AG CYSIS

IT/ OT-Security bei
Internet of Railway Things (IoRT)

Unterstützt von:

Herausgeber:

AG CYSIS
UG IT Security IoRT

06.12.2020

Inhaltsverzeichnis

1 Management Summary

Der zunehmende Einsatz von IP-basierten Objekten, Diensten und Protokollen („things“) sowie die kommunikative Vernetzung eröffnet für den Bahnsektor im Rahmen der Digitalisierungsstrategie vollkommen neue Möglichkeiten zur Steigerung der Kapazitäten bei gleichzeitiger Optimierung von Wirtschaftlichkeit und Rentabilität sowie eine Erhöhung des Kundennutzens. So werden z.B. bei DB Netz die aktuell ca. 3.000 Stellwerke, die auf der einen Seite auf sehr unterschiedlichen Technologien basieren (von mechanisch bis elektronisch) und auf der anderen Seite als vollständig isolierte und geschlossene Systeme arbeiten, im Rahmen von NeuPro auf eine einheitliche architektonische Basis gestellt (Digitale Stellwerke [1]).

Ein Teil dieser Dienste sind IoTs (Internet of Things), die in Form von Sensoren und Aktuatoren verschiedene Daten generieren, mit welchen die Bahneffizienz und Operationen verbessert werden können. Der Begriff IoT impliziert eine Vielzahl von Objekten (Sensoren, Aktuatoren), Technologien und Protokollen, die über Datennetze kommunizieren und Daten austauschen. IoRT (Internet of Railway Things) bezeichnet Objekte, die im bahnbetrieblichen Umfeld eingesetzt werden (am Gleis, im Zug, …).

Die Nutzung von IoT bzw. IoRT sowie insbesondere die Vernetzung sehr vieler Objekte bedingt neue Bedrohungen, Gefährdungen und Risiken bzgl. IT Security, die umfassend und eingehend betrachtet werden müssen. Demzufolge müssen neben Fragen zur Betriebssicherheit „Safety“, die traditionell im Bahnbetrieb Berücksichtigung finden, auch Fragen der „Security“ (Erkennung und Abwehr von Cyberbedrohungen) betrachtet werden.

Im Rahmen dieses Whitepapers erfolgt eine Beschreibung eines Referenzmodells für IoT und anschließend werden unterschiedliche Anwendungsfälle im Bahnkontext analysiert. Im ersten Block sind dies Standardanwendungsfälle zur Optimierung der Passagierverteilung, des Reisendenerlebnisses sowie im Bereich der Gewaltprävention. Im zweiten Block werden zwei Anwendungsfälle im Bereich der Leit- und Sicherungstechnik (LST) betrachtet, bei denen Aktoren und Sensoren zum Einsatz kommen. Dies sind die zustandsbasierte und vorausschauende Instandhaltung („predictive maintenance“, engl.) sowie lokale Situationserkennung im operativen Bahnbetrieb (z.B. fremde Objekte im Gleisbereich).

Basierend auf diesen teilweise sehr unterschiedlichen Anwendungsfällen werden Bedrohungsszenarien auf Basis der BSI ICS-Bedrohungen betrachtet sowie sinnvolle Lösungsansätze skizziert und beschrieben. Eingang finden sowohl die NeuPro-Architektur, die im Rahmen der Digitalisierung der Stellwerkstechnik bei der DB entwickelt wurde, als auch Ergebnisse aus dem Forschungsprojekt „HASELNUSS“ [2] des Bundesministeriums für Bildung und Forschung (BMBF) , die es ermöglichen geeignete IT-Sicherheitsfunktionen in die vernetzen LST-Systeme zu integrieren.

2 Einleitung

Der Begriff „Internet of Things“ bzw. „IoT“ kam erstmalig 1999 auf und sollte eine aus damaliger Sicht zukünftige Welt beschreiben, in der alle physikalischen Objekte mit sogenannten RFID (radio-frequency identification) Anhängern versehen sind, so dass man sie in Echtzeit lokalisieren und über das Internet Datenabfragen initiieren kann. Seit dieser Zeit hat sich der Bedeutungsumfang gleichwohl ausgeweitet und der Begriff IoT umfasst heutzutage eine Vielzahl von Objekten, Technologien und Protokollen, die entgegen der Bezeichnung „Internet“ nicht per se über das Internet verbunden bzw. erreichbar sein müssen. In besonderem Maße haben eingebettete Systeme, die meist mit einer Reihe von Sensoren ausgestattet sind, Einzug in den Alltag gehalten. IoT hegt nunmehr als Vision eine Verknüpfung alltäglicher, elektronischer Geräte und Sensoren, die im gemeinsamen Datenaustausch stehen und Teil einer digitalen Infrastruktur werden. Dadurch wird ein Abbild der realen Welt in Form von Daten geschaffen, durch die effizient eine Vielzahl von Problemen automatisiert bearbeitet werden kann.

Durch die Verknüpfung von lokalen Devices mit einer eindeutigen Identität entsteht eine nutzbare Verbindung zwischen der physischen Welt der Dinge und der virtuellen Welt der Daten [3]. Hiermit wird einem wesentlichen Merkmal der Digitalisierung Rechnung getragen - nämlich dem exponentiellen Anstieg von Datenvolumen auf der einen Seite sowie von für die geschäftsrelevante Verarbeitung dieser Daten erforderlichen Applikationen bzw. Algorithmen und Rechnerleistung auf der anderen Seite. Die Geschäftsrelevanz der Daten bzw. der verarbeiteten Daten erstreckt sich dabei von der gestiegenen Transparenz, die für eine Erhöhung der Sicherheit oder eine Optimierung von Prozessen erforderlich ist, über prognostische Verfahren, die die Grundlage für Effektivitätssteigerungen bilden, bis zu verschiedenen Arten der Automatisierung, sei es mittels regelbasierter Expertensysteme oder mittels neuronaler Netzwerke, die die Grundlage für Effizienzsteigerungen und Risikominimierungen bilden.

Der gewachsene Bedeutungsumfang von IoT machte es erforderlich, einen entsprechenden Referenzrahmen zu schaffen. Dies geschah in umfassender Form beispielsweise durch das IoT World Forum [4] [5]. Angesichts der bereits bestehenden Vielzahl an vernetzten Sensoren und Aktuatoren sowie datenverarbeitenden Komponenten in der Bahninfrastruktur ist es sinnvoll, die für die IoT entwickelten Konzepte auf den Bahnbereich zu übertragen. Hierzu wird in Anlehnung an diesen Referenzrahmen ein Referenzmodell für ein „Internet of Railway Things“ bzw. „IoRT“ beschrieben, wobei IoRT gewissermaßen als Untermenge von IoT verstanden wird – nämlich als IoT für den Einsatz im Rail Umfeld optimierte Objekte und Technologien, die entsprechenden Sicherheitsziele im Bahnbetrieb zu ermöglichen. Durch die vorausschauende Instandhaltung (predictive maintenance) von operativen Komponenten können diese Dienste zur Verminderung von unerwarteten Störungen im Betrieb führen, auch können mit Hilfe von IoRT das Angebot an begleitenden Produkten und Dienstleistungen sowie der Grad der Kundenzufriedenheit durch stärkere Personalisierung der Angebote erhöht werden.

Um die gewünschte Leistungssteigerung dauerhaft zu ermöglichen und die durch die Vernetzung möglichen Sicherheitsbedrohungen auf die Objekte zu minimieren und die nachgelagerten Systeme der IT (Informationstechnologie) und OT (Operationale Technologie) angemessen zu schützen, ist es erforderlich, das Thema IT-Sicherheit der IoRT-Systeme zu untersuchen. Zu diesem Zweck hat sich das Projekt „Internet of Railway Things“ der Arbeitsgruppe Cybersecurity für sicherheitskritische Infrastrukturen“ (AG CYSIS) intensiv mit den Einsatzbereichen der IoRT und den daraus resultierenden Gefährdungen und Schutzmaßnahmen befasst. Hierzu werden Sicherheitsziele definiert, die zu Anforderungen an die IoRT-Systeme führen. Ein weiterer Grund für dieses Whitepaper sind die – auch im Bereich der IoT – stetig zunehmenden Cyberangriffe. Demzufolge darf erwartet werden, dass hiervon zukünftig auch die Bahninfrastrukturen betroffen sein werden. Eingriffe in das System Rail gilt es präventiv zu verhindern, bzw. Maßnahmen zu treffen, um im Angriffsfalle die Auswirkungen zu minimieren um einen reibungslosen und gesicherten Bahnbetrieb aufrecht erhalten zu können.

Das vorliegende Whitepaper ist das Ergebnis dieser Sicherheitsbetrachtungen und stellt allgemeine Sicherheitsanforderungen für den Einsatz von IIoT („Industrial Internet of Things“) und IoRT in bestimmten Bereichen der Bahninfrastruktur auf. Dabei wird auf die unterschiedlichen Aufgaben in Abhängigkeit der Betriebs- bzw. Sicherheitsrelevanz und den sich daraus ergebenden Anforderungen daran sowie Schluss-

folgerungen zur IT-Sicherheit eingegangen. Hierzu wird zunächst die allgemeine Struktur für um IoRT-bezogene Dienste erweiterte Systeme in einem Referenzmodell definiert. Im Anschluss daran werden zwei konkrete repräsentative Anwendungsbereiche, für die bestehende Systemarchitekturen um Komponenten für den Einsatz von IoRT ergänzt worden sind, sogenannte use cases, tiefergehend hinsichtlich der Implikationen für die IT-Sicherheit untersucht. Die hierbei ermittelten Sicherheitsanforderungen werden daraufhin von der Systemarchitektur abstrahiert und zu allgemeinen Sicherheitsanforderungen zusammengefasst.

3 Allgemeine Struktur IoT/IoRT

3.1 Referenzmodell für IoT

In einem IoT-System werden Daten verschiedenster Objekte, denen jeweils eine eineindeutige Identität zugeschrieben ist, generiert und auf unterschiedliche, geschäftsrelevante Weise durch entsprechende Applikationen bzw. Algorithmen verarbeitet. Der Ort sowohl der datengenerierenden Objekte wie auch der datenverarbeitenden Einheiten ist keinen modellbedingten Restriktionen unterworfen und kann in Abhängigkeit von anderweitigen Anforderungen gewählt werden, so kann z.B. die Datenverarbeitung bei Echtzeiterfordernissen direkt am Ort der Datengenerierung erfolgen. Die Datenströme sind mithin multidirektional. Das, im IoT Worldforum, vorgeschlagene IoT-Referenzmodell trägt diesem Sachverhalt Rechnung (siehe Abbildung 1); es umfasst sieben Schichten, denen verschiedene Funktionen zugeordnet werden, die zusammen genommen ein komplettes IoT-System darstellen.

Die **erste Schicht** wird aus den physikalischen Geräten und Controllern, die mehrere Geräte kontrollieren, gebildet – dies sind die eigentlichen Things. Die IoT-„Dinge“ dieser ersten Schicht erfüllen dabei folgende Funktionen: sie generieren Daten, sie wandeln von analog zu digital und sie können über ein Netzwerk abgefragt bzw. kontrolliert werden. Die „Dinge“ dieser ersten Schicht werden vermöge der nachfolgenden Schichten in sehr umfassende Kommunikationsnetzwerke eingebunden. Häufig sind sie ursprünglich jedoch nicht für derartig umfassende Kommunikationsbeziehungen konzipiert worden. Hieraus resultieren insbesondere Herausforderungen bezüglich eines effizienten und skalierbaren Asset- und Lifecycle-Managements auf der einen sowie sicherheitstechnische Herausforderungen auf der anderen Seite. Letztere sind der eigentliche Gegenstand dieses Whitepapers und werden mithin an späterer Stelle aufgegriffen und detaillierter beschrieben.

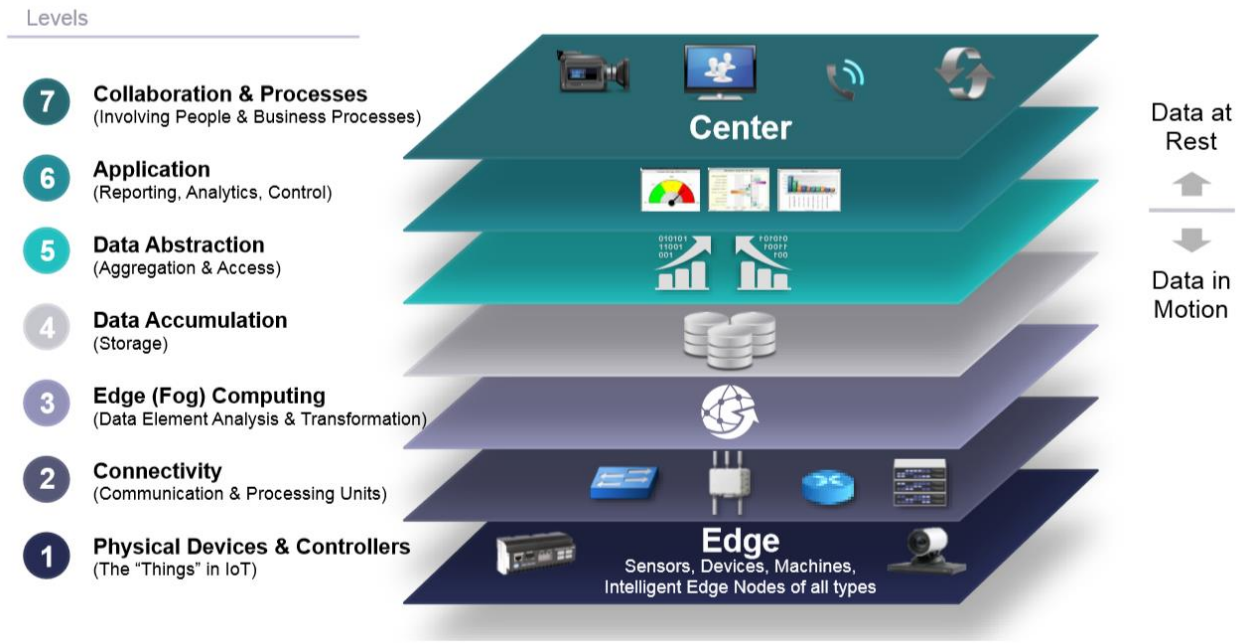

Abbildung 1: IoRT Referenzmodell [5]

Die **zweite Schicht** stellt die Kommunikations- und Verbindungsschicht dar. Sie verbindet die erste Schicht mit dem Netzwerk, ermöglicht den Datentransport über das Netzwerk (east-west-traffic) und sie verbindet das Netzwerk mit der dritten Schicht. Es ist ein Bestreben des IoT-Referenzmodells, bestehende Netzwerke zu nutzen. Da nicht davon ausgegangen werden kann, dass solche bestehenden Netze das Internet-Protokoll (IP) nutzen, werden Gateways eingeführt, mittels derer die IP-fähigkeit des IoT-Systems hergestellt wird, so dass alle Merkmale moderner IP-Netzwerke, die von Routing und Switching über Netzwerk-Analytics bis zu Netzwerk-Security reichen, für IoT-Systeme nutzbar gemacht werden können.

Die **dritte Schicht** bildet die sogenannte *Edge&Fog-Computing* Funktionalität ab. Hiermit wird dem Bestreben Rechnung getragen, Daten in intelligent designten IoT-System so früh wie möglich bzw. an der Stelle zu verarbeiten, an der es aus technischen, geschäftlichen oder regulatorischen Gründen – bspw. zur Bandbreitenreduzierung, um Echtzeiterfordernisse zu erfüllen oder um Intellectual Properties zu schützen - am sinnvollsten ist: nämlich entweder bereits an der Edge, also der Stelle der Datenerzeugung, oder im sogenannten Fog-Bereich, also dem Kontinuum zwischen der Edge und den zentralen Einheiten wie bspw. Rechenzentrum oder in der Cloud. Die Datenverarbeitung im Edge&Fog-Bereich umfasst dabei u.a. folgende Aspekte: die Evaluierung, ob Daten verworfen, in einem data historian persistiert oder an – ggf. verschiedene - höhere Schichten weiter geleitet werden, die Re-Formatierung für eine konsistente Weiterverarbeitung in höheren Schichten, die etwaige Dekodierung verschlüsselter Daten, die etwaige Reduzierung oder Zusammenfassung von Daten, die Untersuchung von Datenpaketen auf sicherheitsrelevante Aspekte hin – Stichwort: Deep Packet Inspection - sowie die Analyse von Daten, wobei letztere von einfachen Schwellwertbetrachtungen bis zur komplexen Analyse unter Zuhilfenahme künstlicher neuronaler Netzwerke – Stichwort: Digital Twin – reichen kann. Das Ergebnis der Datenverarbeitung sind Events oder Alarme und Insights bzw. Informationen. Bei der Datenverarbeitung der dritten Schicht handelt es sich um eine sogenannte In-Transit-Datenverarbeitung; im Gegensatz zur Datenverarbeitung in höheren Schichten werden hier mithin Datenströme, also sich in Bewegung befindliche Daten, untersucht.

Nicht alle Applikationen, die zur Datenverarbeitung zum Einsatz gelangen sollen, können Datenströme, also sich in Bewegung befindliche Daten, verarbeiten, sondern sie benötigen ruhende Daten. Dem wird mit der vierten Schicht, der Datenakkumulationsschicht Rechnung getragen, mittels derer eine eventbasierte Datenerzeugung mit einer abfragebasierten Datenverarbeitung gekoppelt wird. So kann die Brücke von einer Echtzeit-Netzwerk-Welt zu einer Nicht-Echtzeit-Applikationswelt geschlagen werden.

Die Aufgaben dieser vierten Schicht stellen sich dabei wie folgt dar:

- Auswahl der Art des Persistierens, also non-volatile für langfristige Speicherung oder in-memory für kurzfristige Nutzung.
- Auswahl des Speichersystems, also Filesystem, Big-data-System oder relationale Datenbank.
- Formatkonvertierung, also bspw. die Wandlung von Netzwerk-Datenpaketen zu Einträgen relationaler Datenbanken.
- Aggregation, Kombination und Wiederverarbeitung neuer Daten mit bereits vorhandenen Daten, die auch aus anderen, nicht notwendigerweise dem IoT-System zuzurechnenden Datenquellen stammen können.

Ein Ergebnis der **vierten Schicht** ist es, dass Daten ggf. unterschiedlich persistiert werden: so werden z.B. unstrukturierte Rohdatenströme in Big-data-Systemen – Stichwort: Data-lake – gespeichert, wohingegen strukturierte Daten, die bspw. Events repräsentieren, in sogenannten Data-Warehouses abgelegt werden. Daneben gibt es weitere Gründe dafür, nicht alle Daten am selben Orte bzw. im selben System abzuspeichern: sei es, dass die Menge zu groß wird, dass die Daten aus unterschiedlichen Quellen, wie bspw. einem ERP-, HRMS- oder CRM-System, stammen oder einfach, dass die Daten an geographisch weit entfernten Orten generiert werden.

Diese Heterogenität der Datenspeicherung zu vereinheitlichen, ist die Aufgabe der **fünften Schicht**: die sogenannte Daten-Abstraktionsschicht ermöglicht dann die Entwicklung einfacher, performanter Applikationen – mithin die Skalierbarkeit des gesamten IoT-Systems. Die Hauptfunktionen dieser Abstraktionsschicht bestehen darin, verschiedene Datenformate abzustimmen, für eine konsistente Semantik zu sorgen, die Vollständigkeit der Daten im Hinblick auf die höhergelagerten Applikationen sicherzustellen, die Daten zu normalisieren bzw. de-normalisieren und mit Indizes zu versehen, die Daten durch angemessene Authentifizierung und Autorisation zu schützen und die Daten mittels ETL, ELT oder Data Virtualization zugänglich zu machen.

Die **sechste Schicht** ist die Applikationsschicht, in der die durch die fünfte Schicht zur Verfügung gestellten ruhenden Daten verarbeitet und interpretiert werden – entweder direkt oder über die Integration zu einem „Application Abstraction Layer“, wie bspw. einem ESB oder einem Message Broker. Die Art der Applikation variiert dabei in Abhängigkeit von der Branche, den Geschäftsanforderungen oder der Natur der datengenerierenden Dinge: Überwachungs-, Steuerungs-, Business-Intelligence- oder Analytics-Systeme

sind typische Beispiele für Applikationen dieser Schicht, wobei die Entwicklung und der geschützte, SLA-konforme Betrieb dieser Applikationen außerhalb des IoT-Referenzmodelles liegen und durch entsprechende Lösungen aus dem Rechenzentrumskontext adressiert werden. Im Hinblick auf die zugrundeliegende Architektur können grundlegend monolithische Architekturen und Cloud-Architekturen unterschieden werden, wobei letztere eine gewisse Dynamik in dem Sinne mit sich bringen, dass die Funktionen der Applikationen durch Micro-Services abgebildet werden, die in Containern zu unterschiedlichen Zeiten an unterschiedlichen Orten – z.B. in unterschiedlichen Public Clouds – residieren können. Eine entsprechende, intelligente Steuerung der Datenströme kann und muss dabei bereits an der Evaluierungsfunktion der dritten Schicht, dem Edge&Fog-Computing, ansetzen.

Die **siebte und letzte Schicht** des IoT-Referenzmodells ist die Kollaborations- und Prozess-Schicht. Hier wird dem grundlegenden Bestreben von IoT-Systemen Rechnung getragen, dass es letztendlich darum geht, Aktionen zu initiieren, die einen Geschäftsnutzen generieren, die eine regulatorische Anforderung adressieren oder die die Sicherheit von Menschen und Systemen, von tangiblen und intangiblen Ressourcen oder vor Angriffen jedweder Art erhöhen. Manche Aktionen können direkt durch die Systeme der dritten oder sechsten Schicht initiiert werden, andere Aktionen bedürfen der Integration mit übergelagerten Prozessen bzw. der Kollaboration mit Menschen, wobei die Gründe hierfür unterschiedlicher Natur sein können: sei es, weil die generierten Insights per se für eine Weiterverarbeitung in übergelagerten Prozessen bestimmt sind oder weil sie durch künstliche neuronale Netze durch Korrelation generiert worden sind und deshalb bspw. in regulierten, audit-fähigen Kontexten nicht ohne die vorherige Zuordnung von Kausalzusammenhängen durch sogenannte Explainer, also menschliche Experten, die aufgrund ihrer Fachkenntnis eben diese Logikzusammenhänge finden können, verwendet werden dürfen. Die Kernfunktion der siebten Schicht ist mithin, eben diese Kollaboration zwischen Menschen und technischen Systemen sowie die entsprechende Prozessintegration zu ermöglichen.

3.2 Besonderheiten im System Bahn

Der Hauptaspekt des vorliegenden Whitepapers ist das Thema IT Security und damit verbunden die Themen Governance, Eigentumsrechte an Daten sowie Identity & Access Management (IAM). Das Referenzmodell des Worldforums schafft einen Referenzrahmen, der sieben Funktionsschichten beschreibt, jedoch werden darin nicht direkt die Anforderungen erfüllt oder in einer Architektur definiert. Eine Architektur muss eine in-praxi Instanziierung des IoT-Referenzmodells sein, die mindestens die sieben Funktionsschichten adressieren und die den Datenverkehr nicht nur logisch (von Funktionsschicht 1 nach Funktionsschicht 7), sondern de-facto abbilden muss.

Ein IoT-System im Bahnkontext – also ein Internet of Railway Things (IoRT) – ist zunächst eine Untermenge des Internet of Things für bahnrelevante Objekte. Gerade im Hinblick auf die kritische Infrastruktur und die Safety-relevanten Umgebungen, die im Bahnkontext gegeben sind, kommt den Security-Funktionen in einer Architektur als in-praxi Instanziierung eines IoRT-Modells besonderes Augenmerk zu. Die sich hieraus ergebenden Besonderheiten werden nachfolgend detaillierter beschrieben.

1. Viele Objekte und Technologien, die durch ein IoRT-System umfasst sind, müssen die im Bahnkontext erforderlichen Zertifizierungen durch das EBA und/ oder weiterer Behörden aufweisen oder geeignet sein, um solche bahnbetrieblichen Prozesse und Zertifizierungen zu unterstützen.

2. Eine weitere Besonderheit – im Unterschied zu anderen OT-Umgebungen – ist, dass Sicherheitsbelange sich nicht lediglich auf die Aufrechterhaltung des Betriebes und den Schutz von Ressourcen und Eigentumsrechten vor externen Einflüssen (z.B. Cyberangriffe) beziehen (Englisch: Security), sondern auch auf die Vermeidung von negativen Auswirkungen von den Systemen auf die Umgebungen (z.B. die Unversehrtheit von Menschen) (Englisch: Safety).

   Den Anforderungen an die funktionale Sicherheit („Safety“) wird mit den Normen EN 50126 ff., u.a. gemäß IEC 61508, IEC 61511 durch die Einführung sogenannter Sicherheitsstufen, -level

oder Sicherheits-Integritätslevel (SIL) Rechnung getragen.

Den Anforderungen der Cybersecurity wird u.a. gemäß IEC 62443 Serie bzw. der TS 50701 durch die Einführung sogenannter Security Levels (SL) Rechnung getragen.

In Abhängigkeit von der Sicherheitsstufe muss eine Risikobewertung mithin unterschiedlich ausfallen, was zur Folge hat, dass auch die Ausgestaltung eines IoRT-Systems unterschiedlich ausfallen muss: Ein IoRT-System ohne bzw. mit niedriger Sicherheitsstufe muss disjunkt und separiert von etwaigen Systemen höherer Sicherheitsstufen konzipiert werden und kann ausschließlich auf der 7. Funktionsebene des IoRT-Referenzmodells zu rein informativen Zwecken verwendet werden. Die Nutzung gemeinsamer Infrastrukturen erfordert den Nachweis von Rückwirkungsfreiheit und die entsprechenden Zertifizierungen. Eine echte Integration auf der 3., 4., 5., 6. oder 7. Funktionsebene, also bspw. der Aufbau eines Digital Twins, der autonom in den Bahnbetrieb eingreifen kann, bringt im Zweifelsfall die Einordnung des kompletten IoRT-Systems in die höhere Sicherheitsstufe mit allen erforderlichen Nachweisen und Zertifizierungen mit sich – hierauf wird bei der Beschreibung der Use Cases noch vertieft eingegangen.

3. Eine wesentliche Aufgabe der IT/ OT-Security im Bahnumfeld ist der Schutz der Safety-relevanten Systeme vor externen Einflüssen (z.B. Cyberangriffen). Dies kann gewährleistet werden, wenn Security und Safety angemessen getrennt bzw. gekapselt sind (z.B. architektonisch) und die Security regelmäßig gemäß der Bedrohungslage angepasst werden kann (systematisches Einspielen von Patches oder Updates bzw. Möglichkeiten zur Erkennung von Störungen oder Cyberangriffen). Security und Safety müssen dabei getrennt voneinander nachweisbar und aktualisierbar sein. Um die bestehende Safety-Welt wird eine standardisierte Security-Schale gelegt, die die genannten Anforderungen erfüllen kann.

Aber vor allem müssen die verschiedenen Security-Maßnahmen, die sich über alle sieben Funktionsschichten erstrecken können, in einer Architektur konkretisiert werden. Durch das Fehlen einer entsprechenden Security-Funktionsschicht im Referenzmodell ergibt sich die Möglichkeit, dies entsprechend den regulatorischen Anforderungen und den diesbezüglichen Unternehmensanforderungen vorzunehmen. Falls möglich, können so moderne Konzepte der Security-Branche aufgegriffen werden – bspw. das Konzept der Deperimetriesierung. Hier geht man davon aus, dass keine Umgebung vollständig abgeschottet werden kann – sprich: die Identity wird zum Perimeter, durch IAM wird festgelegt, was eine Identity darf und durch – häufig nicht-deterministische - Analytics wie Anomalie Detection wird überprüft, ob diese Festlegungen eingehalten werden. Insbesondere in Organisationen mit kritischen Infrastrukturen (KRITIS) ist eine solche Herangehensweise unter Umständen nicht möglich: hier sind bspw. Umgebungen mit Safety-relevanten Anwendungen in einen Perimeter zu fassen und durch deterministische, auditierbare Maßnahmen abzusichern [6] [7].

Erschwerend für die Erfüllung der hier aufgeführten Anforderungen bzw. Umgang mit den Besonderheiten ist die Tatsache, dass sich die eingesetzten Devices in großer Anzahl im gesamten Bundesgebiet, ohne physischen Zutrittsschutz befinden. Des Weiteren werden die Devices sowohl in Fahrzeugen als auch auf der Infrastruktur eingesetzt. Gerade im Bereich der Fahrzeuge stehen hierbei über 400 Eisenbahnverkehrsunternehmen (EVU), mit dem Transitverkehr über 1000 EVU zu Buche. Mit diesen muss der Informationsaustausch zum Heben der Nutzen möglich sein. Gleichzeitig erschwert dies die Erfüllung der Anforderungen.

3.3 Bedrohungsszenarien

Eine umfassende Bedrohungsanalyse für das Gesamtsystem muss unabhängig erfolgen und bedarf der Berücksichtigung des Gesamtsystems.

Speziell für die IoRT devices können jedoch besonders relevante Bedrohungen ausgemacht werden, welche durch entsprechende Ausnutzung durch einen Angreifer zu einer Gefährdung und mit einer Gelegenheit zum Risiko werden. Folgend soll auf die top zehn Bedrohungen für Industrial Control System Security (ICS) vom BSI [8] eingegangen werden, die Angreifertypen werden nicht näher erläutert, die möglichen Risiken sind in den folgenden Kapiteln beispielhaft ausgeführt.

1. Einschleusen von Schadsoftware über Wechseldatenträger und externe Hardware
2. Infektion mit Schadsoftware über Internet und Intranet
3. Menschliches Fehlverhalten und Sabotage
4. Kompromittierung von Extranet und Cloud-Komponenten
5. Social Engineering und Phishing
6. (D)DoS Angriffe
7. Internet-verbundene Steuerungskomponenten
8. Einbruch über Fernwartungszugänge
9. Technisches Fehlverhalten und höhere Gewalt
10. Kompromittierung von Smartphones im Produktionsumfeld

4 Anwendungen Standard IoT im Bahnkontext

4.1 Einleitung

Es gibt eine Vielzahl möglicher Anwendungsgebiete von IoT im Bahnkontext. Diese folgen in vielen Fällen den Standardanforderungen von Industrial IoT (IIoT) und können daher auch mit den gleichen Lösungsansätzen aus Sicht IT-Sicherheit behandelt werden. Dazu sind nachfolgend drei Beispiele dargestellt.

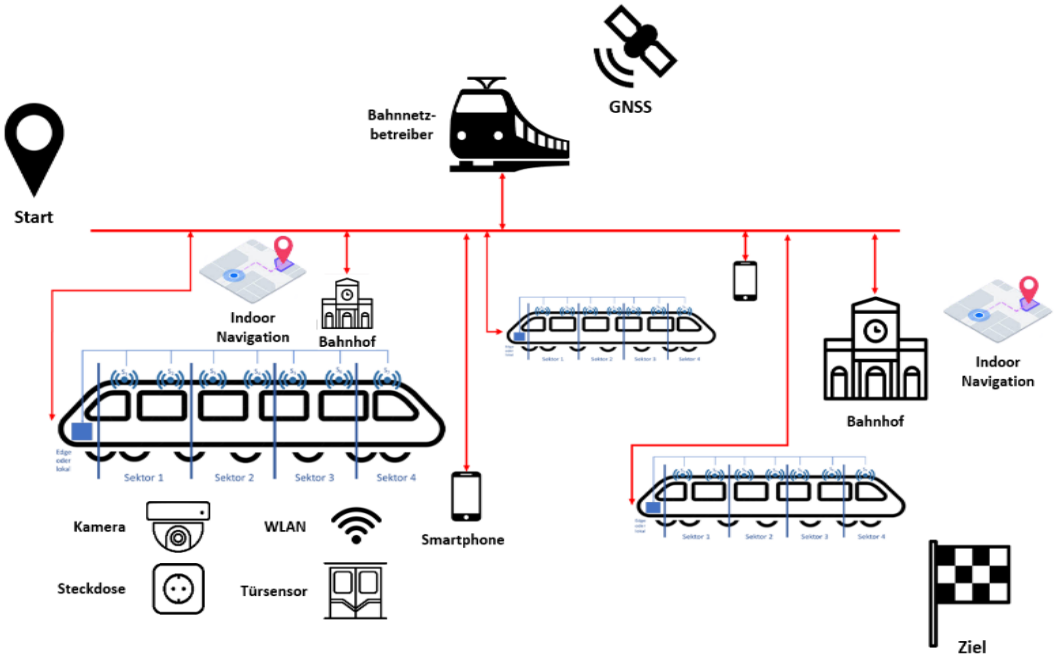

Abbildung 2: Übersicht der benutzten Standard IoT Komponenten im Bahnkontext

4.1.1 Anwendungsfall 1: Optimierung der Passagierverteilung

Bahnpassagiere sind häufig nicht ideal im Zug verteilt, sondern halten sich in Ballungsräumen auf. Dies liegt zum einen an der Lage der Bahnhofsein- und -ausgänge sowie an teils zusätzlich angehängten Waggons. Dadurch entstehen gerade in Stoßzeiten Verzögerungen beim Ein- und Aussteigen, die bei einer besseren Passagierverteilung verhindert werden könnten. Die Vernetzung von Sensoren innerhalb des Zuges erlaubt die Live-Analyse der Passagierverteilung und deren Optimierung. Dazu wird jeder Waggon in Sektoren unterteilt, die durch Kamerasysteme oder Lichtschranken begrenzt sind. Jeder Sektor stellt selbständig über die Sensorik das Passagieraufkommen fest und meldet dies einer zentralen Steuereinheit. Letztere ist im Zug verbaut oder stellt die Edge-Computing-Einheit dar. Die Sektorgröße sowie deren Raumaufteilung legen die ideale Passagierauslastung a-priori fest. Die zentrale Steuereinheit optimiert die Sektorenauslastung live und lenkt Passagierströme durch die im Zug befindlichen Bildschirme oder auf den Bahnsteigen angebrachten Anzeigen in nicht ausgelastete Sektoren. Dadurch wird die frühzeitige bestmögliche Positionierung der Passagiere am Bahnsteigrand ermöglicht, wodurch die Ein- und Aussteigezeiten verkürzt werden. Alternativ zu den genannten Datenquellen ist die Auswertung des zugeigenen WLANs oder auch die Steckdosennutzung denkbar, um die Passagierverteilung abschätzen zu können. Der entscheidende Nachteil hierbei ist die fehlende Verlässlichkeit, da nicht jeder Passagier das WLAN nutzt und auch nicht mit einer Steckdose verbunden ist. Daraus abgeleitete Schätzwerte für die Passagierverteilung sind folglich nicht zu priorisieren.

IT-Sicherheits-Aspekte:

- Kameras: Datenschutz (Privatheit), Personendaten (Vertraulichkeit), Anbringung eines Bildes / eines eigenen Videobildes aus ähnlicher Perspektive
- Auswertungssystem/ Klassifikator: Täuschung der Gesichts-, Körper-Erkennung, Einspeisen eines manipulierten Videostroms

- WLAN: MAC-Adresse, Fingerprint, Manipulation: alle verbinden sich mit dem stärksten Signal (Man-in-the-middle)
- Lichtschranke: Schutz vor Manipulation/ Missbrauch (Unterbrechung der Schranke durch Fahrgäste, obwohl keine Person eingestiegen ist, um mehr Platz zu haben)

4.1.2 Anwendungsfall 2: Gewaltprävention durch automatisierte Kameraauswertung

Bewegungsverläufe und Gesichtszüge lassen Rückschlüsse auf die emotionale und geistige Verfassung einer Person zu. Vandalismus erzeugt jährliche hohe Kosten. Die Sicherheit der Passagiere ist eng verknüpft mit der Bereitschaft, die Fahrdienste der Deutschen Bahn zu nutzen, weswegen durch Sicherheitsdienste bereits seit geraumer Zeit ein Mindestniveau an Sicherheit garantiert werden soll. Problematisch dabei ist die Lokalisierung von Gefahrensituationen innerhalb des Zuges. Das Sicherheitspersonal befindet sich meist am Zugende oder geht auf Kontrollgängen den Zug ab. Die Vernetzung der Kamerasensorik erlaubt die frühzeitige Erkennung von Handgemengen oder Belästigungen durch die Auswertung von Gesten und Bewegungsprofilen. Dazu werden die Daten mithilfe künstlicher Intelligenz im Zug oder „on-the-edge" verarbeitet und anschließend an das DB-Backend versandt. Dieses informiert den Sicherheitsdienst innerhalb des Zuges oder auch an Bahnhöfen live über Gefahrensituationen.

IT-Sicherheits-Aspekte:

- Kameras: Datenschutz (Privatheit), Personendaten (Vertraulichkeit), Anbringung eines Bildes / eines eigenen Videobildes aus ähnlicher Perspektive
- Auswertungssystem/Klassifikator: Täuschung der Gesichts-, Körper-Erkennung, Einspeisen eines manipulierten Videostroms, Architektur: zentral/dezentral (14*10 Kameras), Adaptive Auswerterate (Trendentwicklung: Auswertung mit höherer Bildrate, wenn sich ein Trend abzeichnet)
- Verbindung zwischen Kameras und Auswertesystem: Zugriff auf, Manipulation des Videostroms

4.1.3 Anwendungsfall 3: Optimierung des Reiseerlebnisses durch Erstellung eines Reiseprofils

Das Reiseerlebnis kann durch die Nutzung einer Smartphone-App verbessert werden, die den Nutzer von seinem Startpunkt bis zum Reiseziel begleitet und ihm Vorschläge für Laufrouten sowie die Nutzung von allen verfügbaren Verkehrsmitteln unterbreitet.

Dabei werden dem Nutzer individuelle Echtzeit-basierte Empfehlungen für den Reiseablauf, die Reiseplanung und eine vom unmittelbaren Umfeld abhängige Wegweisung (beispielsweise durch Pfeile in einer Augmented Reality Darstellung auf dem Smartphone) mitgeteilt. Diese Empfehlungen basieren auf

- der aktuellen Verkehrslage (Verspätungen, Ausfälle, Auslastung),
- dem bisherigen personalisierten Reiseverhalten des Nutzers
- sowie feingranularer Indoor- und Outdoor Navigation.

Darüber hinaus erhält der Nutzer auch Hinweise an welcher ÖPNV-Haltestelle er aussteigen muss. Ein weiterer Vorteil für den Nutzer ergibt sich aus der Ankunftszeitabschätzung und der Wegbeschreibung für verschiedene alternative Reisewege und Beförderungsmittel während der Reise. So kann ein Nutzer, der sich bereits im Zug befindet, prüfen ob für ihn beispielsweise die Route

- Bahnsteig -> Ausgang Bahnhof -> ÖPNV -> Ausstieg/Haltestelle -> Fußweg -> Hotel oder die Route
- Bahnsteig -> Ausgang Bahnhof -> Taxistand -> Hotel

besser ist. Insbesondere kann auf diese Weise eine Fahrpreisoptimierung und die Abwägung von Reisedauer und Fahrpreis sowie weiterer Kriterien wie der Mitnahme eines Fahrrads, sperriger Gepäckstücke, behindertengerechter Zugänge etc. durchgeführt werden.

Der App-Anbieter/Reisedienstleister kann mit Hilfe von Reiseprofilen Aussagen für eine feingranulare Bedarfsplanung hinsichtlich der Fahrzeuge, ihrer Kapazität, der Anzahl der Züge, dem Ausbau von neuen Strecken bis hin zur Größe von Bahnhöfen und Maßnahmen für Personen mit eingeschränkter Mobilität treffen.

Hierbei kann die aktuelle und prognostizierte Auslastung der Infrastruktur (Bahnsteige, Züge, Busse, Straßenbahnen) in hoher zeitlicher Auflösung mit Hilfe der Bildanalyse von Kameras, die in den Zügen, an den Bahnsteigen und im Bahnhof angebracht sind, ermittelt werden. Diese Informationen können für die Planung von Baustellen und Umbauarbeiten an Bahnhöfen herangezogen werden. Auch können Reisendenströme bei kurzfristigen Störungen, wie etwa dem Ausfall einer Rolltreppe, auf alternative Routen, wie etwa über die B-Ebene, gelenkt werden. Schließlich kann mit Hilfe der Profile eine entsprechende Fahrpreisoptimierung durchgeführt werden.

IT-Sicherheits-Aspekte:

- Profil-Informationen: App-, Personendaten (Vertraulichkeit), Bewegungsdaten
- Smartphone: Manipulation von Sensordaten, Identitätsdiebstahl
- Manipulation: Verfälschen, Zurückhalten von Belegungsdaten durch Verkehrsunternehmen, um mehr Kunden zu akquirieren
- Kameras: Datenschutz (Privatheit), Personendaten (Vertraulichkeit),
- Auswertungssystem/ Klassifikator: Täuschung der Gesichts-, Körper-Erkennung, Einspeisen eines manipulierten Videostroms,

4.2 Lösung

Die vorgestellten Anwendungsfälle stellen Anforderungen an unterschiedliche Bereiche der IT-Sicherheit, wie den Datenschutz und die Datenintegrität. Insbesondere der Datenschutz ist wichtig, sobald kamerabasierte, intelligente Systeme, wie im zweiten Anwendungsfall beschrieben, eingesetzt oder personenbezogene Daten, wie Bewegungsprofile, wie im dritten Anwendungsfall beschrieben, gespeichert werden.

Insgesamt zeigen diese skizzierten Anwendungsfälle jedoch, dass sie trotz ihres eindeutigen Bezuges zum Bahnbetrieb kaum besondere Anforderungen aus Sicht der IT-Sicherheit besitzen. Anwendungsfälle, die aufgrund ihres Bahnbezugs besondere Maßnahmen erfordern, werden im nächsten Abschnitt analysiert. Nichtsdestotrotz müssen auch in diesen Anwendungsfällen die herkömmlichen Sicherheitsmaßnahmen angewendet werden, wie sie im „normalen“ IoT gängig sind.

Dazu zählt die Verschlüsselung und Authentifizierung jeglicher Netzwerk-Kommunikation, ob zwischen Cloud-Server und Smartphone des Kunden, oder zwischen Sensoren (z.B. Kameras) und Auswertungseinheiten, wie bei der Passagierverteilung oder dem Beispiel der Gewaltprävention. Veränderungen der Konfigurationsdaten des Systems und all seiner Komponenten müssen autorisiert werden, um Manipulation durch Dritte zu verhindern. Hierzu dienen Maßnahmen, wie Passwörter oder sogar Zwei-Faktor-Authentifizierung, aber auch das physische Blockieren von Schnittstellen, wie USB-Ports.

Weiterhin ist es wichtig, die IoRT-Geräte auf Schadsoftware hin zu überprüfen, um diese rechtzeitig erkennen und beseitigen zu können, da das Einschleusen von Schadsoftware zurzeit eine der häufigsten Bedrohungen für digitale Systeme darstellt. Die Beseitigung entdeckter Schwachstellen muss remote durch das Einspielen von Patches/Updates möglich sein. Manuelle Prozeduren, wie bei größeren technischen Systemen teilweise noch üblich, können bei der Menge an IoT-Elementen keine Lösung mehr sein. Diese Updates sind nicht nur notwendig, um die IoT devices selbst zu schützen, sondern auch den Missbrauch für Bot-Netzwerke für DDoS Angriffe zu unterbinden.

Eine Besonderheit, die wir mit den Anwendungsfällen hervorheben möchten, ist die sichere Verarbeitung von personenbezogenen Daten, für die die Vorgaben der EU-Datenschutzgrundverordnung (EU-DSGVO) verbindlich einzuhalten sind und die Umsetzung nachzuweisen ist. Hierzu gehören Maßnahmen wie Beschreibung der Zweckbindung der Verarbeitung, Datensparsamkeit, geeignete Löschfristen sowie die Umsetzung von „geeigneten technischen und organisatorischen Maßnahmen“. Unter technischen Maßnahmen sind alle Schutzversuche zu verstehen, die im weitesten Sinne physisch umsetzbar sind oder die in

Soft- und Hardware umgesetzt werden, unter organisatorischen Maßnahmen solche Schutzversuche, die durch Handlungsanweisung, Verfahrens- und Vorgehensweisen umgesetzt werden. Hierzu können beispielsweise das physikalische Löschen von Daten, die kryptographische Verschlüsselung oder interne IT- und Datenschutz-Regelungen gehören.

Um die Bedrohungen auf die beschriebenen Anwendungsfälle in den Kontext zu setzen und ihre Relevanz zu zeigen, ziehen wir die vom BSI veröffentlichten Top 10 ICS-Bedrohungen und Gegenmaßnahmen heran. In der folgenden Tabelle 1 ordnen wir zu, welche Bedrohungen auf welche Anwendungsfälle aktuell – Stand 2020 - zutreffen. Das Dokument des BSI beschreibt auch Gegenmaßnahmen, die für unsere Anwendungsfälle implementiert werden können, um den Bedrohungen zu entgegnen.

		Passagier-verteilung	Gewaltprä-vention	Reise-profil
1	Einschleusen von Schadsoftware über Wechseldatenträger und externe Hardware	ja	ja	ja
2	Infektion mit Schadsoftware über Internet und Intranet	ja	ja	ja
3	Menschliches Fehlverhalten und Sabotage	ja	ja	ja
4	Kompromittierung von Extranet und Cloud-Komponenten	ja	ja	ja
5	Social Engineering und Phishing	(nein)	(nein)	ja
6	(D)DoS Angriffe	ja	ja	ja
7	Internet-verbundene Steuerungskomponenten	nein	nein	ja
8	Einbruch über Fernwartungszugänge	ja	ja	ja
9	Technisches Fehlverhalten und höhere Gewalt	(ja)	(ja)	(ja)
10	Kompromittierung von Smartphones im Produktionsumfeld	nein	nein	ja

Tabelle 1: Relevanz ICS-Bedrohungen BSI je Anwendungsgebiet

Um zu bestimmen, inwieweit eine Bedrohung auf den Anwendungsfall zutrifft, verwenden wir folgende, allgemein gehaltene, Definitionen für die im beschriebenen Anwendungsfall bereit gestellten Dienste:

- Passagierverteilung: Die Auslastung des Zuges wird korrekt am Bahnsteig angezeigt.
- Gewaltprävention: Eine Gefahrensituation im Zug zwischen Fahrgästen wird korrekt erkannt.
- Reiseprofil: Empfehlungen für Laufrouten und Verkehrsmittel werden korrekt vorgeschlagen.

Im Folgenden werden die Bedrohungen aus der Top-Ten-Liste [8] für die oben beschriebenen Anwendungsfälle konkretisiert.

1. *Einschleusen von Schadsoftware über Wechseldatenträger und externe Hardware*: Insbesondere bei den Geräten, die die Sensordaten zu einem Ergebnis verarbeiten, kann durch angeschlossene Wechseldatenträger Schadsoftware eingeschleust werden. Bei der Passagierverteilung und der Gewaltprävention ist davon auszugehen, dass eine solche Auswerteeinheit auf dem Zug installiert ist und durch Schadsoftware beeinflusst werden kann. Im Falle vom Reiseprofil kann der Betreiber kaum Einfluss auf mögliche Schadsoftware auf dem Endgerät des Nutzers (Smartphone) nehmen. In seinem Einflussbereich liegen jedoch das Sammeln und Auswerten der Rohdaten, um die Empfehlungen zu generieren. Die dafür verwendeten Geräte sind der Bedrohung durch Schadsoftware ebenfalls ausgesetzt.
2. *Infektion mit Schadsoftware über Internet und Intranet*: Um den Service im Anwendungsfall Passagierverteilung und Gewaltprävention zu erbringen ist nicht zwingend eine Anbindung des Systems an das Internet notwendig, jedoch definitiv eine Form von Netzwerk, um die Auslastung an

den nächsten Bahnhof zu kommunizieren bzw. erkannte Gefahrensituationen dem Sicherheitsdienst zu melden. Über dieses Netzwerk (Intranet) kann sich ggf. Schadsoftware verbreiten. Für den Fall Reiseprofil ist natürlicherweise das Internet notwendig, um zum Endnutzer zu gelangen, sodass die Bedrohung durch Schadsoftware auch aus dem Internet zutrifft.

3. *Menschliches Fehlverhalten und Sabotage*: Fehlverhalten und Sabotage ist selten auszuschließen. Ein Fahrgast könnte versuchen die Türsensoren zu täuschen, um fälschlicherweise eine höhere Auslastung zu provozieren. Dadurch wird im nächsten Bahnhof die Auslastung nicht korrekt dargestellt und Passagiere verteilen sich möglicherweise nicht optimal über den Bahnsteig. Endgeräte sind auf verschiedenen Ebenen durch Sabotage bedroht. Kameras bspw. können zerstört oder mit Farbe besprüht werden, um die Aufnahme zu unterbinden. Außerdem kann die Auswertung vorsätzlich getäuscht werden, indem bspw. beim Reiseprofil der Angreifer durch die Nutzung einer Vielzahl von Smartphones der Auslastungsgrad künstlich erhöht wird, um andere, schlechtere Empfehlungen zu provozieren.
4. *Kompromittierung von Extranet und Cloud-Komponenten*: Bei allen beschriebenen Anwendungsfällen sind Cloud-Komponenten involviert, die im Hintergrund Daten auswerten und weiterverarbeiten. Daher trifft diese Bedrohung auf alle Anwendungsfälle zu.
5. *Social Engineering und Phishing*: Social Engineering und Phishing sind vielschichtige Bedrohungen. Sowohl bei der Passagierverteilung als auch bei der Gewaltprävention kann man argumentieren, dass Zugangsdaten nicht ausgespäht werden können, weil keine Nutzerkonten oder Arbeitsplätze mit bspw. E-Mail-Zugang existieren. Andererseits sind Social Engineering oder Phishing Angriffe auf Wartungspersonal, das mit den Geräten befasst ist, denkbar, das beeinflusst wird, um Wartungszugänge zu offenbaren oder Konfigurationen im Sinne des Angreifers zu verändern. Für die Erstellung des Reiseprofils und die resultierenden Empfehlungen ist ein Nutzerkonto erforderlich, dessen Zugangsdaten durch Phishing E-Mails ausspioniert werden können. Außerdem ist das Backend-System möglicherweise ein lukratives Ziel für Angreifer, die Social Engineering oder Phishing durchführen, um das System zu manipulieren. Ein entsprechender Schutz durch Training des Personals und Hinweise an Kunden, organisatorische Maßnahmen und ein Meldewesen ist hier erforderlich.
6. *(D)DoS Angriffe*: In allen vorgestellten Anwendungsfällen lassen sich DoS-Angriffe ausführen, indem die drahtlose Kommunikation zwischen Zug und Streckenseite oder mit dem Endkunden durch Störsender unterbrochen wird. Solche Jamming-Angriffe lassen sich kaum verhindern, stattdessen ist der Betreiber gezwungen den Störsender zu finden, um die Beeinträchtigung zu beseitigen. DoS-Angriffe auf die Geräte selbst sind im Fall der Passagierverteilung und der Gewaltprävention durch die eingeschränkte Zugänglichkeit (kein Internet) bereits erschwert. Allgemeine Maßnahmen gegen DoS-Angriffe umfassen redundante Auslegung der Geräte und Verbindungen und/ oder entsprechende Überspezifizierung der Ressourcen.
7. *Internet-verbundene Steuerungskomponenten*: Die Bedrohung durch Internet-verbundene Steuerungskomponenten lässt sich leicht bei der Passagierverteilung und der Gewaltprävention ausschließen, indem die Komponenten nicht mit dem Internet verbunden werden, weil dies für den Anwendungsfall nicht erforderlich ist. Aufgrund der großen Ausbreitung und Vernetzung im Anwendungsfall Reiseprofil wird es sich nicht vermeiden lassen, dass hier Komponenten über das Internet erreichbar sind. Diese sollten entsprechend durch Zugriffsschutz und kontinuierliches Schließen von Sicherheitslücken abgesichert werden.
8. *Einbruch über Fernwartungszugänge*: Kameras, Sensoren, Endgeräte und Geräte auf allen Ebenen des Internet of Things verfügen heutzutage über Fernwartungszugänge, die – falls nicht korrekt geschützt – zu einem Einfallstor für Angreifer werden können. Daher sollten alle genutzten

Fernwartungszugänge mit wirksamer Authentifizierung und Autorisierung geschützt werden und ungenutzte Fernwartungszugänge deaktiviert werden.

9. *Technisches Fehlverhalten und höhere Gewalt*: Technisches Fehlverhalten und höhere Gewalt lassen sich natürlicherweise nicht ausschließen, treffen jedoch auf eine Vielzahl von Systemen zu und sind nicht Teil der Betrachtung in diesem Whitepaper, in dem es um Angriffe der IT-Sicherheit gehen soll.
10. *Kompromittierung von Smartphones im Produktionsumfeld*: Wir nehmen an, dass die Gefahr durch Smartphones im Produktionsumfeld im Falle der Passagierverteilung ausgeschlossen werden kann, da in keinem Teil des Dienstes Smartphones involviert sind. Im Fall der Gewaltprävention (Alarmierung des Sicherheitspersonals) und des Reiseprofils (Empfehlung für den Kunden) sind jedoch Smartphones in den Szenarien vorhanden. Beim Sicherheitspersonal sind dies Geräte im Eigentum des Betreibers, sodass hier umfangreiche Einflussmöglichkeiten bestehen, um gegen Schadsoftware und Kompromittierung vorzugehen. Im Falle des Endkunden, liegen diese Möglichkeiten jedoch nicht vor, sodass sich der Einflussbereich maximal auf die vom Nutzer installierte Applikation beschränkt.

5 Anwendungen IoRT mit besonderen Anforderungen

5.1 Einleitung

Die Digitalisierung der Bahninfrastruktur und Vernetzung der Leit- und Sicherungstechnik (LST) sind die Grundvoraussetzungen für den Einsatz von IoT im Bahnbetrieb oder IoRT. Die Einführung dieser neuen Technologie erfolgt dabei auf Basis von dem sogenannten Digitalen Stellwerk (DSTW) und der NeuPro Architektur.

Unter Berücksichtigung der Besonderheiten solcher IoRT sind folgend Beispielanwendungen beschrieben, die sowohl einen Nutzen, sowie auch Herausforderungen darstellen. Ein möglicher Lösungsansatz, insbesondere in der Kombination von oder unmittelbarer Nähe zu sicherheitskritischen (im Sinne von Safety) Systemen, ist der Separations-Ansatz. Dieser wird am Ende dieses Kapitels näher erläutert. Erläuterungen zu den Abhängigkeiten der Systeme, möglicher Separation und technologischer Ansätze dazu wurden bereits in früheren Dokumenten erarbeitet und veröffentlicht [9] [10].

5.2 Zukünftige Stellwerk-Technologie und NeuPro Architektur

Die NeuPro Architektur [11] definiert ein digitales Stellwerk (DSTW) und ermöglicht es, die Stellbefehle mittels Informationstechnik (IT), z.B. über ein IP Netz und standardisierte Schnittstellen, an die Feldelemente wie Weichen und Signale zu übermitteln.
Abbildung 3 stellt diese Architektur für das DSTW grob dar.

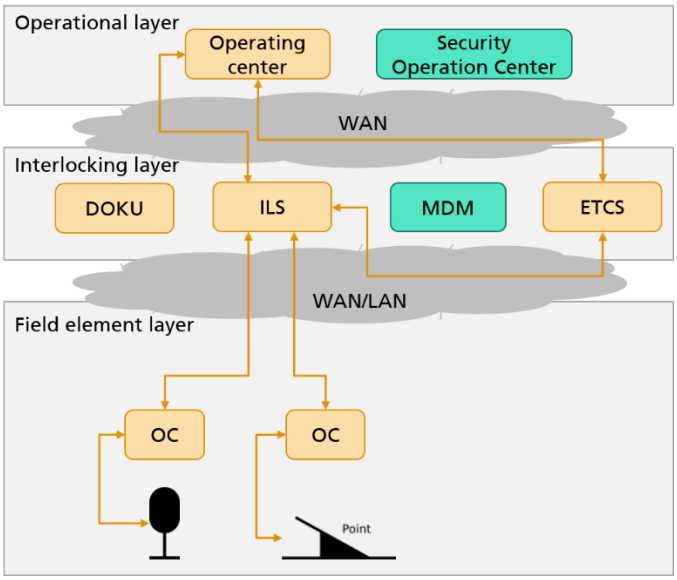

Abbildung 3: NeuPro/DSTW Architektur (basiert auf [11])

Die Architektur besteht aus den Safety-Komponenten (in Orange), die für den sicheren Bahnbetrieb (im Sinne von Safety) verantwortlich sind, sowie den Security-Komponenten (in Grün), die zusätzliche Funktionen implementieren, um die Bahninfrastruktur vor IT-Angriffen zu schützen. Die Komponenten sind in drei Ebenen – operational, Stellwerk, Feldelement - aufgeteilt.

- Auf der **operationalen Ebene** befinden sich die Betriebszentrale mit dem integrierten Bedienplatzsystem sowie die IT-Sicherheitszentrale (Security Operation Center, SOC). In der Betriebszentrale werden die Lenkung und Steuerung des Bahnbetriebes durchgeführt. Hier wird u.a. das Durchführen von Zugfahrten kontrolliert. Das SOC ist für die Bearbeitung der Infrastrukturmeldungen und die Erkennung der Security-relevanten Ereignisse verantwortlich.
- Auf der **Stellwerks-Ebene** befinden sich die wichtigsten Safety-Systeme, wie etwa das DSTW (vgl. ILS), Maintenance and Data Management System (MDM), und DOKU. Das DSTW über-

prüft die Routen von der Betriebszentrale, ermittelt erforderliche technische Abhängigkeiten und stellt die Fahrstraßen sicher, indem es die Kommandos an entsprechende Feldelemente (Start- und Endsignale) sendet. Außerdem bearbeitet das DSTW die Meldungen von Feldelementen und im Fehlerfall z.B. bei technischen Störungen, schaltet es in den sicheren Zustand (fail-safe) um. In diesem Fall wird die Fahrstraße blockiert, bis die Signalabhängigkeit wiederhergestellt werden kann. Das MDM System ist dafür verantwortlich, die Updatedateien (z.B. neue Konfigurationen) für die Feldelemente bereitzustellen. Außerdem leitet das MDM die Security-relevanten Meldungen an das SOC weiter. Das DOKU-System ist eine Art historische Datenbank, die alle Safety-relevanten Ereignisse protokolliert. Diese Logs werden bei der Analyse von Safety-Vorfällen verwendet. Die Schnittstelle zum European Train Control System (ETCS) erlaubt es die notwendigen festdefinierten Betriebsinformationen zwischen dem Fahrzeug und der Infrastruktur auszutauschen.

- Feldelement-Ebene umfasst die Objekt Controller (OC), die Elemente der Streckentechnik wie Weichen, Signale oder Bahnübergänge steuern. Ein OC ist normalerweise analog mit einem einzelnen Element verbunden und wandelt die digitalen Kommandos vom DSTW zur Sicherstellung der Fahrstraßen sowie die analoge Rückmeldung vom Element entsprechend um. In der Regel besitzt der OC keine eigene "Intelligenz".

Alle Komponenten im DSTW System sind bis zum OC über das bahnbetriebliche WAN - auf Ethernet und IP basierendes Transportnetz (LAN oder WAN) - miteinander vernetzt. Die bahnbetriebliche Kommunikation kann dabei über das RaSTA [12] Protokoll erfolgen, um eine verlässliche Zustellung von Nachrichten und die notwendige Ausfallsicherheit zu gewährleisten.

5.3 Ausgewählte Anwendungsfälle

Nachfolgend werden zwei Anwendungsfälle aus dem Bereich der Leit- und Sicherheitstechnik beschrieben und die relevanten Aspekte der IT-Sicherheit analysiert.

5.3.1 Anwendungsfall 1: IoRT für zustandsbasierte und vorausschauende Instandhaltung

Zustandsbasierte (Condition based Maintenance - CbM) und vorausschauende (Prediction based Maintenance - PbM) Instandhaltung ist ein bedarfsgerechter oder zustandsorientierter Wartungsvorgang, der auf der Auswertung der Daten bzgl. des Ist-Zustands von Bahnanlagen und Betriebsmitteln basiert.

Bei CbM werden unterschiedliche betriebsrelevante Parameter automatisch durch Sensoren erfasst. Bei PbM als Weiterentwicklung von CbM werden die vorhandenen Daten mit Hilfe spezieller Modelle und Algorithmen ausgewertet, um eine möglichst genaue Prognose stellen zu können, wann die nächste Wartung für die Komponente notwendig sein sollte. Dabei können durch so eine datenbasierte Instandhaltung verschiedene Ziele erreicht werden, wie dank Vorausplanung die Effizienz des Prozesses zu steigern, Kosten zu sparen sowie die Sicherheit des Betriebs zu erhöhen und die Ausfallzeiten zu reduzieren [13]. In diesem Whitepaper steht insbesondere die Minimierung von ungeplanten Störungen im Fokus.

Vorausschauende Instandhaltung umfasst die folgenden Schritte:

- die Überwachung des Systemzustands und der Umgebung mit Hilfe von Sensoren;
- die Erfassung, Bearbeitung und Übermittlung von Daten;
- die Speicherung und Analyse der erhobenen Daten;
- die Vorhersage von bestimmten Ereignissen (wie Ausfall oder Störung).

Trotz Einsatz von IoRT können die Instandhaltungsmaßnahmen sowie Wartung nie gänzlich entfallen, da sie normativen und behördlichen Vorschriften unterliegen. Somit ist IoRT eine unterstützende Maßnahme für Bahnanlagen, welche die fixen Instandhaltungsfristen verlängern, Störungswahrscheinlichkeit minimieren und die Verfügbarkeit erhöhen kann. Dabei bietet IoRT den größten technischen Mehrwert im Bereich der Inspektion, weil mit Hilfe von Sensoren und CbM der Ist-Zustand ohne einer manuellen vor Ort Inspektion automatisiert kontrolliert, überprüft und dokumentiert werden kann. Den größten operationellen Mehrwert liefert IoRT bei der PbM, womit die Wartung von Anlagen und Zügen so optimiert

werden kann, dass sie zum günstigsten Zeitpunkt durchgeführt wird. So sind notwendiges Material und Personal rechtzeitig vorhanden und es ergeben sich keine ungeplanten Auswirkungen auf den Regelbetrieb.

5.3.1.1 Systemarchitektur für IoRT basierte Instandhaltung

Eine mögliche Architektur des Dienstes zur vorausschauenden Instandhaltung ist in Abb. 4 in Blau dargestellt. Die von dem Dienst verwendeten IoRT-Sensoren sind in einer separaten Sensorebene in gelber Farbe dargestellt.

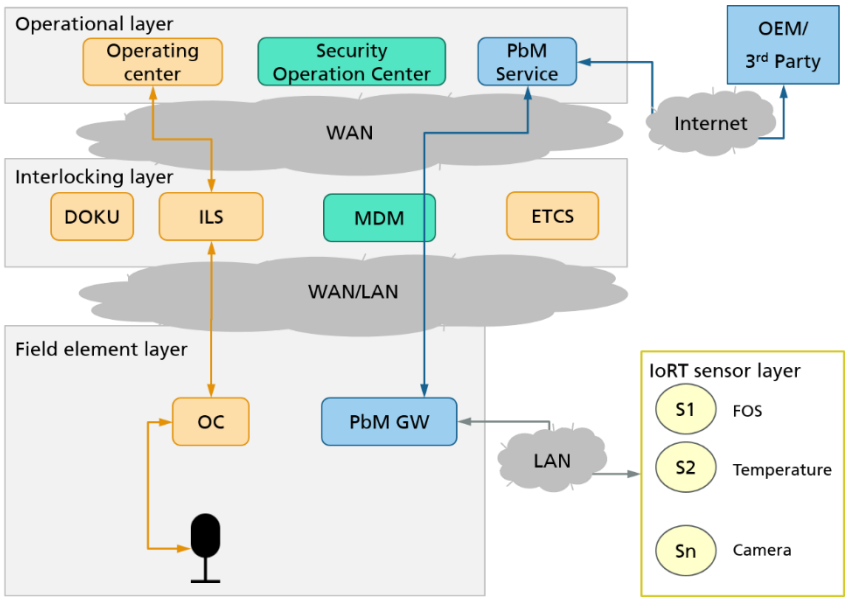

Abbildung 4: IoRT basierte Instandhaltungsdienste

Die IoRT-Sensoren dienen dabei der Überwachung des Ist-Zustands von LST-Systemen und deren Umgebung. Abhängig davon welche physikalischen Werte (z.B. Temperatur oder Luftfeuchtigkeit) oder Informationen für die Errechnung von Prognosen für eine bestimmte Komponente notwendig sind, können verschiedene marktübliche Sensortypen eingesetzt werden. Zum Beispiel erlauben die entlang der Eisenbahnstrecke installierten Faseroptischen Sensoren (FOS) den Betriebszustand von Gleisen zu überwachen und können auch als IoRT-Sensoren dienen.

Die PbM-Anwendung auf einem speziellen Io(R)T Gateway (GW) (cf. Abb. 4) erfasst die Daten von den angeschlossenen IoRT-Sensoren, ggf. werden dabei die analogen Signale in digitale umgewandelt. Die PbM-Anwendung kann die Sensordaten wie FOS-Daten zusätzlich lokal aufbereiten, z.B. indem sie einen Datensatz mit einem Zeitstempel oder auch mit zusätzlichen Informationen, wie Temperatur oder Kamerabild bildet. Um die Zustandsinformationen für die vorausschauende Instandhaltung verwenden zu können, werden die erfassten Daten und aufbereiteten Datensätze an den PbM Dienst in die Betriebszentrale durch die PbM-Anwendung weitergeleitet.

Die PbM-Anwendung kann bei Bedarf auch aktiv durch den entsprechenden Dienst in der Betriebszentrale abgefragt werden. Die PbM relevante Kommunikation mit dem PbM Dienst innerhalb der Betreiberorganisation des Infrastrukturmanagers erfolgt dann über ein geschütztes bahnbetriebliche WAN (IP-Netz).

In der Betriebszentrale werden die Informationen über den Ist-Zustand der Anlagen gesammelt und gespeichert, um die Vorhersage von Störungen und die Berichterstattung sowie den schnellen Informationsaustausch zwischen Betriebsprozessen zu ermöglichen.

Der PbM-Dienst kann zudem die erhaltenen Sensordaten mit weiteren Informationen wie dem Safety-Zustand des Feldelements oder der Safety-Anwendung (Objekt Controller) sowie den Security Meldungen aus dem SIEM (Security Information and Event Management) System des SOC- korrelieren, um eine umfassende Bewertung des aktuellen Streckenzustands ermöglichen zu können sowie die Wahrscheinlichkeit von Fehlprognosen zu reduzieren.

Der PbM Dienst bietet auch den berechtigten externen Akteuren, wie Hersteller von Geräten und Anlagen (s. OEM in Abbildung 4) den Zugang zu den rohen Sensordaten von der PbM-Anwendung oder durch den Dienst vorverarbeiteten Berichten. Dabei können Datenfilter realisiert werden, um die Zugangsberechtigungen (Data Governance) und Präferenzen bei der Weiterleitung von Informationen durchzusetzen und damit auch den Anforderungen der DSGVO Rechnung zu tragen. Dies ist insbesondere für den Austausch von Informationen mit unternehmensexternen Einheiten wichtig und gesetzlich vorgeschrieben.

Zur Kommunikation mit externen Akteuren, die sich außerhalb des bahnbetrieblichen WAN befinden, wird durch den PbM Dienst eine Internet-Schnittstelle bereitgestellt.

5.3.1.2 IT-Sicherheitsaspekte

i. Bedrohungsanalyse auf Basis von BSI ICS Top 10

Die Liste der Top 10 Bedrohungen [8] kann auf den Anwendungsfall IoRT basierte PbM Dienste/Systeme wie folgt abgebildet werden.

1. *Einschleusen von Schadsoftware über Wechseldatenträger und externe Hardware:* Die Verwendung von Wechseldatenträgern kann ohne Funktionsverlust im vorgeschlagenen PbM System verboten und die entsprechenden Schnittstellen deaktiviert werden. Der Datenaustausch und die Updates sollen dabei secure über ein entsprechend geschütztes WAN erfolgen. Im Gegensatz dazu können IoRT-Sensoren und sogar das PbM Gateway im Gleisbereich vom lokalen Angreifer durch infizierte oder manipulierte Komponenten ersetzt werden. Solche kompromittierten Komponenten können u.a. falsche Daten bzgl. des Zustands der Anlagen liefern.
2. *Infektion mit Schadsoftware über Internet und Intranet*: Als hochgradig vernetztes System kann PbM durch Schadsoftware infiziert werden. Nicht-zielgerichtete Schadsoftware (z.B. Würmer oder Bitcoin Miner) kann das PbM in ihrer Funktionalität beeinträchtigen, indem sie die Rechenleistung des Systems einschränkt oder notwendige Daten unbrauchbar macht oder löscht. Im schlimmsten Fall ist der PbM-Dienst nicht mehr erreichbar. Besonders gefährlich ist aber zielgerichtete Software, die z.B. als Teil des manipulierten Updates ausgeliefert wird und entweder einen unbefugten Zugriff auf Systeme und Daten ermöglicht oder so diese Systeme und Daten manipuliert oder mit falschen Informationen (z.B. Eingabedaten, Verfahren oder Modelle) einspeist, dass die Prognosen unbemerkt verfälscht werden.
3. *Menschliches Fehlverhalten und Sabotage*: Das PbM System kann durch Fehlkonfiguration und Fehlbedienung der Komponenten oder Netzwerke, die die Kommunikation zwischen unterschiedlichen Ebenen des Systems ermöglichen, beeinträchtigt werden. So können IoRT-Sensoren abgeschaltet oder ersetzt werden, die Konfiguration der PbM-Anwendung so angepasst werden, dass bestimmte Daten nicht mehr abfragt oder weitergeleitet oder auch mit einem falschen Zeitstempel versehen werden, sodass sie veraltet erscheinen. Dies gilt auch für den PbM-Dienst. Durch Sabotage der Internet-Schnittstelle kann, die mit Hilfe von Datenfilterregeln aufgestellte Beschränkung aufgehoben werden, so dass vollständige Datensätze bzgl. des Anlagenzustands unkontrolliert nach außen gelangen können.
4. *Kompromittierung von Extranet und Cloud-Komponenten:* Die Architektur für den PbM-Dienst trifft keine Entscheidungen über die konkrete Realisierung dieses Dienstes. Die einzige externe Schnittstelle ist die Schnittstelle zu den externen Akteuren, die über das Internet Anfragen an den PbM-Dienst in der Betriebszentrale senden können. Diese Anfragen können durch einen Angreifer manipuliert oder gelöscht werden, was negative Auswirkungen auf Dienstleistungsqualität für die externen Parteien haben wird.
5. *Social Engineering und Phishing*: Auch für das PbM-System können auf diese Weise die Zugangsdaten oder weitere IT Sicherheits-relevante Informationen offengelegt werden. Zudem kann der

Angreifer sich dadurch einen unberechtigten Zugang zum PbM-Dienst in der Betriebszentrale verschaffen.

6. *(D)DoS Angriffe*: Die korrekte Funktion des PbM-Dienstes in der Zentrale hängt von den Daten ab, die der Dienst über das WAN von den IoRT-Sensoren in der Feldelementebene erhält. (D)DoS-Angriffe auf Netzwerkanbindung wird es für den Dienst unmöglich machen, aktuelle Informationen über den Zustand der Anlagen zu sammeln. Die Verzögerung oder wahrscheinlich Verlust dieser Daten, durch überlaufende, dezentrale Speicher, kann auch negative Folgen für die Erstellung von Prognosen haben. Das PbM-Gateway mit der Anwendung sowie der PbM-Dienst (z. B. Datenbank und Server) können auch durch bestimmte Nachrichten gestört oder zum Absturz gebracht werden.
7. *Internet-verbundene Steuerungskomponenten*: Das PbM-System erlaubt keine direkte Verbindung von Steuerungskomponenten mit dem Internet.
8. *Einbruch über Fernwartungszugänge*: Das PbM-System nutzt das WAN für die Kommunikation. Es stellt eine Bedrohung dar, dass Angreifer über Fernwartungszugänge des PbM in der Lage sind, auf dieses System Zugriff zu erhalten.
9. *Technisches Fehlverhalten und höhere Gewalt*: Ausfall oder inkorrekte Funktion des PbM-Dienstes aufgrund von defekten Hardware- oder Software-Komponenten können nicht ausgeschlossen werden. Dies gilt insbesondere für die Komponenten im Gleisbereich, die wechselnden Umweltbedingungen ausgesetzt sind.
10. *Kompromittierung von Smartphones im Produktionsumfeld*: Das primäre Ziel des PbM-Systems ist die Sammlung und Verarbeitung von Informationen, nicht die Steuerung von Anlagen mit oder ohne Fernwartungszugang. Daher ist diese Bedrohung nur dann relevant, wenn die Smartphones als Sensoren eingesetzt werden, was aufgrund der hohen Kosten unwahrscheinlich ist.

ii. Risiken

Um ihre Ziele zu erfüllen und eine Verbesserung im Vergleich zum Stand der Technik zu erzielen, muss das IoRT basierte PbM-System zuverlässige Informationen liefern, die dem Zustand des beobachteten LST-Systems entsprechen.

Sollte das PbM inkorrekte Störungsprognose generieren, kann es zur Erhöhung der Instandhaltungskosten wegen zusätzlichen unnötigen Kontrollen, Anlagensperrungen oder Investitionen (z.B. in Erneuerung bzw. Instandsetzung statt Instandhaltung) führen. Wenn zur Beurteilung des Betriebszustandes des betroffenen Systems der Betrieb ungeplant eingeschränkt oder eingestellt werden muss, wird dies negative Auswirkungen auf die Pünktlichkeit und die notwendigen einzusetzenden Mittel haben.

Die finanziellen Auswirkungen hierzu können als hoch eingeschätzt werden. Die Eintrittswahrscheinlichkeit, ohne Schutz, ist „sehr wahrscheinlich“. Zusätzlich ist es wahrscheinlich, dass es durch Bekanntwerden in der Öffentlichkeit zu Reputationsschaden kommt. Dessen Auswirkungen sind langfristig und können nur schwer abgeschätzt werden.

Die oben genannten Situationen können auftreten, wenn ein System fälschlicherweise in der Prognose als „zu wartendes System“ oder „eingeschränkt funktionsfähig“ eingestuft wird. Auch der umgekehrte Fall ist möglich: Das System, das kurz vor dem Ausfall steht, kann fehlerhaft als gesund bewertet werden. Dies stellt, neben den finanziellen Schäden, zusätzlich ein Risiko für den sicheren Bahnbetrieb dar. Der potentielle Schaden für den Betreiber hängt in diesem Fall davon ab, ob die periodischen manuellen Inspektionen durch Fachpersonal sowie die standardmäßigen Wartungsvorgänge, die durch die Behörden wie Eisenbahn Bundesamt (EBA) vorgeschrieben sind, beibehalten werden oder ob sie aufgrund des hohen Vertrauens in das PbM-System und aus Kostengründen verworfen wurden. Die Probleme, die das PbM-System übersehen hat, können eventuell bei einer nächsten Inspektion noch rechtzeitig festgestellt und behoben werden, auch werden die gesetzlichen Anforderungen dabei eingehalten. Sollte auf „doppelte“ Kontrollen verzichtet werden, können solche Fehler nicht nur rechtliche Folgen haben, sondern im schlimmsten Fall auch Unfälle und sogar Beeinträchtigung der persönlichen Unversehrtheit verursachen.

Insofern wird offensichtlich, dass diese Risiken sowohl auf die Ressourcen des Unternehmens als auch auf dessen Betriebssicherheit Einfluss haben. Nur die ausreichende Berücksichtigung und Bewertung der Risiken und das Ergreifen von adäquaten Maßnahmen kann also den Einsatz der IoRT zur Verbesserung bzw. Optimierung ermöglichen.

iii. Schutzziele und schützenswerte Informationen

Wie diese Diskussion zeigt, spielen die IoRT-Sensordaten, die durch PbM-Anwendung zusammengestellten Datensätze und die darauf basierenden Prognosen des PbM-Dienstes eine kritische Rolle für den sicheren Bahnbetrieb, und müssen entsprechend geschützt werden. Die Authentizität und Integrität der Daten sind dabei besonders wichtig, z.B., dass sie im IoRT-System verifizierbar generiert und nicht auf unbefugte Weise verändert wurden. Sollten z.B. die Sensoren, die den Zustand von den Gleisen beobachten, oder die Messwerte selbst von einem Angreifer manipuliert oder gefälscht werden, kann es dazu führen, dass der PbM-Dienst inkorrekte Störungsprognosen generiert und unangemessene Reaktionen hervorruft. Aber auch die Software- und Hardware- Konfigurationen wie Vorhersageverfahren und Modelle, Filterregeln und Zugangsberechtigungen, sowie Software und Hardware selbst, die die notwendigen Funktionen zur Sammlung, Bearbeitung, Speicherung und Übertragung von PbM Daten ermöglichen, sind schützenswert.

Die Verfügbarkeit von Informationen ist notwendig, um die Qualität des Dienstes zu gewährleisten. Fehlende Daten können zu Fehlentscheidungen führen und so beispielsweise als Systemausfall interpretiert werden. Dies kann von einem Angreifer missbraucht werden, um teure Gegenmaßnahmen auszulösen und auf diese Weise dem Betreiber zu schaden.

Da die Sensordaten keine persönlichen Informationen oder Geschäftsgeheimnisse beinhalten, werden sie normalerweise nicht als vertraulich betrachtet. Deswegen wird üblicherweise die Vertraulichkeit nicht als Schutzziel priorisiert. Allerdings erlauben diese Daten einem Dritten Schlussfolgerungen bzgl. des Zustands der Bahnanlagen zu ziehen, insbesondere, wenn zusätzliche Hintergrundinformationen wie Streckenpläne oder Spezifikationen für die Feldelemente oder Anlagen vorhanden sind. Aus diesem Grund sollten der Infrastrukturbetreiber in Betracht ziehen, die PbM relevanten Daten vor unbefugtem Zugriff und Offenlegung zu schützen.

Die Architektur des PbM-Dienstes in Abbildung 4 bietet dem potenziellen Angreifer viele Ansatzpunkte. Zugriffe sind an den Sensoren und der PbM-Anwendung möglich, auf dem IoRT-Gateway im Gleisbereich, dem PbM-Dienst in der Zentrale sowie an den Kommunikationsverbindungen zwischen den Systemen. Unter der Annahme, dass die Kommunikation zwischen der PbM-Anwendung im Gleisbereich und dem PbM Dienst in der Betriebszentrale über ein für Safety kritische Datenübertragung freigegebenes WAN erfolgt, kann davon ausgegangen werden, dass diese Kommunikation entsprechend sicher ist. Weiterhin wird angenommen, dass die Übertragungskomponenten, außer den IoRT-Devices selbst, adäquaten physischen Zugriffsschutz besitzen, z.B. durch Zutrittskontrollsysteme oder entsprechende Detektoren, die mit planmäßigen Arbeiten an den Geräten korreliert werden können. Damit würden lokale Angriffe und Manipulationen rechtzeitig detektiert oder wirksam unterbunden.

5.3.2 Anwendungsfall 2: Lokale Situationserkennung (SE)

Der lokale Situationserkennungsdienst (situational awareness, engl.) ermöglicht es, anhand von Informationen aus der nächsten Umgebung das Erkennen von Bedrohungen und deren zeitliche Entwicklung zu ermöglichen und auf der Grundlage dieser Informationen Entscheidungen über den Bahnbetrieb vor Ort zu treffen. IoRT-Sensoren liefern in diesem Fall diese notwendigen Informationen. Solcher SE-Dienst stellt eine Safety-kritische Erweiterung der heutigen DSTW-Funktionen dar.

Sobald die Sicherung des Fahrwegs durchgeführt wurde, kann das Stellwerk derzeit nur noch die Fehlermeldungen von OCs bearbeiten und den bestimmten Streckenabschnitt sperren. Es gibt keine Möglichkeit, die lokalen Störungen wie fremde Objekte im Gleisbereich oder auf der Strecke automatisch zu erkennen und darauf zu reagieren. Nehmen wir an, die IoRT-Sensoren sind der Strecke entlang installiert und je nach Reichweite mit einem nächstgelegenen IoRT-Gateway verbunden. Wenn die Sensoren oder die entsprechende SE-Anwendung auf dem Gateway (durch Korrelation von Daten aus mehreren Quellen)

ein Hindernis auf den Gleisen erkennen, kann die Betriebszentrale darüber informiert werden, einen Nothaltauftrag auslösen oder das entsprechende Gleis sperren, bevor ein Zug in das Gleis einfährt, oder diese Information mithilfe einer ETCS L2 Schnittstelle dem Triebfahrzeugführer zu liefern bzw. eine Verkürzung der Mouvement Authority (MA) vorzunehmen, so dass der Zug rechtzeitig vor einem Gefahrenpunkt angehalten werden kann.

Dementsprechend können die IoRT-Sensoren dabei helfen Echtzeitinformationen über die Situation auf der Strecke zu sammeln, potenziell gefährliche Zustände zu identifizieren und auf dieser Grundlage die notwendigen Maßnahmen einzuleiten. So könnten Störungen effizient behoben werden und Gefahrensituationen vermieden bzw. eine weitere Automatisierung des Eisenbahnbetriebs vorangetrieben werden. Beispielsweise FOS-Sensoren können zusätzlich zur Überwachung des Gleiszustands gefährliche Objekte (Baum, Schafherde, Person, usw.) im Streckenbereich erkennen. Eventuell können zusammen mit FOS auch weitere Io(R)T-Sensoren, beispielsweise eine IP-Kamera verwendet werden, um die Erkennungsergebnisse zu verbessern.

5.3.2.1 Systemarchitektur für IoRT basierte Situationserkennung

Die Komponenten und Kommunikationsverbindungen, die den IoRT-basierten SE-Dienst ausmachen, sind in Abbildung 5 in Rot dargestellt.

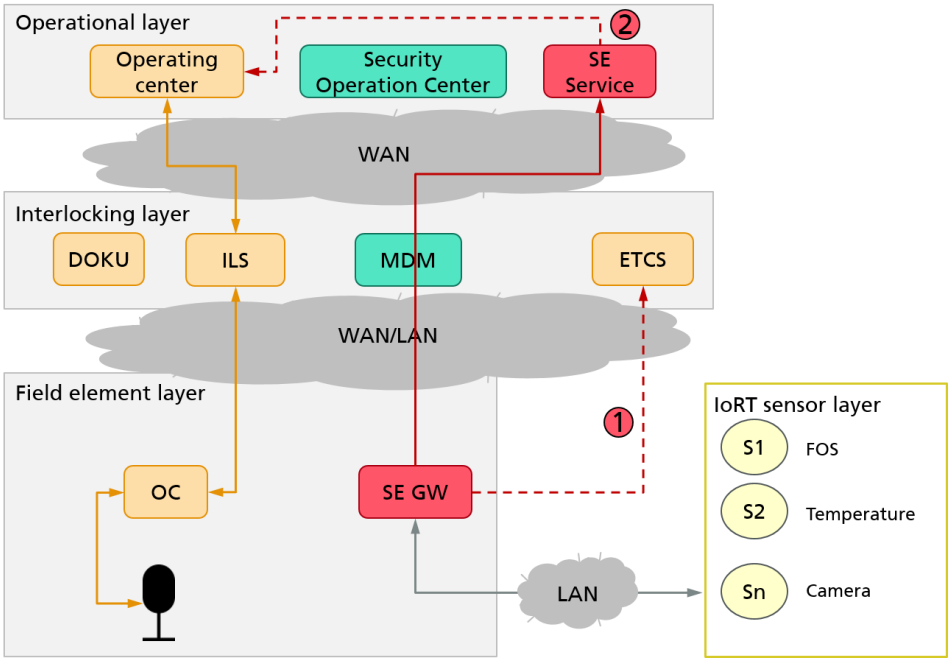

Abbildung 5: IoRT basierte Dienst zur Situationserkennung im Gleisbereich

Die SE-Anwendung auf einem speziellen IoRT-Gateway (in Abbildung: SE GW) sammelt Daten von den Sensoren in ihrem Netzwerk, bei analogen Sensoren werden die Signale in digitale umgewandelt. Die SE-Anwendung verarbeitet und analysiert die Sensordaten lokal, um sicherheitsrelevante Ereignisse auf der Strecke in Echtzeit erkennen zu können. Da die Rechenleistung des Gateways begrenzt ist, kann der Entscheidungsprozess auch durch einen SE-Dienst in der Betriebszentrale unterstützt werden. Der SE-Service sammelt außerdem die Informationen von mehreren Streckenabschnitten und analysiert sie, um die Entwicklungsmuster zu erkennen und die Gefahren vorherzusagen. Der Dienst stellt auch die entsprechenden Warnmeldungen für das integrierte Bedienplatzsystem bereit.

Wird ein solches, sicherheitsrelevantes Ereignis erkannt, kann die SE-Anwendung autonom reagieren. Ziel ist es, das Einfahren von Zügen in den Streckenabschnitt mit Gefährdung zu verhindern. Da der SE-Anwendung die Positionen der Züge nicht bekannt sind, müssen folgende Schritte durchgeführt werden, um den betriebssicheren Zustand (fail-safe) zu gewährleisten:

① Die SE-Anwendung sendet eine Benachrichtigung an das RBC, welches wiederum das Fahrzeuggerät bzw. den Triebfahrzeugführer erreichen und zum zeitgerechten Anhalten des Zuges auffordern kann.

② Die SE-Anwendung sendet eine Information an das „Operation Center“, also beispielsweise die Betriebszentrale oder das TMS (Traffic Management System), um je nach aktueller Situation entweder den betroffenen Triebfahrzeugführer und/ oder weitere Triebfahrzeugführer zu informieren und, wenn möglich, eine andere Route vorzugeben.

Die entsprechenden Informationsflüsse sind in Abbildung 5 durch rote Pfeile markiert und entsprechend nummeriert.

Um einen Eingriff in sicherheitskritische Funktionen zu vermeiden, kann die SE-Anwendung alternativ einen Alarm an MDM oder SOC senden, die ihrerseits die Betriebszentrale auf dem üblichen Weg über das erkannte Problem informieren können.

Die Kommunikation zwischen der SE-Anwendung in der Feldelementebene und dem SE-Dienst in der Betriebszentrale erfolgt über das WAN das Infrastrukturbetreibers.

5.3.2.2 IT-Sicherheitsaspekte

I. Bedrohungsanalyse auf Basis von BSI Top 10

Im Folgenden werden die Bedrohungen aus der Top-Ten-Liste [8] dem Anwendungsfall IoRT basierte SE Dienst/ System zugeordnet. Viele Erkenntnisse sind dabei dem vorherigen LST Anwendungsfall ähnlich. Der Hauptunterschied zwischen den Anwendungsfällen besteht darin, dass in diesem Fall die Echtzeitinformationen aus der SE-Anwendung eine höhere betriebliche Relevanz haben, da sie unmittelbar relevant sind. Daher sind auch die Bedrohungen, die die Echtzeitübertragung dieser Informationen beeinträchtigen, von höherer Relevanz.

1. *Einschleusen von Schadsoftware über Wechseldatenträger und externe Hardware:* Wie bereits für den PbM-Dienst erläutert, sind die IoRT-Sensoren und das Gateway im Gleisbereich einem besonderen Risiko ausgesetzt. Wechseldatenträger sind für die Funktion nicht vorgesehen und dürfen nicht verwendet werden.
2. *Infektion mit Schadsoftware über Internet und Intranet:* Wie auch im Fall von PbM ist der SE-Dienst vernetzt und anfällig für solche Angriffe. Dabei spielt bei dem SE-Dienst eine schnelle Reaktion auf die aktuellen Ereignisse eine wichtigere Rolle als die Prognosen, deswegen ist auch die Schadsoftware, die diese Reaktionszeit beeinträchtigt, gefährlicher. In diesem Fall werden die Vorhersagen auf mehreren verteilten Informationsquellen basieren und weniger anfällig für Infektionen oder Manipulationen einzelner Komponenten sein.
3. *Menschliches Fehlverhalten und Sabotage:* Die Erkenntnisse für das PbM-System gelten auch für den SE-Dienst. Die Ausnahme ist die Internet-Schnittstelle nach außen, die in diesem Fall nicht vorhanden ist. Der SE-Dienst stellt einen besonderen Anreiz für böswillige Handlungen dar, da sie es dem Angreifer im Erfolgsfall ermöglichen, den Bahnverkehr in einem bestimmten Gebiet umfangreich zu stören. Dies ist ein sehr sichtbarer Effekt, über den auch die Presse berichten würde und der besonders für Script-Kiddies, die durch Ruhm motiviert sind, oder auch verärgerte Mitarbeiter attraktiv ist.
4. *Kompromittierung von Extranet und Cloud-Komponenten*: Eine Anbindung zur Cloud ist für den SE-Dienst nicht vorgesehen. Obwohl einige Bahnbetreiber ihre sicherheitskritischen Anwendungen in die Cloud auslagern möchten, handelt es sich dann um on-premise-Systeme. So haben diese und auch die SE-Komponenten in der Feldelementebene keinen Zugang zu anderen Netzwerken außer dem bahnbetrieblichen WAN und können daher nicht direkt mit einer public Cloud verbunden werden.

5. *Social Engineering und Phishing:* Die Erkenntnisse aus dem PbM Anwendungsfall gelten auch für den SE-Dienst.
6. *(D)DoS Angriffe*: Da die SE-Anwendung in vielen Fällen auch lokal die Sensordaten verarbeiten kann, kann fehlende Kommunikation mit der Betriebszentrale nur die Reaktion verzögern. Dabei kann die SE-Anwendung die Schnittstelle zum RBC des ETCS verwenden, um über die potenzielle Gefahr im Betrieb zu informieren. Da der SE-Dienst die Daten aus mehreren verteilten Quellen sammelt, kann ein temporärer Ausfall von einem SE-Gateway so ausgeglichen werden. Ähnlich wie im PbM können die Gateways mit der Anwendung sowie der SE Dienst durch bestimmte Nachrichten gestört oder zum Absturz gebracht werden.
7. *Internet-verbundene Steuerungskomponenten*: Das SE System erlaubt keine direkte Verbindung von Steuerungskomponenten mit dem Internet.
8. *Einbruch über Fernwartungszugänge*: Die Erkenntnisse aus dem PbM-Anwendungsfall gelten auch für den SE-Dienst.
9. *Technisches Fehlverhalten und höhere Gewalt*: Die Erkenntnisse aus dem PbM-Anwendungsfall gelten auch für den SE-Dienst. Da insbesondere die Komponente im Feld wegen wechselnden Umweltbedingungen und fehlender Kontrolle durch Personal verwundbar sind und genau diese Komponenten für die lokale Entscheidungsfindung verantwortlich sind, sollten zusätzliche Schutzmaßnahmen zur Vorbeugung von False Positives durch defekte Komponenten implementiert werden.
10. *Kompromittierung von Smartphones im Produktionsumfeld:* Diese Bedrohung ist relevant, wenn die Personen im Gleis anhand Smartphones erkannt würden. In diesem Fall kann der Angreifer die Smartphones verwenden, um bestimmte Situationen vorzutäuschen. Das Szenario ist jedoch nicht vorgesehen.

II. Risiken

Die Zuverlässigkeit der Informationen spielt für den SE-Dienst ähnlich wie im vorherigen Anwendungsfall eine sehr wichtige Rolle.

Die Manipulation von IoRT-Sensoren oder den übertragenen Daten durch einen aktiven Angreifer kann zu zwei unerwünschten Ergebnissen führen. Die SE-Anwendung kann es versäumen, ein Hindernis (rechtzeitlich) zu erkennen und den Verkehr positiv zu beeinflussen (False Negativ). In diesem Fall sind die derzeit geltenden Standard-Sicherheitsmaßnahmen verfügbar, reichen aber möglicherweise nicht aus, um einen Zwischenfall zu verhindern. Je nach Schwere des Vorfalls kann dies für den Bahnbetreiber katastrophale Folgen haben.

In einem alternativen Fall kann der Angreifer die SE-Anwendung dazu verleiten, ein Hindernis zu erkennen, wo überhaupt kein Hindernis vorhanden ist (False Positive), oder es falsch zu bewerten und so eine kritische Reaktion mit Gefährdung (False Negative) hervorzurufen. Dies mindert einerseits das Vertrauen in das System und hat auch negative Folgen für den Betreiber. Dabei ist insbesondere mit Verzögerungen durch die ungeplante und unnötige Beeinträchtigung des Verkehrs und die Sicherung von Alternativrouten zu rechnen. Sollte es dem Angreifer gelingen, mehrere SE-Anwendungen gleichzeitig zu manipulieren, kann es auch zu einer regionalen oder flächendeckenden Beeinträchtigung des Betriebs führen. Dies wiederum wäre mit hohen finanziellen Schäden und Reputationsverlust verbunden. Auch zusätzliche Investitionen in diesen SE-Dienst dürften sich nachteilig auswirken, wenn sich dieser Dienst aufgrund hoher Fehlerquoten nicht durchsetzen kann.

III. Schutzziele und Schützenswerte Informationen

Demensprechend spielen auch in diesem Anwendungsfall die IoRT Sensordaten, die durch SE-Anwendung zusammengestellten Datensätze und die darauf basierenden Bewertungen von der Sicherheit bestimmter Routen eine kritische Rolle für den sicheren Bahnbetrieb und sollen entsprechend geschützt werden. Da die SE-Anwendung und der SE-Dienst außerdem die Meldungen an die Betriebszentrale und das RBC sen-

den, die den Bahnbetrieb beeinflussen können, sind diese Informationen auch als Primary Assets einzustufen. Die Authentizität und Integrität dieser Informationen sind dabei besonders wichtig. Das heißt, sie müssen beispielsweise im IoRT System verifizierbar generiert und nicht auf unbefugte Weise verändert werden können. Aber auch die Software- und Hardware- Konfigurationen wie Analyse- und Klassifizierungsverfahren und Modellen, Filterregeln und Zugangsberechtigungen, sowie Software und Hardware selbst, die die notwendigen Funktionen zur Sammlung, Bearbeitung, Speicherung und Übertragung von SE Daten ermöglichen, sind schützenswert.

Die Verfügbarkeit inklusive Rechtzeitigkeit (Timeliness) von SE-Informationen ist notwendig, um den adäquaten Schutz vor Vorfällen zu gewährleisten. Der Angreifer kann die von den IoRT-Sensoren an die SE-Anwendung oder Dienst gesendeten Daten blockieren oder verzögern, was im ersten Fall die Frühwarnung verhindert (aber auch im gesamten Bahnsystem korrekt als Ausfall der SE-Funktionalität adressiert werden kann), im zweiten Fall durch unkoordinierte Reaktion auf die verzögerten Daten wegen der kurzen Reaktionszeit Schaden verursachen kann.

Da die IoRT-Sensordaten keine persönlichen Informationen oder Geschäftsgeheimnisse beinhalten sollten, wird die Vertraulichkeit nicht als Schutzziel priorisiert. Beim Einsatz bildverarbeitender Sensoren, z.B. Kameras, müssen die Anforderungen der DSGVO berücksichtigt werden, so dass Vertraulichkeit wiederum Relevanz erhält. Hier sollten die Anforderungen aus den Standardanwendungsfällen (vgl. Abschnitt 4) implementiert werden. Es ist zu vermerken, dass die SE-Anwendung lediglich die Information erfordert, dass sich ein Objekt auf dem Fahrweg befindet, weitere Einzelheiten sind nicht unbedingt erforderlich.

Die Architektur des SE-Dienstes bietet dem potenziellen Angreifer viele Ansatzpunkte, von Sensoren und SE-Anwendung auf dem Gateway im Gleisbereich bis dem SE-Dienst in der Zentrale sowie den Kommunikationsverbindungen. Wie auch im Fall vom PbM-System, kann von einer sicheren (secure) Kommunikation über das bahnbetriebliche WAN sowie physischen Schutzvorrichtungen in der Betriebszentrale ausgegangen werden.

5.4 Lösung

Die obige Analyse zeigt, dass viele der Standardbedrohungen für industrielle Steuerungssysteme auch für IoRT-Anwendungen im LST-Bereich relevant sind. Aus diesem Grund sollten auch die Standardempfehlungen und IoT-Sicherheitsrichtlinien des BSI [8] und anderer IT-Sicherheitsbehörden für die untersuchten Anwendungsfälle umgesetzt werden. Die Studie [14] analysierte die Anwendbarkeit verschiedener IoT-Sicherheitsrichtlinien und Best Practices für den Einsatz im Bahnbereich und definierte die entsprechenden IT-Sicherheitsanforderungen zum Schutz des IoRT vor Cyberattacken über den gesamten Lebenszyklus. Die Studie konzentrierte sich auf die Sicherung von IoRT-Edge-Geräten und Kommunikationsnetzwerken und weniger auf die IT-Sicherheit von Rechenzentren und der Cloud.

Die Berücksichtigung der folgenden Anforderungen ist demensprechend für die IT-Sicherheit kritisch:

- sichere Speicherung von Geheimnissen (Zugangsdaten, kryptographische Schlüssel, usw.),
- Sicherstellung der Systemintegrität und Erkennung von Manipulationen,
- sichere Software Update-Mechanismen,
- Erkennung von Angriffsversuchen über das Netzwerk (u.a. (D)Dos),
- sichere Kommunikation zwischen Endpunkten,
- sichere Wiederherstellung der Funktionalität nach einem Angriff.

Die Besonderheit der IoRT-Nutzung im Bereich von LST besteht darin, dass das LST-System sowohl als Zielsystem für PbM- und SE-Dienste als auch als IoRT-Komponente selbst betrachtet werden kann. Darüber hinaus müssen die IoRT-Sensoren und -Gateways, die von PbM- und SE-Diensten verwendet werden, nicht nur den Umgebungsbedingungen, sondern auch strikten Safety und Security-Anforderungen entsprechen, um das bahnbetriebliche WAN für die Kommunikation zu nutzen, das sonst nur zur Gewährleistung des Bahnbetriebs verwendet wird. Eine weitere Besonderheit besteht darin, dass die IoRT-Komponenten im Feldelementbereich ähnlich wie vernetzte LST-Systeme lokalen Angreifern ausgesetzt sind, die

die Systeme unbemerkt manipulieren können. Beim Einsatz von handelsüblichen Produkten (COTS) können solche Angriffe auch problemlos skaliert werden. Diese Angriffsmöglichkeiten stellen eine Herausforderung für die IT-Sicherheit von LST-Systemen und IoRT-Diensten gleichermaßen dar.

Um die Safety kritischen LST Systeme gegen solche Angriffe zu schützen, wurde im Rahmen vom Forschungsprojekt HASELNUSS (haselnuss-projekt.de) des Bundesministeriums für Bildung und Forschung (BMBF) eine Referenzarchitektur entwickelt, die es ermöglicht geeignete IT-Sicherheitsfunktionen in die vernetzen LST-Systeme zu integrieren. Die HASELNUSS-Architektur [15], [16] [17] zeigt wie IT-Sicherheitsfunktionen und Safety-kritische Anwendungen rückwirkungsfrei auf der selben Hardware-Plattform umgesetzt und daher stärker integriert werden können. Bisher erfolgte die Implementierung dieser Funktionen strikt getrennt, normalerweise auch physikalisch getrennt, um die Rückwirkungsfreiheit nicht einzuschränken und den Safety-Zulassungsprozess zu erleichtern.

Die HASELNUSS Referenzarchitektur besteht aus einem MILS (Multiple Independent Levels of Safety and Security) Betriebssystem, einem Hardware-Sicherheitsmodul in Form eines Trusted Platform Modules (TPM) 2.0 und verschiedenen Security-Diensten (siehe Abbildung 6).

Dank der Datenisolation und Informationsflusskontrolle durch das MILS Betriebssystem können eine Safety-Anwendung (z. B. Objekt Controller, SIL 4) und Security-Anwendungen (mit geringerem SIL) so separiert werden, dass sie in komplett abgeschirmten Partitionen auf derselben Hardware-Plattform laufen können, ohne sich gegenseitig zu beeinflussen. Mittels TPM kann dabei aus der Ferne festgestellt werden, ob die gestartete Software der erwarteten Konfiguration (z.B. die mit SIL-Zertifizierung) entspricht oder ob sie manipuliert wurde. Die Security-Dienste werden innerhalb der dedizierten Security-Partitionen ausgeführt und beinhalten z.B. Verfahren zur wechselseitigen Authentifikation zwischen dem Objekt Controller und dem Stellwerk, die Überwachung der Integrität von Systemen, Sichere Software Updates und Intrusion Detection System (IDS).

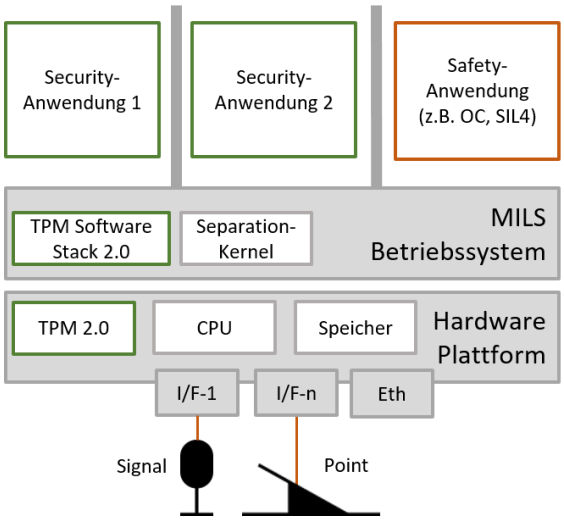

Abbildung 6. HASELNUSS Referenzarchitektur auf Basis von MILS Plattform

Im Rahmen des Forschungsprojekts wurde die HASELNUSS-Architektur als eine Erweiterung der NeuPro Architektur implementiert, um die vernetzten Objekt Controller im Feldelementbereich gegen Angriffe zu schützen. Auf dieser Grundlage können auch IoRT-Anwendungen sicher (safe und secure) betrieben werden. In diesem Fall kann der Objekt Controller die Funktionen von einem IoRT Gateway übernehmen. Vorteilhaft ist dabei, dass dank der HASELNUSS-Architektur dieselbe Safety und Security zertifizierte Hardware-Plattform nicht nur für LST-, sondern auch für IoRT-Anwendungen eingesetzt wird, was gleichzeitig Angriffsfläche, Instandhaltung, und Kosten reduziert. Die Verwendung von spezialisierten industriellen IoRT-Gateways ist auch weiterhin möglich, dabei sollten die Standardlösungen auf Basis von offenen Spezifikationen bevorzugt werden. Um diese HASELNUSS-basierte Lösung der IoT-Referenzarchitektur gegenüber zu stellen, sollten bestimmte Einschränkungen berücksichtigt werden.

Derzeit kann der OC nur mit den Systemen auf der DSTW-Ebene über das interne bahnbetriebliche WAN kommunizieren. Die Safety-Kommunikation (Kommandos und Meldungen) läuft dabei nur über DSTW. Die Logs werden durch MDM/DOKU gespeichert. Im HASELNUSS Projekt wird das MDM auch als eine Security-Komponente betrachtet, die z.B. die Security-Alarme an das SOC weiterleitet oder auch den Zustand des OCs abfragen kann. D.h. ein aktueller OC kann nicht direkt durch das SOC oder einen weiteren Dienst abgefragt werden und kann in diesem Fall nur begrenzt als IoRT-Gateway funktionieren (ohne Internet/ Cloud Anbindung).

Im Fall des HASELNUSS-OC werden bestimmte Edge Computing Funktionen direkt unterstützt. Zum Beispiel werden Netzwerkpakete analysiert und Security Ereignisse generiert. Diese Ereignisse werden über den MDM an das SOC weitergeleitet. Außerdem kann das System lokale Diagnostik durchführen und ggf. auch einen sicheren Zustand wiederherstellen. Dasselbe gilt auch für die beiden IoRT-Anwendungen, PbM und SE. Hier werden die Sensordaten analysiert und teilweise Reaktionen abgeleitet. Um die Informationen auf höheren Ebenen bereitzustellen, findet die Kommunikation mit der Betriebszentrale statt.

Da die Feldelemente derzeit keine IP-Kommunikation unterstützen und einzeln mit dem OC verbunden sind, kann ein OC (Safety-Anwendung) als Physical Device betrachtet werden. In diesem Fall werden die Daten einfach von analog zu digital und umgekehrt umgewandelt und an das DSTW/MDM weitergeleitet.

6 Fazit

Der Einsatz von Sensoren im bahnbetrieblichen Kontext bietet offensichtliche Vorteile zur Optimierung der Prozessabläufe für den Kunden, die Sicherheit und für den eigentlichen Betriebsprozess. Dies konnte im Rahmen der erläuternden Beispiele im Kontext Personenbahnhöfe für Reisendenstromlenkung sowie Sicherheit an Bahnhöfen und für Anwendungen im bahnbetrieblichen Kontext zur Instandhaltungsoptimierung gezeigt werden.

Gleichzeitig bieten die stark verteilten Sensoren mit eigener Intelligenz und deren Interpretation von Rohdaten eine erweiterte Angriffsfläche aus Sicht IT-Sicherheit. In diesem Kontext konnte im Verlauf herausgearbeitet werden, dass die bereits am Markt verfügbaren Lösungen bzw. Konzepte zur Sicherung von IoT-Devices, speziell IIoT, geeignet sein können, um die notwendige IT-Sicherheit herzustellen. Dies gilt insbesondere dann, wenn keine direkte Verbindung zu Systemen mit Sicherheitsrelevanz und dementsprechend umfangreichen Akkreditierungen vorhanden sind.

Für Systeme mit direktem Bezug zum Eisenbahnbetrieb, entweder durch Relevanz der Dateninhalte für die Betriebssicherheit oder durch direkte Kommunikationsverbindung, sind neue bzw. modifizierte Ansätze notwendig, um den Anforderungen zu begegnen. Die mit diesen IoRT-Devices gewonnen Informationen werden zur Instandhaltungsoptimierung oder Betriebsoptimierung eingesetzt und stellen so z.B. einen Verbrauch des Abnutzungsvorrats einer Einheit dar. Werden diese Daten unzulässig verändert, kann es zu Ausfällen im Sinne der Verfügbarkeit jedoch auch zu sicherheitskritischen Vorfällen kommen. Aus diesem Grund hat die Integrität der Daten eine besondere Bedeutung. Gleichzeitig muss sichergestellt bleiben, dass die IoRT-Devices in regelmäßigen Abständen Updates oder Upgrades erfahren können und auch in Zyklen <= 5 Jahre getauscht werden können, um die entsprechenden Innovationszyklen aber teilweise auch Lebenserwartungen von Standardprodukten zu berücksichtigen. Hierfür ist neben der hohen Sicherheitsanforderung also auch eine Flexibilität notwendig.

In der Lösungsfindung wurde festgestellt, dass die IoRT-Devices entsprechende Security Gateways benötigen, um datensicher zu kommunizieren. Hierbei können die Datenabnehmer der Betreiber selbst und ggf. auch der Hersteller für Service oder weitere Dienstleistungen sein. Zwei Lösungen wurden hierbei in Betracht gezogen. Einerseits die Integration eigener Security Gateways, andererseits die datenseitige Integration der IoRT-Devices in die OT-Devices im Gleisfeld und Nutzung des vorhandenen, bereits aus Security Sicht geschützten Netzwerks. In der Abwägung konnte festgestellt werden, dass die Integration in die vorhandenen Systeme den Vorteil hat, dass kein weiteres Element im Gleisfeld hinzugefügt werden muss und gleichzeitig keine direkte Internetverbindung ins Gleisfeld hergestellt werden muss. Diese Lösung reduziert einerseits die Angriffsfläche, andererseits kann eine effiziente Integration sichergestellt werden. Darüber hinaus verbleibt unter dem Gesichtspunkt der Geheimhaltung und des Datenschutzes die Hoheit über die Weitergabe der Daten an Hersteller oder andere Dritte vollständig beim Betreiber.

Die vorgeschlagene Lösung einer MILS-Architektur, vergleichbar der Lösung aus dem HASELNUSS-Projekt, stellt eine mögliche Integrationslösung von IoRT-Devices und deren Informationen in den bahnbetrieblichen Kontext dar. Es kann und wird weitere mögliche Integrationen geben. Diese sollten jedoch alle folgenden Eigenschaften gemeinsam haben:

1. Trennung von Safety und Security
2. Sicherstellung von Datenintegrität und Hoheit über Datenweitergabe beim Bahnbetreiber
3. Vermeidung direkter Internetzugriffe auf das Gleisfeld zur Vermeidung der Vergrößerung der Angriffsfläche
4. Kontinuierliches Security Monitoring, beispielsweise durch ein SIEM bzw. SOC, zur Angriffs- oder Missbrauchserkennung

Zusammenfassend kann festgestellt werden, dass auch im Eisenbahnkontext IoT einen erheblichen Mehrwert bieten kann. Für die technische Integration sind sowohl Industrial IoT-Devices mit Lösungen nahe dem Standard sowie IoRT-Devices möglich. Die Auswahl hängt vom Einsatzgebiet und der Relevanz für den Eisenbahnbetrieb ab. Die Entscheidung sollte basierend auf einer fundierten Bedrohungsanalyse und anschließenden Risikoanalyse mit Auswirkungsanalyse (Impact) erfolgen.

In der Zukunft wird ein starker Anstieg der Nutzung von IoT, IIoT, IoRT-Devices erwartet. Insofern wird empfohlen, bereits langfristig und im Voraus Konzepte zu entwickeln bzw. in laufende IT-Sicherheitsbetrachtungen die Sensorik über IoT zu integrieren, um ein harmonisches Gesamtkonzept sicherstellen zu können. Im Kontext der europäischen Spezifikation für bahnbetrieblich nahe Systeme erfolgt eine grundsätzliche Berücksichtigung in den Standardisierungen von EULYNX [18] und RCA [19]. Hier wurde unlängst eine Security-Guideline, basierend auf den Normen prTS 50701 und IEC 62443, konkretisiert für die Anwendung in EULYNX, RCA und OCORA [20] erarbeitet und wird in Q1/2021 veröffentlicht. Unabhängig davon ist immer eine individuelle Betrachtung erforderlich, um die Berücksichtigung der länderspezifischen Bedrohungslage sowie vorhandenen Systeme (legacy) sicher zu stellen.

7 Abkürzungsverzeichnis

BMBF: Bundesministerium für Bildung und Forschung

CbM: Condition Bases Maintenance (DE: Zustandsbasierte Instandhaltung)

COTS: commercial off-the-shelf

(D)DoS: (Distributed) Denial of Service

DSTW: Digitale Stellwerk

EBA: Eisenbahn Bundesamt

ETCS: European Train Control System

FOS: Faseroptische Sensornetzwerk

GW: Gateway

IDS: Intrusion Detection System (DE: Angriffserkennungssystem)

IIoT: Industrial Internet of Things

ILS: Interlocking System

IoRT: Internet of Railway Things (DE: Internet der Bahn Dinge?)

IoT: Internet of Things (DE: Internet der Dinge)

IT: Informationstechnologie

LAN: Local Area Network

LST: Leit- und Sicherungstechnik

MA: Movement Authority (DE: Fahrerlaubnis – aus ETCS)

MDM: Maintenance and Data Management System

MILS: Multiple Independent Levels of Safety and Security

MitM: Man in the Middle

OC: Objekt Controller

OT: Operational Technology

PbM: Prediction based Maintenance (DE: vorausschauende Instandhaltung)

RaSTA: Rail Safe Transport Application

RBC: Radio Block Center (aus ETCS)

SE: Situationserkennung (EN: Situational Awareness)

SIEM: Security Information and Event Management

SOC: Security Operation Center (DE: IT-Sicherheitszentrale)

TMS: Traffic Management System (DE: Verkehrssteuerungssystem)

TPM: Trusted Platform Module

WAN: Wide Area Network

8 Verweise

[1] DB Netz AG, „deutschebahn.com," 30 Oktober 2019. [Online]. Available: https://www.deutschebahn.com/de/presse/pressestart_zentrales_uebersicht/DB-setzt-Digitalisierungsoffensive-fort-Kuenftig-steuern-280-digitale-Stellwerke-Zugverkehr-in-Deutschland-4578022. [Zugriff am 07 Dezember 2020].

[2] BMBF, „forschung-it-sicherheit," Januar 2017. [Online]. Available: https://www.forschung-it-sicherheit-kommunikationssysteme.de/projekte/haselnuss. [Zugriff am 07 Dezember 2020].

[3] Bundestag, „Bundestag.de," 2012. [Online]. Available: https://www.bundestag.de/blob/192512/cfa9e76cdcf46f34a941298efa7e85c9/internet_der_dinge-data.pdf.

[4] IEEE, „IoT World forum," 2020. [Online]. Available: https://wfiot2020.iot.ieee.org/.

[5] CISCO, „CDN," 2014. [Online]. Available: http://cdn.iotwf.com/resources/71/IoT_Reference_Model_White_Paper_June_4_2014.pdf .

[6] AG CYSIS, „Whitepaper: Security for Safety – Anforderungen an eine digitalisierte Bahnwelt," AG CYSIS, Frankfurt am Main, 2018.

[7] AG CYSIS, „Security for Safety," DVV Media Group, 2018.

[8] BSI, „Industrial Control System Security. Top 10 Bedrohungen und Gegenmaßnahmen 2019," Bundesamt für Sicherheit in der Informationstechnik (BSI), 2019.

[9] M. Kant und D. A. Priebe, „Security for Safety," *Signal&Draht,* p. 8, Mai 2018.

[10] M. Schubert, „IT-Sicherheit im Bahnbetrieb," *Deine Bahn,* Juni 2020.

[11] C. Schlehuber, M. Heinrich, T. Vateva-Gurova, S. Katzenbeisser und N. Suri, „A Security Architecture for Railway Signalling," *International Conference on Computer Safety, Reliability and Security,* 17 August 2017.

[12] DKE, Elektrische Bahnsignalanlagen - Teil 200: Sicheres Übertragungsprotokoll RaSTA. DIN VDE V 0831-200, DKE, 2015.

[13] P. Fraga-Lamas; T. Fernández-Caramés; L. Castedo, „Towards the Internet of Smart Trains: A Review on Industrial IoT-Connected Railways," Basel, 2017.

[14] D. A. T. D. T. P. SNCF, „AG Cysis," Juni 2020. [Online]. Available: https://www1.deutschebahn.com/innovationsallianz/forschung/AG_CYSIS-875054.

[15] Markus Heinrich; et. al., „Security Requirements Engineering in Safety-Critical Railway Signalling Networks," in *Security and Communication Networks*, 2019.

[16] H. Birkholz; M. Zhdanova; C. Krauß; T. Arul; M. Heinrich; S. Katzenbeisser; T. Vateva-Gurova; N. Suri; D. Kuzhiyelil; C. Schlehuber, „A reference architecture for integrating safety and security applications on railway command and control systems. In International Workshop on MILS: Architecture and Assurance for Secure Systems," in *MILS@DSN 2018*, Luxembourg, 2018.

[17] C. Krauß, M. Zhdanova, M. Eckel, S. Katzenbeisser, M. Heinrich, D. Kuzhiyelil, J. Cosic und M. Drodt, „IT-Sicherheitsarchitektur für die nächste Generation der Leit- und Sicherheitstechnik," *Deine Bahn ,* 2020.

[18] EULYNX, „eulynx.eu," 2020. [Online]. Available: https://www.eulynx.eu/. [Zugriff am 07 Dezember 2020].

[19] E. ERTMS, „eulynx.eu," 07 Dezember 2018. [Online]. Available: https://eulynx.eu/index.php/documents2/press-releases/194-18c044-1-white-paper-reference-ccs-architecture-final/file. [Zugriff am 07 Dezember 2020].

[20] R. Mühlemann, „OCORA – Die europäische Initiative zur ETCS-Fahrzeugausrüstung der Zukunft," *Signal+Draht,* September 2020.

9 Abbildungs- und Tabellenverzeichnis

10 Kontakt und Impressum

Kontakt

Dr. Matthias Drodt, DB Netz AG, Mainzer Landstraße 205, 60326 Frankfurt a.M.
Telefon: 069 265 17502 | Mail: Matthias.Drodt@deutschebahn.com

Markus Heinrich, M.Sc., TU Darmstadt, Mornewegstr. 32, 64293 Darmstadt
Telefon: 06151 16 25631 | Mail: heinrich@seceng.informatik.tu-darmstadt.de

Die folgenden Autoren der Untergruppe der AG CYSIS für IoRT – „UG IoRT“ haben zur Erstellung des Whitepapers gewirkt:

- Dr. Tolga Arul, Universität Passau
- Dr. Jasmin Cosic, DB Netz
- Dr. Matthias Drodt, DB Netz
- Marcus Friedrich, ÖBB
- Markus Heinrich, INCYDE GmbH
- Michael Kant, Berater DB Netz
- Prof. Dr. Stefan Katzenbeisser, Universität Passau
- Helmut Klarer, ÖBB
- Patrick Rauscher, DB Netz
- Max Schubert, INCYDE GmbH
- Gerhard Still, Cisco
- Detlef Wallenhorst, Cisco
- Maria Zhdanova, Fraunhofer Institute for Secure Information Technology SIT

Weitere Informationen

Die Arbeitsgruppe Cybersecurity für sicherheitskritische Infrastrukturen – CYSIS“ wurde am 25. Januar 2016 von der Deutschen Bahn AG und der TU Darmstadt im Rahmen der Innovationsallianz und des bestehenden DB RailLab gegründet. Ziel der AG ist es, den durch die Digitalisierung im Eisenbahnsektor gestiegenen Herausforderungen der Cybersecurity in sicherheitskritischen Infrastrukturen wirksam begegnen zu können.
Die AG Cybersecurity ist eine Basis für intensiven Informationsaustausch zwischen Industrie und Wissenschaft im Eisenbahnsektor, um von den gegenseitigen Erkenntnissen profitieren zu können. Mit Hilfe der Partner aus dem wissenschaftlichen Bereich, u.a. CYSEC, dem Profilbereich für Cybersicherheit an der TU Darmstadt, können effektive Abwehrtechniken und Gegenmaßnahmen erforscht und weiterentwickelt werden. Angestrebter Effekt ist die Vernetzung des Eisenbahnsektors mit der akademischen Forschung zum Thema Cybersecurity.

Webseite

www.seceng.tu-darmstadt.de/cysis