Hochschule Bremen
City University of Applied Sciences

Sachbericht zum Teilvorhaben

EMILIE – Kurzdarstellung (Teil 1)

Sichere und robuste Zustandsüberwachung und Prozess-Steuerung mittels intelligenter Edge-Elektronik

Zuwendungsempfänger:	Hochschule Bremen
Verbundvorhaben:	EMILIE
Teilvorhaben:	IT-Sicherheit in der Prozess-Steuerung mittels intelligenter Edge-Elektronik
Förderkennzeichen:	16ME0560
Laufzeit des Vorhabens:	01.07.2022 – 30.09.2025
Berichtsdatum:	06.02.2026

Firma:	Hochschule Bremen
Anschrift:	Flughafenallee 10 28199 Bremen
Telefon:	+49 421 5905 5483
Ansprechpartner:	Prof. Dr. Richard Sethmann
E-Mail:	Richard.Sethmann@hs-bremen.de

Gefördert durch:

Bundesministerium
für Forschung, Technologie
und Raumfahrt

Autoren

Hochschule Bremen

Prof. Dr. rer. nat. Richard Sethmann

Bastian Fraune, M. Sc.

Torben Woltjen, M. Sc.

Julia Albers, B. Sc.

Dirk Schmidt, B. Sc.

Jan Steinmüller, B. Sc.

Inhaltsverzeichnis

Teil I – Kurzbericht

1. Ziel, Inhalt und Aufgabenstellung

Ziel von EMLIE war die signifikante Verbesserung von Mikroelektronik und passgenauer Systemsoftware in dezentralen, lokal an Industrieanalgen angebrachten Sensoren (magnetostriktive Sensoren und hochauflösende Kameras) und Edge-Gateways zur sicheren, KI-basierten Datenerfassung und Informationsverarbeitung. Die umzusetzenden technischen Maßnahmen sollten messbare Verbesserungen im Durchsatz, Energieeffizienz und betrieblichem Verschleiß erzielen. Beispielsweise können solche Maßnahmen durch Überwachung von Betriebszuständen mit ressourcenschonender prädiktiver Instandhaltung zur Minimierung geplanter und ungeplanter Ausfälle sowie automatisierte und zustandsbasierte Prozesssteuerung des Betriebsmodus energieintensiver Anlagen in energieoptimierte bzw. effizientere Bereiche dargestellt werden.
Die HSB konzentriert sich dabei auf das Querschnittsthema der IT-Sicherheit. So gilt es, eine vertrauenswürdige, lokal verbleibende Datenhaltung durch intelligente Datenvorverarbeitung in Sensoren und Edge-Gateways sicherzustellen. Der Fokus liegt dabei auf der Sicherstellung der Vertrauenswürdigkeit durch hardwarebasierte Absicherung von Kommunikationsprotokollen und der Plattformintegrität. Dabei wird ein Hardware-Vertrauensanker in die abzusichernden Hardwareplattformen integriert. Dieser agiert als Root-of-Trust (RoT) und führt sicherheitsspezifische Funktionen aus und stellt als eigenständiger Kryptoprozessor sichere kryptografische Operationen zur Verfügung, z. B. das sichere Erstellen und Speichern von Schlüsselmaterial sowie einen Zufallszahlengenerator. Außerdem erlauben Hardwarevertrauensanker die Möglichkeit Prinzipien von „Remote Attestation“ umzusetzen und damit aus der Ferne die Integrität eines Gerätes sicher abzufragen. Darüber hinaus werden die ressourceneffiziente und digitale Weitergabe von gesicherten Informationen und relevanten Historien zu erkannten Ereignissen ohne Übermittlung der Rohdaten in den Fokus gestellt.

2. Wissenschaftlich-technischer-Stand

Im Bereich der digitalen Sensorik ist vor allem der Übertragungsweg der Daten interessant, da hier Angreifer unbemerkt Daten abgreifen oder manipulieren können. Wie alle digitalen Datenströme können auch die Messwerte digitaler Sensoren kryptographisch abgesichert werden. Beispielsweise kommen bei größeren Entfernungen sowie Datenmengen zwischen Sensor und Datenempfänger oft IP-basierte Übertragungsprotokolle über Schnittstellen wie Ethernet zum Einsatz. Hier ist eine kryptographische Absicherung in der Praxis deutlich häufiger anzutreffen als bei kurzen Leitungen im Kontext hardwarenaher Schnittstellen wie SPI (Serial Peripheral Interface). Die Erfahrung aus der Praxis zeigt allerdings, dass in Prozessnetzen viele Sicherheitsmechanismen noch nicht umgesetzt wurden, die in der Office-IT bereits Standard sind (siehe [VDE-AR-E 2842-61]).
Industrielle Kamerasysteme bieten heutzutage bereits einige Sicherheitsmechanismen wie Intrusion Detection (Veränderungen am Gehäuse werden erkannt) und digitale Signaturen für die gesendeten Bilddaten. Die Kommunikation mit diesen Geräten erfolgt bei einigen Firmen wie Mobotix mit gesicherten Standardprotokollen wie HTTPS und Transport Layer Security (TLS). Viele Systeme bieten ein User Management an und unterstützen IP-basierte Zugriffskontrolle (Whitelisting, Blacklisting) oder auch portbasierte Authentifizierung wie sie z. B. im IEEE 802.1X vorgesehen ist. Weitergehende Mechanismen fehlen weitestgehend.
Ein weitverbreiteter Ansatz, der den Schutz und die Kontrolle der Identität und der Integrität von IT-Systemen ermöglicht, wird unter dem Begriff Trusted Computing (TC) zusammengefasst. TC beschreibt ein technologisches Konzept, das von der Trusted Computing Group (TCG) spezifiziert wurde und den Schutz von Hard- und Software-Komponenten ermöglicht. Hierzu wird eine Vertrauenskette, ausgehend von einem unveränderlichen Vertrauensanker (z. B. Trusted Platform Module (TPM), Smartcard) gebildet, die die Messung der Systemintegrität, anhand der Verkettung einzelner Systemkomponenten (Hard- und Software) ermöglicht. Bei der Absicherung des Boot-Prozesses über solch eine Vertrauenskette wird beispielsweise von Secure/Measured Boot gesprochen. Neben der Erfassung der Systemintegrität definiert die TCG einen Prozess zur Überprüfung der gemessenen Integrität aus der Ferne - der Remote Attestation. Basierend auf den Funktionalitäten des TPM 2.0 lassen sich hardwareseitig abgesichert diverse Kryptographiefunktionen umsetzen [TC07]. Von 47 angeschauten Gateways/Industrial PCs bringen hardwaretechnisch 27 einen TPM-Chip mit, aber nur 7 haben beschrieben, dass

sie den Chip auch für Funktionen wie Secure Boot oder Verschlüsselung einsetzen. Von diesen 7 Produkten bringen 6 aber keine Unterstützung in der Applikation mit, sodass auch hier wieder kein Vergleich zur in EMILIE umzusetzenden Lösung gefunden wurde. Keines der untersuchten Produkte hatte einen Manipulationsschutz der Software und des Betriebssystems. Im Forschungsprojekt SiDaFab wurde von der HSB prototypisch in einem Demonstrator Remote Attestation auf Basis von TPM-2.0-Chips zwischen einem Gateway und einem Cyber-Physical-System (CPS) umgesetzt. In SiDaFab wurde vorrangig die Umsetzung eines sicheren Gateways betrachtet und entwickelt. In diesem Projekt steht nicht mehr die Umsetzung eines sicheren Gateways im Vordergrund, sondern die Gesamtsicherheitsarchitektur. Um Sicherheit und Vertrauen im Edge-Gateway zu etablieren, muss die Sicherheitsarchitektur über das Gateway hinaus konzeptioniert und entwickelt werden.

3. Planung und Ablauf des Vorhabens

Die Weiterentwicklung von Elektronik und Firmware der magnetostriktiven Sensoren in AP 1 erfolgte unter der Leitung des Herstellers Magnetic Sense, die der hochauflösenden Kameras in AP 2 unter Leitung des Herstellers Mobotix und die Verbesserung der Edge-Gateways in AP 3 durch den Hersteller Congatec. Die Hardware-Entwicklung wurde durch AP 7 in Form der Entwicklung sicherer Kommunikations- und Datenschnittstellen unter der Leitung der HSB ergänzt. Der Arbeitsbereich AP 4 getrieben durch ITWM stellte durch Support der Weiterentwicklung der Firmware von Sensorik und Kameras sowie der Implementierung von KI-basierten Datenerfassung und Informationsverarbeitung auf dem Edge-Gateway das Interface zwischen Anwendung und Hardware dar. Die Anpassung, Umsetzung und Demonstration der entwickelten Hardware und KI-Methoden erfolgte im Bereich des Condition Monitoring und Predictive Maintenance für Turbinen und Zementmühlen in AP 5 unter Leitung von ITWM und der Prozessoptimierung bei energieeffizientem Betrieb in AP 6 am Beispiel der Zementmühlen durch den Mühlenhersteller GPSE.

4. Wesentliche Ergebnisse

Die HSB hat in Zusammenarbeit mit den Projektpartnern ein Gesamtszenario entwickelt, und anhand dessen Bedrohungsszenarien identifiziert und dokumentiert. Dabei wurden Sicherheitsanalysen eingesetzter Protokolle und Schnittstellen (wie CAN-Bus oder MQTT) durchgeführt. Ein Netz- und Datensicherheitskonzept mit durchgehender Vertrauenskette mit Fokus auf Plattformsicherheit und Verbindungssicherheit wurde konzeptioniert und prototypisch umgesetzt. Dazu gehören unter anderem die Integration von TPM 2.0-Chips, die Absicherung der Kommunikationswege durch TLS-Verschlüsselung in Kombination mit den TPM 2.0 und der Verifikation der Geräteintegrität durch Measured Boot und Remote Attestation. Abschließend wurden die erarbeiteten Sicherheitskomponenten aus dem Netz- und Datensicherheitskonzept in einen Demonstrator integriert.

5. Zusammenarbeit mit anderen Forschungseinrichtungen

Die Forschungsgruppe Rechnernetze und Informationssicherheit (FRI) der Hochschule Bremen bearbeitet als Kernthemen Trusted Computing, sichere Zugangs- und Zugriffsverfahren, Vertrauensstellungen in komplexen Systemen sowie Fachkenntnisse im Bereich der Netztechnik. Diverse Forschungsprojekte im Bereich Informationssicherheit wurden bereits mit Projektpartnern der Hochschule Bremen durchgeführt und zudem ist aktuell ein weiteres Forschungsprojekt durchgeführt worden.

Trusted-Computing-Konzepte für ein Smart Gateway I4.0 wurden im Forschungsprojekt "Sichere Daten-kommunikation für die verteilte Fabrik der Zukunft" (SiDaFab) untersucht und weiterentwickelt. Ein Schwerpunkt lag dabei auf dem Einsatz eines TPM 2.0 für Measured Boot und Remote Attestation. Ziel war es, eine Referenzarchitektur für ein Security Gateway für den Austausch von Industriedaten und Diensten zu schaffen. In einem anderen Forschungsprojekt befasste sich die Hochschule Bremen mit der Entwicklung von „Methoden für Energienetzakteure zur Prävention, Detektion und Reaktion bei IT-Angriffen und -Ausfällen“ (MEDIT). In einem weiteren Forschungsprojekt werden „Polymorphe Agenten als querschnittliche Softwaretechnologie zur Analyse der Betriebssicherheit von cyber-physischen Systemen” (PYRATE) entwickelt. Das Forschungsprojekt tbiEnergy erforschte, wie ein ganzheitlicher Blockchain-Ansatz für die Realisierung eines lokalen Energiemarktes aussehen könnte und wie entsprechende Hardwaresicherheitsmechanismen wie z. B. ein TPM 2.0 integriert werden können.

Quellen

[TC07] A Practical Guide to Trusted Computing: Challener, David; Yoder, Kent; Catherman, Ryan. - 1st edition, 2007.

[GKRW15] N. Gottert, N. Kuntze, C. Rudolph, and K. F. Wahid, “Trusted neighborhood discovery in critical infrastructures,” in 2014 IEEE International Conference on Smart Grid Communications (SmartGridComm), 2014, pp. 976–981.

[VDE-AR-E 2842-61] Entwicklung und Vertrauenswürdigkeit von autonom/kognitiven Systemen, 2021.

Hochschule Bremen
City University of Applied Sciences

HSB

Sachbericht zum Teilvorhaben

EMILIE -Schlussbericht (Teil 2)

Sichere und robuste Zustandsüberwachung und Prozess-Steuerung mittels intelligenter Edge-Elektronik

Zuwendungsempfänger:	Hochschule Bremen
Verbundvorhaben:	EMILIE
Teilvorhaben:	IT-Sicherheit in der Prozess-Steuerung mittels intelligenter Edge-Elektronik
Förderkennzeichen:	16ME0560
Laufzeit des Vorhabens:	01.07.2022 – 30.09.2025
Berichtsdatum:	06.02.2026

Firma:	Hochschule Bremen
Anschrift:	Flughafenallee 10
	28199 Bremen
Telefon:	+49 421 5905 5483
Ansprechpartner:	Prof. Dr. Richard Sethmann
E-Mail:	Richard.Sethmann@hs-bremen.de

Gefördert durch:

Bundesministerium
für Forschung, Technologie
und Raumfahrt

Autoren

Hochschule Bremen

Prof. Dr. rer. nat. Richard Sethmann

Bastian Fraune, M. Sc.

Torben Woltjen, M. Sc.

Julia Albers, B. Sc.

Dirk Schmidt, B. Sc.

Jan Steinmüller, B. Sc.

Inhaltsverzeichnis

TEIL II: Schlussbericht – Eingehende Darstellung

Der Zweite Teil dieses Schlussberichtes fokussiert sich auf die ausführlichere Darstellung der durchgeführten Arbeiten der Hochschule Bremen (HSB).

1. Magnetostriktive Sensorik – Schnittstellen- und Sicherheitsanforderungsdefinition

Die HSB hat zusammen mit dem Gateway-Hersteller congatec (ehemals Real-Time System ehemals Arendar) und dem Sensorhersteller Magnetic Sense die vorhandenen Hardwareschnittstellen und Möglichkeiten zur Konnektivität zusammengetragen. Ziel war die Definition gemeinsamer und geeigneter Datenschnittstellen aus Sicht aller Beteiligten. Diese sollen die in verschiedenen APs definierten Use-Cases und Szenarien erfüllen können. Im Folgenden werden die Ergebnisse der Anforderungsanalyse mit Fokus auf die IT-Sicherheit kurz beschrieben.

1.1. Anforderungen

Im AP konnten verschiedene Anforderungen definiert werden. Neben den Anforderungen zur Absicherung der Kommunikation ist auch eine Betrachtung technischer und räumlicher Gegebenheiten notwendig, z. B. um maximale Leitungslängen und eine entsprechende Abschirmung gegen Störeinflüsse zu gewährleisten – letztere waren z. B. bei den Anlagen der Gebr. Pfeiffer zu erwarten. Pro Anlage wurden ein bis zwei Sensoren als sinnvoll erachtet, die mit einer Abtastrate im Bereich von einem kHz arbeiten. Die Reichweite des Signals variiert je nach Aufstellort des Edge-Gateways, der Interface-Box, etc. im Bereich 10 m – 100 m. Tabelle 1.1 zeigt, welche Anforderungen sich an die IT-Sicherheit ergeben haben.

Tabelle 1.1: Anforderungen an die IT-Sicherheit der Komponenten

ANFORDERUNG	BESCHREIBUNG
INTEGRITÄT DER ÜBERTRAGENEN WERTE	Notwendig, möglichst ab dem Sensor über das Edge-Gateway bis hin zum Nutzer
VERTRAULICHKEIT DER ÜBERTRAGENEN WERTE	Notwendig, über den gesamten Lebenszyklus hinweg
ABSICHERUNG GEGEN ÜBERTRAGUNGSFEHLER	Notwendig, bei z. B CAN-Bus bereits per CRC vorgesehen
PASSWORTSCHUTZ UND HARDWARE-SCHLÜSSEL-MANAGEMENT	Mit Passwortschutz versehen, möglichst nicht aus Flash auslesbar, in Hardwarevertrauensanker geschützt (TPM 2.0). Passwort sollte zwangsweise vom Standardpasswort geändert werden müssen

1.2. Analyse der ausgewählten Schnittstellen- und Sicherheitsanforderungsdefinition

Der CAN-Bus (Controller Area Network) ist ein weit verbreitetes Kommunikationssystem in der Automobilindustrie, das ursprünglich für die zuverlässige, nicht jedoch für die sichere Kommunikation entwickelt wurde. Es fehlen dem CAN-Bus eingebaute Sicherheitsmechanismen wie Verschlüsselung und Authentifizierung, was das Protokoll anfällig für verschiedene Angriffsarten macht. [1] In diesem Abschnitt werden die verschiedenen Sicherheitslücken und Angriffsvektoren des CAN-Bus-Systems beleuchtet, sowie mögliche Gegenmaßnahmen zur Verbesserung der Sicherheit beschrieben.

Angriffe auf CAN-Bus

Tabelle 1.2 zeigt eine Auswahl an potentiellen Angriffen auf eine CAN-Kommunikation. Sie zeigt deutlich, dass reines CAN zu grundlegenden und schwerwiegenden Sicherheitsproblemen neigt.

Tabelle 1.2: Angriffsvektoren auf CAN-Bus [2]

ANGRIFF	BESCHREIBUNG
BUS FLOOD ATTACK	Bei dieser Art von DoS-Angriff (Denial of Service) werden viele CAN-Frames gesendet, um die verfügbare Bandbreite zu verbrauchen und den normalen Verkehr zu blockieren.
SIMPLE FRAME SPOOFING	Der Angreifer sendet gefälschte Nachrichten, die vom Empfänger als legitim anerkannt werden, was zu einer Authentifizierungs-Attacke führt.
ADAPTIVE SPOOFING	Gefälschte Nachrichten werden zwischengespeichert und in kleinen Zeitfenstern gesendet, um die echten Nachrichten zu überholen.
ERROR PASSIVE SPOOFING ATTACK	Häufig gesendete Spoofing-Frames können durch Netzwerkverkehrsanalyse entdeckt werden. Wenn der CAN-Controller in den „Error-Passive"-Modus fällt, werden weitere Fehler nicht korrekt übertragen.
WIRE-CUTTING SPOOFING ATTACK	Erfordert physischen Zugriff, um CAN-Frames abzufangen und mit eigenen Daten weiterzusenden.

Gegenmaßnahmen zur Verbesserung der CAN-Bus-Sicherheit

Um den oben genannten Angriffen entgegenzuwirken, wurden verschiedene Gegenmaßnahmen vorgeschlagen, die jedoch jeweils Vor- und Nachteile mit sich bringen.

1. **Netzwerk-Segmentierung**
    - **Beschreibung:** Das CAN-Netzwerk wird in mehrere Subnetze aufgeteilt, um den Schaden bei einem Angriff zu begrenzen.
    - **Nachteil:** Wenn das Gateway kompromittiert wird, ist die gesamte Sicherheit hinfällig.
2. **Verschlüsselung**
    - **Beschreibung:** CAN bietet keine eingebaute Verschlüsselung, daher muss eine gewünschte Verschlüsselung selbstständig integriert werden, was einen dynamischer Schlüsselaustausch notwendig macht.
    - **Nachteil:** Zusätzlich integrierter Schlüsselaustausch und Verschlüsselung erhöht die Rechenleistung und Latenzzeit, was die Vereinbarkeit mit sicherheitskritischen Echtzeitsystemen erschwert.
3. **Authentifikation**
    - **Beschreibung:** Identifikation des Absenders einer CAN-Nachricht ist von Haus aus nicht möglich und müsste selbständig integriert werden, was zusätzliche Authentifizierungsnachrichten notwendig machen.
    - **Nachteil:** Zusätzliche Authentifizierungsnachrichten verdoppeln den Netzwerkverkehr.
4. **Intrusion Detection Systeme (IDS)**
    - **Beschreibung:** Analysiert konstant Datenpakete und erkennt Angriffe.
    - **Nachteil:** Verändert weder CAN-Controller noch den Bus Verkehr, sondern erkennt lediglich Angriffe

Schlussfolgerung

Die fehlenden Verschlüsselungs- und Authentifizierungsmechanismen im CAN-Bus bieten eine Vielzahl von Angriffsmöglichkeiten. Mit der zunehmenden Vernetzung der Systeme steigt die Gefahr von „Wireless"-Attacken. Die vorgeschlagenen Gegenmaßnahmen erfordern jedoch erheblichen Mehraufwand und bewegen sich an den Grenzen der vorhandenen Ressourcen wie Bandbreite und Rechenleistung. Zudem verringern sie die Kompatibilität mit bestehenden CAN-Systemen.

Umsetzungskonzept

Da das CAN-Protokoll in den Möglichkeiten zur Absicherung der Kommunikation beschränkt ist, sollte das analoge CAN-Signal so schnell wie möglich in ein sicheres digitales Signal wie z.B. über WebSockets umgewandelt werden.

Das WebSocket-Protokoll bietet die Möglichkeit die Kommunikation mithilfe von Transport Layer Security (TLS) zu verschlüsseln und eine wechselseitige Authentifizierung zu aktivieren. So können Integrität und Vertraulichkeit gewährleistet werden. Um die angewendeten Maßnahmen zu verstärken kann ein Hardware-Security-Chip wie der TPM 2.0 die Maßnahmen unterstützen. Die weitere Konzeptionierung und Umsetzung des CAN-Converters werden im Weiteren erläutert.

2. Edge Computing – Bildgebende Sensorik

2.1. Systemgrenzen und Spezifikation

Zur Bestimmung der Systemgrenzen und Spezifikationen (AP 2.1) sowie für die Abstimmung der Schnittstellen-Implementierung (AP 2.2) wurde das System wie in Abbildung 1 dargestellt entworfen. Darin zu sehen sind die einzelnen Hauptkomponenten, welche für das EMILIE-Projekt relevant sind und für die Sicherheitsanforderungen gelten. Im Projekt EMILIE erhält das Kamerasystem eine eigene Analysesoftware, welche als „3rd-Party-Software für Image-Processing“ in der linken oberen Hälfte eingezeichnet ist. Diese Software wurde vom Fraunhofer ITWM entwickelt und macht eine Schwingungsanalyse auf die beweglichen Teile der Mühle. Diese Analyse findet direkt auf der Kamera Hardware statt. Eine Ausgabe oder externe Bildverarbeitung ist nicht vorgesehen, sodass als Kommunikationsprotokoll MQTT ausgewählt wurde.

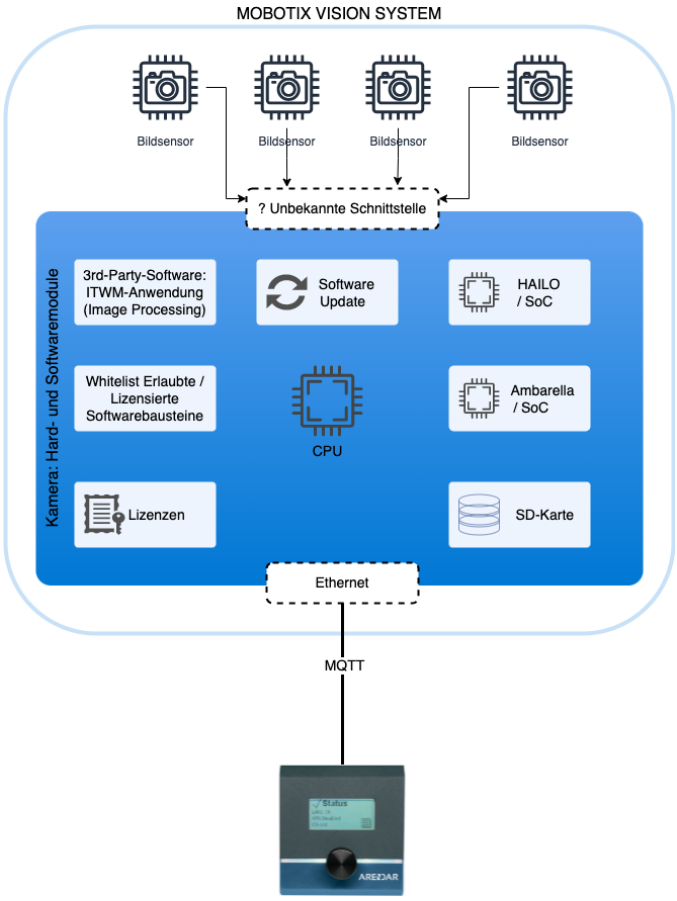

Abbildung 1: Mobotix Vision System Vereinfachte Komponenten

2.2. Schnittstellen-Implementierung

Im Rahmen von AP 2.2 wurde die Schnittstellen-Implementierung genauer betrachtet. Die HSB hat dabei gemeinsam mit Mobotix die Sicherheitsanforderungen definiert und Security-by-Design Ansätze in das Konsortium gebracht.

Sicherheitsanforderungen Mobotix

Mobotix hat allgemein bereits sehr hohe Sicherheitsanforderungen etabliert und betrachtet auch eine Umsetzung nach IEC 62443. In gemeinsamen Gesprächen und daraus resultierenden Analysen wurden drei Aspekte zur Stärkung der Systemintegrität geplant.

- → Eine Diebstahlsicherung der SD-Karte im Kamerasystem, die bei Entwendung der Speicherkarte die Vertraulichkeit der Daten auf der SD-Karte durch z. B. Verschlüsselung gewährleistet.
- → Die Beispielhafte Integration von TPM 2.0-Funktionalitäten wie der Remote Attestation, um damit die Systemintegrität gegenüber Dritten nachweisen zu können.
- → Eine Sicherheitsbetrachtung des neuen KI-Chips in der Kamera.

TPM 2.0-Integration

Aufgrund unterschiedlicher Faktoren ist es zur Projektlaufzeit nicht möglich gewesen einen echten TPM 2.0-Chip auf die Platine des Kamerasystems zu integrieren und in Betrieb zu nehmen. Um dennoch mit den Vorteilen des TPM 2.0 auf der Kamera zu experimentieren wurde seitens der HSB eine Möglichkeit gesucht, einen TPM 2.0-Simulator auf der Kamera als Software zu betreiben. Die Umsetzungen der Anforderungen an die Sicherheit, wie der SD-Kartenschutz, der Einsatz vom TPM 2.0 in Verbindung mit OpenSSL sowie die Integration der Remote Attestation via MQTT wurde im AP7 genauer betrachtet.

Ambarella-Chip Analyse / Sicherheitsbetrachtung des KI-Chips

Die HSB hat eine Sicherheitsbetrachtung des KI-Chips Ambarella vorgenommen. Die ausführliche Analyse ist im Anhang 1 zu finden. Zusammenfassend scheint es möglich eine Vertrauenskette mit dem Chip aufzubauen, sodass das System als „sicher“ eingestuft werden kann.

Security-by-Design

Das Thema Security-by-Design wurde erörtert und als Präsentation dem Konsortium vorgestellt. Der Vortrag beinhaltete vor allem einen Überblick des Themas und sollte Entwicklern aufzeigen, wie der Ansatz umgesetzt werden kann und wo es gutes Begleitmaterial gibt.

3. High-end Edge Computing

Im Bereich des Edge Computing war das Ziel eine elektronische Erweiterung des Edge-Gateways ARENDAR durch eine Co-Prozessorkarte, um die Edge-Fähigkeit zu Stärken und die damit verbundenen Potentiale zu demonstrieren.

3.1. Anforderungsanalyse

Die HSB hat zunächst gemeinsam mit congatec Sicherheitsanforderungen aufgenommen, strukturiert und für die weitere Analyse priorisiert.
Als zentrale Themen haben sich dabei herauskristallisiert:

- → Manipulationssicherheit
- → Schutz vor Datendiebstahl, zum Beispiel von Lizenzdateien
- → Sicheres Booten
- → Passwortschutz
- → Physischer Zugriffsschutz
- → Schutz gegen Lizenzdiebstahl

3.2. Analyse von möglichen Sicherheitsstandards in der Industrie und Sicherheitskonzept für Softwareanbindung des Co-Prozessors

Die HSB hat die Bauteilrecherche begleitet. Es sollte ein ComputePi eingesetzt werden und über einen internen Kommunikationsbus mit der Hauptplatine verbunden werden. Die Anbindung des Co-Prozessors erfolgt als Erweiterungskarte, welche ein eigenständiges Betriebssystem stellt. Die Erweiterungskarte kann einerseits als eigenständiges Betriebssystem betrachtet werden, andererseits kann das Hauptsystem über einen im CongaConnect internen SPI-Bus auf das System zugreifen.
Aus diesem Grund wird auch die Spezifikation „Security Protocol and Data Model" (SPDM) der Distributed Management Task Force (DMTF) als Sicherheitsstandard genannt. SPDM ist ein Entwurf für die sichere Kommunikation von Komponenten innerhalb eines Gerätes mit dem Ziel, zusätzliche Sicherheit durch Authentifizierung zwischen den einzelnen Komponenten auf der Hardware bereitzustellen. SPDM bietet die Möglichkeit eine Integritätssicherung zu integrieren welche die Anbindungen an Trusted Computing Konzepte wie der Remote Attestation erlauben soll. Die dafür nötigen Spezifikationen waren und sind teilweise bisher nur im Mitgliederbericht als Entwurf vorliegend. Im Januar 2024 wurde die Version 1.0 des TCG-Standards zur Integration von DICE und SPDM unter dem Titel „Concise Evidence Binding for SPDM" [2] veröffentlicht und ist seitdem frei zugänglich. Darin wird die Anbindung von DICE an SPDM beschrieben. Der Standard stellt die Authentifizierung von Komponenten in einem Hardwaresystem sicher und bietet dazu Konzepte, Datenmodelle und Sequenzdiagramme für Prozesse an. Zum Zeitpunkt der Entscheidungsfindung in EMILIE war die Reife für den Einsatz im Projekt allerdings noch nicht gegeben. Als weitere Standards wurden vor allem Normen betrachtet, welche technische Sicherheitsanforderungen stellen. Darunter:

- → BSI IT-Grundschutzhandbuch [3]
- → IEC 62443-4-2 [4]
- → IEC 62443-3-3 [5]

Der BSI IT-Grundschutz bietet vor allem praktische Handreichungen für KMU mit dem Ziel, dass diese schnell und unkompliziert umgesetzt werden können, da vor allem pragmatische Lösungen vorgestellt werden. Außerdem ist eine einfache Integration in die ISO 27001 und das daraus resultierenden ISMS möglich, da die Risikoanalyse und dessen Bewertung für die Standardanforderungen von KMU bereits im Grundschutz generalistisch übernommen wurde.
Die IEC 62443 ist eine internationale Normenreihe mit dem Titel „Industrielle Kommunikationsnetze - IT-Sicherheit für Netze und Systeme". Die Normenreihe ist in verschiedene Teile und Bereiche gegliedert, die z. B. technische und prozessuale Themen beschreiben. Dazu gehören Themen zur sicheren Softwareentwicklung, Anforderungen an den sicheren Betrieb (u. a. Patch-, Update- und Konfigurationsmanagement), die Beschreibung technischer Sicherheitsanforderungen für Produkte und Komponenten. Darüber hinaus werden Reifegradmodelle (sog. Maturity Level) vorgegeben und Sicherheitslevel definiert. Die Sicherheitslevel helfen, den für die jeweilige Organisation notwendigen Schutzbedarf zu ermitteln, um daraus die Sicherheitsanforderungen abzuleiten. Die Sicherheitsanforderungen wurden ebenfalls in Sicherheitslevel gegliedert. Die IEC 62443 verfolgt außerdem das Prinzip von „Denfense in depth", welches in EMILIE durch Security-by-Design-Ansätze für die Softwareentwicklung adressiert wurde. Im Projekt EMILIE wurden Anforderungen den Teilen IEC 62443-3-3 [5] und der IEC 62443-4-2 [4] eingesetzt, um Sicherheitsanforderungen gemäß Level 3 und 4 abzuleiten. Organisatorische Standards wie die ISO 27001 wurden in EMILIE nicht betrachtet, weil primär technische Lösungen angestrebt werden und keine organisatorischen.

3.3. Anpassungen am Boot-Vorgang

Die HSB hat ein Konzept für die gegenseitige Identifikation mit der Kamera erstellt und die Anpassungen demonstrativ umgesetzt. Mithilfe der Konzepte „Remote Attestation" und „Measured Boot" konnte die Integrität der Edge-Geräte bewiesen werden. Von der HSB wurde ein Konzept entwickelt, um das TPM 2.0-basierte Messen vom Bootvorgang in ARM-Systemen umzusetzen.

Im Verlauf des Projekts wurde aus der Firma Arendar Security GmbH die Real-Time-Systems GmbH bzw. schlussendlich congatec. Dadurch sind die zuvor geplanten Hardwarekomponenten gegen vergleichbare der Firma congatec ausgetauscht worden. Um die Änderungen auszugleichen wurde mit Blick auf AP 3.4 (Anpassungen am Bootvorgang) Gespräche mit Experten von congatec über das Thema Architektur der neuen Hardwarekomponenten geführt. Die demonstrative Umsetzung wurde mit vergleichbaren Komponenten der Raspberry Pi Foundation umgesetzt.

3.4. Test und Evaluation

Unterstützung bei Tests und Evaluation wurde gestellt. Dies beinhaltet eine Installationsanleitung für die Integration von „HyBrid-Measured Boot“ für ARM-Systeme. Diese Integrationslösung für TPM 2.0-basiertes Messen von Bootvorgängen in ARM-Systeme wurde ebenfalls auf der Hardware der HSB getestet. Die dazu verwendete Entwicklungsplattform war der Raspberry Pi 4. Auf diesem wurde das Verfahren mehrfach erfolgreich getestet. Außerdem wurde Measured Boot im Demonstrator des Sicherheitskonzepts erfolgreich eingebaut.

4. Intelligente, Edge-basierte multisensorische und bildbasierte Datenverarbeitung

4.1. Schnittstellendefinition für vertrauensbasierte Verfahren in der Datenerhebung

Für die Auswahl von geeigneten Schnittstellen für die vertrauensbasierten Verfahren wurde die Gewährleistung von Vertraulichkeit, Integrität und Verfügbarkeit als Anforderung definiert. Das WebSocket-Protokoll wurde von der HSB als passend ausgewählt, da die Möglichkeit besteht mithilfe von TLS die Kommunikation zu verschlüsseln und die Vertraulichkeit zu gewährleisten. Durch die Integrierungsmöglichkeit der wechselseitigen Authentifizierung kann die Integrität aller Kommunikationspartner sichergestellt werden. Die verfügbaren Möglichkeiten im WebSocket-Protokoll bietet von sich aus schon eine solide Basis für die Absicherung der Kommunikation. Allerdings besteht die Möglichkeit, durch eine Integration der Funktionen des TPM 2.0 in die Kommunikation, mit WebSockets die Sicherheit deutlich zu steigern. Das WebSocket-Protokoll wurde genauer untersucht und die Einschätzungen dokumentiert. Die Absicherung der WebSocket-Kommunikation wurden konzeptionell und prototypisch umgesetzt.

4.2. Vorverarbeitung & Kalibrierung

Aufgabe der HSB war es bei der Auswahl der sicheren Kommunikationsschnittstelle zur Kamerahardware mitzuarbeiten. Die HSB hat bei der Anforderungsanalyse unterstützt und ein Konzept skizziert, wie die Kommunikationsschnittstelle zur Kamerahardware abgesichert werden kann. Die Umsetzung, Test und Evaluation des Konzepts sind im Rahmen von AP 7 erfolgt.

5. Smart Computing Industrie 4.0 CM & PM

Die Inbetriebnahme, Umsetzung der Funktionstests und Evaluation der sicheren Datenkommunikation wurde im Rahmen des Sicherheitsdemonstrators der HSB umgesetzt. Näheres dazu ist im Folgenden im Kapitel 7 Netz- und Datensicherheit beschrieben. Die HSB hat zusätzlich mithilfe von Magnetic Sense das Gerät für die Konvertierung des analogen CAN-Signals in eine mit TPM 2.0 geschützte WebSocket-Kommunikation den anderen Projektpartnern bereitgestellt. So hatten die Projektpartner die Möglichkeit das Gerät auch im Demonstrator des Frauenhofer ITWM namens „VibDemo“ einzusetzen.

6. Smart Edge Computing Prozessoptimierung / Energiemanagement

6.1. Anforderungsspezifikation Betriebsoptimierung

Die Unterstützung der beteiligten Projektpartner bei der Anforderungsanalyse hinsichtlich der Sicherheitsanforderungen ist erfolgt und somit erfolgreich abgeschlossen.

6.2. Integration der Sensorik, Aktorik und Datenerfassung

Die HSB hat das Sicherheitskonzept für die Datenübertragung in einem eigenen Demonstrator im Rahmen des AP 7 umgesetzt. Der HSB-Demonstrator bildet die Kommunikationsumgebung, inklusive der Kamera und der magnetostriktiven Sensoren, nach.

7. Netz- und Datensicherheit

Die im Projekt EMILIE angestrebten Schutzstufen 3 und 4 des IEC 62443-Standards bieten Schutz gegen technisch versierte Angreifer mit spezifischen Fähigkeiten. Die Klassifizierung der Schutzlevel ist in Tabelle 7.3 dargestellt. Eine Unterscheidung der Schutzlevel erfolgt vor allem hinsichtlich der Motivation und des Aufwands für den Angreifer. Die Schutzlevel 1 und 2 sind in der Regel mit vergleichsweise einfachen Mitteln zu erreichen und meist bereits durch organisatorische Maßnahmen realisierbar, da es sich in der Regel um sehr typische Sicherheitsmaßnahmen handelt. Grundsätzlich ist auch zu berücksichtigen, dass die Angriffe über den Cyberspace erfolgen und rein physische Gewalt gegen Produktionsanlagen und Güter nicht betrachtet werden kann.

Tabelle 7.3: Schutzlevel nach IEC 62443 [5]

SCHUTZLEVEL (SL)	MISSBRAUCH	EINGESETZTE MITTEL	AUFWAND	KOMPETENZEN	MOTIVATION
1	Ungewollt	Keine	„Zufall“	/	/
2	Gewollt	Einfach	Niedrig	Allgemein	Niedrig
3	Gewollt	Technisch ausgefeilt	Moderat	Spezifisch	Moderat
4	Gewollt	Technisch ausgefeilt	Erheblich	Spezifisch	Hoch

Die zunehmende Integration von IoT-Geräten in industrielle Produktionsanlagen vergrößert die Angriffsfläche auf das Gesamtsystem deutlich. Typische industrielle Steuerungsanlagen und -Komponenten (industrial control system, ICS) arbeiten mit einem Produktionssystem zusammen, um ein Ziel zu erreichen, z. B. die Herstellung eines Produkts. Industrielle IoT (IIoT) hingegen hat verschiedene Fähigkeiten, die oftmals aus der Datenerfassung (Sensor) und dem Speichern und Verarbeiten von Informationen aus und über den Produktionsprozess bestehen. Diese schaffen primär neue und große Datenmengen, mit den Zielen der Produktionsrationalisierung und Effizienzsteigerung [6]. Neben dem IIoT-Gerät sind in der Regel weitere Rechenressourcen notwendig, die ebenfalls geschützt werden müssen. Bei IIoT-Geräten ist die Wertschöpfungskette ein vollständig digitaler Prozess. Dieser muss entlang des „Datenstroms“ gesichert werden, da eine Manipulation der Daten die Ziele von IIoT gefährdet.

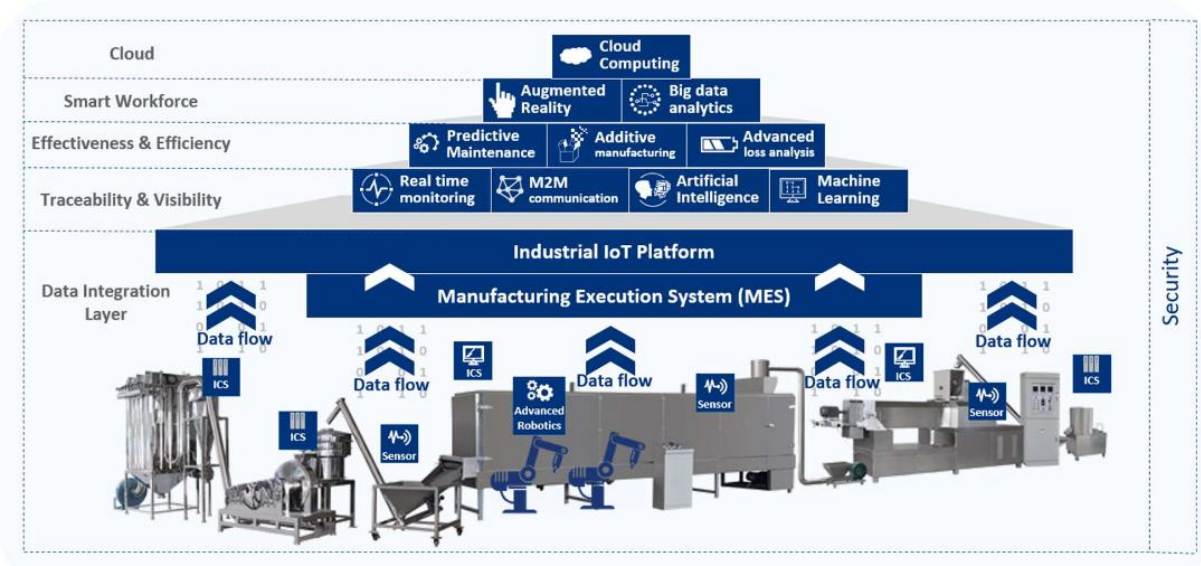

Abbildung 2: Industrie 4.0 und Smart Manufacturing. Quelle: [6]

Abbildung 2 verdeutlicht dies visuell: Ganz unten sind Maschinen, deren Sensorik Daten an eine IoT-Plattform senden (Industrial IoT Platform). Basierend auf dieser Plattform können die Daten für neue Dienste verwendet werden. Die gezeigten Beispiele der Echtzeitüberwachung, Maschinelles Lernen (künstliche Intelligenz), Predictive Maintenance basieren auf der Korrektheit der Daten. Können Daten zuvor manipuliert werden, dann kommen diese auf dem Daten lernenden System zu falschen Einschätzungen. Diese wiederum verhindern bestenfalls eine Produktivitätssteigerung, schlimmstenfalls erzeugen sie jedoch das Gegenteil.

7.1. Szenariendefinition mit Fokus auf mögliche Bedrohungsszenarien

7.1.1. Szenariendefinition

Im Rahmen von AP 7.1 hat die HSB ihr Know-how im Bereich der IT-Sicherheit eingebracht und konnte zusammen mit den Projektpartnern das Arbeitspaket wie im Projektplan vorgesehen abschließen. Auf Grundlage von Gesprächen mit einzelnen Projektpartnern konnte das in Abbildung 3 dargestellte Gesamtszenario entwickelt werden. Der Projektfokus liegt dabei auf den OT-IT-Verbindungen, die insbesondere dem Energieeffizienzmanagement sowie der Predictive Maintenance dienen und nicht auf der bestehenden Aktorik und Sensorik bzw. sicherheitsrelevanten bestehenden OT-Steuerungen. An der Industrieanlage (z.B. eine Zementmühle der Gebr. Pfeiffer) werden ein magnetostriktiver Drehmomentsensor (Magnetic Sense) und eine Industriekamera (Mobotix) installiert. Die Daten werden über verschiedene Kommunikationsprotokolle wie MQTT oder WebSockets auf dem Edge-Gateway gesammelt und anschließend an eine Leitstelle weitergeleitet oder in einer Cloud-Umgebung zum Trainieren und Verbessern von KI-Modellen eingesetzt.

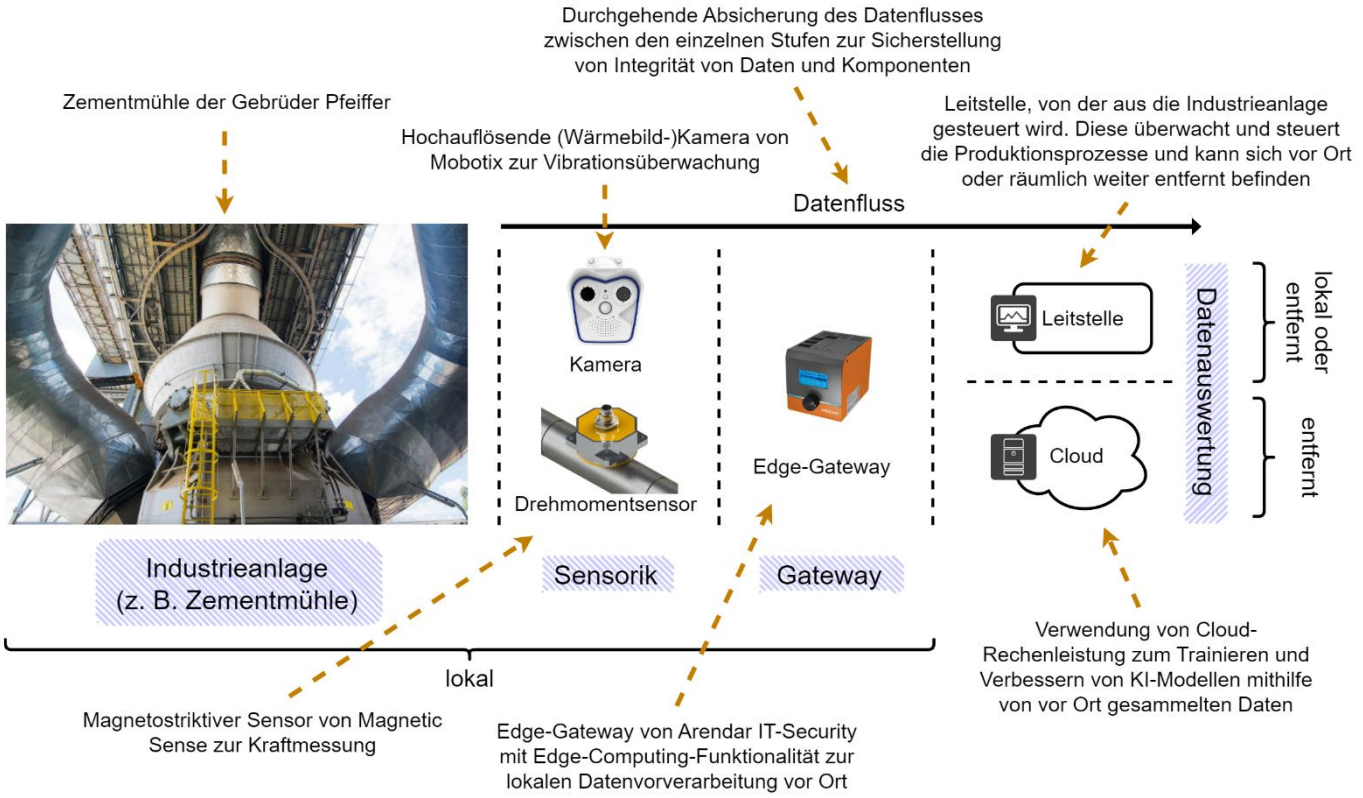

Abbildung 3: Darstellung des EMILIE-Gesamtszenarios an einer Zementmühle

7.1.2. Bedrohungsszenarien

Zunächst wurde für die Bedrohungsanalyse das Gesamtszenario in kleinere Einzelszenarien unterteilt. Pal und Jadidi [7] fassen mehrere Vorgehensweisen aus verschiedenen Veröffentlichungen zusammen und bieten drei Vorschläge von Schicht-IIoT-Modellen mit jeweils unterschiedlicher Granularität an. Die Datenflüsse der einzelnen

Komponenten wurden auf die drei Modelle angewendet. Dabei zeigte sich, dass alle Modelle das Problem haben das untersuchte Gesamtszenario nicht korrekt wiederzugeben, da die Support-Schicht, die für die Datenanalyse zuständig ist, in unserem Szenario in der Sensorik (Kamera) stattfinden sollte und sich somit zwischen der Perception- und Network-Schicht befindet. [7]
Eine signifikante Datenvorverarbeitung am Sensor ist in den angegebenen Modellen nicht vorgesehen, was konträr zum Projektziel von EMILIE steht. Daher wurden die Datenflüsse auf ein angepasstes 5-Schichten-IIoT-Modell angewendet, in dem zwischen der Perception- und Network-Schicht noch eine weitere Schicht hinzugefügt wurde: die Preprocessing-Schicht. [7]
Zur Erarbeitung der Bedrohungen wurde weiterführend das von Microsoft entwickelte STRIDE-Modell (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege) ausgewählt und auf die fünf Schichten angewendet. Fokus der HSB war es dabei die Bedrohungslage der einzelnen Geräte (congatec, Mobotix, Magnetic Sense) sowie die Netzwerkinfrastruktur und IT-Server genauer zu betrachten.
Die Ergebnisse wurden in einem Bedrohungsanalyse-Dokument festgehalten.

7.2. Sicherheitsanalyse eingesetzter Protokolle und Schnittstellen

Maßstab für die Analyse der Sicherheit sind die primären Eigenschaften der Informationssicherheit: Vertraulichkeit, Integrität, Authentifizierung, Autorisierung und Verfügbarkeit. Gegen diese Eigenschaften wurden zunächst die Analogen Signale und Übertragungsstrecken bewertet. Zusammen mit den Projektpartnern haben sich folgende Übertragungsprotokolle herauskristallisiert:

- → **CAN-Bus (Controller Area Network)**: Ein serielles Bussystem, das für die zuverlässige Übertragung von Daten entworfen wurde. Mehrere gleichberechtigte Akteure werden über eine Busleitung miteinander verbunden. Das Protokoll bietet eine hohe (elektrische) Störsicherheit, geringe Kosten und Echtzeitfähigkeit.

- → **MQTT (Message Queueing Telemetry Transport)**: Ein leichtgewichtiges Publish/Subscribe-Protokoll, das häufig in IoT-Anwendungen verwendet wird. Es ist für die effiziente Kommunikation bei niedriger Bandbreite ausgelegt.

- → **OPC-UA (Open Platform Communications Unified Architecture)**: Ein plattformunabhängiges Kommunikationsprotokoll, das speziell für die sichere Datenkommunikation in der Industrie entwickelt wurde. Es bietet umfangreiche Sicherheitsfeatures.

- → **WebSockets**: Ein Protokoll für die bidirektionale Kommunikation zwischen Client und Server über eine einzelne, langlebige Verbindung. Es wird häufig in Webanwendungen verwendet und ermöglicht Echtzeitkommunikation.

Eine Tabellarische Zusammenfassung der Sicherheitsanalyse der eingesetzten Protokolle zeigt Tabelle 7.4. Analoge Bussysteme können kaum abgesichert werden, ohne dass die Protokolle vom erwarteten Quality-of-Service abweichen bzw. die vorgesehenen Funktionen nicht mehr ohne Beeinträchtigung ausführen zu können. Aus diesem Grund müssen analoge Signale frühestmöglich in digitale umgewandelt und durch erweiterte Sicherheitsmaßnahmen wie Hardwaresicherheitsmodule abgesichert werden. MQTT, WebSockets und OPC-UA können über TLS abgesichert werden. Bei MQTT und WebSockets hängt die Sicherheit maßgeblich von der Implementierung der Bibliothek ab, da diese TLS für die Verbindung zur Verfügung stellen muss. Bei MQTT sei anzumerken, dass es sich nur um die Verbindung zum Broker handelt. Ob die Daten ab dem Broker zu einer dritten Partei ebenfalls mittels TLS übertragen werden ist nicht gewährleistet. Hierzu ist es notwendig die Kontrolle über den Broker zu besitzen und dort lediglich TLS-Verbindungen zu akzeptieren.

Tabelle 7.4: Überblick über Sicherheitsattribute der eingesetzten Übertragungsprotokolle

SICHERHEITS ATTRIBUT	CANBUS	MQTT	OPC-UA	WEBSOCKETS
VERTRAULICHKEIT	Keine Verschlüsselung	TLS optional	TLS optional	TLS optional
INTEGRITÄT	Keine Integritätsprüfungen	Nachrichten-integrität durch TLS	Nachrichtenintegrität durch TLS	Nachrichtenintegrität durch TLS
AUTHENTIFIZIE-RUNG	Keine Authentifizierung	Authentifizierung über TLS-Zertifikate	Integrierte Benutzer- und Zertifikatsauth.	Authentifizierung über TLS-Zertifikate
AUTORISIERUNG	Keine Autorisierungs-mechanismen	Abhängig vom Imple-mentierungsumfang	(Granulare) Zugriffs-kontrolle integriert	Abhängig vom Imple-mentierungsumfang
VERFÜGBARKEIT	Anfällig für DoS-An-griffe	Anfällig für DoS-An-griffe	Hohe Verfügbarkeit durch Redundanzkon-zepte	Anfällig für DoS-An-griffe

7.3. Planung eines Netz- und Datensicherheitskonzeptes mit durchgehender Vertrauenskette

Das Netz- und Datensicherheitskonzept der HSB basiert auf drei Standbeinen: Plattformsicherheit, Verbindungssicherheit und Sicherheitsverifikation. In allen drei Bereichen wurden die drei Informationsschutzziele Vertraulichkeit, Authentizität und Integrität sichergestellt. Im Folgenden werden die Konzepte der drei Bereiche ausführlicher beschrieben.

7.3.1. Plattformsicherheit

Basierend auf Konzepten des Trusted Computing der Trusted Computing Group stellt ein Trusted Platform Module Version 2 (TPM 2.0) die Vertrauensbasis in unserem Konzept dar und wurde in alle möglichen Geräte integriert. Da die Integration eines TPM 2.0-Chips in die Mobotix Kamera nicht im Rahmen der Projektlaufzeit möglich war, wurden mit einem TPM 2.0-Simulator die möglichen Schutzmechanismen prototypisch dargestellt.
Der TPM 2.0 bietet als Kryptoprozessor-Chip viele Vorteile, die in unserem Konzept genutzt werden können. Neben einem Random Number Generator können viele kryptografische Algorithmen vom TPM 2.0 übernommen werden. Außerdem bietet der Chip persistenten und flüchtigen Speicher, in denen kritische Daten wie Schlüsselmaterial sicher abgelegt werden können. Jeder TPM 2.0 besitzt sogenannte Root-Keys, die die Integrität des Gerätes zweifelsfrei belegen können.

Measured Boot

Für die weitere Absicherung der Hardwareplattformen wurde der Bootvorgang kryptografisch gemessen und die Messergebnisse in den Plattform Configuration Registern (PCRs) des TPMs verkettet. In der Regel spricht man an dieser Stelle von Measured Boot, manchmal auch vom Secure Boot. Im EMILIE-Projekt wird der Begriff Measured Boot verwendet. Beim Measured Boot werden die Systemzustände während der Schritte des Bootvorgangs erfasst und als ein Hashwert in die einzelnen PCR-Bänke geschrieben. Dabei werden die einzelnen Schritte miteinander verkettet. Außerdem können die PCR-Bänke nach Vollendung des Bootvorgangs nicht mehr verändert oder manipuliert werden.

Wechselspeicher/SD-Karten-Absicherung

Bei manchen IIoT-Geräten ist der Speicher nicht fest in dem Gerät verbaut, sondern zum leichten austauschen designt. Im EMILIE-Projekt ist dies im Szenario der Industriekamera von Mobotix der Fall. Die Gefahr dabei, dass ein fremdes Betriebssystem durch austauschen von z.B. SD-Karten auf ein Gerät geschleust wird ist dabei sehr hoch. Um dies abzusichern besteht die Möglichkeit die SD-Karte an den TPM 2.0 zu binden sodass keine „fremden“ Speichermedien vom System akzeptiert werden. Die Entschlüsselung kann dann nur mit dem fest verbauten TPM 2.0 und dessen geheimen Schlüsselmaterial stattfinden.

7.3.2. Verbindungssicherheit

Um die Vertraulichkeit und Integrität bei der Kommunikation der Geräte zu gewährleisten wurde, sofern möglich, in allen Protokollen die TLS-Verschlüsselung genutzt. Um dies noch zu steigern, unterstützt der TPM 2.0 bei der Erstellung und Speicherung des Schlüsselmaterials. Sowohl MQTT als auch WebSockets bieten die Möglichkeit der TLS-Verschlüsselung bereits im Protokoll an. Beim analogen CAN-Bus-Signal wurde so bald wie möglich auf ein digitales Signal (z.B. WebSocket) gewechselt, um auch dort von den Vorteilen der TLS-Verschlüsselung profitieren zu können. Für die Maximierung der Sicherheit wurde sich nicht nur auf eine serverseitige Authentifizierung fokussiert, sondern auch eine wechselseitige Authentifizierung betrachtet.

7.3.3. Sicherheitsverifikation

Für die Verifizierung der Systemstatus bietet sich das Konzept der Remote Attestation an. Dabei werden die durch das Measured Boot gewonnenen Systemzustände der Geräte attestiert. Für die Attestierung werden die frisch gemessenen Systemzustände an einen „Verifier“ gesendet und dort mit einem vorher definierten Referenzzustand verglichen. So kann eine Veränderung oder Manipulation am Gerät frühzeitig erkannt und Gegenmaßnahmen ergriffen werden.

7.4. Entwurf einer Softwarearchitektur zur Umsetzung des geplanten Konzeptes und Implementierung der Software-Komponenten zur Hardware-Einbindung im Demonstrator

Die Realisierung einer durchgängigen Vertrauenskette für den industriellen Einsatz wurde auf möglichst unterschiedlichen Hardwareplattformen ermöglicht. Dazu wurde eine komponentenbasierte Architektur angestrebt. Die Komponenten sind in Abbildung 4 als virtuelles IIoT-Gateway dargestellt.
Durch die komponentenbasierte Umsetzung des Konzepts konnte jede Komponente in der am besten geeignetsten Programmiersprache implementiert werden, was zu einer schnelleren Umsetzung von Prototypen führt. Ein weiterer Vorteil dieser Architektur ist, dass sie eine klare Trennung der Verantwortlichkeiten ermöglicht und jede Komponente separat gewartet werden kann. Die einzeln entwickelten Komponenten werden zu einem virtuellen Referenz-Gateway zusammengefügt. Ausgehend vom Referenz-Gateway werden die Komponenten in die Plattformen der Partner integriert und an deren Bedürfnisse angepasst. Für jede Komponente wird die Architektur im Folgenden vorgestellt.

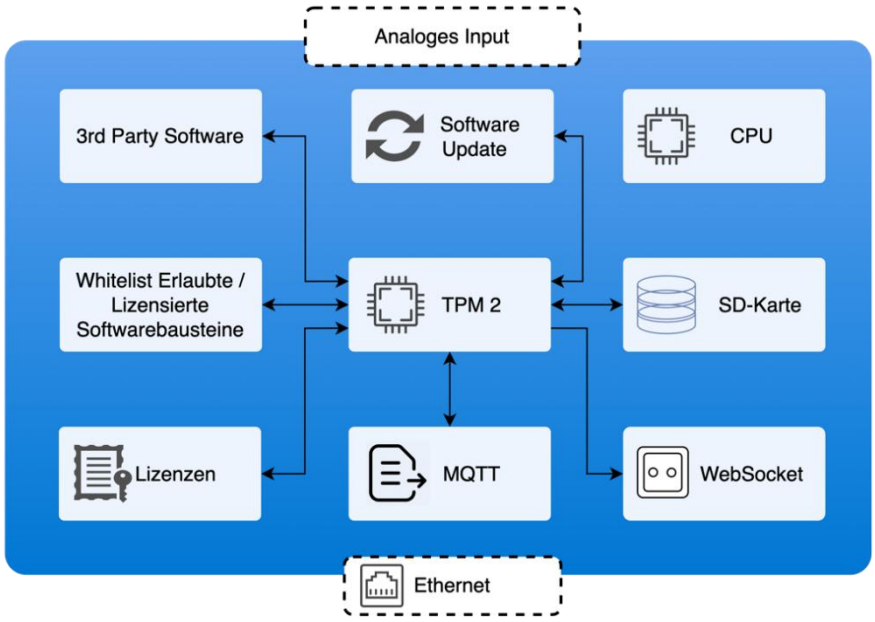

Abbildung 4: Softwarekomponenten des virtuellen IIoT-Gateways

7.4.1. SD-Karten mit TPM 2.0 verschlüsseln

In Anforderungsmeetings des Arbeitspakets 2.2 (Edge Computing – Schnittstellen) stellte sich heraus, dass der Diebstahl von Videomaterial auf internen Wechseldatenträgern der IIoT-Geräte und Sensoren ein Sicherheitsrisiko darstellt. Deshalb sollte eine sichere Verschlüsselung des Materials erreicht werden. Eine Verschlüsselung benötigt typischerweise einen (geheimen) Schlüssel, mit dem die Daten ver- und entschlüsselt werden können. Der Schlüssel wird entweder vom Benutzer eingegeben, was in diesem Falle nicht praktikabel ist, oder er wird ebenfalls mit im IIoT-Gerät gespeichert. In diesem Falle kann der Schlüssel jedoch ebenfalls gestohlen werden, da er sich auf dem Gerät befindet. Beide Lösungen stellen daher keine geeigneten Sicherheitsmaßnahmen dar. Als Lösungsmaßnahem für das beschriebene Problem, wurde der Datenträger kryptografisch an einen Hardware-Security-Modul (HSM) „fest-gebunden“. Eine Entschlüsselung des Datenträgers ist ohne das kamerainterne HSM nicht mehr möglich, da nur dieser den Schlüssel besitzt und diesen gegen Diebstahl schützt. Die Bindung ist technisch so gestaltet, dass der Wechseldatenträger nur durch den TPM 2.0 entschlüsselt werden kann, mit dem auch die Verschlüsselung erstellt wurde. Ein anderer TPM 2.0 ist nicht in Lage den Datenträger zu entschlüsseln. Um dies zu erreichen werden TPM 2.0-Spezifische Sicherheitsmechanismen der Schlüsselerzeugung und Ableitung von Schlüsselmaterial genutzt. Damit wurde erreicht, dass Beispielsweise bei IIoT-Geräten keine Daten durch entwenden der Speichermedien gestohlen werden können. Für die Umsetzung wurde das Open Source Tool namens „Clevis“ zusammen mit einem TPM 2.0 SLB 9670 Modul für den Raspberry Pi 3 und die Softwarebibliothek tpm2_tools verwendet. Das Open Source Tool „Clevis“ wurde genutzt, um eine automatische Entschlüsselung beim Booten zu realisieren. Die eigentliche Verschlüsselung der SD-Karte wurde mit einem Open Source Tool namens „cryptsetup“ ausgeführt. Darüber hinaus wurden weitere Konfigurationsmöglichkeiten für den TPM 2.0 identifiziert, mit welchen die Sicherheit erhöht werden kann.

7.4.2. MQTT-Komponente

Aus dem Gesamtszenario und den vorangegangenen Anforderungsgesprächen hat sich ergeben, dass das MQTT-Protokoll an verschiedenen Stellen im Projekt für den Datenaustausch zwischen Sensorik und dem Edge-Gateway vorgesehen ist.

MQTT

MQTT ist ein Netzwerkprotokoll für „Message Queueing Telemetry Transport“ und dient hauptsächlich dem Austausch von Telemetriedaten. Es wurde primär für die Machine-to-Machine (M2M) Kommunikation entwickelt und wird deshalb zunehmend im Bereich des Industrial IoT und IoT eingesetzt. Telemetriedaten werden hauptsächlich von Sensoren und anderen ereignisgesteuerten Datenerzeugern (Producern) erzeugt. Das Protokoll basiert auf dem Publish and Subscribe Prinzip und verwendet einen Broker zwischen dem Datenerzeuger (Producer) und dem Datennutzer (Consumer). Ein Producer kann Daten für andere Kommunikationsteilnehmer bereitstellen, indem die Daten unter einem vorher definierten Topic an den Broker gesendet werden. Der Broker verwaltet die Topics und sorgt dafür, dass die Consumer, die ein Topic abonniert haben, die dazugehörigen Daten bereitgestellt bekommen. Diese Topics sind hierarchisch organisiert. Demnach ist MQTT primär zum Senden und Empfangen von Daten. Eine gezielte Datenabfrage kann dabei nicht erfolgen.

Ablauf Remote Attestation

Bei der Remote Attestation (RA) fordert der Verifier zunächst einen Quote beim Attester an. Die Aufforderung enthält die zu attestierenden PCR-Bänke sowie eine "Nonce" (vereinfacht: Zufallszahl). Der Attester empfängt diese, erzeugt aus der PCR einen sogenannten Quote und sendet diesen Quote an den Verifier zurück. Der Quote enthält neben den PCR-Hashes und der Signatur auch die Nonce. Die Nonce dient dabei als Nachweis, dass der Quote "frisch" erzeugt wurde. Damit kann der Verifier sicherstellen, dass der Quote nicht veraltet ist. Der Verifier validiert den Quote anschließend und vergleicht ihn gegen einen „goldenen Quote“ der den erwartetet Systemzustand repräsentiert.

Integrationskonzept

Das Problem bei MQTT ist, dass die Daten nur in eine Richtung fließen. Vom Produzenten zum Broker und vom Broker zum Konsumenten. Um den Datenfluss mit MQTT in beide Richtungen zu ermöglichen, müssen Verifier und Attester zwei Topics abonnieren. Der Attester abonniert das für ihn vorgesehene Topic, um darüber die

Aufforderung eines Quotes zu erhalten (inkl. Nonce und PCR-Bänken). Der Verifier abonniert ebenfalls das für ihn vom Attester vorgesehene Topic, um darüber den Quote zu erhalten. Die Abbildung 5 zeigt das angestrebte Konzept.

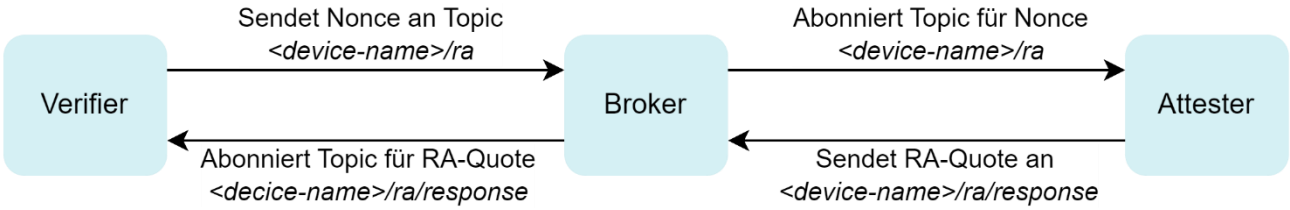

Abbildung 5: Umsetzungskonzept Remote Attestation via MQTT - Publish/Subscribe Mechanismen

Implementierung

Die Implementierung wurde in Python 3 umgesetzt. Die Abbildung 6 zeigt das Schichten und Komponentenmodell der Implementierung. Diese benötigt auf der untersten Ebene einen Docker-Container oder andere Unix-Umgebung, welche einen TPM 2.0 oder einen TPM 2.0-Simulator bereitstellt. Außerdem wird der TPM2-Software-Stack (TSS) benötigt, welcher die Kommunikation zum TPM 2.0 stellt und auf die nächste Schicht mit den Python-Bibliotheken kommunizieren kann. In der Python 3.9 Umgebung wurde die Bibliothek tpm2-pytss eingesetzt. Diese stellt die Bindings zum TPM 2.0-Software-Stack bereit und realisiert innerhalb der Applikation den eigentlichen Quote bzw. dessen Verifikation. Der TPM 2.0-Software-Stack und die tpm2-pytss sind Open Source und werden von der Entwicklergemeinschaft “Linux TPM 2.0 & TSS Software” realisiert. Einige zentrale Entwickler sind bei Infineon und dem Fraunhofer SIT beschäftigt und übernehmen die Federführung bei der Implementierung der APIs und Infrastrukturen der TCG TSS2 Spezifikationen.

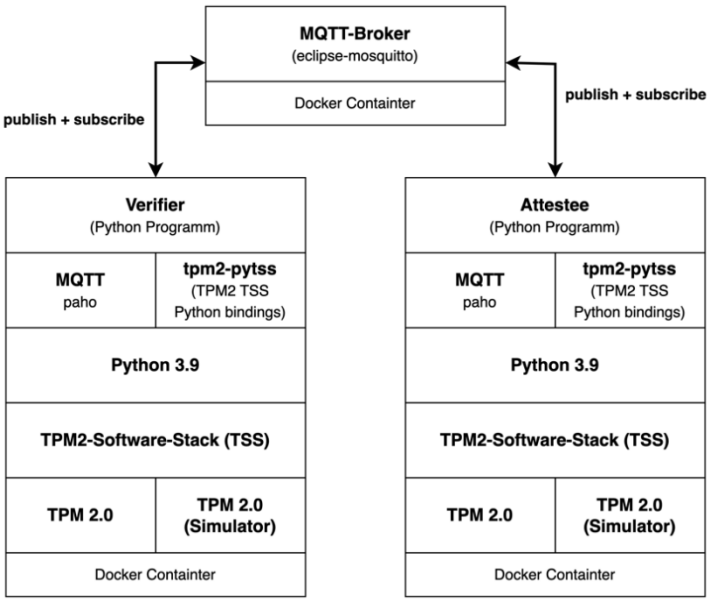

Abbildung 6: Technologie-Stack der MQTT-Kommunikation

7.4.3. WebSocket-Komponente

Vergleichbar zur MQTT-Komponente kam auch das WebSocket-Protokoll bei der Datenübertragung von Sensoren zum Gateway zum Einsatz.

WebSocket

Das WebSocket-Protokoll stellt eine bidirektionale Verbindung zwischen Server und Clients her. Während bei reinem HTTP nur unidirektionale und kurzweilige Verbindungen zustande kommen, bieten WebSockets die

Möglichkeiten die Verbindung aufrecht zu erhalten und Nachrichten unabhängig vom gegenüber zu initiieren. Da das Protokoll auf TCP basiert kann eine Verschlüsselung der Übertragung durch „Transport Layer Security“ (TLS) gewährleistet werden.

TLS Verschlüsselung mit TPM 2.0

Die TLS-Verschlüsselung der WebSocket-Kommunikation wurde im Rahmen des Projektes mit dem Einsatz des TPM 2.0 unterstützt. Grundsätzlich authentifiziert sich der Server gegenüber dem Client mittels eines Zertifikats während des Handshakes. Der Client überprüft die Identität des Servers anhand des gesendeten Zertifikats. Wird der Server als vertrauenswürdig eingestuft, einigen sich beide Kommunikationsparteien auf ein gemeinsames Geheimnis, z.B. durch den Diffie-Hellman-Schlüsselaustausch. Aus dem Geheimnis wird anschließend von beiden ein kryptographischer Schlüssel abgeleitet, der in der folgenden symmetrisch verschlüsselten Kommunikation genutzt wird. Um die Sicherheit noch zu verstärken setzen wir zusätzlich die wechselseitige Authentifizierung ein. Das bedeutet, auch der Client muss sich mit einem Zertifikat beim Server authentifizieren. Der Schutz des Schlüsselmaterials ist hierbei kritisch. Sollte z. B. ein Zertifikat mit einem kompromittierten Zertifikat ausgetauscht werden und so ein Kommunikationspartner fälschlicherweise als vertrauenswürdig eingestuft werden, obwohl es sich um einen Angreifer handelt, gewährleistet die Verschlüsselung nicht mehr die Integrität und Authentizität der Nachrichten. Um das und weitere Angriffsszenarien zu verhindern wird der TPM 2.0 in das Sicherheitskonzept integriert.

Implementierung

Abbildung 7 zeigt das Schichten- und Komponentenmodell der Implementierung für die WebSocket-Komponente. Für die Umsetzung wurde ebenfalls der TPM 2.0-Software-Stack (TSS) als Grundlage für die Kommunikation mit dem TPM 2.0 verwendet. Die Bibliothek tpm2-openssl bietet die Möglichkeit einen Provider in OpenSSL zu integrieren, der die Nutzung des TPM 2.0 ermöglicht. Dadurch werden die Algorithmen für die Verschlüsselung der Kommunikation, soweit möglich, auf den Hardware-Krypto-Chip ausgelagert. Die Einbindung in Python funktioniert über einen SSL-Kontext der im Code angegeben werden kann.

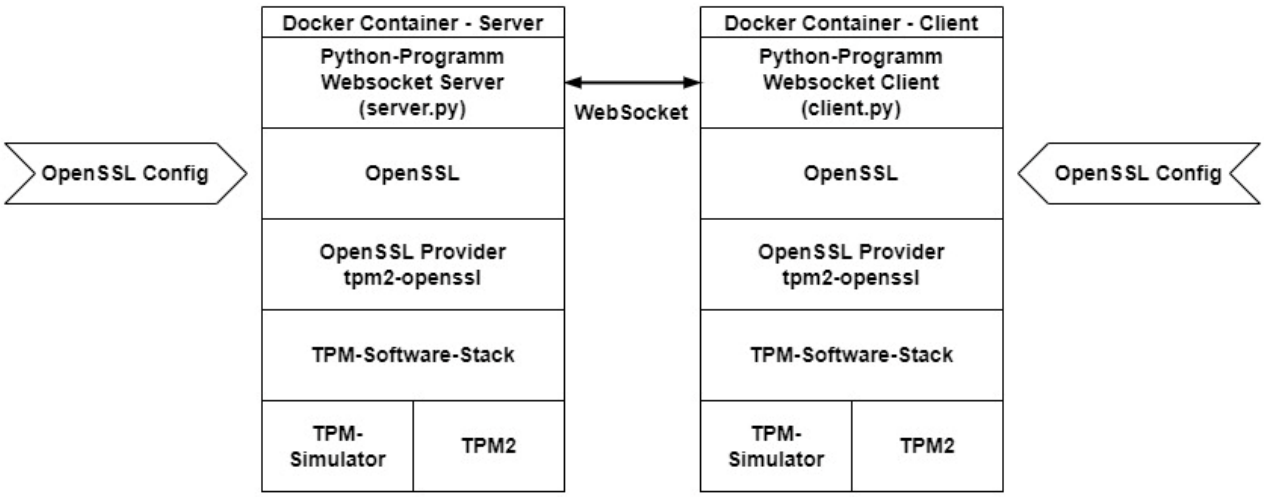

Abbildung 7: Schichtmodell der WebSocket-Komponente

7.4.4. Software-Update

Aufbau

Die Absicherung der Software-Updates zielt darauf ab, die Integrität, Authentizität und Vertraulichkeit der ausgelieferten Software zu gewährleisten. Der Signierungsschlüssel wird im TPM 2.0 des Build-Systems, auch Hostsystem genannt, generiert und verwahrt. Der öffentliche Teil dieses Schlüssels wird an die Zielsysteme ausgeliefert und ebenfalls im dortigen TPM 2.0 verwahrt. Die Verwahrung des Schlüssels im TPM 2.0 sollte verhindern, dass dieser in die Hände von Dritten gelangen kann. Nur authentifizierten Nutzern ist es möglich, auf den Schlüssel und somit auf die damit verbunden Operationen zuzugreifen.

Der Signierungsprozess umfasst die Erstellung eines Hash-Werts der zu signierenden Datei, der dann mit dem Schlüssel des Hostsystems signiert wird. Diese Signatur wird zusammen mit der Software archiviert und an die Zielsysteme ausgeliefert. Während des Update-Prozesses authentifiziert sich der Nutzer auf dem System und startet den Update-Prozess. Zur Überprüfung der Authentizität und Integrität der empfangenen Datei wird erneut ein Hash-Wert ermittelt. Der öffentliche Teil des Signierungsschlüssels, der zuvor auf dem Zielsystem gespeichert wurde, wird verwendet, um den Hash-Wert zum Zeitpunkt der Erstellung abzuleiten. Diese Werte werden miteinander verglichen, um den aktuellen Zustand der Dateien zu überprüfen. Bei Übereinstimmung wird die Datei als vertrauenswürdig betrachtet, bei Abweichungen wird der Prozess unterbrochen.

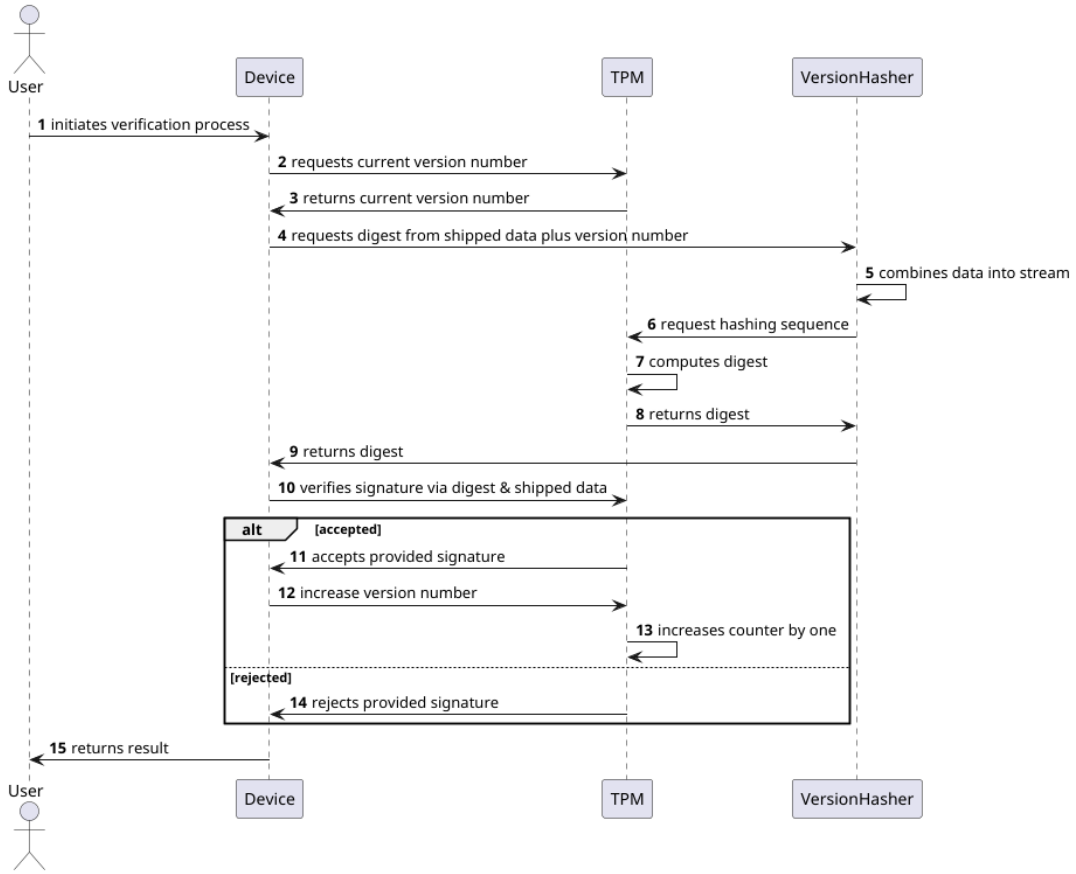

Abbildung 8: Verifizierungsprozess für sichere Software-Updates

Um Rollback-Attacken zu verhindern, bei denen ältere und potenziell gefährdete Versionen aufgespielt werden, wird ein monotonischer Zähler (NV Index) im TPM 2.0 verwendet. Dieser Zähler kann nur um den Wert 1 erhöht werden und ermöglicht eine eindeutige Zuordnung der Versionsnummer zu den jeweiligen Software- und Firmware-Versionen. Die Verifikation setzt eine identische Versionsnummer voraus, um ein Update erfolgreich zu validieren. Bei Nichtübereinstimmung wird der Update-Prozess abgelehnt und der Nutzer informiert. Durch die Erweiterung der Hash-Wert-Berechnung um einen zusätzlichen, synchronisierten Wert auf Host- und Zielplattform wird eine Manipulation des Systems verhindert und Kompromittierungen können erkannt werden.

Implementierung

Grundsätzlich dient der TPM 2.0 als zentraler Ankerpunkt für alle Sicherheitsoperationen, einschließlich der Erstellung und sicheren Verwahrung von Schlüsseln zur Signierung von Daten sowie der Verifizierung signierter Daten. Die Absicherung der Software-Updates erfolgt somit ausschließlich durch den TPM 2.0 und dem dazugehörigen TPM Software Stack. Da ein reguläres Linux-Betriebssystem verwendet wird, kann die Feature API (FAPI) des TPM 2.0-Software-Stacks (TSS) genutzt werden, um viele Operationen und Konfigurationen zu vereinfachen. Der Zugriff erfolgt hier über die TPM Tools, die das Ausführen der nötigen Funktionen auf der Benutzerseite ermöglichen.

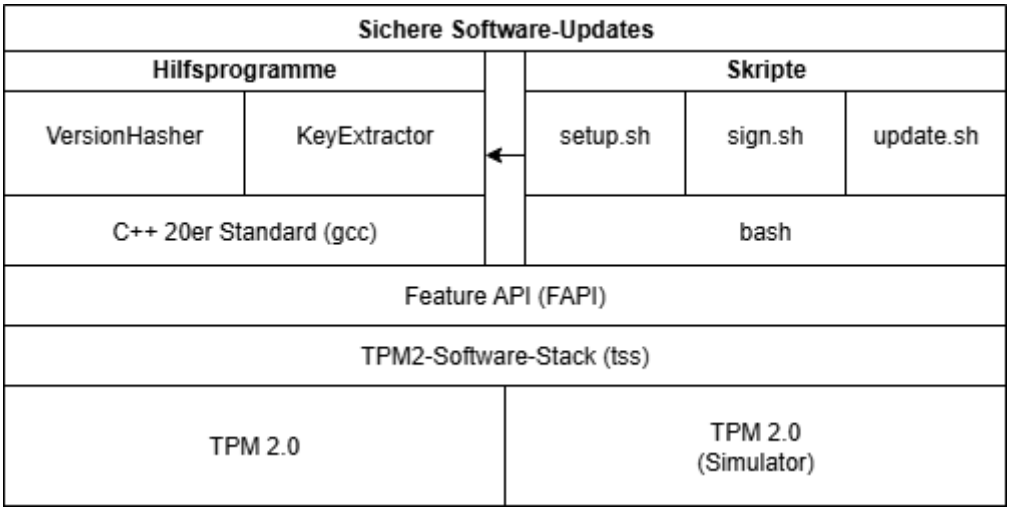

Abbildung 9: Implementierung der sicheren Software-Updates

Weiterhin können viele der Schritte unter Zunahme von Skripten gebündelt und automatisiert werden. Insgesamt existieren drei solcher Skripte für die Umsetzung des oben gezeigten Konzepts: setup.sh, sign.sh und update.sh. Das erste Skript dient lediglich dem erstmaligen Aufsetzen und Einrichten der jeweiligen Plattform (Initialisierung des TPM 2.0, Erstellen und Verwahren des Signierungsschlüssel, Ableiten, bzw. Speichern des öffentlichen Schlüssels im TPM 2.0). sign.sh steht synonym für den Signierungsprozess, bei der das Update zusammen mit einer Signatur versehen und in ein Archiv komprimiert wird. Bei update.sh handelt es sich wiederum um den Verifikationsprozess, welcher das Update entpackt und mit der ausgelieferten Signatur unter Zunahme des öffentlichen Schlüssels vergleicht.
Des Weiteren wurden zudem zwei weitere Hilfsprogramme entwickelt, namentlich der VersionHasher und der KeyExtractor. Das Programm VersionHasher wird benötigt, um einen Hash unter Zunahme eines NV Index zu berechnen. Somit ist dieses Programm unerlässlich für den Signierungs- sowie dem Verifizierungsprozess. Wiederum dient der KeyExtractor lediglich der Deserialisierung eines Schlüssels aus dem TPM 2.0 und konvertiert diesen in eine PEM-formatierte Datei. Beide Programme wurden in der Sprache C++ mit dem Standard 20 realisiert. Dadurch wird ein direkter Zugriff auf die FAPI des TSS möglich, was eine granuläre Kontrolle bei der Steuerung des TPM 2.0 zulässt. Beide Hilfsprogramme sind in den Prozessen der Skripte integriert und müssen zum Zeitpunkt der Ausführung der Skripte vorhanden sein.

7.5. Integration der Software-Komponenten mit den Partnern in den Demonstrator

Für die Umsetzung des Sicherheitskonzeptes wurde ein Demonstrator (Abbildung 10) entwickelt, der das Szenario der Überwachung einer Industrieanlage mithilfe von Sensoren und Edge-Elektronik so nah wie möglich darstellt.
Als Industrieanlage wurde ein Modell einer Windkraftanlage verbaut. Die drehende Achse der Windkraftanlage hat Ähnlichkeiten mit der drehenden Achse der Zementmühle, ist anschaulicher und ausreichend für die Darstellung der Sicherheitskonzepte. Als Sensorik wurde die Industriekamera vom Mobotix und ein magnetostriktiver Drehmomentsensor von Magnetic Sense eingesetzt. Für die Konvertierung des analogen CAN-Signals in ein digitales Signal sorgt ein Raspberry Pi 4 als „CAN-Converter“. Die Funktionen des Edge-Gateways übernimmt ebenfalls ein Raspberry Pi 4. Das Gateway sammelt die Daten von den Sensoren ein und leitet sie an die Leitstelle weiter, die die gesammelten Daten in einer kleinen GUI darstellt. Alle Geräte wurden mit einem „TPM 2.0 Evaluation Board“ der Firma Infineon ausgestattet. Bei der Plattform der Kamera war die Integration eines physischen TPM 2.0-Chips nicht möglich, daher wurden die Konzepte exemplarisch mit dem TPM 2.0-Simulator auf Softwareebene umgesetzt.

Remote Attestation

Um die Absicherung der Plattformen umzusetzen wurde auf allen Plattformen Measured Boot eingerichtet und mithilfe von Remote Attestation die Status der Geräte verifiziert. Die Rolle des Verifier hat die Leitstelle übernommen. Als Verifier sammelt die Leitstelle die Measured Boot Ergebnisse aller Geräte ein und vergleicht sie mit den erwarteten Werten. Die Status der Geräte wird in der GUI dargestellt.

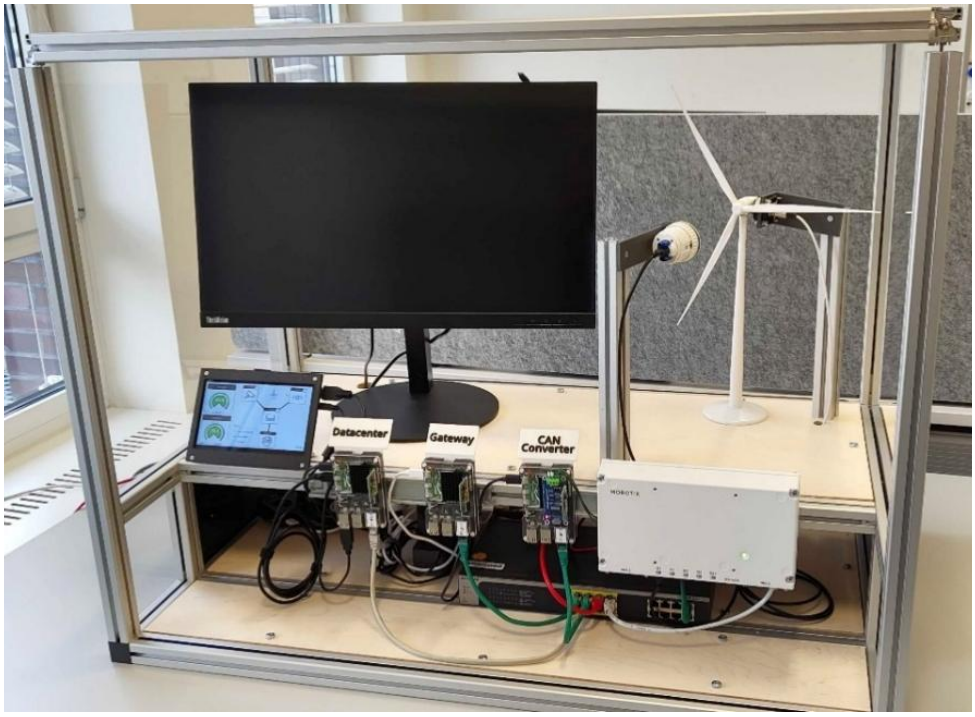

Abbildung 10: Demonstrator des Sicherheitskonzepts „Secure Mill“

Verschlüsselung

Die WebSocket-Kommunikation zwischen CAN-Converter, Edge-Gateway und Leitstelle wurde mithilfe des TPMs und TLS verschlüsselt. Das Schlüsselmaterial wurde mit dem TPM 2.0 generiert. Zusätzlich wurde die Wechselseitige Authentifizierung für die Kommunikation aktiviert.

8. Nutzen und Verwertung

Ein besonders wichtiger Teil in der Verwertungskette einer praxisorientierten Forschungs- und Bildungseinrichtung ist der Beitrag zur Lehre durch die Aktualität der Themen aus den Forschungsprojekten. Auch spannende und aktuelle Themen für Abschlussarbeiten werden aus den Problemstellungen der Forschungsprojekte abgeleitet und liefern damit gleichzeitig einen Beitrag zur regionalen Kompetenzstärkung. Die Hochschule Bremen publiziert Ergebnisse aus den Forschungsprojekten auf nationalen und internationalen Konferenzen sowie in regionalen Foren.

Literaturverzeichnis

[1] M. Bozdal, M. Samie, S. Aslam und I. Jennions, „Evaluation of can bus security challenges," *Sensors,* 2020.

[2] Trusted Computing Group, „TCG DICE Concise Evidence," 2024.

[3] Bundesamt für Sicherheit in der Informationstechnik (BSI), IT-Grundschutz-Kompendium, Bonn: Reguvis Fachmedien GmbH, 2023.

[4] Internationale Elektrotechnische Kommission (IEC), *IEC 62443-4-2:2019: Sicherheit für industrielle Automatisierungs- und Steuerungssysteme - Teil 4-2: Technische Sicherheitsanforderungen für Komponenten,* Genf, 2019.

[5] Internationale Elektrotechnische Kommission (IEC), *IEC 62443-3-3:2013: Industrielle Kommunikationsnetze - IT-Sicherheit für Netze und Systeme - Teil 3-3: Systemanforderungen zur IT-Sicherheit und Security-Level,* Genf, 2013.

[6] European Network and Information Security Agency, Good practices for security of Internet of things in the context of smart manufacturing, Publications Office, 2018.

[7] S. Pal und Z. Jadidi, *Analysis of Security Issues and Countermeasures for the Industrial Internet of Things,* Brisbane, 2021.

[8] Bundesamt für Sicherheit in der Informationstechnik, „BSI – Technische Richtlinie - Kryptographische Verfahren: Empfehlungen und Schlüssellängen - BSI TR-02102-1," 31. 01. 2025. [Online]. Available: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102.pdf?__blob=publicationFile&v=13. [Zugriff am 05. 11. 2025].

[9] R. Smart, „Implementing the 10 Security Goals – Anti-rollback Explained," 27. 04. 2021. [Online]. Available: https://www.psacertified.org/blog/anti-rollback-explained/.

[10] ISO, „ISO 26262-1:2018(en)," 2018. [Online]. Available: https://www.iso.org/obp/ui/#iso:std:iso:26262:-1:ed-2:v1:en. [Zugriff am 05. 11. 2025].

[11] M. Palkar, „Functional safety for automotive vision processors," Ambarella, 27. 07. 2020. [Online]. Available: https://www.ambarella.com/blog/functional-safety-for-automotive-vision-processors/. [Zugriff am 05. 11. 2025].

[12] W. Lawrenz und N. Obermöller, CAN - Controller Area Network: Grundlagen, Design, Anwendungen, Testtechnik, Berlin: VDE Verlag GMBH, 2011.

[13] T. Dee und A. Tyagi, „Message integrity and authenticity in secure CAN," *IEEE Consumer Electronics Magazine 10.5 ,* pp. 33-40, 2020.

[14] K. Tindell, „CAN Bus Security - Attacks on CAN bus and their mitigations," *Canis Automotive Labs,* 2020.

Anhang

I. Ambarella-Chip Analyse / Sicherheitsbetrachtung des KI-Chips

Das Kamerasystem ist modular aufgebaut und beinhaltet unterschiedliche System-on-Chip (SoC) Module. Diese Module basieren oft auf einer ARM-Architektur und werden zunehmend beliebt, daher folgt eine Analyse der Sicherheitsfunktionen des Ambarella-Vision-Chip.

Einleitung

Die Analyse der Sicherheitsfunktionen basiert auf den Funktionen, die auf der Webseite von Ambarella bereitgestellt werden. Im Folgenden werden diese Funktionen (Features) aufgelistet und eine Einschätzung dazu abgegeben, ob und inwiefern diese Funktionen einen Beitrag zu IT-Sicherheit leisten können. Was diese Analyse nicht berücksichtigen kann, ist eine Einschätzung, ob die Funktionen vom Chip genutzt werden, ob sie tatsächlich auch vorhanden sind und ob nicht andere Hintertüren bzw. Schwachstellen vorhanden sind, welche ausgenutzt werden können, um Sicherheitsmaßnahmen zu umgehen.

Feature: Mask-programmed boot ROM acts as a hardware root-of-trust.

> *Initial stages of the boot process are verified via on-chip memory with keys stored in the on-chip OTP area. Signature verification uses 2048-bit keys and SHA-256.*

Unser Verständnis: Diese Funktion zielt darauf ab, dass das allererste Stück Software, welches beim Booten ausgeführt wird, vertrauenswürdig ist. Nach unserem Verständnis wird hier Schlüsselmaterial zur Verifizierung genutzt, welches in einem „One-Time-Programmable“ (OTP[1]) Speicherbereich liegt. Das heißt, dieser Bereich kann nur einmal einen Schlüssel speichern. Danach kann er nicht mehr verändert werden. Unklar ist, was für ein Typ von Schlüssel dort hinterlegt werden sollte und wer darauf wie Zugriff hat.
Einschätzung: Das Absichern des Schlüssels (Key) in einem solchen OTP-Bereich gilt als manipulationssicher. SHA-256 als Hashfunktion gilt ebenfalls als manipulationssicher [7].
Bei der angesprochenen Schlüssellänge von 2048 Bit bei Feature 1 fehlt die Angabe darüber, welches kryptografische Verfahren verwendet wird. Gängige Verfahren sind RSA, ECDH oder ECDSA. Vermutlich wird RSA verwendet, da es in der Praxis sehr oft eingesetzt wird. Auch die Länge des Schlüssels würde dazu passen. Hier ist zu beachten, dass die Empfehlung für die Länge der Schlüssel beim RSA-Verfahren laut dem BSI bei 3000 Bit liegen sollte, um auch in Zukunft einen hohen Schutz zu bieten. Dennoch wird dies von uns als grundsätzlich sicher eingeschätzt, da es nicht genutzt wird, um Geheimnisse außerhalb des Systems zu übertragen (z.B. bei der Aushandlung eines symmetrischen Schlüssels).

Feature: Secure Boot

Beschreibung: Unter dem Begriff „Secure Boot“ wird im Allgemeinen ein abgesicherter Bootvorgang gemeint, welcher nur die vorgesehenen und signierten Boot-Dateien in der ersten Bootphase lädt und ausführt. Damit sollen die Integrität und Authentizität der geladenen Firmware (und zugehörige Komponenten) sichergestellt werden.

Feature: Device Unique ID

Beschreibung: Der Begriff Device Unique ID ist nicht im kryptografischen Sinne definiert, deshalb kann an dieser Stelle nur vermutet werden, wofür er eingesetzt werden soll bzw. vorgesehen ist. Wie der Begriff erkennen lässt, handelt es ich um eine einmalige ID, welche kein zweites Mal vorkommt (wie ein Autokennzeichen).
Dieses kann genutzt werden, um es in für die Kamera erstellte Zertifikate zu integrieren. Man kann damit (kryptografisch) den Nachweis erbringen, dass es sich wirklich um genau diesen einen Chip mit dieser ID handelt. Dies setzt

[1] One-Time-Programmable Area leicht erklärt: https://semiengineering.com/knowledge_centers/memory/one-time-programmable-memory/

allerdings voraus, dass die Software auf dem Chip, die das Zertifikat generiert, vertrauenswürdig ist und durch das Secure-Boot-Verfahren vor Manipulation geschützt ist. Nach unseren Recherchen ist der Zugriff auf die DeviceUniqueID nicht geschützt.
Einschätzung: Dies ist eine sehr sinnvolle Maßnahme, die genutzt werden kann, um die „Identität" des Gerätes jederzeit einwandfrei nachweisen zu können. Dies erhöht das Vertrauen. Allerdings setzt es voraus, dass alle Software vorher auch korrekt implementiert und provisioniert wurde und nicht manipuliert ist.

Feature: Device Unique Encryption Key

Beschreibung: Beim „Device Unique Encryption Key" handelt es sich vermutlich um einen asymmetrischen privaten (sprich geheimen) Schlüssel. Dies kann z.B. der geheime Teil eines RSA- oder ECDH-Schlüsselpaars sein. Liegt für den öffentlichen Schlüssel ein Zertifikat vor bzw. kann erzeugt werden, dann wird daraus ein sinnvolles Konzept. Wenn dieses Zertifikat zusätzlich die *Device Unique ID* enthält, ist es möglich, den Chip zweifelsfrei zu identifizieren und dieser kann seine Identität kryptografisch beglaubigen.
Einschätzung: Diesen Punkt am besten mit dem Hersteller abklären. Es konnte nicht herausgefunden werden, ob es sich hierbei um eine Seed handelt oder um einen Teil für ein größeres Sicherheitskonzept zur Identitätsbeglaubigung.

Feature: Secure Random / True Random Number Generator

Beschreibung: Ein Secure Random oder auch True Random Number Generator (TRNG) kommt in der Regel beim Erzeugen von kryptografischen Schlüsseln zum Einsatz. Viele kryptografische Verfahren benötigen eine Zufallszahl. Ist die Zufallszahl von vorn herein vorhersagbar, so kann kein sicherer Schlüssel erzeugt werden, da der Angreifer im Vorfeld oder parallel den erzeugten kryptografischen Schlüssel ebenfalls erzeugen kann. Ein TRNG hingegen ist so konzipiert, dass die erzeugten Zahlen echte Zufallszahlen sind.
Hintergrund: Das dahinterstehende Problem ist, dass ein Zufallszahlengenerator nach einem bestimmten Schema Zahlen generiert. Auch, wenn dieses Muster nicht einfach erkennbar ist, können durch intensives Beobachten manchmal Rückschlüsse gezogen werden, auf deren Grundlage Zufallszahlen vorausgesagt werden können. Dabei spricht man auch von einem Pseudo-Zufallsgenerator.
Einschätzung: Zufallszahlen auf Grundlage eines TRNG zu erzeugen ist sehr empfehlenswert und erhöht definitiv die Sicherheit. Besonders gegenüber einem Pseudozufallszahlengenerator steigt die „Zufälligkeit" enorm. Um welchen Typ von TRNG es sich handelt und wie dieser genau spezifiziert ist, kann allerdings nicht entnommen werden.

Feature: JTAG/Debug Enable

Beschreibung: Hierbei handelt es sich um eine Hardwareschnittstelle definiert durch die Joint Test Action Group (JTAG), welche zum Debuggen von Hardwarekomponenten verwendet wird. Grundsätzlich verschafft eine solche Schnittstelle den vollen Zugriff auf einen Chip oder eine Schaltung. Damit hat ein Angreifer auch die volle Kontrolle über das System / den Chip.
Einschätzung: Diese Schnittstelle ist zum Debuggen gedacht und bietet damit weitreichenden Zugriff auf das System. Daher sollte eine solche Schnittstelle im Produktivbetrieb unbedingt deaktiviert sein. Zusätzlich muss sichergestellt werden, dass sie nicht einfach wieder aktiviert werden kann. Es gibt hier und da Informationen und Konzepte von unterschiedlichen Herstellern, um eine solche Schnittstelle abzusichern. In diesem Falle ist allerdings von Aktivierung die Rede (Debug Enable). Daher muss genau geklärt werden, was dies bedeutet. Nach unserer Einschätzung stellt diese Schnittstelle damit einen Angriffsvektor dar.

Feature: Arm® TrustZone®

Beschreibung: Die ARM TrustZone ist eine von ARM entwickelte Umgebung, die als besonders sicher gilt. Dieser ist hardwareseitig vom restlichen System getrennt. Der unsichere Teil hat keinen Zugriff auf die sichere Umgebung. Die sichere Umgebung hat eigene Peripherie und eigenen Speicher. Zu den Aufgaben der sicheren Umgebung zählen die Secure-Boot-Mechanismen und sichere Firmware-Updates. Die Idee dahinter entspricht dem, was unter einer Trusted Execution Environment (TEE) verstanden wird. Dabei handelt es sich um eine vertrauenswürdige Umgebung, welche Zugriff auf die CPU hat, aber die unsichere Welt kann darauf nicht zugreifen. Diese Umgebung gilt als sicher, da die Mechanismen wie Secure Boot, Zufallszahlengenerator und andere kleine Software dort abgelegt sind und sie insgesamt einen sehr kleinen Funktionsumfang bietet. Dieser kann von außen auch nicht erweitert

werden und hält damit die Angriffsfläche klein. Außerdem kann die ARM TrustZone in den sicheren Bootvorgang einbezogen werden.
ARM selber bietet unterschiedliche TrustZones mit verschiedenen Funktionen und Versionen an. Detaillierte Informationen über die ARM TrustZone finden sich unter: **Learn the architecture - TrustZone for AArch64 (arm.com)**
Einschätzung: Die ARM TrustZone gilt allgemein als eine sichere Komponente. Das Konzept dahinter ist ebenfalls schlüssig und durchdacht. Die Nutzung der TrustZone erhöht die Informationssicherheit enorm. Wie genau diese hier eingesetzt und verwendet wird ist allerdings unklar. Wird diese wie vorgesehen genutzt, erhöht dies die Sicherheit des Systems.

Feature: Data-at-Rest Encryption

Beschreibung: Unter „Data-at-Rest" werden im allgemeinen Daten verstanden, welche gerade in einem Speicher „ruhen". Dies sind Daten, welche gerade nicht aktiv genutzt werden. Diese Daten zu verschlüsseln soll auch gegen Datendiebstahl und gegen Datenschutzverletzungen vorbeugen bzw. diese minimieren.
Einschätzung: Eine Verschlüsselung dieser Daten erhöht in jedem Fall die Informationssicherheit und gehört zu den best-practices.

Feature: Secure Wipe

Beschreibung: Das sichere Löschen von Daten auf einem Datenträger wird oft auch als „Secure Wipe" bezeichnet. Damit ist auch gemeint, dass alle Daten sicher entfernt wurden und nicht durch ein Wiederherstellungsprogramm oder durch Dritte wiederhergestellt werden können. Normales Löschen hingegen löscht in der Regel nicht die Daten, sondern gibt den Bereich auf dem Speicher zum Wiederbeschreiben frei. Dies bedeutet, dass die Daten nach dem „Löschen" auf dem Datenträger selber vorhanden sein können. Für bestimmte Speichermedien gibt es bestimmte Vorgaben, wie diese überschrieben werden müssen, um als wirklich gelöscht zu gelten.
Der Begriff „Secure Wipe" wird oftmals auch mit einem Reset in Verbindung gebracht, kann allerdings auch bedeuten, dass jegliche Software auf dem Gerät sicher entfernt wird.
Einschätzung: Eine solche Funktion erhöht die Informationssicherheit und kann insbesondere für Datenschutzaspekte nützlich sein, da man sichergehen kann, dass das verarbeitete Bildmaterial sowie möglicherweise vertrauenswürdige Konfigurationen wirklich gelöscht wurden.

Feature: Secure Credential Provisioning

Beschreibung: Secure Credential Provisioning meint die initial sichere Bereitstellung von Authentifizierungsinformationen. Vermutlich handelt es sich dabei um eine sichere Erzeugung von privatem Schlüsselmaterial, welches so erzeugt wird, dass auch der Hersteller bzw. Softwareentwickler keinen Zugriff darauf hat und ebenfalls nicht in der Lage ist, die initialen „Credentials" in irgendeiner Form zu kennen oder nachträglich rekonstruieren zu können.
Ein Beispiel aus der Praxis: Ein neuer Mitarbeiter im Unternehmen bekommt seinen Computer und muss sich zum ersten Mal anmelden. In der Regel geschieht dies mit einem Passwort, welches die Administratoren initial festgelegt haben und daher auch kennen. Dies ist das *Gegenteil* von Secure Credential Provisioning, da die Admins das Passwort kennen. Beim Secure Credential Provisioning würde niemand vorher ein Passwort festlegen oder es kennen.
Einschätzung: Solche Verfahren liefern einen wichtigen Beitrag zur Sicherheit und Vertrauenswürdigkeit der Hardware bzw. Softwaresysteme und stellen einen wichtigen Baustein für die Informationssicherheit dar. Wie das Secure Credential Provisioning bei diesem Chip umgesetzt wird, kann allerdings nicht ausgemacht werden.

Feature: Rollback Prevention

Beschreibung: Mit dem Begriff ist eine Maßnahme bzw. ein Mechanismus gemeint, der verhindert, dass zum Beispiel die Software auf dem System gegen eine niedrigere Version ausgetauscht werden kann. In der Praxis enthält jede Software Schwachstellen, die ausgenutzt werden können. Diese werden in der Regel durch ein Update und eine neue Softwareversion geschlossen. Angreifer können versuchen, über den Update-Mechanismus eine frühere Software einzuspielen, welche eine bekannte Schwachstelle enthält, die sie dann ausnutzen können.
Eine solche Angriff wird auch Downgrade-Angriff genannt. Eine verständliche Quelle dazu ist unter [8] zu finden.
Einschätzung: Eine sehr sinnvolle Maßnahme, da damit Downgrade-Angriffe verhindert werden können. Dieser Angriffstyp ist relativ weit verbreitet und sollte daher unterbunden werden.

Feature: Zertifizierung nach ISO 26262

Beschreibung: Der Hersteller Ambarella behauptet auf seiner Webseite, dass sie intern Prozesse und Verfahren implementiert haben, um den Vorgaben der ISO 26262 für ihre Produkte zu entsprechen.
Bei der ISO 26262 handelt es sich um eine Normenreihe für sicherheitsrelevante elektronische Systeme in Kraftfahrzeugen (Kfz), im Sinne der „safety“. Die Norm zielt darauf ab, dass die funktionale Sicherheit elektronischer Komponenten im Kfz gegeben ist. Die Normenreihe ist laut der ISO eine Adaption der IEC 61508 [9].
Einschätzung: Da die Norm aus dem Bereich der Funktionalen Sicherheit für Kfz kommt, können wir lediglich Schlussfolgerungen aus den öffentlichen Dokumenten ziehen. Über die genaue Umsetzung oder einen konkreten Zertifizierungsnachweis konnten keine Belege bzw. Nachweise bei Ambarella.com gefunden werden. Der Hersteller informiert aber ausführlich über die Norm und beschreibt den Umgang damit (siehe [10]) und wirkt insgesamt glaubwürdig. Für konkrete Rückfragen geben sie ebenfalls eine Kontaktadresse an.
Grundsätzlich erscheint die Einhaltung bzw. Umsetzung einer Norm, welche eine Referenz für den Produktlebenszyklus im Bereich der Automotive-Safety darstellt, sehr sinnvoll. In wie weit die Norm auch das Thema „Security“ behandelt, kann ohne weiteres nicht geklärt werden. Laut Wikipedia ist die Einhaltung der Norm in Deutschland rechtlich nicht direkt gefordert.

Allgemeine Zusammenfassung

Insgesamt werden viele Technologie, Mechanismen und Verfahren zur Erhöhung der IT-Sicherheit vom Hersteller genannt. Zum Teil sind es anerkannte Verfahren und zum anderen Teil sind diese Verfahren auch bei anderen Herstellern zu finden. An manchen Stellen ist unklar, wie der Mechanismus oder das Verfahren genau aussieht. Dies kann vor allem an den Bezeichnungen liegen, bzw. es fehlt zu manchen Funktionen der genaue Kontext. Mit den genannten Verfahren scheint es möglich zu sein, eine Vertrauenskette aufzubauen und das System als „sicher“ einzustufen.