erarbeitet. Die Daten werden hierbei zunächst gefiltert und anschließend in den Prozess zur Analyse übergeben. Dabei wird unterschieden zwischen bekannten (kritisch, unkritisch) sowie unbekannten Szenarien.

Unbekannte Szenarien werden anhand des Expertenwissens im Systemmodell, bekannter kritischer Pfade im System sowie anhand ihres statistischen Auftretens klassifiziert. Den Daten wird so sukzessive Information in Form von Metadaten und Tags hinzugefügt, um ein Bild über das Ereignis zu erhalten. Das Vorgehen zu dieser Klassifikation ist in Arbeitspaket 2.2 beschrieben.

Im Projekt stellte sich heraus, dass für die Einordnung unbekannter Szenarien die beteiligten Systemkomponenten eine wesentliche Rolle spielen. In der Rückmeldung von Daten zu unbekannten Vorfällen ist daher abgelegt, welche Daten von welcher Systemkomponente stammen, um eine Zuordnung zu jenen zu ermöglichen. Daraus lässt sich anschließend für einzelne Systemkomponenten eine Auftretenswahrscheinlichkeit für beziehungsweise die Beteiligung an einem Vorfall ermitteln. Dies kann sowohl durch statistische Methoden als auch durch die händische Analyse der Daten mit dem zugrundeliegenden Systemmodell erfolgen. Ergebnis des Analyseprozesses ist eine Liste an Vorfällen sowie deren Klassifikation.

In AP2.3 und AP2.4 wurde ein Prozess zur Einordnung von Anomalien und der darauffolgenden Unterteilung in Safety- und Securityvorfälle entwickelt. Der gesamte Prozess ist in Abbildung 5 dargestellt. Um Methoden und Werkzeuge für die kontinuierliche Analyse entwickeln zu können wurde ein szenariobasiertes Datenmodell erarbeitet. Das Datenmodell besteht aus ausgewählten Bussignalen für einen spezifischen Zeitraum. Wenn die Bussignale für den Zeitraum als unbekannt oder von Interesse für die Analyse gelten wird von einer Anomalie gesprochen.

Der Prozess ist so konzipiert, dass er zuerst regelbasiert diese Anomalien untersucht (Anomaliedetektion aus AP3). Aus der kontinuierlichen Anomaliedetektion werden bei einer detektierten Anomalie Szenarien gebildet, die aus den Bussignalen für einen Zeitraum von mehreren Sekunden bestehen. Anschließend wird mittels eines Neuronalen Netzwerkes das aufgetretene Szenario mit einem Katalog an bekannten Szenarien verglichen. Sollte es ähnlich genug zu den bereits bekannten Szenarien sein wird das Szenario direkt an eine statistische Untersuchung weitergeleitet. In der statistischen Auswertung werden Auftretenswahrscheinlichkeiten von Szenarien gesammelt, sowie die zu dem Szenario verfügbaren Metadaten (z.B.: Wetter, Manöver und Spur). Anhand dieser Daten können Untersuchungen angestellt werden, ob ein bestimmtes Verhalten in Szenarien durch statistische Ausfälle erklärbar ist, oder ob es sich um eine Häufung von Ausfällen handelt (RiSA). Wenn das Szenario durch die automatisierte Klassifikation nicht zugeordnet werden konnte wird das Szenario mit Informationen über die Abweichung zu den bekannten Szenarien an eine systemische Analyse (ENCO) weitergeleitet. Hier wird eine Analyse der Signalflüsse im Systemkontext durchgeführt. Durch die Analyse der Signalflüsse im Systemkontext können potentiell kritische Pfade in der E/E-Architektur identifiziert werden. Anhand der Analyse im Systemkontext, sowie der statistischen Einordnung der Auftretenswahrscheinlichkeiten und Ausfallraten der einzelnen Komponente kann für ein Szenario abgeschätzt werden, ob es sich primär um einen Safety- oder -Securityvorfall handelt.

Szenarien, die nicht automatisiert zugeordnet werden konnten werden nach der manuellen Analyse in den Katalog an bekannten Szenarien eingepflegt. Anhand dieses stetig wachsenden Kataloges können neue Regeln für die Anomaliedetektion aufgestellt werden und das Neuronale Netz nachtrainiert werden, sodass ähnliche Szenarien beim nächsten auftreten automatisiert zugeordnet werden können. Ziel dieses wachsenden Kataloges ist es, den manuellen Aufwand soweit wie möglich zu reduzieren und gleichzeitig Auftretenswahrscheinlichkeiten von immer mehr Szenarien während des Betriebs des

Fahrzeuges zu sammeln. Nach der Übergabe der neu ermittelten Szenarien und dem Update der Monitoring-Komponente, nimmt diese alle weiteren künftig auftretenden Szenarien auf und leitet entsprechende Vorfälle ins Backend weiter.

2.2.2 Festlegung von Daten, Modellen und Schnittstellen

Aufbauend auf Arbeitspaket 1 wurde festgelegt, anhand welcher Daten und welcher Modelle die beispielhaften Analysen durchgeführt werden können.

Datensatz eines Sicherheitsvorfalls: Prämisse war, dass Sicherheitsvorfälle anhand der im Fahrzeug aufgezeichneten Daten erkannt und analysiert werden können. Sie bilden den Ausgangspunkt des Analyseprozesses und werden in Form von Zeitreihendaten vom Fahrzeug an den Entwickler versendet. Inhalt der Daten sind die datenschutz-konform erhobenen Fahrdaten, die von der betroffenen Funktion innerhalb des Fahrzeugs erhoben und verwendet werden und die mittels eines Monitors (siehe AP3) aufgezeichnet und verschickt werden.

Systemmodelle: Aufgrund der Vorerfahrungen von Partnern im Projekt und der verbreiteten Verwendung wurden UML-Modelle zur Darstellung der untersuchten Systeme verwendet. In diesen sind die Software- und Hardwarekomponenten des betroffenen Systems, sowie die Kommunikationsverbindungen zwischen diesen, modelliert. So kann eine Zuordnung der aufgezeichneten Daten und den logischen Verbindungen und funktionalen Zusammenhängen im Fahrzeug dargestellt werden. Dies bildet die Grundlage für die händischen und automatisierten Analysen, die im Prozess durchgeführt werden.

Schnittstellen: Innerhalb des Prozesses wurden geeignete Übergabepunkte festgelegt. Diese ermöglichen einerseits das Zusammenspiel der verschiedenen Werkzeuge, die durch die Partner entwickelt wurden. Garantieren aber andererseits eine Modularisierung und Erweiterbarkeit der entwickelten Methodik.

2.2.3 Automatische Analyse

In der automatischen Analyse der Daten werden die vom Monitoring-System gemeldeten Vorfälle durch automatisierte Tools untersucht. Ergebnis dieser Untersuchung ist die Einschätzung, ob ein Vorfall bekannt oder unbekannt, kritisch oder unkritisch ist. Ähneln der Vorfall einem bekannten Sicherheitsvorfall (beispielsweise bösartige Busnachrichten eines bestimmten Musters), wird die Meldung Vorfällen dieses Typs angehängt. Dies erlaubt später eine statistische Analyse der Einzelvorfälle dieses Typs. Die statistische Auswertung kann Aufschluss darüber geben, ob die Vorfälle-Klasse durch zufällige Ausfälle oder durch gezielte Manipulation ausgelöst wurden. Außerdem lassen sich Vorkehrungen ableiten, um eine weitere Propagation des Fehlers im System zu verhindern.

Die Einteilung in bekannte und unbekannte Vorfälle kann durch den Vergleich des Vorfalls mit einer Datenbank geschehen. Hierbei werden ähnliche Methoden verwendet, wie in der Monitoring-Plattform, allerdings mit Zugriff auf eine erweiterte Szenariendatenbank sowie Möglichkeiten zur Resimulation konkreter Szenarien. Außerdem ist es möglich, durch Digital-Twin-Methoden die Kritikalität von Vorfällen abzuschätzen. Dazu werden ähnliche Fehlerfälle wie sie im Feld aufgetreten sind in einem

digitalen Zwilling des Systems abgespielt und die Reaktion des Systems ermittelt. Zeigt sich, dass Vorfälle dieser Art zu gefährlichem Verhalten des Systems führen können, müssen Maßnahmen zur Verhinderung dieses Verhaltens eingeleitet werden.

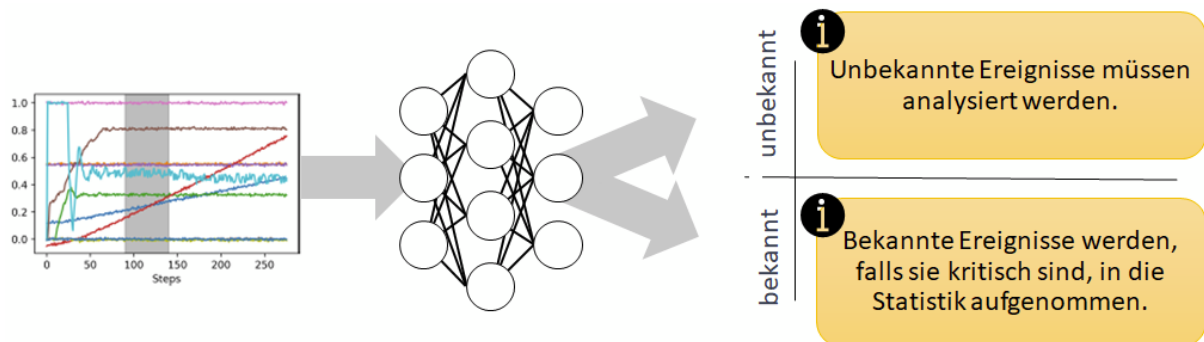


Abbildung 6: Automatisierter Analyseprozess

2.2.4 Händische Analyse

Nicht alle Vorfälle lassen sich automatisiert einordnen. Ist am Ende der automatisierten Analyse nicht klar, welche Auswirkungen ein Vorfall hat oder ist der Vorfall noch nie aufgetreten, ist es nötig die Analyse händisch zu ergänzen oder fortzuführen. Dabei werden die Messdaten aus dem Monitoring-System dem Entwickler zugänglich gemacht und er kann unter Zuhilfenahme des Systemmodells sowie weiterer Dokumentation eine Einschätzung vornehmen.

Das Wissen über die Zusammenhänge und Funktionsweisen des Systems sind dabei wichtige Ressourcen, auf die ein Mensch Zugriff hat. Stellt sich bei der Analyse heraus, dass es sich um ein unkritisches Szenario handelt, das nicht durch eine Fehlfunktion oder einen Angriff aufgetreten ist, deutet das darauf hin, dass im Systemdesign Kontextinformationen vernachlässigt wurden. Das erfordert folglich keine oder nur geringe Anpassungen des Systems, es ist aber wichtig, das Szenario zu den bekannten Szenarien hinzuzufügen, um es bei der weiteren Entwicklung zu berücksichtigen. Wird das Szenario als kritisch klassifiziert, muss am System eine Änderung vorgenommen werden. Außerdem ist es wichtig, weitere Szenarien dieser Art zu finden, um ein genaueres Bild über die Ursachen und Auswirkungen zu erhalten.

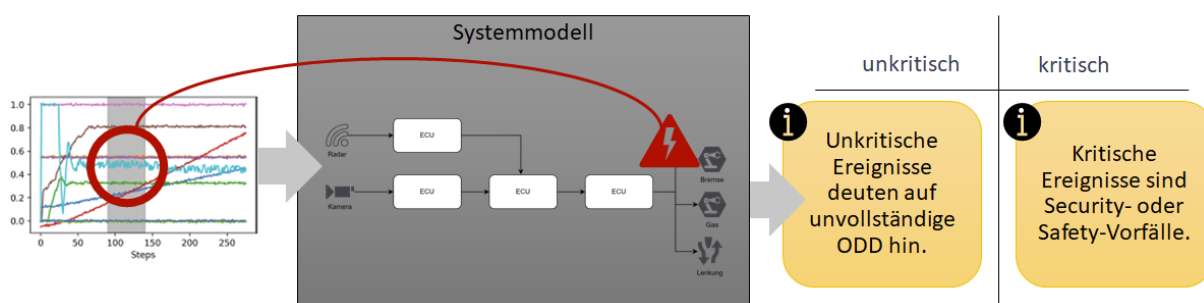


Abbildung 7: Händische Analyse

2.3 AP3: Monitoring-Plattform zur Erkennung von Security- und Safety-Vorfällen

In AP3 wurden Methoden für die kontinuierliche Entwicklung von HW/SW-Systemen und einer konfigurierbaren Monitoring Plattform entwickelt. Die Methoden für die kontinuierliche Entwicklung dienen nicht nur der Rekonfiguration der Monitoring Plattform, sondern ermöglichen auch die dynamische Anpassung von HW/SW-Systemen zur Erkennung von und Reaktion auf Sicherheitsvorfälle.

2.3.1 Überblick über die Monitoring Plattform

Die Monitoring-Plattform überwacht die Signale verschiedener ECUs im virtuellen Fahrzeug und nimmt eine erste Klassifikation von Ereignissen vor. Das System wird a priori mit bekannten Szenarien aus einem Szenarienkatalog trainiert. Eine Simulationsumgebung mit virtueller Sensorik liefert Stimuli für die ECUs, die daraufhin verarbeitete Sensorsignale durch das System propagieren und virtuelle Steuersignale zurück an die Simulationsumgebung geben. So können logische Szenarien, beispielsweise ein Überholvorgang, mit verschiedenen Parametern simuliert werden. Parameter sind beispielsweise der Abstand zwischen den Fahrzeugen, die Differenzgeschwindigkeit sowie die Fahrspur-Anzahl. Die Aufzeichnungen der in der Simulation gewonnenen Daten können verwendet werden, um einen Klassifikator zu trainieren. Dieser bestimmt ein Ähnlichkeitsmaß der im Feld vorliegenden Signale zu den ihm bekannten Szenarien. Die Erkennung von Anomalien basiert auf einer Unsicherheits-Abschätzung durch Monte-Carlo (MC)-Sampling, und durch Rückführung der entdeckten Anomalie zurück zu den Eingängen, wird die Anomalie im Eingang lokalisiert. Das vorgeschlagene System klassifiziert nicht nur bekannte Szenarien, es ist auch in der Lage, anomale Szenarien zuverlässig zu erkennen. Diese Informationen können genutzt werden um Wissen zu extrahieren und möglicherweise die Szenarien und das ADAS zu überarbeiten. Die Anpassung des Anomalie-Detektors an einen erweiterten Satz von Szenarien kann mit minimalem Retraining erfolgen. Eine schematische Darstellung der Integration der Monitoring Plattform in den Datenfluss ist in der unteren Abbildung zu sehen.

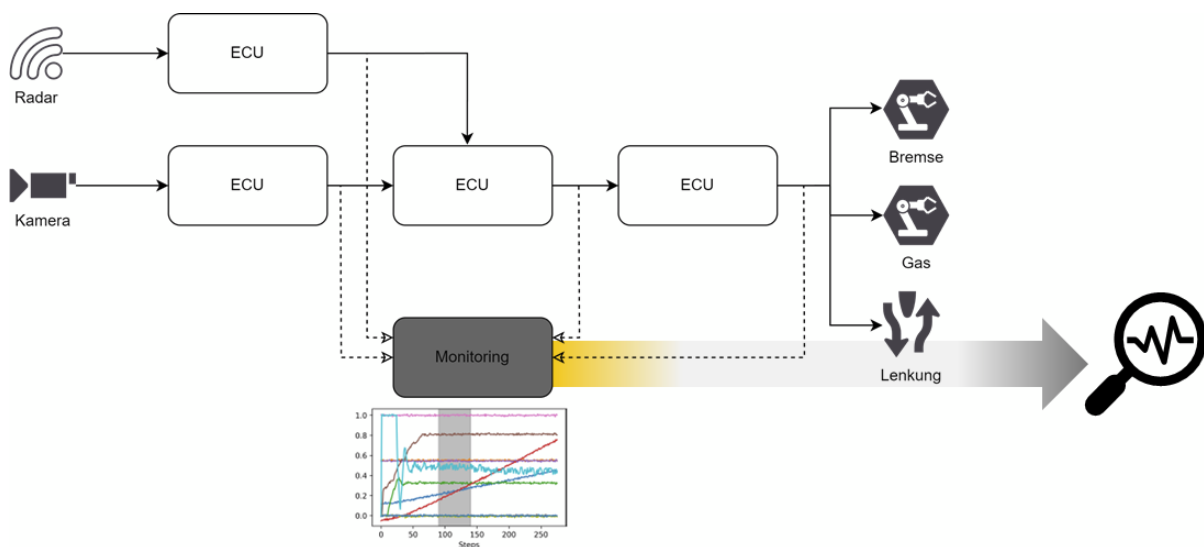


Abbildung 8: Schematische Darstellung der Integration einer Monitoring Plattform

Dies ist relevant, da neu aufgezeichnete Szenarien, die als unkritisch klassifiziert wurden, den bekannten Szenarien des Monitors hinzugefügt werden müssen. So lässt sich die Menge an gemeldeten Auffälligkeiten im zeitlichen Verlauf über den Lebenszyklus eines Fahrzeugs immer weiter verringern. Das senkt den Analyseaufwand und erhöht die Wahrscheinlichkeit, dass kritische Szenarien schnell entdeckt und behandelt werden.

2.3.2 Kontinuierliche Entwicklung von HW/SW Systemen für E/E-Architekturen

Kontinuierlicher Entwicklungsprozess

Die kurzen Zyklen bei der System- und Softwareentwicklung, die für moderne Edge Systeme charakteristisch sind, erfordern kontinuierliche Entwicklungsansätze, was zur Verbreitung von agilen Methoden geführt hat. Diese zielen darauf ab, die Zeit zu verkürzen, die für die Entwicklung, Bereitstellung, Implementierung und Wartung funktionierender, stabiler Systeme benötigt wird. Der Ansatz für einen kontinuierlichen Entwicklungsprozess ist die explizite Berücksichtigung von geänderten Sicherheitsanforderungen und Maßnahmen aus den Erkenntnissen der Betriebsphase, sowie das ReDesign in der Entwurfsphase und das erneute Deployment. Für eine Darstellung des Prozesses lehnt sich das Konzept an das kontinuierliche Entwicklungsparadigma DevOps an.

Das DevOps Paradigma¹ eignet sich für die iterative und agile Entwicklung neuer Funktionen. Bei dem Prozess wird eine enge Verknüpfung von Entwicklung und Betrieb angestrebt. Mit einer zusätzlichen modellbasierten Unterstützung des Prozesses können Modelle während der gesamten Entwicklungs- und Betriebsphase eingesetzt werden, um den gesamten Prozess effizienter zu gestalten². Darauf aufbauend besteht der Ansatz darin, die notwendigen Schritte für die Bearbeitung von Sicherheitsvorfällen wie in AP2 und AP4 sowie das Redeployment zu integrieren, um einen kontinuierlichen Prozess zu erreichen (siehe Abbildung 9).

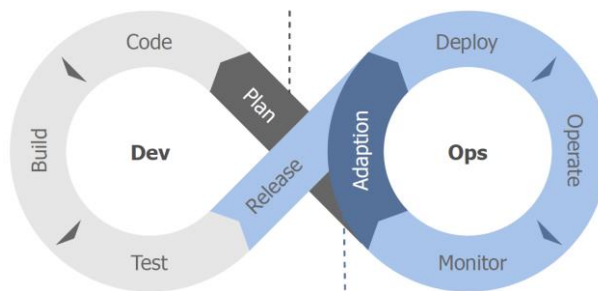


Abbildung 9: DevOps Prozess mit relevanten Phasen für kontinuierliche Entwicklung

Im Entwurfszyklus (Dev) ist die Planungsphase besonders wichtig. Hier wird das System geplant und entworfen. In dieser Phase sollten neben den Modellen der Systemarchitektur auch die für die Allokation erforderlichen Informationen definiert werden. Während des Designs oder beim Übergang

¹ M. A. Lopez-Pena, J. Diaz, J. E. Perez, and H. Humanes, "DevOps for IoT systems: Fast and continuous monitoring feedback of system availability," IEEE Internet of Things Journal, vol. 7, pp. 10695–10707, oct 2020.

² V. P. Betancourt, B. Liu, and J. Becker, "Model-based development of a dynamic container-based edge computing system," in 2020 IEEE International Symposium on Systems Engineering (ISSE), IEEE, oct 2020.

von Dev zu Ops kann die Allokation von Anwendungen zu Hardwarekomponenten und die Konfiguration der Monitoring Plattform automatisch auf Basis der zuvor definierten Informationen bestimmt werden.

Im Betriebszyklus (Ops) ist der Übergang von Monitor zu Deploy besonders wichtig. Diese Phase ist eine implizite Planungsphase, die vom System automatisch gesteuert werden sollte. Im Folgenden wird dies als Adaption bezeichnet, um die notwendigen Schritte für die automatische Entscheidung über das Deployment zur Laufzeit zu integrieren. Zuvor werden in der Monitorphase Änderungen im System und Kontext sowie Sicherheitsvorfälle überprüft. Ist eine Anpassung des Systems erforderlich, wird eine neue Zuordnung und Konfiguration für das System berechnet. Die Berechnung basiert auf den in der Planungsphase definierten Informationen, so dass sie mit den Entwurfsdefinitionen übereinstimmt.

On-Demand Ereignisse für Adaption

Das Monitoring und die anschließende Adaption sind zwei wichtige Komponenten für die Reallokation im Betriebszyklus (Ops). On-Demand-Ereignisse, die auch als dynamische Ereignisse bezeichnet werden, sind Ereignisse, die im System auftreten und eine Änderung verursachen. Im Folgenden wird eine Liste von On-Demand-Ereignissen aufgezeigt, die auf den in³ vorgestellten Reallokations-Szenarien und einer Übersichtsstudie zu dynamischen Ereignissen in selbstadaptiven Internet of Things (IoT)-Systemen basiert⁴, in der analysiert wurde, welche dynamischen Ereignisse im Edge-Kontext die häufigsten Ursachen für die Auslösung von Anpassungen in einem IoT-System sind.

- Neue Funktionen: Neue Funktionen müssen auf das bestehende Edge Netzwerk verteilt werden.
- Zusätzliche Funktionen: Für eine Anwendung können je nach Situation mehrere Instanzen einer Funktion erforderlich sein.
- Softwareausfall und Alterung: Die Ausgeführte Anwendung ist wegen Fehlverhaltens nicht erreichbar. Softwareausfälle, bspw. aufgrund von Speicher-, Hardware- oder Konnektivitätsfehlern.
- Cyberangriffe auf Funktionen: Die ausgeführte Anwendung kann kompromittiert werden und entweder nicht mehr verfügbar sein oder es können Datenschutz- oder Vertraulichkeitsprobleme auftreten.
- Update von Funktionen: Bei der Aktualisierung einer Funktion müssen diese und eventuell neu hinzukommende Funktionen verteilt werden, z. B. um eine Sicherheitslücke zu schließen.

³ V. P. Betancourt, B. Liu, and J. Becker, "Towards policy-based task self-reallocation in dynamic edge computing systems," in 2021 IEEE 19th International Conference on Industrial Informatics (INDIN), IEEE, jul 2021.

⁴ I. Alfonso, K. Garcés, H. Castro, and J. Cabot, "Self-adaptive architectures in IoT systems: a systematic literature review," Journal of Internet Services and Applications, vol. 12, dec 2021.

2.3.3 Überführung von Änderungen und Analysen auf HW/SW Systeme und Monitoring Plattform

Modellbasierte Entwicklungsunterstützung

Um den Entwurf, die Konfiguration und den Einsatz von komplexen dynamischen Edge Computing Systemen zu systematisieren, wurde ein Framework zur Modellierung entwickelt, der die Neuordnung von Services für das kontinuierliche Deployment mit einbezieht. Die Modellierung basiert auf die Beschreibung von vernetzten, serviceorientierten Industrie 4.0 Systemen aus dem SysKit_HW Projekt. Der SysKit Ansatz wurde erweitert, um ihn an das DevOps Paradigma anzupassen. Auf der Grundlage der Modellbeschreibungen werden Deployment Konfigurationen generiert.

Mit der Modellunterstützung sind Anpassungen des Systems möglich. Der vorgesehene Entwicklungsprozess ist in Aktivitäten zur Entwurfszeit und zur Laufzeit unterteilt. Der Schwerpunkt liegt darauf, jeden Schritt mit modellbasierten Techniken zu unterstützen, um die Komplexität zu reduzieren und das Redeployment zu erleichtern. Damit soll es möglich sein, die Services und Maßnahmen nach der Aufarbeitung von Sicherheitsvorfällen wieder in Betrieb zu nehmen.

Transitionen zwischen Entwurf und Betrieb

Die Aktivitäten zur Entwurfszeit und zur Laufzeit sowie die Transitionen sind in Abbildung 10 dargestellt. Der Schwerpunkt liegt darauf, jeden Schritt mit modellbasierten Techniken zu unterstützen, um die Komplexität zu reduzieren und die automatische Überführung von Änderungen zu erleichtern.

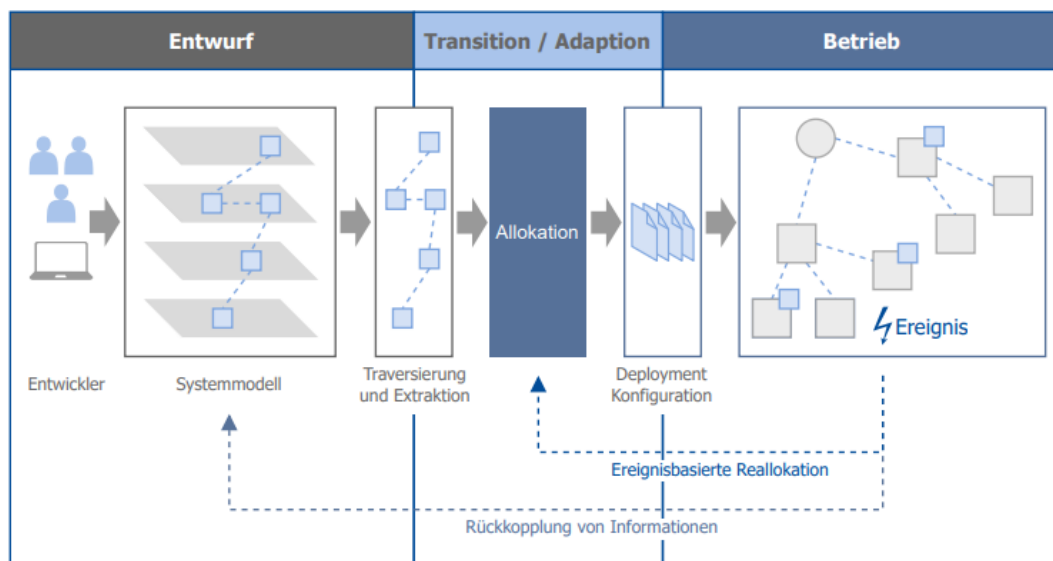


Abbildung 10: Transitionen zwischen Entwurf und Betrieb

Im Entwurf werden die Systemebenen modelliert und die Zuordnungs-, Konfigurations- und Änderungsinformationen miteinander verknüpft beschrieben. Dabei werden u.a. die Umgebung, das Anwendungsszenario, die servicebasierten Funktionen sowie die Wirkungsstruktur und die HW/SW-

Komponenten modelliert. Insbesondere werden Dienste auf der Basis der in ⁵ vorgestellten modellbasierten Servicebeschreibungssprache beschrieben. Die Beschreibung der Services ist von den HW/SW-Komponenten entkoppelt, so dass die Zuordnung der servicebasierten Funktionen zu den HW-Komponenten nachgelagert erfolgen kann.

Beim Übergang von der Entwurfs- in die Betriebsphase müssen die notwendigen Informationen aus der Planungsphase extrahiert werden, um die Metadateninformationen für die Zuordnung während des Betriebs auf schlanke Weise zu nutzen. Hintergrund ist, dass die Systemmodelle weit mehr Informationen und Details enthalten können als die für die Allokation benötigten Informationen. Zu den benötigten Informationen gehören z.B. Kennzahlen zu Ressourcen, Ausführungskosten, Konfigurationen, Änderungen oder Einschränkungen. Um eine schnelle Berechnung der Zuordnung im laufenden Betrieb durchführen zu können, ist eine vorherige Reduktion der zugrundeliegenden Daten auf das Wesentliche vorteilhaft.

Im Betrieb wird der Adaptionsschritt detaillierter betrachtet. Die während des Betriebs von Monitoren gesammelten Ereignisinformationen werden für die ereignisbasierte Anpassung genutzt. Die Ereignisinformationen werden zunächst verarbeitet, um z.B. zu ermitteln, welche Funktionsumfänge und Hardwarekomponenten betroffen sind. Mit diesem Wissen und den Metadaten des Systemmodells wird die Zuordnung im Betrieb vorgenommen. Die Ergebnisse werden in Deployment-Dateien und Konfigurationen übersetzt, so dass auf dieser Basis ein neues Deployment durchgeführt werden kann.

2.3.4 Framework für kontinuierliche Entwicklung und Deployment von HW/SW-Systemen

Entwicklungsframework

Das Entwicklungsframework ist auf Basis des Eclipse Modeling Framework entwickelt. Die benutzten Frameworks sind open source und unter der Eclipse Public License verwendbar. Darauf aufbauend werden drei Hauptteile modelliert: Systemmodelle, Anwendungsszenarien und Abfragen. Diese werden durch einen Bibliotheksmechanismus unterstützt, womit Modelle, Szenarien und Abfragen wiederverwendet werden können. Durch das Zusammenspiel von den drei Teilen und die integrierte verzahnte Modellierung der Allokationsinformationen wird die spätere Extraktion der notwendigen Daten für eine kontinuierliche Adaption ermöglicht. Ein Diagramm der Softwarearchitektur des Werkzeuges ist in Abbildung 11 zu sehen.

Die Umsetzung der Metamodelle basiert auf eigenentwickelten Beschreibungssprachen (DSLs) statt bspw. SysML Modellen, weil dadurch vereinfachtere und gezieltere Beschreibungssprachen für die während der Arbeit analysierten Domänen möglich waren. Die Ansätze dieser Arbeit limitieren sich jedoch nicht auf die hier umgesetzten Metamodelle und können durchaus in einem SysML basierten Tool integriert werden. An der Stelle ist das EMF-basierte Modellierungswerkzeug als eine Demonstrationsplattform für die entwickelten Ansätzen zu verstehen.

⁵ B. Liu, T. Glock, V. P. Betancourt, M. Kern, E. Sax, and J. Becker, "Model driven development process for a service-oriented industry 4.0 system," in 2020 9th International Conference on Industrial Technology and Management (ICITM), IEEE, feb 2020.

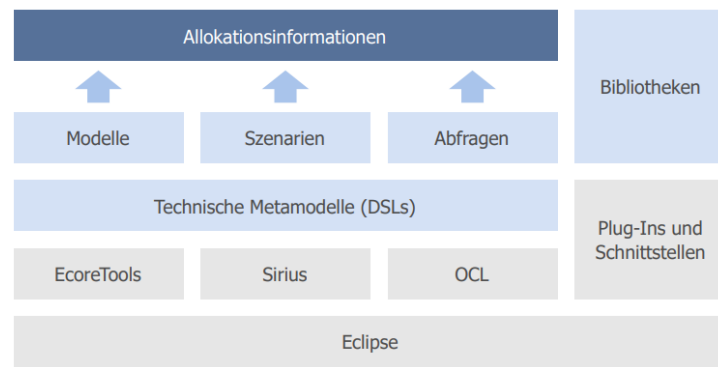


Abbildung 11: Aufbau des Entwicklungsframeworks

HW/SW-Plattformen für kontinuierliche Entwicklung und Deployment

Um ein kontinuierliches Deployment zu realisieren, ist die Integration der oben beschriebenen Methoden in den Betrieb notwendig. Um eine Überführung von Änderungen zu realisieren, ist jedoch nicht nur die Berechnung über eine Zuordnungsentscheidung notwendig, sondern auch eine Hardware/Software-Umgebung, die dies realisieren kann, im Folgenden Edge Framework genannt.

Daher wurde die Softwarearchitektur für Edge Computing Anwendungen analysiert, um eine Kapselung und lose Kopplung von Funktionen (Tasks) zu ermöglichen, so dass sie unabhängig voneinander angepasst, betrieben und aktualisiert werden können. Zu dem Zweck wurde eine serviceorientierte bzw. servicebasierte Architektur gewählt. Darüber hinaus ist eine Softwareumgebung erforderlich, damit die gekapselten Funktionen im laufenden Betrieb geändert, integriert und aktualisiert werden können. Dafür wurden Virtualisierungskonzepte analysiert und der Einsatz von Containern gewählt. Außerdem wird eine Instanz im Framework benötigt, die das Deployment der gekapselten Funktionen koordiniert und durchführt, sowie in der die Entscheidungen über eine Allokation integriert werden können. Zu diesem Zweck wurde ein Orchestrierung Framework ausgewählt und Mechanismen zur Steuerung des Deployments eingesetzt bzw. erweitert.

Eine detaillierte Beschreibung des Edge Frameworks, das teilweise im Projekt entwickelt und verwendet wurde, ist in Kapitel 7 der im Kontext dieses Projekts entstandenen Dissertation⁶ zu finden. Die wichtigsten Bestandteile werden im Folgenden zusammengefasst.

Service basierte Architektur für Edge Systeme: Die Flexibilität, die eine serviceorientierte Architektur mit sich bringt, eignet sich für die Realisierung von selbstadaptiven Edge Computing Systemen. Daher wird diese als Basis für die Softwarearchitektur des Frameworks verwendet. Das setzt voraus, dass die Softwarekomponenten durch die Definition von Service Consumer und Service Provider miteinander kommunizieren. Für die Verwendung im Projekt werden die Funktionen in Services gekapselt.

Virtualisierungsansätze für Edge Systeme: Verschiedene Ansätze existieren für das flexible Deployment von Anwendungen im Edge Computing Kontext. Die beiden wichtigsten Alternativen zur Softwarevirtualisierung sind die Virtualisierung mittels Container oder mittels Hypervisor. Ein

⁶ V. P. Betancourt, "Task Allokation für effiziente Edge Computing Systeme," Karlsruher Institut für Technologie (KIT), 2023, doi: 10.5445/IR/1000158306.

schematischer Aufbau der Container Virtualisierung im Vergleich zum Hypervisor ist in Abbildung 12 dargestellt. In einer Studie⁷ wurde die Verwendung von Containern für das kontinuierliche Deployment von Funktionen und deren Vergleich mit anderen Technologien analysiert. Verschiedene Technologien wie Hypervisoren und Container sowie Computing-Ansätze wie Edge⁸ und Fog Computing⁹ wurden bereits verglichen. Als Fazit für dieses Projekt lässt sich ableiten, dass Container für Edge Computing Systeme nicht nur für industrielle, sondern auch für Fahrzeuganwendungen zunehmend an Relevanz gewinnen¹⁰.

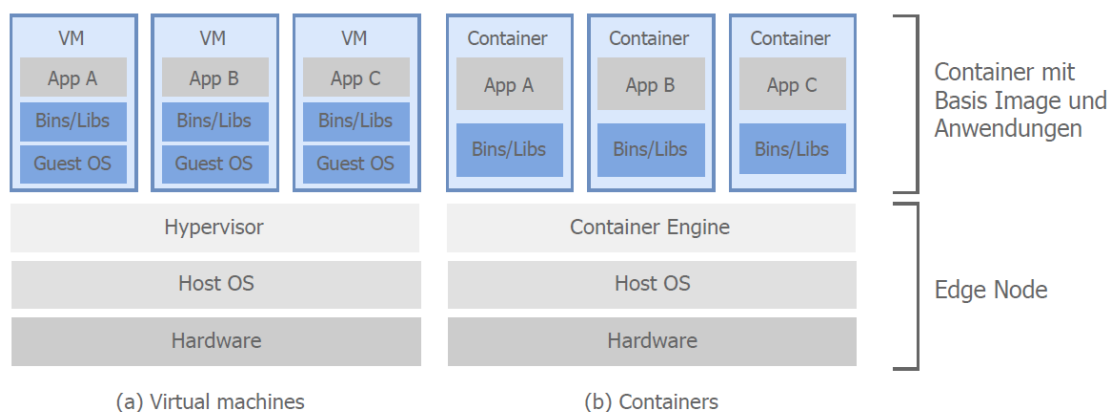


Abbildung 12: Schematischer Aufbau von Hypervisor und Container Virtualisierung

Für Teilarbeiten im Projekt wurde aus den folgenden Gründen ein containerbasierter Ansatz gewählt. Erstens ermöglicht es ein flexibles, schnelles und kontinuierliches Deployment von Anwendungen. Daher ist der Ansatz im Cloud Bereich weit verbreitet. Die Nutzung für Edge Computing hat in den letzten Jahren zugenommen und optimierte Software Stacks für den Einsatz in eingebetteten Systemen sind heute verfügbar. Darüber hinaus gibt es Arbeiten zur Containerisierung von Microservices mit einer sehr effizienten Boot-up Zeit, die für ein flexibles Deployment von Tasks interessant ist. Wenn das Basis-Image bereits deployed ist, werden nur die Microservices geladen. Das ist ein Faktor, der bei der Entscheidung über die Containerplatzierung berücksichtigt werden kann.

Orchestrierung und Deployment Mechanismen: Orchestrierung wird häufig im Zusammenhang mit serviceorientierten Architekturen und Virtualisierung eingesetzt, um die Ausführung dynamischer Dienste zu koordinieren. Orchestrierungslösungen wie k3s bringen Managementmechanismen mit sich, die das Deployment von containerisierten Diensten durch deklarative Konfiguration oder Automatisierungen erleichtern. Der deklarative und indirekte Weg ist durch die Verwendung von Konfigurationsdateien. Hierzu werden aus der Allokationsmethode nach der Berechnung die

⁷ V. Cardellini, F. L. Presti, M. Nardelli, and F. Rossi, "Self-adaptive container deployment in the fog: A survey," in *Algorithmic Aspects of Cloud Computing*, pp. 77–102, Springer International Publishing, 2020.

⁸ O. Oleghe, "Container placement and migration in edge computing: Concept and scheduling models," *IEEE Access*, vol. 9, pp. 68028–68043, 2021.

⁹ S. Rahul and R. Aron, "Fog computing architecture, application and resource allocation: A review," 2021.

¹⁰ Naren, A. K. Gaurav, N. Sahu, A. P. Dash, G. S. S. Chalapathi, and V. Chamola, "A survey on computation resource allocation in IoT enabled vehicular edge computing," *Complex & Intelligent Systems*, jul 2021.

zugehörigen Konfigurationsdateien mit den neuen Allokationen generiert. Die Konfigurationsdateien werden an den Orchestrator übergeben, um das Deployment von Anwendungen zu veranlassen.

Aufbau des Edge Frameworks: Die Struktur des Edge Frameworks, welches zum Teil im Kontext dieses Projekts entwickelt wurde, ist in der schematischen Darstellung in Abbildung 13 zu sehen. Als Beispiel sind drei EdgeNodes dargestellt. Jeder hat ein Host Betriebssystem, eine Agenteninstanz für die Orchestrierung und eine Container Laufzeit. Auf diesen werden Container ausgeführt, die die Implementierung der Services oder Tasks mit den notwendigen Bibliotheken kapseln. Außerdem gibt es einen Masternode, auf dem die zentrale Instanz des Orchestrators ausgeführt wird. Dieser besitzt die Komponenten zur Verwaltung der Agenten und damit der containerisierten Services. Hierbei lassen sich der Controller Manager und der Scheduler hervorheben. Änderungen werden in der Monitoring Phase überwacht. Im Falle einer Änderung aktiviert der Controller Manager die Allokationsmethode, um eine neue Allokation zu finden. Die Allokationsmethode berechnet die Allokation auf der Grundlage der Metadaten und der aufgetretenen Änderungen. Für die neue Zuweisung werden die entsprechenden Konfigurationsdateien erstellt und an den Orchestrator übergeben. Anschließend führt der Orchestrator die neue Bereitstellung auf der Grundlage der berechneten Zuweisung aus.

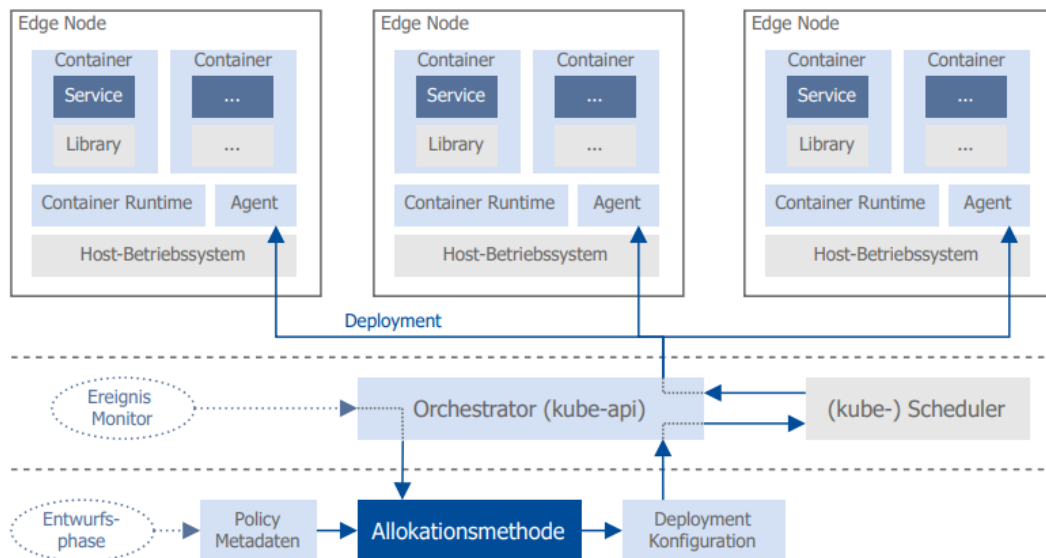


Abbildung 13: Schematischer Aufbau des Edge Frameworks

2.4 AP4: Methoden für datengetriebene Unterstützung der Entwurfsphase

AP4 befasst sich mit der automatischen und manuellen Analyse des UNCOVER-Prozesses gemäß der Darstellung des UNCOVER Prozesses in AP2. Ziel der automatischen Analyse ist es, unbekannte Szenarien zu untersuchen und mit bekannten Szenarien aus der Designzeit zu vergleichen. Dieser Vergleich wird in mehreren Schritten durchgeführt. Die automatische Analyse beinhaltet eine KI-basierte Identifikation von Anomalien, die über traditionelle regelbasierte Ansätze hinausgeht. Dabei werden maschinelle Lernverfahren eingesetzt, um Muster in den Daten zu erkennen, die von bekannten Szenarien abweichen. Besonderes Augenmerk wird dabei auf die Bereiche gelegt, in denen die Abweichung von bekannten Szenarien auf Komponentenebene am größten ist.

2.4.1 Konzept und Methodik für datengetriebene Entwurfsunterstützung – Analysemethoden, Taxonomie und Metadaten

Die in AP1 identifizierten Signale wurden in AP4 untersucht. Diese Signale werden systematisch erfasst und klassifiziert, um ein umfassendes Verständnis der Wechselwirkungen zwischen Fahrzeug und Umwelt zu gewährleisten. Die identifizierten und aufgenommenen Signale sind:

- ACC Differenzgeschwindigkeit [m/s]
- ACC Abstandsunterschied [m]
- ACC Zielabstand [m]
- Objekt-ID [1]
- Gaspedalstellung [0, 1]
- Lenkradwinkel [-1, 1]
- Bremspedalstellung [0, 1]
- Fahrzeug-ID [1]
- Geschwindigkeit [m/s]
- Ego-Position in Y [m]
- Position in X [m]
- Relative Position Objekt in X [m]
- Relative Position Objekt in Y [m]

In AP4 sind diese Daten nun verfügbar und als Zeitreihen organisiert, was eine detaillierte Analyse und Weiterentwicklung des automatisierten Fahrsystems ermöglicht. Ziel der Analyse ist die Erkennung von Anomalien in den aufgenommenen Szenarien. In der Datenanalyse werden Anomalien häufig in verschiedenen Dimensionen betrachtet. Dabei wird zwischen 1-dimensionalen, 2-dimensionalen und n-dimensionalen Anomalien unterschieden, siehe Abbildung 14.

Ein-dimensionale Anomalien beziehen sich auf Abweichungen entlang eines einzigen Merkmals. Ein Beispiel hierfür ist die Geschwindigkeitsüberwachung, bei der Abweichungen von einem festgelegten Grenzwert als Anomalie betrachtet werden. Bei zweidimensionalen Anomalien werden Abweichungen in einem zweidimensionalen Raum betrachtet, was bedeutet, dass zwei Merkmale gleichzeitig analysiert werden. Ein Beispiel wäre die Betrachtung von Geschwindigkeit und Lenkwinkel, wobei Anomalien auftreten können, wenn beide Werte gleichzeitig von den erwarteten oder normalen Bereichen abweichen.

Mit zunehmender Dimensionalität (N-dimensionale Anomalien) wird es immer schwieriger, Anomalien zu erkennen. Dies liegt daran, dass in höherdimensionalen Räumen die Daten komplexer werden und traditionelle regelbasierte Ansätze, die auf festen Grenzwerten oder Anforderungen basieren, oft nicht mehr ausreichen. In niedrigeren Dimensionen können regelbasierte Methoden effektiv sein und werden

in UNCOVER auf der Monitoring-Plattform eingesetzt. Höherdimensionale Daten, wie sie in diesem Projekt vorliegen, erfordern jedoch den Einsatz von KI-Methoden, um Muster und Anomalien in den komplexen Datensätzen zu erkennen und zu verstehen. Daher wird im Folgenden die verwendete KI-Methode beschrieben.

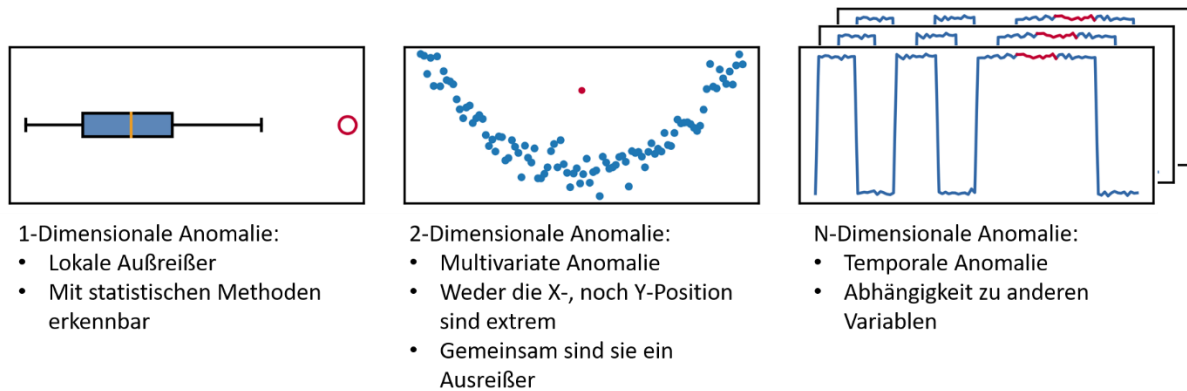


Abbildung 14: Definitionen von Anomalien

2.4.2 Ansätze zur Integration in eine modellbasierte Entwicklungsumgebung

Um Sicherheitsvorfälle anhand ihrer Eigenschaften zu gruppieren (eng.: „clustern“) und die Kritikalität einzelner Zeitreihen abzuschätzen wird ein Neuronales Netz entwickelt und mit vordefinierten Szenarien trainiert. Unbekannte Szenariendaten können auf Sicherheitsvorfälle in Bezug auf Betriebs- und Informationssicherheit hinweisen. Dies liefert erste Indikatoren zur Einordnung der Vorfälle.

Dabei wird folgendes Vorgehen angewandt: Anhand der Trainingsdaten und dem initialen, manuellen Clustern der Szenarien werden Ähnlichkeiten zwischen den Szenarien definiert. Anschließend wird das Netz mit bekannten unkritischen Clustern trainiert und lernt, bekannte von unbekannten Szenarien zu unterscheiden. Ausgabe des Netzes sind die Distanzen zu den existierenden Clustern, sowie die Kritikalität der einzelnen Zeitreihen der Signale.

Das Zuordnen (eng.: „mapping“) von Sicherheitsvorfällen in Szenarien auf Komponenten und Teilfunktionen der Software und die Abschätzung der Kritikalität der zugehörigen Zeitreihen der Signalflüsse wird konzeptionell erarbeitet. Die Abschätzung der Kritikalität entsteht in der automatisierten Analyse (siehe AP2) der Szenarien durch das Neuronale Netz. Durch die Kombination aus der Kritikalität der Zeitreihen und dem in AP2 von ENCO entwickelten Systemmodell können Vorfälle in Bezug auf ihre Auswirkungen auf einzelne Komponenten des Systems klassifiziert werden.

Durch das Clustern der Szenarien und des Mappings der Sicherheitsvorfälle auf Komponenten und Softwarefunktionen können neue Cluster definiert werden, oder bereits bestehende Cluster ergänzt werden. Das Netz kann mit den neuen Clustern und Szenarien erneut trainiert (eng.: „retrained“) werden, sodass die Szenarien im Analyseprozess automatisiert erkannt und zugeordnet werden können.

Das Entwickelte NN verwendet einen Autoencoder, um eine latente Repräsentation zu lernen und diese dann in bekannte Szenarien zu klassifizieren. Der Decoder hilft beim Training und reduziert die Notwendigkeit für erneutes Training. Das Modell verwendet MC-Dropout-Sampling, um die

Unsicherheit der Klassifikationsvorhersage zu schätzen, und markiert Eingabemuster als Anomalien basierend auf einer definierten Unsicherheitsschwelle. Im Falle einer Anomalie wird der DeepLIFT-Algorithmus angewendet, um sie in den Eingabedaten zu lokalisieren.

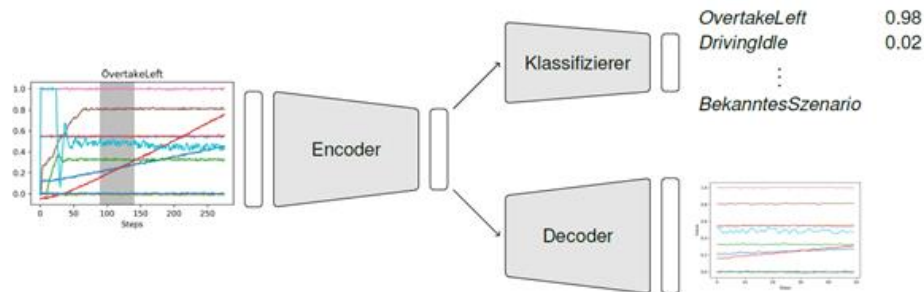


Abbildung 15: Struktureller Aufbau des Neuronalen Netzes

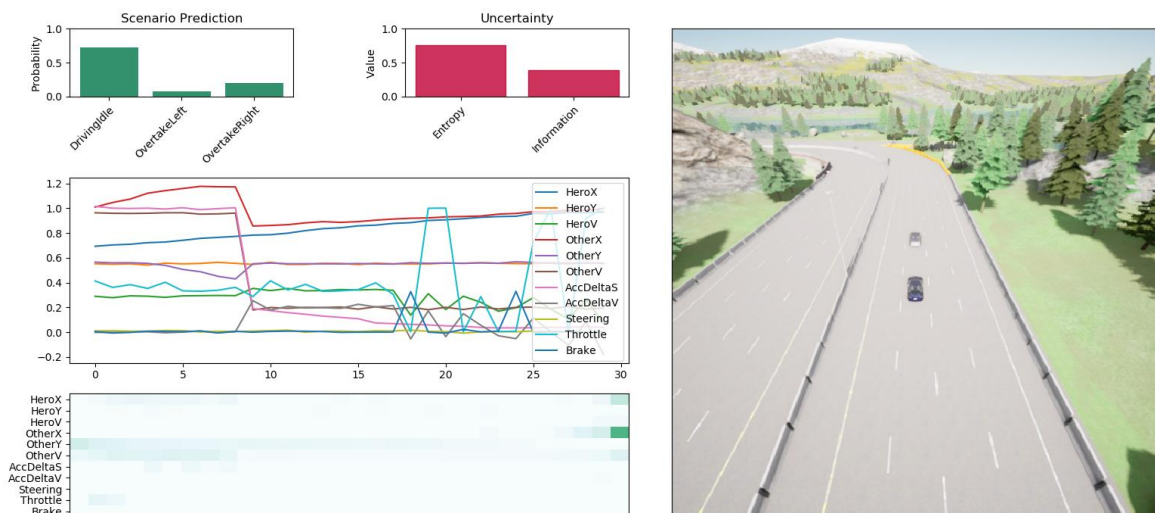


Abbildung 16: Ergebnis des Neuronalen Netzes

2.4.3 Ansätze zur Integration in einen modellbasierten Entwurf

Das Ergebnis der automatischen Analyse ist entweder, dass die Anomalie mit Hilfe der KI-basierten Methoden einem bestimmten, bereits existierenden Cluster zugeordnet werden konnte. In diesem Fall erfolgt die Übergabe an RiSA zur statistischen Auswertung. Hier können Häufungen und Muster erkannt werden, die weitere Einblicke in die Situationen geben, in die das Fahrzeug verwickelt war.

Kann die Anomalie keinem Cluster zugeordnet werden, wird sie im Systemmodell, siehe Abbildung 17, lokalisiert und an ENCO weitergeleitet. Dort werden weitere Untersuchungen durchgeführt, um die Ursache der Anomalie zu identifizieren und geeignete Maßnahmen zu ergreifen.

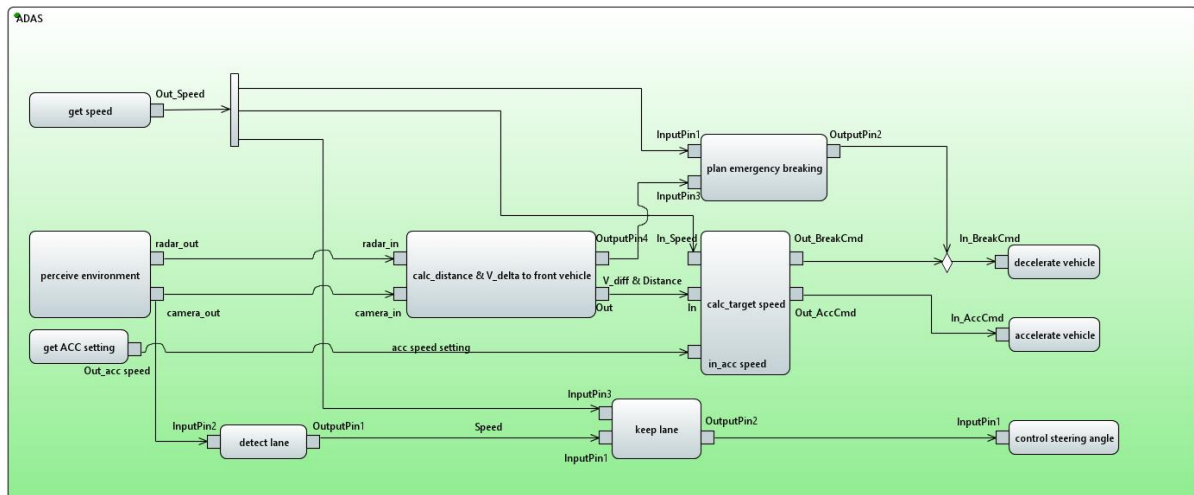


Abbildung 17: Systemmodell der Fahrfunktion

Dieser Prozess trägt dazu bei, ein wachsendes Wissen und einen umfassenden Szenarienkatalog über die verschiedenen Situationen, in denen sich das Fahrzeug befindet, zu schaffen. Durch die kontinuierliche Analyse und Weiterentwicklung können potenzielle Risiken frühzeitig erkannt und behoben werden, was zu einer kontinuierlichen Verbesserung der Leistungsfähigkeit und Sicherheit des Fahrzeugs beiträgt. Risiken frühzeitig erkannt und behoben werden, was zur kontinuierlichen Verbesserung der Leistung und Sicherheit des Fahrzeugs beiträgt. Die gesamte Prozesskette ist in dargestellt.



2.5 AP5: Datenschutzrechtliche Betrachtung

2.5.1 Rechtswissenschaftliche Analyse und Sachverhaltsmodellierung

Es wurde ein Sachverhalt entwickelt, bei dem von einem nicht näher definierten Sicherheitsvorfall ausgegangen worden ist, der in einem Kraftfahrzeug mit automatisierten Fahrfunktionen i.S.d. § 1a Abs. 2 StVG während einer Fahrt auftritt und der als erkannte Anomalie an den Hersteller zwecks weiterer Bearbeitung gesendet wird. Es wurde untersucht, welche Rechtsnormen aus welchen Domänen im Kontext des automatisierten und vernetzten Fahrens in Bezug auf den Usecase einschlägig sind. Bei dem Abgleich (Mapping) der straßenverkehrs- und haftungsrechtlichen Rollen auf das Datenschutzrecht, konnten Limitierungen der datenschutzrechtlichen Rollen in Bezug auf die Schutzrichtung der Betroffenen identifiziert werden.

	Verantwortliche Stelle gemäß DSGVO	Betroffene Person gemäß DSGVO
Datenschutz		
	Halter	Fahrer
	Hersteller	Mitfahrer
	Werkstätten und Händler	Halter
	Mobilitätsdienstleister	Eigentümer
	Infrastruktur- und	Verkehrsteilnehmer
	Telekommunikationsanbieter	
	Notrufstelle und Pannenhilfe	
	Versicherung	
	Datentreuhänder	
StVG und BGB		

Abbildung 19: Mapping Rollen StVG-Datenschutz

Beispielhaft wurde das Rollenmodell im Datenschutz am Beispiel des datenschutzrechtlich Verantwortlichen gemäß Art. 4 Nr. 7 DSGVO auf das Straßenverkehrsrecht übertragen. Dabei wurden als datenschutzrechtliche Pflichten u.a. Transparenz gemäß Art. 5 Abs. 1a DSGVO, Privacy by Design gemäß Art. 25 Abs. 1 DSGVO, Art. 32 Abs. 1 DSGVO sowie die Gewährleistung der Rechte der betroffenen Person gemäß Art. 13 ff. DSGVO.

Normenhierarchie

Als Basis für die spätere Modellierung von Anforderungen wurde die Systematik der Normenhierarchie abstrakt-generell und sachverhaltsspezifisch aufbereitet.

Beispielsweise können nationale Rechtsverordnungen (z.B. eine datenschutzrechtliche Regelung) durch internationale Verordnungen (Datenschutzgrundverordnung) verdrängt werden, sofern keine Öffnungsklausel in der höherrangigen Norm eine Konkretisierung durch eine niederrangige Norm erlaubt. (Beispiel: Öffnungsklauseln in der DSGVO, die Konkretisierungen im nationalen Recht ermöglichen oder Regelungen in Gesetzen die eine zukünftige Konkretisierung durch

Rechtsverordnungen ermöglichen). Zu den in AP 5.1 identifizierten einschlägigen Normen zählen sowohl internationale als auch nationale Rechtsvorschriften (wie z.B. Wiener Übereinkunft, StVG und AFGBV) mit unterschiedlichem Rechtscharakter (Verordnungen, Richtlinien, Gesetze) sowie Vorgaben von Standardisierungsgremien (UNECE /ISO). Die Rangfolge der Rechtsvorschriften hinsichtlich der Anwendbarkeit muss berücksichtigt werden. Grundsätzlich sind Normen von Standardisierungsgremien nicht bindend. Durch einen Verweis eines Gesetzes oder einer Verordnung auf eine technische Norm werden sie rechtsverbindlich. Bei den im Rahmen des Projekts betrachteten Normen wurden diese durch die jeweiligen Verweise rechtsverbindlich.

Zum weiteren Monitoring wurden im Coodex-Tool exemplarische rechtliche Anforderungen an die Sensoren des Fahrzeugs als tabellarische Einträge getrackt. Die Daten, die aufgrund gesetzlicher Regelungen erfasst werden müssen, wurden kategorisiert und für die Integration in die Methodenentwicklung bereitgestellt. Hierzu wurde ein Fragebogen erstellt und ausgewertet.

Als gesetzlich erforderliche Daten wurden insbesondere § 1g Abs. 1, 3 StVG identifiziert. Diese Norm hat den Hersteller als Adressat und gibt in § 1g Abs. 2 StVG konkrete Datenarten und Dateiformate vor.

(Fundstelle: BGBl. I 2022, 1007)

Während des Betriebs sind bei den in § 1g Absatz 2 des Straßenverkehrsgesetzes genannten Anlässen im Kraftfahrzeug mit autonomer Fahrfunktion folgende Daten zu erfassen.

Daten	Beispiel Dateiformat
1. Fahrzeugidentifizierungsnummer	Alphanummerische Zeichen [A-Z; 0-9] Beispiel: AAAAAA654398GFRDE
2. Positionsdaten	Breiten- und Längengrad [±ddd.ddddd, Angabe in ± Graden (°) und Dezimalgraden, 5 Nachkommastellen] Höhenangaben in Meter Ausgabe im Globalen Positionsbestimmungssystem – Austauschformat als Abfolge von Punkten, in denen eine Änderung der Fortbewegungsrichtung erfolgt; Angabe des (Karten-)Bezugssystems.
3. Anzahl und Zeiten der Nutzung sowie der Aktivierung/Deaktivierung der autonomen Funktion	Datum (Jahr:Monat:Tag), Zeit (Stunde:Minute:Sekunde), Beispiel: 2019-07-16, 05:25:12
4. Anzahl und Zeit der Freigabe von alternativen Fahrmanövern	Anzahl, Einzelzeiten (Stunde:Minute:Sekunde)
5. Systemüberwachungsdaten (Beginn/ Ende) samt Softwarestand	Alphanummerische Zeichen [A-Z; 0-9] samt Erklärung Beispiel: P0601 Motorsteuergerät – Speicher Prüfsummenfehler
6. Umwelt- und Wetterbedingungen	Temperatur/°C, Helligkeit/Beleuchtungsstärke/lux, Stellung des Scheibenwischers an/aus
7. Vernetzung	Vernetzungsparameter wie beispielsweise Übertragungslatenz und verfügbare Bandbreite
8. Name der aktivierten/deaktivierten passiven und aktiven Sicherheitssysteme, Zustand, auslösende Instanz (System oder extern)	Name des Systems, Zustand, Instanz Beispiel: Notbremssystem, aktiv, Systemfunktionsfähigkeit
9. Fahrzeugbeschleunigung in Längs- und Querrichtung	Numerische Werte in Meter pro Sekunde zum Quadrat
10. Geschwindigkeit	Numerischer Wert in Meter pro Sekunde
11. Status der lichttechnischen Einrichtungen	Beispiel: Blinken an/aus Tagfahrlicht an/aus
12. Spannungsversorgung des autonomen Kraftfahrzeugs	Numerischer Wert in Volt
13. Von extern an das Fahrzeug gesendete Befehle und Informationen	Gesendetes Format der Befehle sowie Metadaten zu Informationen: Dateigröße, Dateiformat, Quelle, Ziel, Übertragungszeit

Abbildung 20: Datenarten und -formate nach § 1g StVG

Es wurde untersucht, inwiefern die Verarbeitung und Weitergabe zum Zweck der Fehlerbehebung nach § 1 g Abs. 5 Nr. 1.2 StVG durch Hersteller erfolgen kann. Hierbei konnte festgestellt werden, dass zunächst die Einschränkung besteht, dass keine personenbezogenen Daten übermittelt werden dürfen. Auch sind die erlaubten Zwecke auf solche des verkehrsbezogenen Allgemeinwohles sowie die wissenschaftliche Forschung im Bereich der Digitalisierung, Automatisierung und Vernetzung der Unfallforschung im Straßenverkehr beschränkt. Als erlaubte Empfänger der Daten Hochschulen und Universitäten sowie außeruniversitäre Forschungseinrichtungen aufgezählt. Hersteller wären somit davon ausgenommen.

Allerdings ist eine Übertragung an das Fahrzeug gemäß Anlage 1 Nr. 13 AFGBV an das Fahrzeug selbst vorgesehen, damit die Daten in einem Datenspeicher ereignisbasiert und zu dem Zweck der Verbesserung der Verkehrssicherheit erfasst, gespeichert und verwendet werden sollen. Zudem sind gemäß Anlage 1 Nr. 15 AFGBV Anforderungen bezüglich der Sicherheit im Bereich der Informationstechnologie in der jeweils geltenden Fassung der UN-Regelung Nr. 155 einzuhalten. Sofern die Daten einen Personenbezug enthalten, sind gemäß Anlage 1 Nr. 6 AFGBV technische und organisatorische Maßnahmen sowie die Grundsätze von Privacy by Design und by Default gemäß Art. 25 DSGVO einzuhalten.

Als Mittel zur Umsetzung dieser Anforderungen wurden Datenminimierungsmöglichkeiten untersucht, wobei zunächst die Möglichkeiten von Anonymisierungstechniken näher betrachtet wurden.

Rechtliche Anforderungen an die Anonymisierung von Daten

Die Anforderungen an eine Datenübertragung gemäß der Anlage 1 der AFGBV Teil 1 Nr. 6 wurden untersucht und die Anonymisierung als datenminimierendes Mittel zur Umsetzung diesen Anforderungen gegenübergestellt. Hierbei wurden verschiedene Level und Methoden der Anonymisierung betrachtet sowie die rechtlichen Optionen bei fehlender Möglichkeit der Anonymisierung betrachtet. Hierzu wurden dafür geeignete technische und organisatorische Maßnahmen identifiziert.

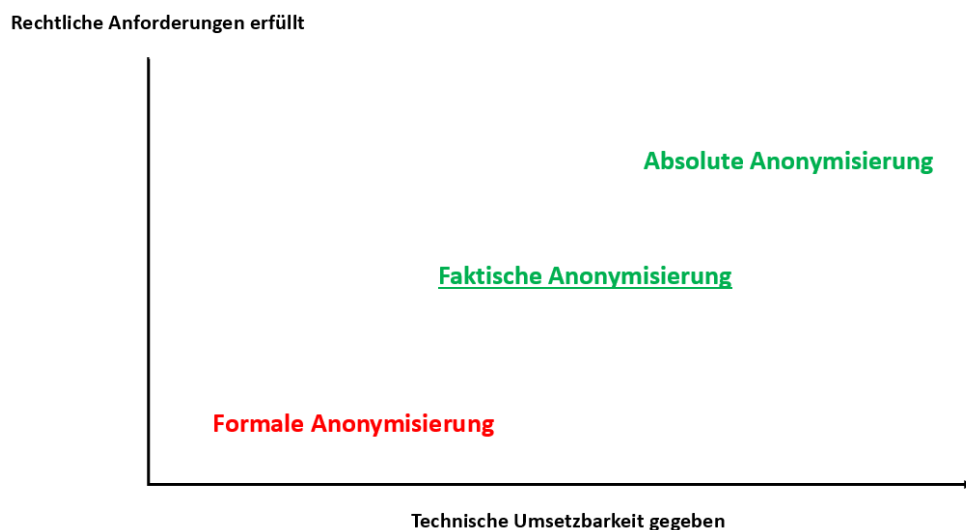


Abbildung 21: Anonymitätslevel

2.5.2 Konzeption/Modellierung Überführung der Anforderungen

Im Rahmen des AP 5.2 wurde auf Basis der Analyse in AP 5.1 die Modellierbarkeit der Normenhierarchie sowie die Modellierbarkeit des Prüfprozesses zur Anonymisierbarkeit von relevanten Mobilitätsdaten zur Rückführung in die Monitoring Plattform untersucht.

Die in AP 5.1 identifizierten rechtlichen Anforderungen erfordern eine Berücksichtigung der identifizierten Normenhierarchie. Die relevanten ISO-Normen und die UN ECE Regulations werden in Anhang 1 AFGVB referenziert. Eine Abbildung der rechtlichen Anforderungen als Modell wurde zunächst als Klassendiagramm konzipiert. Die rechtlichen Normen werden als Klassen mit entsprechenden Attributen modelliert. Zwischen der privatrechtlichen Normierung und der gesetzgeberischen Normierung wird die Relation *verweistAuf* eingeführt um somit die Einbindung der privatrechtlichen Normierung abzubilden. Die Normenklassen werden mit *Namen*, *Datum*, *Autor* als Attribute versehen. Einzelne Paragraphen eines Gesetzes werden als Unterklassen des Gesetzes modelliert. Diese beinhalten Attribute wie *"recht"*, *"pflicht"*, *"gebot"*, *"verbot"* um die Klassifikation der jeweiligen Norm abzubilden. Die Normenebene auf der sich die Regulierung befindet (international, national) wird durch die Benennung der Klasse abgebildet. Die Art der Norm (Gesetz, Verordnung, Richtlinie, Satzung) wird als Attribut dargestellt. Die Höherrangigkeit einer Norm kann somit über den Namen und die Normenart abgebildet werden. Das Konzept ist grobgranular in Abbildung 22 dargestellt. Eine konkrete Abbildung der Modellierung der Normenhierarchie ist in Abbildung 23 ER-Model exemplarisch für die Klassen "Gesetz" und "Rechtsverordnung" auf nationaler Ebene dargestellt und liefert abstrakt-generelle Elemente, die bei der konkreten Umsetzung in ein Tooling zu berücksichtigen sind.



Abbildung 22: Sachverhaltsspezifische Abbildung der Normenhierarchie (Datenschutz und IT-Sicherheit beim autonomen Fahren)

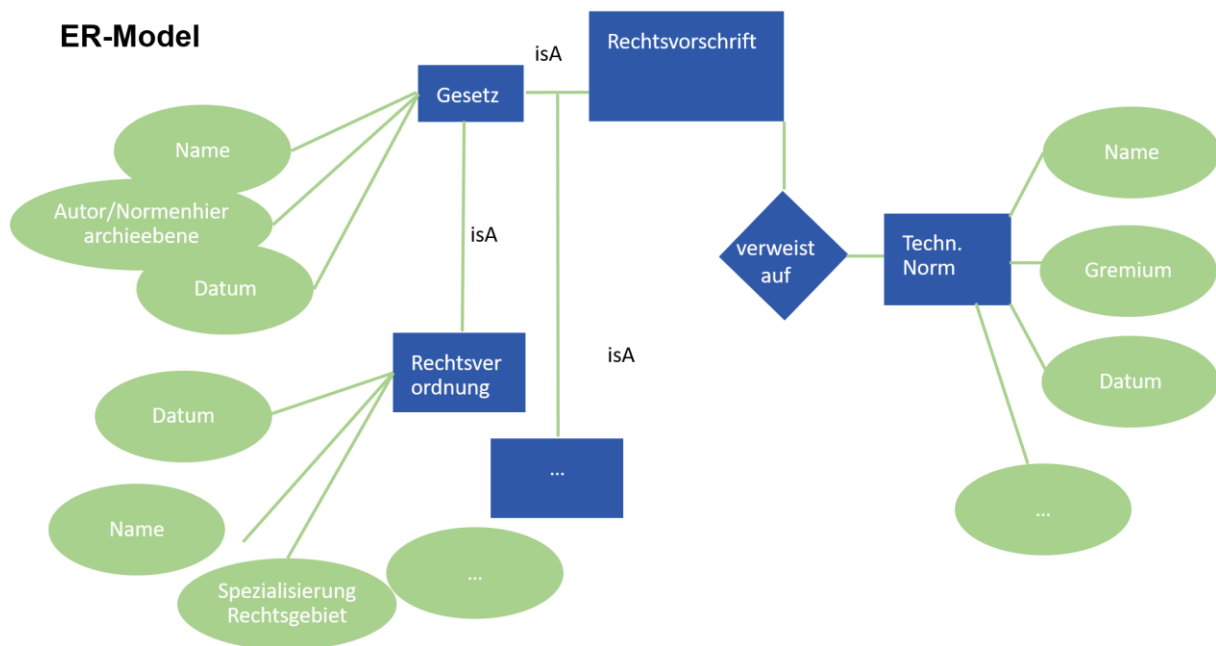


Abbildung 23: Modellierung der Normenhierarchie

Für die Anonymisierung wurde ein Prüfprozess entwickelt, der die einzelnen Prüfprozessschritte beinhaltet. Im Rahmen des Prüfprozesses ist zunächst zu beurteilen, inwiefern ein Personenbezug in den Daten vorliegt. Diese Beurteilung ist nicht trivial, da sie das jeweilige Wissen desjenigen zu berücksichtigen hat, der mit den Daten umgeht. Im vorliegenden Fall handelt es sich hierbei um den Hersteller des Fahrzeugs, der über weiteres Wissen zu den einzelnen Fahrzeugen verfügt. Wenn die Daten keinen Personenbezug aufweisen können sie in die Monitoring Plattform überführt werden. Sofern die Daten jedoch einen Personenbezug aufweisen, ist das Vorliegen einer Rechtsgrundlage für die Verwendung in der Monitoring Plattform zu prüfen. Wofern dieser vorliegt, können die Daten verwendet werden, andernfalls ist die Anonymisierbarkeit der Daten zu prüfen. Zu berücksichtigen ist hierbei das Vorliegen einer Rechtsgrundlage für die Anonymisierung der Daten. Sofern diese vorhanden ist, kann die Anonymisierung durchgeführt werden. Hierbei ist das Zusatzwissen, der Zeitpunkt der Anonymisierung und der Aufwand für die Anonymisierung zu berücksichtigen.

Überführung in Tool als Proof of Concept: Eine exemplarische Umsetzung wurde mit dem AP Partner RISA im Tool Coodexx als Proof of Concept durchgeführt. Die Abbildung 24 zeigt die Modellierung einzelner Paragraphen der StVG. Die Berücksichtigung von datenschutzrechtlichen Anforderungen kann mit Hilfe des Tools, wie in Abbildung 25 ersichtlich, einzelnen, erfassten Datenströmen hinzugefügt werden. Hier setzt dann der Prüfprozess zur Anonymisierbarkeit der Daten an mit dessen Hilfe eine erste Orientierung zur Anonymisierung der verwendeten Daten erfolgt. Eine automatisierte Durchführung dieses Prüfprozesses ist bisher aufgrund der Komplexität der Bewertungsfaktoren (Zeit, Wissen, Aufwand) nicht möglich. Die abstrakt-generelle Abbildung der Prozessschritte kann jedoch für eine Workflow-Implementierung herangezogen werden.

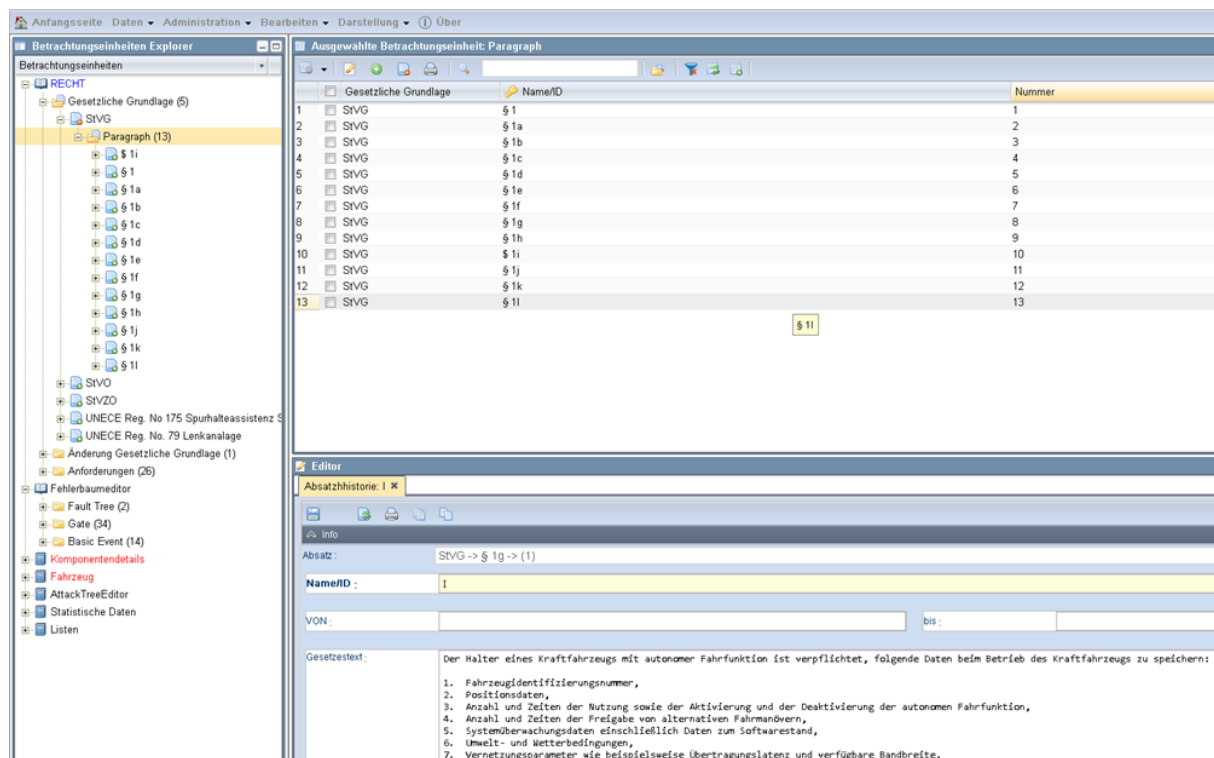


Abbildung 24: Auszug Überführung in Coodexx-Tool I

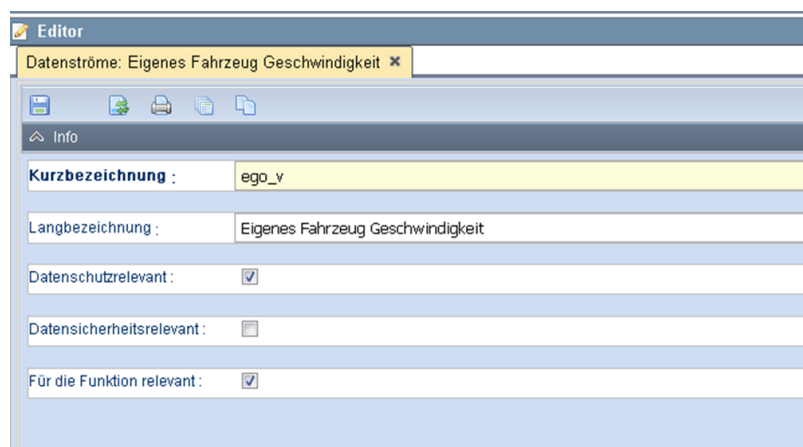


Abbildung 25: Auszug Überführung in Coodexx-Tool II

2.5.3 Handlungsempfehlungen

Als Handlungsempfehlungen wurden folgende Erkenntnisse im Projektverlauf gewonnen und aufbereitet dargestellt: Die "Flucht aus dem Datenschutz(recht)" ist im engen Rahmen generell möglich durch technische Maßnahmen, die den Personenbezug im Rahmen von Anonymisierungsmaßnahmen entfallen lassen. Hersteller sind jedoch auf personenbezogene Daten angewiesen. Als Regelungslücke wurde die nicht vorhandene Rechtsgrundlage zur Sicherheitsvorfallserkennung identifiziert. Insoweit ist der Gesetzgeber gehalten, diese im Wege einer Rechtsanpassung zu erlassen.

Zunächst gilt es Rechtsgrundlagen zu schaffen und diese mit Regelbeispielen zu konkretisieren bei gleichzeitigen risikobasierten Transparenz-pflichten und kompensierenden Schutzmaßnahmen. Dies könnte im Wege einer neu zu schaffenden Mobilitätsdatenverordnung realisiert werden.

Eine solche wäre nur auf Unionsebene umsetzbar, da eine Schaffung dieser umfassenden Regelungen in den Mitgliedsstaaten nur im Rahmen von Öffnungsklauseln erfolgen dürfte. Eine solche Mobilitätsdatenverordnung müsste differenzierte Rollenkonzepte, sowie eine Pflichtenzuweisung nach Einflussphären beinhalten (da bspw. technischer Datenschutz nur herstellerseitig sicherstellbar ist und eine Unterscheidung zwischen Privathaltern und gewerblichen Haltern sachnah erscheint).

Prozess für die Rückführung der Daten in die Monitoring Plattform

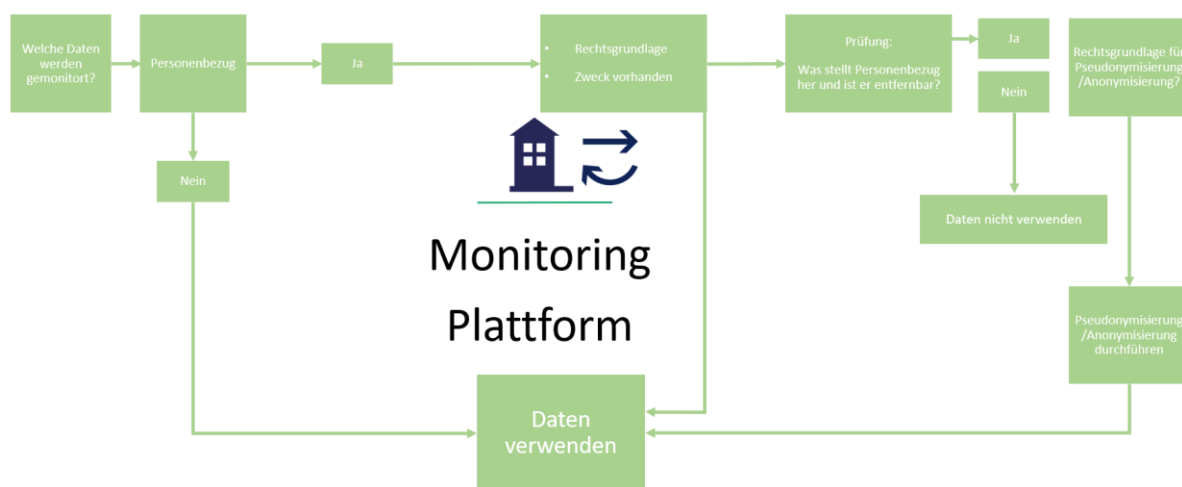


Abbildung 26: Prozess zur Rückführung von Daten in die Monitoring Plattform

2.6 AP6: Evaluation und Demonstration

2.6.1 UNCOVER Prozess

Der Demonstrator soll den UnCOVER Prozess (siehe Abbildung 5) evaluieren und veranschaulichen. Hierfür wurde ein Demonstrator (siehe Abbildung 27) aufgebaut. Er besteht aus einer Simulation des Fahrzeuges und seiner Umgebung, der Monitoring Plattform und der Automatischen, sowie Händischen Analyse.

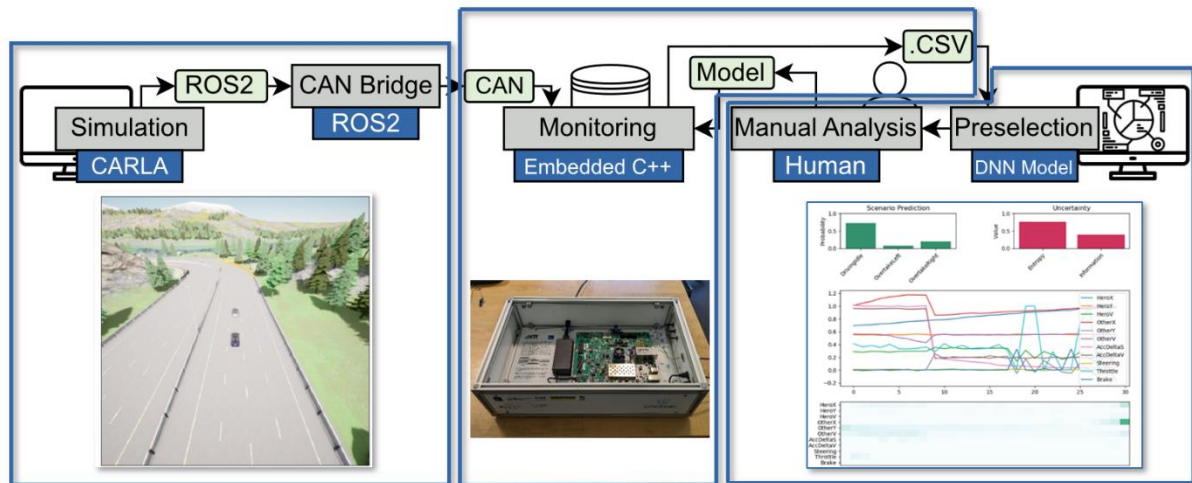


Abbildung 27: Aufbau des Demonstrators

2.6.2 Simulation und CAN Bridge

Um Eingangsdaten für die Monitoring Plattform und die nachgelagerten Analyseschritte zu generieren wurde eine auf CARLA¹¹ basierende Simulation genutzt. CARLA simuliert ein Ego-Fahrzeug mit verschiedenen Sensoren (Kamera, Lidar, Radar, GPS, ...) in einer Umgebung mit statischen Objekten sowie anderen Fahrzeugen und Fußgängern. Über den sogenannten Scenario Runner lassen sich verschiedene im OpenSCENARIO Format definierte Szenarien abspielen und systematisch testen.

Als zusätzliche Komponenten wurden ein Adaptive Cruise Control (ACC) Modul und eine ROS2-CAN-Bridge entwickelt. Das ACC Modul stellt die zu überwachende Funktionalität dar. Es besteht aus einem einfachen Regler, der basierend auf einer gegebenen Maximalgeschwindigkeit und Abstandsmessungen zum vorausfahrenden Fahrzeug Gas- und Bremssignal des Ego-Fahrzeugs regelt. Auf Knopfdruck lässt sich in der Simulation ein Security Vorfall auslösen, woraufhin der ACC eine Vollbremsung ausführt. Dieser Vorfall soll erkannt und verhindert werden.

Die entwickelte ROS2-CAN-Bridge dient zum Übersetzen von ROS2 Nachrichten in CAN Pakete, quasi als Schnittstelle zwischen Simulation und Monitoring Plattform. Das Software Modul empfängt alle ROS2 Nachrichten aus CARLA, zerlegt diese in CAN Pakete, ordnet je nach Nachrichtentyp eine CAN ID zu und gibt sie an einen CAN Sender weiter. Für die Übertragung größerer ROS2 Nachrichten über den CAN Bus wurde in der ROS2-CAN-Bridge multi frame transmission (ISO 15765-2) umgesetzt.

2.6.3 Monitoring Plattform

Die Simulation ist über einen USB-CAN Adapter mit der Monitoring Plattform verbunden. Die Monitoring Plattform verfügt über Regeln nach denen sie entscheidet ob in den vorliegenden BUS-

¹¹ Dosovitskiy, Alexey, et al. "CARLA: An open urban driving simulator." *Conference on robot learning*. PMLR, 2017.

Signalen eine Anomalie vorliegt. Wenn solch eine Anomalie vorliegt wird die Monitoring Plattform getriggert und zeichnet ein Szenario (Zeitreihen der Überwachten Signale) auf. Dieses Szenario wird dann in der Manuellen Analyse weiterverarbeitet.

2.6.4 Manuelle Analyse

Um Teile der Prozesskette zu demonstrieren wurde ein Graphical User Interface (GUI) entwickelt. Die GUI ist in Abbildung 28 dargestellt. Die GUI sucht permanent nach neuen, von der Monitoring Plattform erkannten Anomalien. Nachdem die Anomalien vom Neuronalen Netz (NN) bewertet wurden, werden sie auf der linken Seite tabellarisch dargestellt. Die einzelnen Signale können pro Anomalie in der Mitte visualisiert werden. Auf der rechten Seite der GUI wird die Anomalie im Bezug zu anderen Szenarien in den gleichen Clustern dargestellt.

Nach der Darstellung des Monitorings, sowie NN Ergebnisse in der GUI, kann entschieden werden, wie weiter mit der Anomalie verfahren werden soll. Entweder wird sie manuell einem Cluster in der Statistik zugeordnet oder für eine händische Analyse ausgewählt.



Abbildung 28: GUI des Demonstrators

3 Nutzen und Verwertbarkeit der Ergebnisse und Erfahrungen

Das Projekt umfasste den Entwurf und die Implementierung von Verfahren zur strukturierten Erkennung von Sicherheitsvorfällen in hochautomatisierten Fahrzeugen, sowie Werkzeugen zur systematischen Rückführung der Erkenntnisse über Sicherheitsvorfälle in den Entwurfsprozess unter Berücksichtigung rechtlicher Aspekte.

Ein besonderer Schwerpunkt lag auf der Entwicklung eines Analyseprozesses zur Erkennung von Anomalien in Steuersignalen zwischen ECUs und zur stufenweisen Bewertung nach Bekanntheit und Kritikalität um eine Einordnung in Safety- und Security-Vorfälle vornehmen zu können. Dabei wurden vor allem die Normen für Security (ISO 21434) und SOTIF (ISO 21448) berücksichtigt.

Eine Monitoring Plattform zeichnet regelbasiert auffällige Signale zwischen ECUs auf und gibt diese zur Analyse weiter. Zur Erkennung von Anomalien wurde ein datengetriebener Ansatz entwickelt, der mit Hilfe eines neuronalen Netzes die aufgezeichneten Fahrzeugdaten zu vordefinierten Szenarien zuordnet. So lassen sich unbekannte Szenarien erkennen, wenn sich die Daten keinem bekannten Cluster an Szenarien zuordnen lassen. Mit Hilfe des von EnCo entwickelten Tools SOX lassen sich erkannte Sicherheitsvorfälle auf einzelne Komponenten abbilden um genauere Analysen durchführen zu können und die Ursache für den Vorfall zu finden. Mit Hilfe der von RiSA untersuchten statistischen Auswertungen lässt sich bewerten ob sich die Anomalie z.B. auf Alterung von Komponenten zurückzuführen ist, was auf einen Safety-Vorfall hindeutet oder ob es sich um einen Security Vorfall handelt. Neu erkannte, unkritische Szenarien können verwendet werden um das neuronale Netz zur Erkennung von Vorfällen kontinuierlich zu trainieren und zu verbessern.

Abschließend wurde der gesamte Analyse Prozess mit den einzelnen Analyse Stufen in einen Demonstrator integriert, bei dem ein automatisiert fahrendes Fahrzeug in einer Simulation Security-Vorfällen ausgesetzt ist. Diese werden erkannt, klassifiziert und bei zukünftigem Auftreten verhindert.

Wichtig für das FZI als gemeinnützige Forschungstransferinstitution ist zunächst insbesondere die wissenschaftliche Verwertung. Neben der industriellen Bedeutung und der Marktrelevanz der genannten Themen spiegelt sich darin auch die am FZI vorhandene Expertise wider, die in einer Vielzahl von geförderten Projekten genutzt wurde und derzeit ausgebaut wird, so dass die technischen Erfolgsaussichten als gut eingeschätzt werden können.

Durch die Vernetzung des UNCOVER-Projekts mit anderen Projekten im Bereich der IT-Sicherheit und Automotive Elektronik, wie z.B. dem SASVI-Projekt, CeCaS, EMDRIVE und dem Testfeld Autonomes Fahren Baden-Württemberg, wird ein intensiver Forschungstransfer der Ergebnisse in die jeweiligen Arbeitsfelder gewährleistet. Damit besteht eine hohe Erfolgchance für die im Projekt definierten Ziele in wissenschaftlicher und technischer Hinsicht.

4 Fortschritt auf dem Gebiet an anderer Stelle

Straßenverkehrsrecht

Am 28. Juli 2021 wurde das Straßenverkehrsgesetz um das Gesetz zum autonomen Fahren ergänzt. Damit trat auch die Verordnung zur Genehmigung und zum Betrieb von Kraftfahrzeugen mit autonomer Fahrfunktion in festgelegten Betriebsbereichen (AFGBV) in Kraft. In dieser Verordnung ist auch geregelt, dass sich Fahrzeuge mit automatisierten und autonomen Fahrfunktionen kontinuierlich selbst überwachen müssen. Außerdem wird eine Gefährdungsanalyse erforderlich, deren Methoden dem Stand der Wissenschaft und Technik entsprechen. Insbesondere zählen zu den Sicherheitsmaßnahmen organisatorische Maßnahmen, wie die Eingrenzung des Betriebsbereichs und spezifische Anweisungen an das Fahrpersonal. Außerdem müssen Alterungs- und Nutzungserscheinungen an den Systemkomponenten durch geeignete Maßnahmen erkannt und ausgeglichen werden. Die Projektergebnisse können aus unserer Sicht maßgeblich zur Erfüllung der Anforderungen beitragen.

EU AI-Act

Des Weiteren wurde während der Laufzeit des Projekts der Entwurf des AI-Act, der Regulierung von KI-Anwendungen auf europäischer Ebene, bekannt. Der AI-Act schafft den Rechtsrahmen für den Einsatz von KI und reguliert insbesondere sogenannte Hochrisiko-KI Systeme. Die Auswirkungen auf das automatisierte und vernetzte Fahren können auf mehreren Ebenen erwartet werden: Zum einen werden voraussichtlich konkrete UNECE-Regelungen aus dem AI-Act abgeleitet werden, um Überschneidungen bei bestehenden Regulierungsmechanismen, Konformitätsbewertungen und der Überwachung und Marktaufsicht für Fahrzeuge zu vermeiden. Sie könnten in den bestehenden Rahmen für die Typengenehmigung von Fahrzeugen in Zukunft integriert werden.

Die neue EU-Verordnung zur künstlichen Intelligenz wird somit einen großen Einfluss auf die Entwicklung von Fahrzeugen und die Zusammenarbeit von Herstellern haben, um die Sicherheits- und Zuverlässigkeitsanforderungen des EU AI Act zu erfüllen.

EU Data Act

Die EU Kommission hat mit dem EU Data Act zeitgleich ein weiteres neues Gesetz auf den Weg gebracht. Um KI Systeme zu entwickeln und in den Einsatz zu bringen, müssen Daten vorhanden sein, die den Anforderungen des EU Data Acts entsprechen. Somit hat der EU Data Act direkte Auswirkungen auf den AI Act.

Konkret bedeutet dies, dass die Datenverarbeitungen Kriterien der Transparenz und Nachvollziehbarkeit erfüllen werden müssen sowie angemessene Maßnahmen zum Schutz von personenbezogenen Daten Datensicherheit ergriffen werden müssen. Auch hier können die Projektergebnisse maßgeblich zur Erfüllung der zukünftigen Anforderungen beitragen.

IT-Sicherheitsrecht

Auch auf IT-sicherheitsrechtlicher Ebene hat es gesetzliche Novellierungen und Entwürfe gegeben. Beispielsweise wurde im Rahmen des Cyber Resilience Act (CRA) auf europäischer Ebene ein harmonisierter, der Wertschöpfungskette entlang wirkende Sicherheitsstandardisierung vorgenommen. Da die IT-Sicherheit für autonome Fahrzeuge bereits in den UN ECE Regulation No. 155 normiert wird, ist der CRA für das autonome Fahren nicht anwendbar.

5 Veröffentlichung der Ergebnisse und Publikationen

<i>Jahr</i>	<i>Konferenz</i>	<i>Ort, Land</i>	<i>Titel</i>	<i>Mehrwert für UNCOVER</i>
2022	VDI-Tagung Fahrerassistenzsysteme und automatisiertes Fahren	Aachen, Deutschland	Abbildung rechtlicher Anforderungen auf die Architektur komplexer Fahrerassistenzsysteme und autonomer Fahrzeuge	Vorstellung eines Konzepts zur Verknüpfung von Datenschutzanforderungen und E/E-Architekturen und Feedback aus dem Fachpublikum
2022	IEEE ISSE 2022	Wien, Österreich	A viewpoint-based evaluation method for future Automotive Architectures	Vorstellung einer Methode zur Analyse künftiger Änderungen an der E/E-Architektur und von Vorfällen sowie Feedback aus dem Fachpublikum
2023	IEEE ISADS 2023	Mexico City, Mexico	Policy-Based Task Allocation at Runtime for a Self-Adaptive Edge Computing Infrastructure	Konzept und Framework für kontinuierliche Entwicklung und Deployment nach Vorfällen und Feedback aus dem Fachpublikum

Kurzfassung zum Schlussbericht

zum Vorhaben

Datenbasierte EntwurfsUNterstützung durch kontinuierliches MOnito-
ring Von SichERheitsvorfällen (UNCOVER)



FÖRDERKENNZEICHEN 16KIS1410K



FZI Forschungszentrum Informatik

Haid-und-Neu-Str. 10-14

76131 Karlsruhe

Autoren: Victor Pazmino Betancourt, Laurenz Adolph, Maximilian Kirschner, Carl Philipp Hohl,
Daniel Vonderau

Telefon: +49 721 9654-190

E-Mail: pazmino@fzi.de

Die sichere Einführung autonomer Fahrzeuge erfordert ein durchgängiges Zusammenspiel von Funktionen, Systemen und Diensten über den gesamten Produktlebenszyklus. Dies umfasst die Kommunikation zwischen Steuergeräten im Fahrzeug sowie die Interaktion mit der Umgebung über mobile Endgeräte und Infrastruktur. Wichtige Informationsdienste wie Navigations- und Wetterdienste unterstützen dabei die Entscheidungsfindung des Fahrzeugs hinsichtlich Navigation, Spurführung und Stabilisierung. Die Sicherheit dieser Informationen ist von entscheidender Bedeutung, da Fehler oder Manipulationen zu gefährlichem Verhalten führen können. Die Sicherheit autonomer Fahrzeuge wird durch anfängliche Sicherheitsmaßnahmen im Rahmen von Security-by-Design gewährleistet, aber während des Betriebs können unvorhergesehene Schwachstellen auftreten, die zusätzliche Risiken für die Cybersicherheit und die funktionale Sicherheit darstellen.

Daher ist eine **kontinuierliche Überwachung und Anpassung über den gesamten Produktlebenszyklus** erforderlich, um sicherheitskritische Situationen zu vermeiden. Dieses Projekt adressiert diese Herausforderungen, indem etablierte Security-by-Design-Ansätze um eine Rückkopplung von Sicherheitsvorfällen aus dem Betrieb ergänzt werden. **Identifizierte Vorfälle werden analysiert und mit den Sicherheitsmaßnahmen aus der Entwurfsphase verknüpft**, um eine kontinuierliche Verbesserung zu ermöglichen und die Sicherheit der autonomen Fahrfunktionen zu gewährleisten, insbesondere unter Berücksichtigung relevanter Normen wie ISO 21434 und ISO 21448. Abbildung 1 zeigt das gängige V-Modell in der Entwicklung, sowie die in UnCOVER erforschte Rückführung der Felddaten in den Entwurfsprozess mittels kontinuierlicher Analysen.

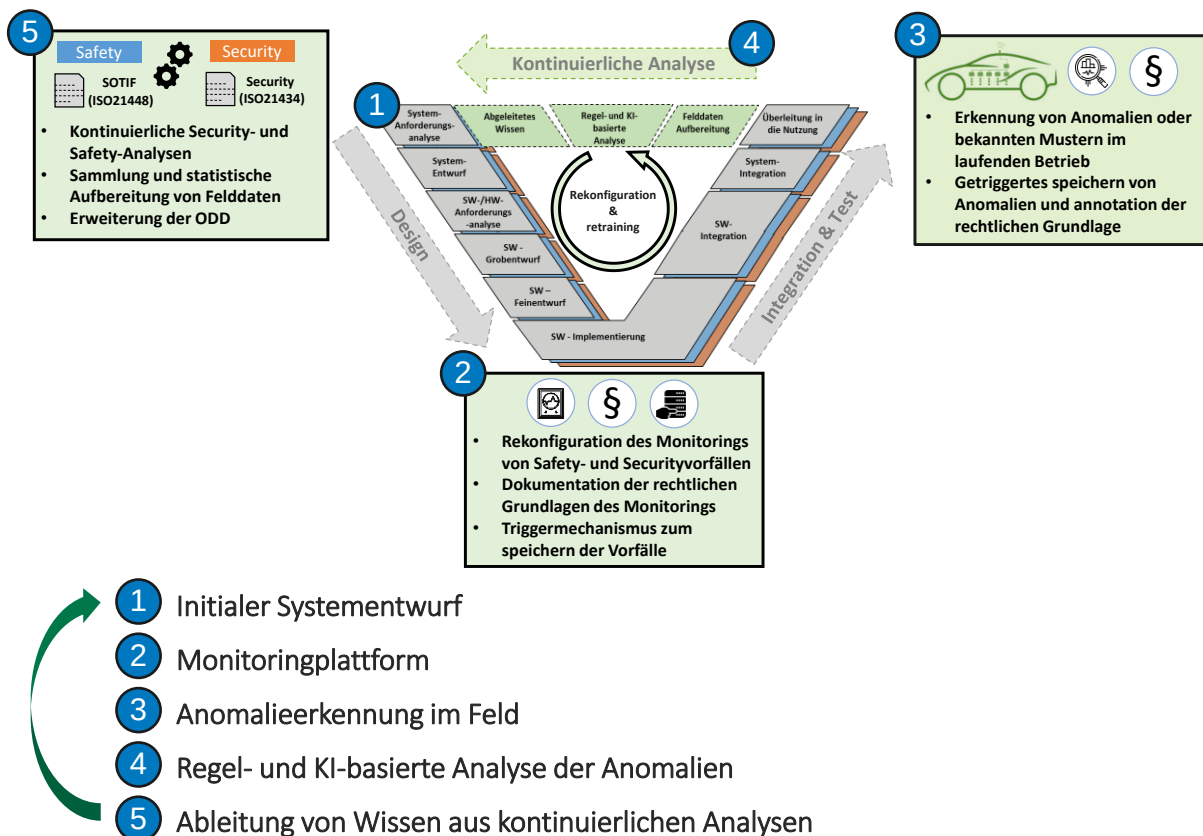


Abbildung 1: Big Picture des Projekts

In *Schritt 1* wird ein initialer Systementwurf entwickelt. Anhand dieses Systementwurfes wird dann bereits zu Designzeit bekanntes Sollverhalten identifiziert und in *Schritt 2* während der Konfiguration der Monitoringplattform mitberücksichtigt. In *Schritt 3* werden im Betrieb Abweichungen zum bekannten Normalverhalten identifiziert. Hier wird zuerst jede Anomalie als Safetyvorfall behandelt, da der potentielle Auslöser für die Anomalie noch nicht bekannt ist. *Schritt 4* umfasst eine KI-gestützte Analyse der aufgetretenen Anomalien und dient als Hilfe um in *Schritt 5* zu differenzieren ob es sich um einen Safety- oder Security-Vorfall gehandelt hat. In beiden Fällen fließt das neugewonnene Wissen im nächsten Designprozess ein und ist damit die Ausgangslage für die nächste Iteration der Monitoringplattform und der KI-gestützten Analyse.

Die Ziele des FZIs im Projekt UnCOVER lassen sich in die folgenden Teilbereiche gliedern:

- **Methoden zur datenbasierten Entwurfsunterstützung:** Daten über sicherheitsrelevante Ereignisse werden analysiert, um Fehler zu identifizieren und entsprechende Korrekturmechanismen zu entwickeln. Regel- und KI-basierte Ansätze wurden verwendet, um sicherheitsrelevante Ereignisse und Abweichungen im Fahrzeugbetrieb zu erkennen. Diese Methoden lieferten Informationen für die Fehleranalyse und die Lokalisierung von Sicherheitslücken.
- **Methoden und Werkzeuge für kontinuierliche Safety- und Security-Analysen:** Die aus den Daten abstrahierten und gewonnenen Informationen unterstützen bei der Fehlerbehebung. Das Vorgehen und die Methoden und Werkzeuge, die für den kompletten Automobil-Entwicklungsupdatezyklus anfallen gilt es zu evaluieren, um ein kontinuierliches Safety- und Security-Monitoring zu erreichen. Dafür werden Methoden für eine systematische Zusammenführung der Informationen aus dem Betrieb dieser Systeme in die Entwicklungsphase angewandt, um diese mit Anforderungen, Modellen und Sicherheitskonzepten im Entwurf zu verknüpfen. Die Normen SOTIF (ISO 21448) und ISO 21434 werden dabei berücksichtigt.
- **Monitoring-Plattform zur Erkennung von Security- und Safety-Vorfällen:** Ein essentieller Baustein des Vorhabens ist die Entwicklung einer flexiblen Monitoring-Plattform zur Erkennung sicherheitsrelevanter Ereignisse im laufenden Betrieb. Sie stellt die technische Basis für die Integration von konfigurierbaren Monitoring-Mechanismen und einem Redeployment-Prozess in eine E/E-Architektur dar. Zu diesem Zweck wurden auch ein zugehöriger kontinuierlicher Entwicklungsprozess und ein HW/SW-Framework für das Deployment erarbeitet.
- **Datenschutzaspekte** müssen nach dem Prinzip des "Privacy by Design" gemäß Art. 25 DSGVO bereits in der Entwurfsphase in die technischen Sicherheitsmechanismen integriert werden. Dies umfasst die Festlegung von Mitteln zur Umsetzung der Datenschutzgrundsätze und zum Schutz der Rechte und Freiheiten der betroffenen Personen. Rechtliche Aspekte werden sowohl bei der Datenanalyse als auch beim Re-Design berücksichtigt und als zusätzliches Plugin implementiert.

Für das FZI steht in erster Linie die wissenschaftliche Verwertung der Projektergebnisse im Vordergrund. Die erzielten Ergebnisse bilden die Grundlage für vier Dissertationen, von denen eine im Rahmen des Projekts erfolgreich abgeschlossen wurde. Zusätzlich wurden im Rahmen des Vorhabens sechs studentische Abschlussarbeiten betreut. Die Veröffentlichung der Ergebnisse des Teilvorhabens des FZI erfolgte in Form von drei Publikationen. Die Erfahrungen und Ergebnisse werden in aktuellen Forschungsprojekten aufgegriffen und weiterentwickelt.