2024

AK IT-SICHERHEIT | WARTUNGSSCHNITTSTELLE

CNA INNOVATION CIRCLE |05| RAIL CYBERSECURITY

AUTOREN: MELANIE MAITERTH, MAX SCHUBERT, FRIEDRICH FEISTLE, DANIEL LÜDICKE, THOMAS STRANG, MAX PERNER, PHILIPP RÖßLER, MATHIAS BEER

Inhalt

1 Management Summary

Zentrales Element zur Beherrschung der IT-Sicherheitsrisiken einer industriellen Steuerung ist eine Bewertung der Risiken durch eine Risikoanalyse. Diese besteht aus den Schritten *High Level Risikoanalyse* und *detaillierte Risikoanalyse*.

Eine frühere Arbeitsgruppe des Arbeitskreises Cybersicherheit des CNA betrachtete in ihrem Bericht [1] wesentliche Aspekte der *High Level Risikoanalyse*. In diesem Dokument werden beispielhaft die konkreten Schritte zur Durchführung einer *detaillierten Risikoanalyse* vollzogen.

Als Beispiel wird die Wartungsschnittstelle einer Türsteuerung eines Schienenfahrzeuges gewählt. Hierüber sind erhebliche Eingriffe – wie z.B. SW-Aktualisierung oder Änderung der Konfiguration – möglich, die mit entsprechend großen Gefahren für die Cybersicherheit verbunden sind.

Die technischen Aspekte dieser Risikoanalyse werden im vorliegenden Dokument bis hin zur Umsetzung in einem beispielhaften Fahrzeug – sowohl für lokale Zugänge als auch für Fernzugriffe - behandelt. Darüber hinaus werden ergänzende Hinweise zu Maßnahmen in der übergeordneten Organisation gegeben.

Dieses Dokument dient der Hilfestellung für den Betreiber der Schienenfahrzeuge zur Beschaffung von Fahrzeugen, die ausreichend gegen Bedrohungen der IT-Sicherheit geschützt sind. Daraus abgeleitet ergeben sich Aufgaben für den Betreiber sowie für die Komponentenhersteller und Systemintegratoren zur Umsetzung der Anforderungen zur IT-Sicherheit.

2 Einleitung

Die Digitalisierung ist die größte Chance im Bahnsektor, die Klimaziele Deutschlands und Europas zu erreichen. Durch die Digitalisierung sowie autonomes Fahren kann die Wettbewerbsfähigkeit der Bahnen gesteigert, die Transportkapazitäten erhöht und die Kundenzufriedenheit verbessert werden. Durch Vernetzung und Standardisierung können zudem Vorhersagen und Echtzeit-Optimierungen erreicht werden. Damit einher geht jedoch eine erhöhte Abhängigkeit von der Verfügbarkeit der Daten sowie der digitalen Infrastruktur der Bahnen. Dies erhöht gleichzeitig auch die Verwundbarkeit gegen Cyberangriffe. Die Entwicklung der letzten Monate und Jahre zeigt, dass die kritische Infrastruktur Bahn zunehmend in den Fokus von Angreifern gerät. Allen Beteiligten ist klar, dass der Transport von Personen und Gütern schützenswert aus vielerlei Hinsicht ist, was den Schutz der IT-Sicherheit der Systeme hinsichtlich der Vertraulichkeit (Confidentiality), der Integrität (Integrity) oder der Verfügbarkeit (Availability) mit abdeckt.

Obwohl die Risiken und Bedrohungen bekannt und viel diskutiert sind, tut sich die Branche dennoch schwer mit einheitlichen Vorgaben und Lösungen. Warum ist das so?

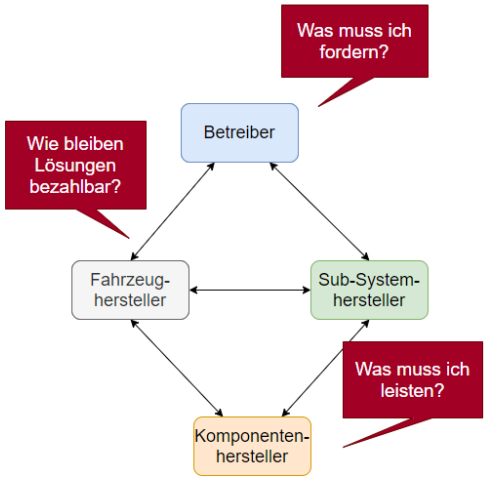

Abbildung 1 Unklarheiten in der aktuellen Beziehung der Interessensgruppen

Bei Betrachtung der verschiedenen Interessensgruppen (Bahn-Betreiber und ÖPNV-Betreiber, sowie Fahrzeug-, System- und Komponenten-Hersteller) fällt auf, dass noch kein einheitliches Verständnis über die Anforderungen und Lösungen im Bereich der Security vorliegt.

Der vorliegende Bericht diskutiert die benannten Herausforderungen stellvertretend am Beispiel der Wartungsschnittstelle für Schienenfahrzeuge. Die Wartung über Fernzugriff findet bereits heute umfassend Anwendung, um eine möglichst effiziente und kostengünstige Instandhaltung der Fahrzeuge durchführen zu können. Hierfür kommen Funktechnologien über öffentlichen Mobilfunk, große Datenmengen sowie hohe Ansprüche an Verfügbarkeit, Integrität und Vertraulichkeit zusammen.

2.1 Digitalisierung und die Schiene

Die Digitalisierung und damit einhergehender vermehrter Nutzung von IT-Systemen birgt großes Potential für neue Services und die Optimierung von Prozessen in allen Branchen und Anwendungsbereichen. Durch die damit verbundene Vernetzung, nehmen gleichzeitig die Angriffe auf IT-Systeme von Jahr zu Jahr massiv[1] zu. Häufig sind die Angriffe mit Diebstahl und Erpressung verbunden und erzeugen, allein in Deutschland, jährlich Schäden in Milliardenhöhe. Der Schutz dieser Systeme vor solchen Angriffen steht daher immer stärker im Focus.

Der Trend der Digitalisierung und die Erhöhung der Verwundbarkeit durch IT-Angriffe setzt sich auch im Industriebereich fort. Hier werden die Komponenten der Regelungs- und Steuerungs-Systeme als

[1] BSI: Die Lage der IT-Sicherheit in Deutschland, https://www.bsi.bund.de/DE/Service-Navi/Publikationen/Lagebericht/lagebericht_node.html

Operational Technology (OT) bezeichnet. Auch diese Komponenten sind zunehmend Ziele von Angriffen. Unabhängig von der gesetzlichen Anforderung des IT-Sicherheitsgesetzes, nimmt die IT-Sicherheit der OT-Systeme zum Schutz der Unternehmenswerte einen immer größeren Stellenwert ein.

2.2 Vorgaben und Regularien

Die Vorgaben für eine strukturierte Analyse und Auswahl von IT-Security für OT-Systeme definiert die Norm IEC 62443. Seit Ende 2021 wird sie im Bahnbereich durch die auf europäischer Ebene erarbeitete technische Richtlinie TS 50701 ergänzt, die die Anwendung der IEC 62443 im Eisenbahnbereich präzisiert. Die TS 50701 wird zudem aktuell als Grundlage für die Erarbeitung einer weltweit gültigen IEC (IEC 63452) herangezogen. Gemäß dieser Spezifikation und Normen, wird jedem Risiko eine Eintrittswahrscheinlichkeit zugeordnet und hinsichtlich der möglichen Auswirkungen der Bedrohung bewertet.

In beiden Dokumenten wird ein Lebenszyklus von OT-Systemen beschrieben, der im Wesentlichen in die Phasen Anforderung, Entwicklung und Betrieb gegliedert ist. Die Phasen bauen aufeinander. Dabei ist das Ziel des Systems – der Betrieb – in den vorangehenden Phasen jeweils bereits zu berücksichtigen.

In diesem Bericht bauen wir auf den Vorbericht „generisches IT Security Architekturmodell von Schienenfahrzeugen“ [1] auf, in dem eine High Level Risikoanalyse für ein Schienenfahrzeug beispielhaft durchgeführt wurde. In dessen High Level Risikoanalyse wird die Eintrittswahrscheinlichkeit des Risikos zunächst als sehr wahrscheinlich angenommen. Dies entspricht dem Vorgehen nach TS 50701. Das Risiko für das OT-System wird zunächst also nur anhand der Auswirkungen der Cyber Security Bedrohungen charakterisiert. Auf Basis der Schwere dieser Auswirkungen werden die Subsysteme in Kategorien eingeordnet, die eine erste Übersicht über ihren Schutzbedarf geben. Diese initiale Risikoanalyse nach IEC 62443 und TS 50701 wird daher in der Praxis oft als Schutzbedarfsfeststellung bezeichnet bzw. verwendet.

Das vorliegende Dokument schließt daran an und beschreibt das Vorgehen der daran anschließenden Phase der detaillierten Risikoanalyse (ohne jedoch selbst eine in jeder Hinsicht detaillierte Analyse vorzunehmen). In dieser Phase wird eine umfassende Risikoanalyse durchgeführt, bei der, auf einzelne Bedrohungen betrachtet, auch die Eintrittswahrscheinlichkeit anhand einer Skala abgeschätzt wird.

2.3 Aufbau des Berichtes

Um den komplexen Prozess einer Bewertung nachvollziehbar zu machen und den Einstieg zu erleichtern, wird der Prozess anhand des konkreten Beispiels der Wartungsschnittstelle einer Türsteuerung illustriert.

Die Wartungsschnittstelle wurde gewählt, da sie in vielen Fällen tiefe Eingriffe in technische Systeme und sicherheitsrelevante Funktionen des Zuges erlaubt und sie als eine der ersten Digitalisierungsmaßnahmen bereits in einigen Fahrzeugen zu finden ist. Da diese Funktionen und Schnittstellen zunehmend zur Fernwartung von Schienenfahrzeugen implementiert werden und sich ihr Funktionsumfang ständig erweitert, ist ihre Absicherung von besonderer Relevanz.

Zur Vorbereitung fasst das folgende Kapitel die Stakeholder der IT-Security für Schienenfahrzeuge zusammen. Der allgemeine Prozess der Risikoanalyse und Maßnahmendefinition ist in Kapitel 4 beschrieben und wird anschließend in Kapitel 5 auf die Wartungsschnittstelle bezogen. In Kapitel 0 werden weitere abgeleitete Maßnahmen aufgeführt und das 7. Kapitel diskutiert ein

Bestandsbeispiel aus der Praxis. Abschließend gibt der Bericht im Kapitel 8 eine Zusammenfassung Empfehlungen für das weitere Vorgehen.

3 Anwendungsbereich und Umfeld

Für eine erfolgreiche IT-Security ist immer eine vollständige Kette zu betrachten in der jeder Beteiligte (engl. Stakeholder) seine Sicherheitsziele und -anforderungen kennt und entsprechende Lösungen abstimmen muss. Mit einzelnen Maßnahmen ist eine wirkungsvolle IT-Security in der Regel nicht erreichbar.

3.1 Ausgangssituation

IT-Security stand bei der Entwicklung bei bestehenden Ausrüstungen nicht im Vordergrund. Heutige Schienenfahrzeuge haben die Nachweise, dass sie, vorwiegend in Bezug auf funktionale Sicherheit, als ausreichend sicher gelten. Als böswillige Eingriffe in der betrieblichen Praxis sind eher mechanische Schäden durch Vandalismus angenommen worden. Fahrzeugausfälle entstehen nach früher dominierender Bewertungen durch geplante und ungeplante Wartungsarbeiten, Unfälle und Vandalismus. Angriffe auf technische Anlagen durch Sabotage und insbesondere die IT waren bisher selten, deren Häufigkeit und Ausmaß nehmen jedoch stark zu.

Eine wesentliche Rolle spielen dabei Netzwerke; diese sind bisher eher funktional strukturiert und die funktionalen Zonen z.B. TCMS- und Betreiber-Netzwerke durch die Einrichtung unterschiedlicher Netzwerkzonen voneinander getrennt. Die Trennung wird technisch in der Regel durch Standard-Switche und Router, sowie durch räumliche Trennung sichergestellt.

Die Notwendigkeit und Anerkennung von IT-Security als eigenes Schutzziel hat sich in den vergangenen Jahren durch verschiedene Vorfälle und intensive Diskussionen auch im Bahnsektor weitgehend durchgesetzt. Für die weitere Digitalisierung wird IT-Security, inklusive des Datenschutzes, als eine Grundvoraussetzung für einen erfolgreichen Einsatz von IT-Systemen und deren Komponenten angesehen. Heutige Netzwerke in Schienenfahrzeugen werden häufig bereits von den Betreibern hinsichtlich der IT-Security analysiert und einfache Schutzmaßnahmen umgesetzt. Der aus der Gesetzgebung und Normung bekannte allgemeine Begriff der Sicherheit wird nun auch stärker auf die IT-Security bezogen. Rückwirkungen von IT-Security auf die funktionale Sicherheit (Safety) sind für heutige, neue (inkl. ReDesign) und zukünftige Fahrzeuge zu berücksichtigen.

3.2 Stakeholder

Dieses Kapitel betrachtet nun die Stakeholder: Welche gibt es, wer hat welches Interesse, welche Probleme sehen diese heute und was treibt die Stakeholder an?

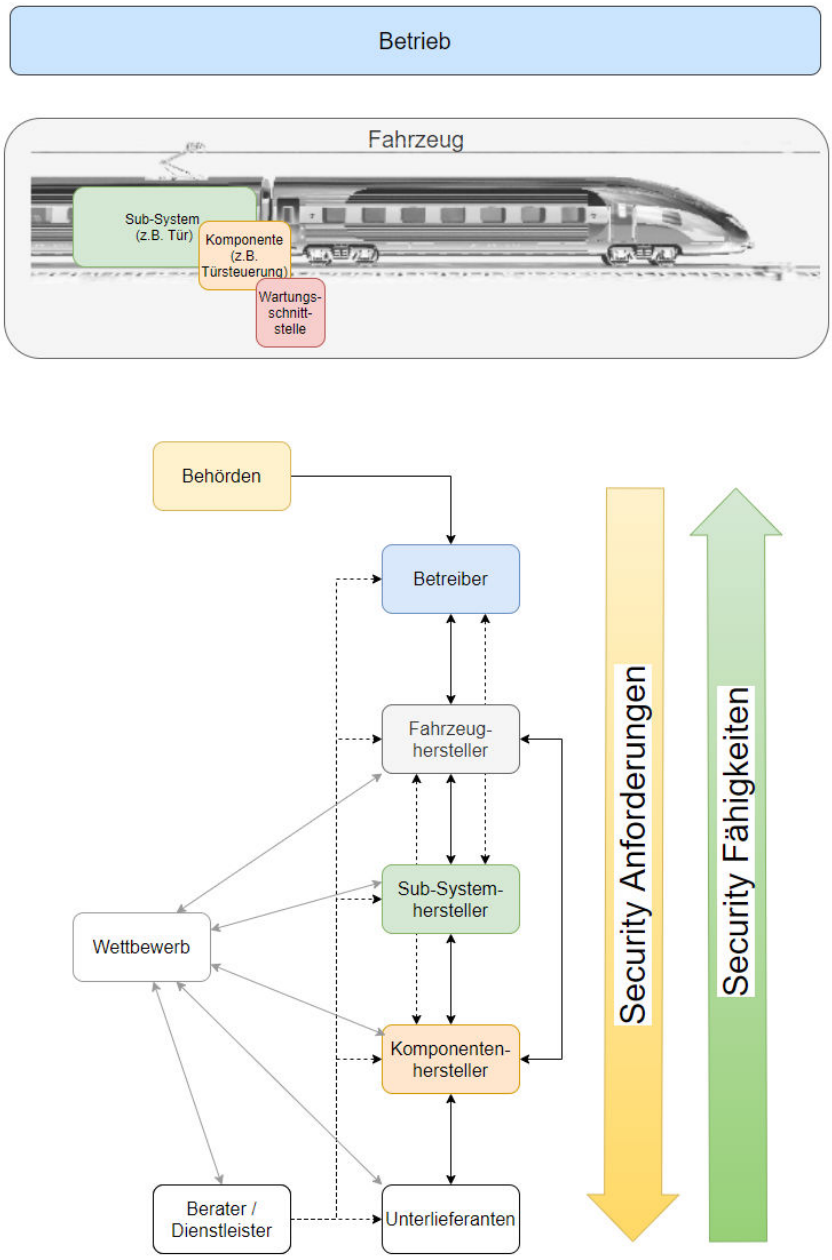

Abbildung 2: Stakeholder und Beteiligte in der Prozesskette

Der Bericht betrachtet vordergründig die Fahrzeuge des Schienenverkehrs. Für die Infrastrukturseite gelten weitestgehend ähnliche Betrachtungen.

Mit der Herstellung der Fahrzeuge und ihrem Betrieb sind vordringlich folgende Stakeholder befasst:

- Betreiber (Fahrbetrieb und Service)[2]
- Fahrzeughersteller
- Sub-Systemhersteller
- Komponentenhersteller

[2] An dieser Stelle wird angelehnt an die IEC 62443-2-1 der Begriff der Betreiber verwendet. Abweichend davon sind in Konstellationen von Bestellern und Anbietern von Verkehrsdienstleistungen die Rollen eines hier genannten Betreibers aufgeteilt.

Indirekt sind zusätzlich weitere Gruppen wie z.B. Behörden, Berater etc. involviert. Der Bericht beschäftigt sich aber aus Gründen der Kompaktheit vorrangig mit den zuerst genannten.

3.3 Betreiber

Um eine durchgängige IT-Sicherheit zu gewährleisten, müssen alle Beteiligten genau wissen, was zu fordern und umzusetzen ist, angefangen bei den Betreibern (Eisenbahnverkehrsunternehmen, EVU).

Die Hauptaufgabe der Betreiber ist das Befördern von Personen und Gütern. Dementsprechend konzentrieren sich die Betreiber auf die Durchführung des Fahrbetriebs und die Beschaffung, Bereitstellung und Wartung der dafür benötigten Fahrzeuge.

In Folge der Bahnreform in den 1990er Jahren gingen große Teile der Leistungs- und Finanzierungsverantwortung für den Schienenpersonennahverkehr auf die Länder über, was Auswirkungen auf die Rolle der Betreiber hatte. Insbesondere mit der Einführung des sog. „Besteller-Prinzips“ bestellt ein Bundesland über eine dazu bevollmächtige Organisation (z.B. die BEG in Bayern oder die LNVG in Niedersachsen) Verkehrsleistungen bei einem Betreiber, der dazu aus einem wettbewerblichen Verfahren als Sieger hervor gegangen ist. Hierbei gestaltet die Besteller-Organisation auch das Anforderungsprofil über die zu verwendenden Fahrzeuge teilweise bis zu deren Beschaffung. Auch Wartungsaufgaben werden zunehmend von Betreibern auf dafür spezialisierte Wartungs-Organisationen ausgelagert, die oft den Fahrzeugherstellern angegliedert sind.

Die IT-Sicherheit ist erst in den letzten Jahren als begleitende Anforderung dazugekommen, so dass vielfach Lücken bei Ressourcen und /oder Fachwissen bestehen, um IT-Sicherheit in den Sub-Systemen und Fahrzeugen, aber auch in den Prozessen bei Besteller-Organisation, Betreiber und Wartungs-Organisation zu implementieren.

Betreiber, ob groß oder klein, stehen also vor der Herausforderung, ihr Unternehmen strategisch auf die Anforderungen von IT-Sicherheit auszurichten, eine Roadmap zu erstellen und entsprechend Ressourcen dafür bereitzustellen.

3.4 Zulassungsbehörden

Auch bei den Zulassungsbehörden ist keine einheitliche Beurteilung des Themas festzustellen. Noch gibt es hier keine einheitliche Sicht, welche Normen im Einzelnen anzuwenden sind.

Aktuell wird u.a. die ISO 27001, IEC 62443 oder auch TS 50701 herangezogen, wobei diese teilweise für andere Branchen entwickelt wurden und nur bedingt auf das System Schienenfahrzeug angewendet werden können.

Aufgrund dieser uneinheitlichen Lage ist die effiziente Umsetzung der IT-Security für Produkte und Prozesse im Schienenfahrzeugbereich nach wie vor schwierig. Die Folgen sind hoher Aufwand sowie zusätzliche Kosten. Beispielsweise müssen in manchen Anwendungsfeldern Fahrzeuge alle 2 Jahre einer kompletten Risikoanalyse unterzogen werden - mit entsprechendem Aufwand an spezialisierten Fachleuten. Werden bei Bestandsfahrzeugen Sicherheitslücken aufgedeckt, kann ein massiver Aufwand entstehen, diese technisch auf den aktuellen Sicherheitsstand zu heben. Dies geht oft auch mit hohen Anschaffungskosten für zusätzliche Hardware einher.

Im Beschaffungsfall von Neufahrzeugen durch Betreiber oder Besteller stellt sich die Frage, welche Sicherheitsanforderungen nach welchen Normen zu stellen sind. Hier ist enger Austausch mit den Herstellern unabdingbar. Eine eindeutige Vorgabe existiert noch nicht. Eine vollständige Auslagerung

der Problematik an den Hersteller ist aber auch nicht möglich, da IT-Sicherheit erst organisationsübergreifend entsteht.

3.5 Hersteller / Systemhäuser

Ähnlich verhält es sich bei den Herstellern, sowohl für Fahrzeuge, Sub-Systeme als auch Komponenten. Im Vergleich zur funktionalen Sicherheit mit klar definierten Prozessen aus EN 5012x herrscht bei der IT-Sicherheit im Bereich Schienenfahrzeuge aktuell Verunsicherung, es fehlen klare Prozesse und abgestimmte Vorgehensweisen. Wenngleich die großen Systemhäuser bereits eine hohe Eigenkompetenz aufgebaut haben, fehlen oft übergeordnete Anforderungen aus einer IT-Sicherheits-Architektur auf Sub-System- und Komponenten-Ebene. Die Hersteller solcher Sub-Systeme und Komponenten erhalten also oft keine klaren Vorgaben, haben selbst aber nicht notwendigerweise die Kapazitäten, sich mit den Regularien auseinander zu setzen, die Normen durchzuarbeiten und die richtigen Ableitungen zu definieren. In diesem Zusammenhang lässt sich die Entwicklung beobachten, dass Hersteller, ähnlich wie bei der Umweltzertifizierung eines Produkts, häufig mit Dienstleistern zusammenarbeiten, die die Komplexität reduzieren und für den konkreten Anwendungsfall die richtigen Anforderungen herauskristallisieren.

3.6 Zwischenfazit

Zusammengefasst bergen die zunehmenden Anforderungen an IT-Sicherheit viele Herausforderungen für alle Beteiligten der Prozesskette, schaffen aber gleichwohl viele Chancen. Ohne Investition in Mitarbeiter, Prozesse und IT-sichere Produkte wird es nicht gelingen, die zukünftigen Anforderungen zu erfüllen. Der bisherigen Methode der Abschottung der Fahrzeuge von der Außenwelt steht der Wunsch des „always connected“, Live-Diagnose und Fernwartung von Sub-Systemen und Fahrzeugen entgegen, als auch die Tatsache, dass immer mehr elektronische Systeme Einzug finden, diese aber – anders als bisher – update-bar sein müssen, um zukünftig aufkommende Sicherheitslücken (z.B. in Betriebssystemen) zu beherrschen.

Die Wartungsfähigkeit und die Wartungshäufigkeit der Sub-Systeme in Fahrzeugen wird zunehmen. Der bisherige, oft nur physische Zugang, reicht hierfür nicht mehr aus und es werden Fernwartungskonzepte zwingend erforderlich. Vor diesem Hintergrund erhält die Wartungsschnittstelle in Bezug auf IT-Sicherheit in diesem Dokument besondere Aufmerksamkeit.

Die nachfolgenden Kapitel geben eine Handlungsanweisung für Hersteller und Betreiber speziell bezogen auf die Wartungsschnittstelle. Wie ist ein System, speziell dessen Wartungsschnittstelle zu konzipieren, wie zu bedienen?

4 Prozessbeschreibung

4.1 Überblick

Die TS 50701 wendet die Prozesse der IEC 62443 auf das V-Modell aus der für den Bahnbereich relevanten IEC 50126 an. Der absteigende Ast des V-Modells legt dabei die Grundlage für die Entwicklung durch die Hersteller und kann daher als „Anforderungsphase“ benannt werden. Sie ist im Wesentlichen durch die Analyse und Beschreibung der späteren Nutzung geprägt. Das heißt, sie ist von besonderem Interesse für den Betreiber und Käufer der Systeme und Komponenten. Hier werden sowohl die funktionalen als auch nicht funktionalen Anforderungen definiert und in den Einklang mit Risikobehandlung sowie Betriebsführung und Technikstrategie gebracht. Im Detail folgt das Vorgehen für die Anforderungsphase den folgenden Schritten:

1. Systemdefinition
2. Konzept
3. Risikoanalyse
4. Systemspezifikation
5. Komponentenspezifikation

Die Systemdefinition legt den Betrachtungsraum (System under Consideration, SuC) der Analyse fest. Es wird das Gesamtsystem beschrieben, Rahmenbedingungen und Grundannahmen getroffen und globale Ziele definiert.

In der Konzeptphase erfolgt die Präzisierung der technologischen Grundlagen. Es wird eine Systemarchitektur definiert, welche Security-Prinzipien wie beispielsweise Security by Design festgelegt, sowie das Vorgehen für die weiteren Phasen der Risikoanalyse und Spezifikation definiert. Weiterhin werden wichtige Grundlagen des späteren Betriebs in einem groben Betriebskonzept erfasst. Hier wird beispielsweise bereits auf Annahmen zum Security Information and Event Management (SIEM) und Betriebsführung von IT-Security-Komponenten eingegangen. Bereits in der Konzeptphase erfolgt die Schutzbedarfsfeststellung (initiale Risikoanalyse), welche das Zonen/Conduit-Konzept als Ergebnis hervorbringt.

In der Risikoanalyse wird das detaillierte Risikomanagement durchgeführt. Es werden die in der Folge im Detail beschriebenen Analyse-Phasen mit Betrachtung der Bedrohungen, Risiken, Eintrittswahrscheinlichkeit und anschließenden Risikobehandlung durch Security-Maßnahmen je Zone durchlaufen.

Das Ergebnis der Risikoanalyse ist die Grundlage für die Systemspezifikation. Ausgehend von den Security-Maßnahmen der IEC 62443-3-3 aus der Risikoanalyse, werden diese nun in konkrete Anforderungen für das System under Consideration (SuC) überführt. Hier soll klare Anforderungssprache (Muss/Soll/Info) verwendet werden. Alle Maßnahmen beziehen sich hier auf Security-Zonen, d.h. auf Systeme oder Teilsysteme.

In der anschließenden Komponentenspezifikation erfolgt die Zuordnung der Systemanforderungen auf Einzelkomponenten in der Architektur. Das kann alle Komponenten betreffen und beschränkt sich nicht nur auf Security-Komponenten. Wie detailliert die Anforderungen definiert werden, oder ob der Anforderer auf Systemebene (Phase 4) endet, kann projektbezogen definiert werden. Die Detailtiefe kann auch je Zone bzw. Teilsystem variieren. Dies wird häufig angewendet in Abhängigkeit von der Verfügbarkeit von Standard-Komponenten und Systemen, die Anforderungen bereits erfüllen und von Zielen der Austauschbarkeit.

Die Definitionen der Systemspezifikation und Komponentenspezifikation können im Projektmanagement als Lastenheft angesehen werden. Der Hersteller setzt auf dieser Grundlage auf und verfeinert, nach Bedarf, die Anforderungen, sodass die Phase 5 (Komponentenspezifikation) auf Herstellerseite durch das Pflichtenheft abgeschlossen wird.

Das Vorgehen zum Erhalt der Anforderungen ist zwar durch die Normen und Standards definiert, jedoch in der praktischen Anwendung eine große Herausforderung. Das Anforderungs-Team muss Wissen über die folgenden Bereiche mitbringen:

- Betrieb der OT-Systeme
- Betrieb von IT-Systemen und IT-Security-Systemen
- Risikomanagement
- Eindeutige Anforderungsdefinition
- Stand der Technik in OT und IT
- Kenntnis mindestens der Normen und Standards IEC 62443, TS 50701, EN 50159 sowie EN 50126

Dieser Prozess wird in der Folge beispielhaft an einer konkreten Anwendung analysiert und dokumentiert. Für ein Schienenfahrzeug und seine Subsysteme sowie die konkrete Anwendung der Wartungsschnittstelle mit Remote-Wartung wurde der Prozess durchlaufen und die Ergebnisse in diesem Bericht zusammengefasst.

4.2 Grundlagen und Ziele der Beteiligten

Aus Sicht des Fahrzeugbetreibers sind kostengünstige Lösungen in der Beschaffung und über den Lebenszyklus das Ziel. Die Hersteller der Lösungen wiederum haben das Ziel, ihre Produkte einer möglichst breiten Kundschaft anbieten zu können, um genau die Ziele des Betreibers wirtschaftlich umsetzen zu können. Aus diesen Zielen der Betreiber und Hersteller resultiert das Ziel, auch IT-Sicherheitslösungen im Bahnbereich nach Standard-Industrie-Normen zu definieren. Dies ermöglicht nicht nur bahnsystemweiten Einsatz dieser Komponenten, sondern auch in verwandten Industriezweigen, die ebenfalls auf derselben Norm aufbauen. Darüber ermöglicht die Anwendung von Standards die objektive Vergleichbarkeit von Produkten - ein entscheidender Vorteil für Betreiber bei der Ausschreibung mit Qualitätskriterien. Für den Hersteller wird so die Positionierung am Markt erleichtert. Diesen Grundlagenstandard stellt für die IT-Sicherheit bei Industrieanlagen die IEC 62443 dar. Daher kommt diese auch im Bahnbereich zum Einsatz.

4.3 IEC 62443

Die IEC 62443 teilt sich in mehrere Module auf, welche die unterschiedlichen Lebenszyklen und Rollen abbilden. Für die Bestimmung der notwendigen Security-Maßnahmen eines Systems beschreibt die IEC 62443-3-2 den zu durchlaufenden Prozess. Dies geschieht in zwei Stufen, mit dem Ziel zunächst Anforderungen auf Systemebene und anschließend auf Komponentenebene abzuleiten.

Kurz zusammengefasst folgt die Ableitung der Anforderungen dem folgenden Prinzip[3]:

1. Definition des Betrachtungsraumes (System under consideration - SuC)
2. Definition von Zonen um Systeme mit gleichem Schutzbedarf, basierend auf einer ersten Risikoanalyse

[3] Schritte 1-3 wurden in Bericht [1] durchgeführt, Schritte 4 und 5 sind Inhalt dieses Berichtes

3. Ableitung des notwendigen IT Sicherheits-Schutzlevel, genannt Security-Level (SL), für die jeweilige Zone
4. Ableitung der Maßnahmen aus vordefinierten Katalogen auf Systemebene nach IEC 62443-3-3
5. Ableitung der Maßnahmen aus vordefinierten Katalogen auf Komponentenebene oder Teilsystemebene nach IEC 62443-4-2

Aus diesem Ablauf wird ersichtlich: Es muss das zu schützende Gesamtsystem betrachtet werden. Aus dieser Betrachtung lassen sich dann die Anforderungen auf Teilkomponenten oder -systeme herunterbrechen, die Lieferanten bereitstellen können.

Das heißt, entweder der Betreiber muss eine Vorgabe zur Verteilung der Anforderungen in seinem Gesamtsystem machen oder über Technische Standards, Best Practices oder Ähnliches wird eine weithin akzeptierte Verteilung der Anforderungsanalyse etabliert. In beiden Fällen muss die Betreibersicht eingenommen werden, um den Lebenszyklus und die Bedrohungen sowie Risiken auf das System im Betrieb geeignet bewerten zu können. Das heißt, ohne eine definierte Betreibersicht, ist es einem Hersteller nicht möglich, vollständige und zielführende Anforderungen an die eigene Komponente und deren Entwicklung abzuleiten.

4.4 Risikokriterien

Ergänzend zur IEC 62443 legt die TS 50701 dafür eine ergänzende Methode zur Ermittlung der Risiken für sicherheitsrelevante Systeme fest. Darüber hinaus werden noch weitere Aspekte der VDE 0831-104 angewendet.

Für die Konkretisierung werden Attribute für die Eintrittswahrscheinlichkeit und die mögliche Auswirkung verwendet. Die Attribute sind nicht vorgegeben, sondern dürfen unternehmensspezifisch definiert werden. Für die Auswirkungsbeschreibung ist es ratsam, das Risikomanagement des Unternehmens zur Anwendung zu bringen. So können einheitliche Risikokriterien unternehmensweit verwendet werden. Für die Eintrittswahrscheinlichkeit sind zwei Ansätze best practice:

- Exposure und Vulnerability nach dem Vorschlag der TS 50701
- Ressourcen, Wissen und Ort des Angriffs nach dem Vorschlag der VDE 831-104

Nachdem das jeweilige Risiko durch Einzelbedrohungen, deren Eintrittswahrscheinlichkeit und Auswirkung konkretisiert wurden, wird durch die Anwendung von Security-Maßnahmen das Risikolevel reduziert. Dabei hilft das zuvor definierte SL-Level bei der Auswahl der geeigneten Security-Maßnahmen aus der IEC 62443-3-3.

Um das notwendige Maß der Risikoreduktion zu kennen, muss zu Beginn ein Ziellevel (akzeptiertes Restrisiko) festgelegt werden. Weiterhin ist es möglich, erhöhte Restrisiken zu akzeptieren. Dafür sollen vorab Kriterien definiert werden, die diese Risikoakzeptanz erlauben und wer sie übernehmen darf. Zum Beispiel:

- Wenn die Umsetzung weiterer Security-Maßnahmen zur Risikoreduktion auf das Ziellevel die Kosten aus einer möglichen Auswirkung im Abschätzungszeitraum von 10 Jahren übersteigt, kann das Risiko begründet akzeptiert werden.
- Bei Abweichungen aus dem Risikomanagementverfahren müssen der CISO und der Geschäftsführer/CEO explizit zustimmen.

Aus diesem Prozess lässt sich auch erkennen, dass nicht zwingend alle IEC 62443-3-3 Maßnahmen entsprechend dem definierten SL-Level umgesetzt werden (müssen). Es können aber auch zusätzliche

Maßnahmen definiert werden. Das risikobasierte Vorgehen ermöglicht also das nachvollziehbar dokumentierte und kommunizierte „Auslassen“ von Maßnahmen nach IEC 62443-3-3.

Wurden die Anforderungen nach IEC 62443-3-3 für die Systemebene abgeleitet, kann die Ableitung der Maßnahmen nach IEC 62443-4-2, d.h. auf Komponentenebene erfolgen. Ob eine Definition nach IEC 62443-4-2 für einen Betreiber sinnvoll ist, hängt von der geplanten Beschaffungsstrategie ab.

4.5 Modulare Einzelkomponenten

Sollen Einzelkomponenten durch Lösungen verschiedener Anbieter aus Sicht des Beschaffenden austauschbar sein, empfiehlt es sich die Security-Anforderungen auf die Komponenten aufzuteilen. Andernfalls wird ein späterer Herstellerwechsel wahrscheinlich zu Inkompatibilitäten oder Security-Schwachstellen führen. Sind Neubeschaffungen ganzer Systeme geplant, ist eine Definition auf Systemebene ausreichend.

Die Ablaufgrafik in Abbildung 3 stellt die Kombination der Anwendung der IEC 62443-3-3 und TS 50701 dar. Durch die jeweiligen Referenzen an den Seiten wird verdeutlicht, dass die Norm dabei vollständig umgesetzt und lediglich durch konkrete risikobasierte Bewertung (bottom-up) ergänzt wird.

4.6 Anforderungen Betreiber und Hersteller

Im Ergebnis werden die wesentlichen Anforderungen eines Betreibers und eines Herstellers umgesetzt.

Aus Sicht Betreiber:

- Nachvollziehbares Maß der IT-Sicherheit und des verbleibenden, akzeptierten Risikos des Systems und der Komponenten
- Konkrete, einheitliche Zuweisung von Anforderungen an Teil-Komponenten und Systeme, zur Ermöglichung von Wettbewerb
- Vergleichbarkeit der angebotenen Lösungen

Aus Sicht Hersteller:

- Eindeutige Anforderungen an Teil-Komponenten und Systeme, zur Vermeidung einer Variantenvielfalt, welche unwirtschaftlich für den Kunden und damit den Hersteller sind
- Wirtschaftlichkeit der angebotenen Komponenten und Systeme

Die praktische Umsetzung der Bedrohungs- und Risikoanalyse erfolgt üblicherweise tool-gestützt, um die Nachvollziehbarkeit und spätere Anpassbarkeit zu erhöhen. Hierbei existieren am Markt spezielle, kostenpflichtige Tools. Im Automotive- und Bahn-Bereich haben sich die letzten Jahre mehrheitlich Tools auf Basis von Excel durchgesetzt. Auch wenn die Möglichkeiten begrenzt sind und automatisierte Workflows nicht oder kaum unterstützt werden, ist über Excel ein Austausch unternehmensweit und über Unternehmensgrenzen hinweg möglich.

Die ERTMS Users Group – eine Interessensgemeinschaft europäischer Bahnen, wie DB, SNCF, ProRail, SBB und viele mehr – hat hierzu ihre Methode und das entsprechende Excel-Tool [2] veröffentlicht. Das Vorgehen entspricht dem in Abbildung 3 dargestellten Prozess.

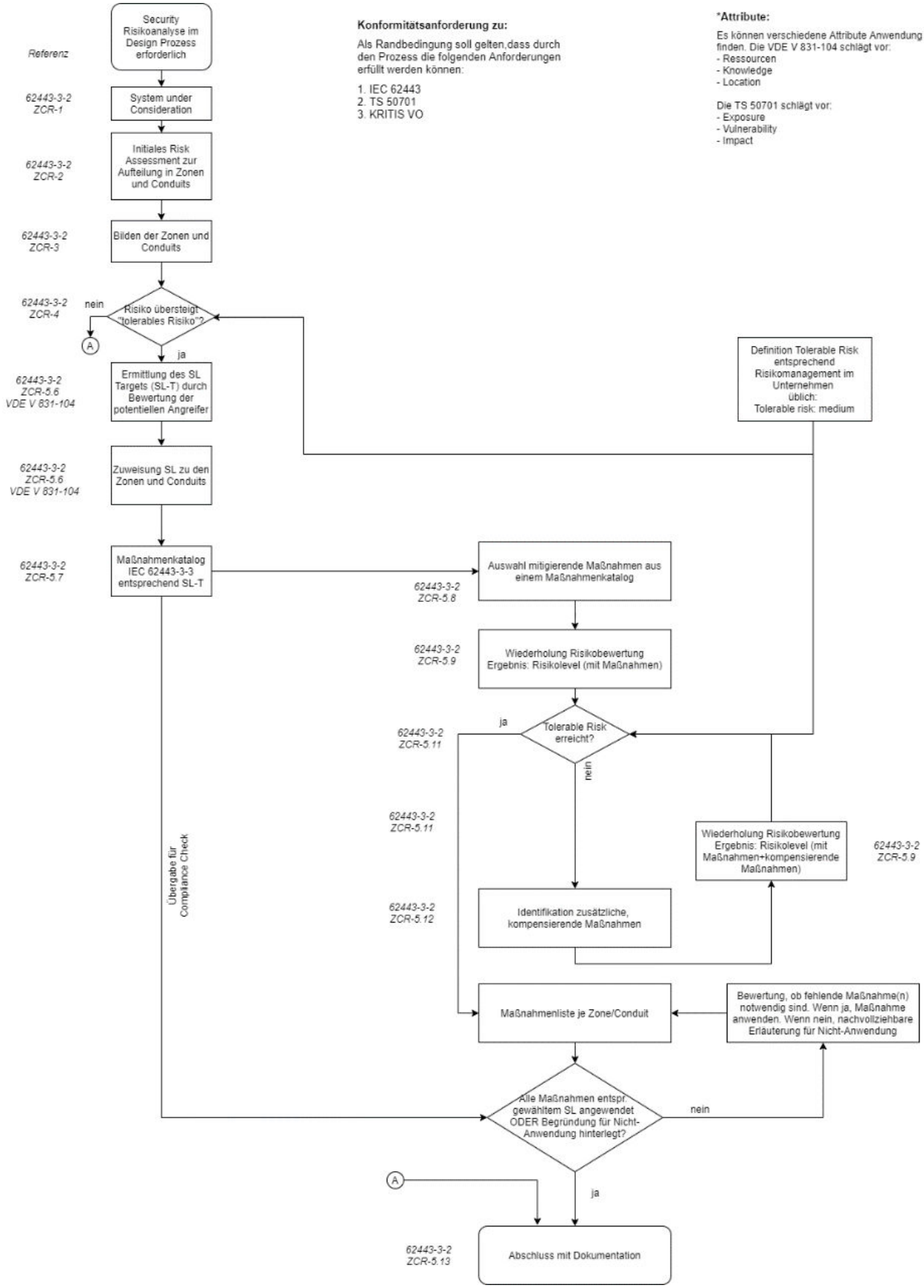

Abbildung 3: Prozessbeschreibung Risikoanalyse

5 Anwendung der IEC 62443 auf die Wartungsschnittstelle

5.1 Eigenschaften der Wartungsschnittstelle

Nachfolgend wird der Prozess zur Security Analyse und Anforderungsdefinition auf das Beispiel der Wartungsschnittstelle angewendet. Für diesen Zweck wird zunächst das System under Consideration (SuC), definiert. Das zu betrachtende System umfasst die folgenden Komponenten:

- Conduit zum Service-PC
- Conduit zum zentralen Update-Rechner für Fernwartung
- Türsteuerung
- Schnittstelle zum TCN-Netzwerk
- Sensoren der Türsteuerung
- Aktoren der Türsteuerung

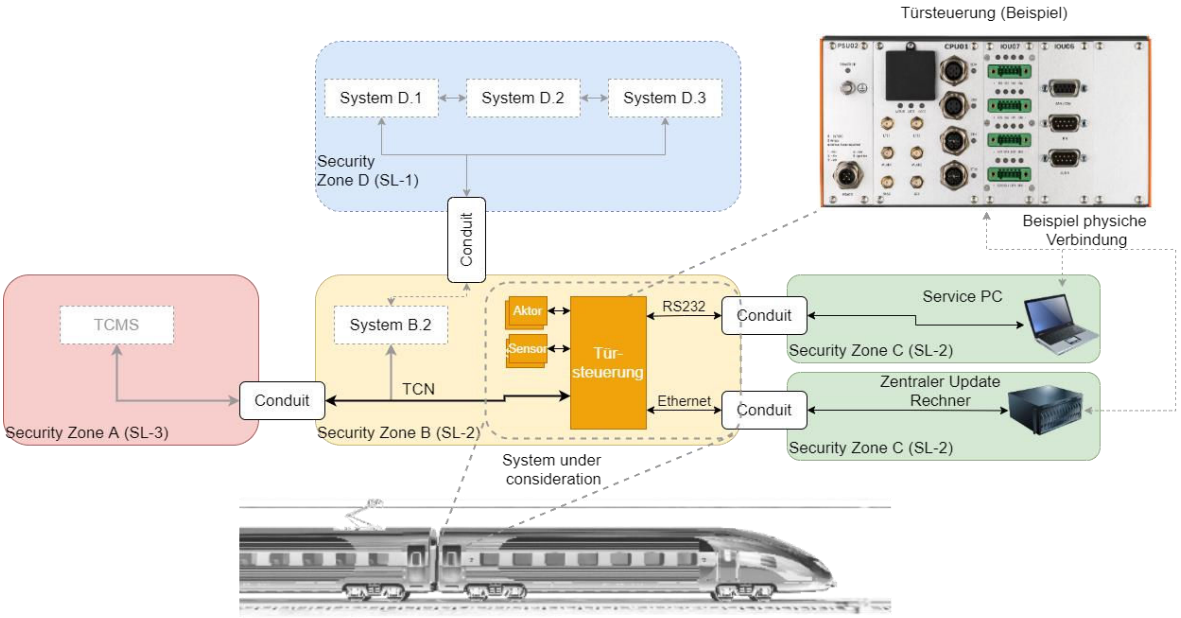

Abbildung 4: Kontext des "System under Consideration" – Türsteuerung

Folgende Rahmenbedingungen und Funktionen werden für das SuC (in diesem Beispiel bezogen auf das gewählte Subsystem Türsteuerung) angenommen bzw. definiert:

Türen in der Bahn sind sehr komplexe Subsysteme und setzen sich aus verschiedenartigsten Komponenten (Mechanik, Hydraulik, Elektronik, Dichtungen) zusammen. Sie obliegen hohen Beanspruchungen durch Umweltbedingungen, aber auch durch Fahrgäste und sind dadurch besonders wartungsintensiv.

Der Service-Zugang am Türensystem wird im Wesentlichen verwendet, um

- Statusinformationen sowie tiefergehende Diagnoseinformationen über den Zustand (Türstromprofile, Fehlermeldungen der Steuerung) zu erhalten,
- Ggf. Softwareupdates durchzuführen oder
- Konfigurationen (Türschließzeit, Schließdruck) auszulesen sowie zu setzen.

Türsteuerungssysteme sind typischerweise wie folgt in Fahrzeuge integriert:

Aufgrund der Vielzahl von Türpaaren sind i.d.R. auch in gleicher Anzahl Türsteuerungen verbaut. Aus Gründen der Zeiteffizienz bei der Instandhaltung und aus Kostengründen werden die Türsteuerungssysteme über eine Service-Schnittstelle an ein zentrales Diagnosesystem angebunden.

Daher wird die Definition des SuC um die folgenden Komponenten ergänzt:

- Lokale Service-Schnittstelle
- Schnittstelle zum zentralen Update-Rechner

Schnittstellen zu weiteren Geräten sowie zu den Sensoren oder Aktoren sind nicht in die Betrachtung einbezogen. In den folgenden Ausführungen bezüglich der Wartungsschnittstelle wird davon ausgegangen, dass eine initiale Risikoanalyse nach IEC 62443-3-2 [3] und eine Detailierung der Einteilung in Zonen durchgeführt wurde. Die folgenden Ausführungen nehmen die dort gefundene Einteilung in Security Zonen als gegeben an. Für die detaillierte Risikoanalyse kam der Bedrohungskatalog des BSI zur Anwendung. Dieser ist ebenfalls im Tool der ERTMS User Group hinterlegt [2].

Die Bedrohungen werden einzeln je Zone zur Anwendung gebracht. Für das vorliegende Beispiel wird die Security Zone B (Abbildung 4) herangezogen. Für den Bericht werden exemplarisch einige der wichtigsten Bedrohungen im Detail dargestellt, um die Herangehensweise und späteren Ergebnisse nachvollziehen zu können. Dabei wurde der Prozess aus Kapitel 4 zur Anwendung gebracht und daraus konkrete Maßnahmen bezogen auf Design, Nutzung und Pflege von Wartungsschnittstellen, festgelegt, die das jeweils identifizierte Risiko mindern bzw. beherrschbar machen. Folgende Analysen wurden unter der Annahme durchgeführt, dass vorab keine systematischen Security-Analysen und -Maßnahmen eingeführt wurden.

5.2 Bewertung konkreter Bedrohungen

5.2.1 T040 Bedrohung Verhinderung von Diensten (Denial of Service)

Denial of Service (DOS)-Attacken zielen darauf ab, Systeme so stark zu beschäftigen, dass ihre Verfügbarkeit für den eigentlichen Dienst eingeschränkt ist bzw. eine Überlast herbeigeführt wird, die im Extremfall zu einem Ausfall führt. Ziel der im Weiteren beschriebenen Maßnahmen ist es, dies zu verhindern.

DOS-Attacken können sowohl auf Netzwerkkomponenten zielen als auch auf Applikationssysteme. Im vorliegenden Fall wird zwischen einer lokalen Wartungsschnittstelle an der Applikation (im Beispiel der Türsteuerung) und einer Fernwartungsschnittstelle über das Netzwerk unterschieden.

5.2.1.1 Lokale Wartungsschnittstelle

Im Falle der lokalen Wartungsschnittstelle würde bei einem DOS-Angriff statt des Wartungs-Laptops ein Rechner des Angreifers angeschlossen werden, der das Applikationssystem attackiert. Um dies auszuschließen, muss die Wartungsschnittstelle über einen entsprechenden physischen Schutz verfügen, der den Anschluss solcher Rechner verhindert.

Anmerkung: DOS-Attacken werden üblicherweise so ausgeführt, dass die Ressourcen eines Systems über einen längeren Zeitraum sukzessive aufgebraucht werden. So lange müsste der zugehörige Rechner unbemerkt an die lokale Wartungsschnittstelle angeschlossen sein.

5.2.1.2 Fernwartungsschnittstelle

Im Folgenden werden die Auswirkungen einer DOS/DDOS-Attacke auf die Fernwartungsschnittstelle betrachtet.

Bedrohung	**T040 Bedrohung Verhinderung von Diensten (Denial of Service)**	
Kurzerläuterung der Bedrohung	Unterbrechung des Zugriffs auf die Wartungsschnittstelle, Verhindern des Services z.B. durch Fluten des Kommunikationskanals.	
Annahmen zur Bewertung	Im Status quo existiert kein Schutz gegen DoS.	
Risikobetrachtung	**Ergebnis**	**Erläuterung**
Einstufung Exposure	3	Ohne Security-Maßnahme direkter physischer Zugriff möglich.
Einstufung Vulnerability	3	Ohne implementierte Security-Maßnahme können Daten, Software oder Ähnliches irreversibel zerstört werden.
Einstufung Likelihood	5	Exposure+Vulnerability-1 (entspr. TS 50701)
Einstufung Impact	B	Es kommt zu Einschränkungen der Nutzung der Wartungsschnittstelle. Maximal finanzielle und Reputationsschäden können auftreten.
Resultierendes Risiko	Hoch	entspr. Risikomatrix
Risiko-Differenz	**3**	Ggü. Target-Risk: Low
Maßnahmen IEC 62443-3-3 System-Requirements	SR 5.1 SR 7.1 RE 1	
Maßnahmen IEC 62443-4-2 Komponenten-Requirements *Konkreter Vorschlag der Umsetzung*	Siehe nachfolgende Ausführungen	
Kompensierende Maßnahmen	Physischer Zugriffsschutz: physische Netztrennung, wenn nicht möglich, logische Netztrennung und Security Gateway	
Note: Bericht aus der Praxis	Zusätzlich physischer Zugriff vermeiden	
Risikobetrachtung *mit implementierten Maßnahmen*	**Ergebnis**	**Erläuterung**
Einstufung Exposure	1	Zugriff auf das Onboard-Netz eingeschränkt
Einstufung Vulnerability	2	Durch Authentifikation eingeschränkt.
Einstufung Likelihood	2	Exp+Vuln-1
Einstufung Impact	B	Es kommt zu Einschränkungen der Nutzung der Wartungsschnittstelle. Maximal finanzielle und Reputationsschäden können auftreten. Keine Absenkung Impact möglich.
Resultierendes Risiko	Low	Entspr. Risikomatrix
Risiko-Differenz	**1**	Das ermittelte Risiko entspricht dem Ziel-Risiko (Low)
Weitere kompensierende Maßnahmen	-	

Dies geschieht durch folgende Maßnahmen:

CR 5.1 Netzaufteilung

Die eingesetzten Netzwerkkomponenten (Switche, Router, Firewalls etc.) müssen in der Lage sein, die logische Segmentierung des Netzwerkes zur Abschottung der Funktionsbereiche zu gewährleisten.

CR 5.2 Schutz der Zonengrenze

Die eingesetzten Netzwerkkomponenten (Switche, Router, Firewalls etc.) müssen in der Lage sein, die Kommunikation an den Zonengrenzen zu überwachen und zu steuern, um die im Zonen- und Conduits-Modell definierte Trennung zu gewährleisten.

SR 5.4 Aufteilung von Anwendungen (Systemanforderung)

Das Steuerungssystem bestehend aus Netzwerkkomponenten und Applikationssystemen muss so ausgelegt sein, dass die Partitionierung von Daten, Anwendungen und Diensten auf der Grundlage der Kritikalität unterstützt wird, um die Umsetzung des Zonenmodells zu gewährleisten.

CR 7.1 RE1 – Schutz gegen DoS-Ereignisse

Die Komponenten (Applikationssysteme, Switche etc.) müssen so ausgelegt sein, dass sie während eines DOS-Angriffs in einer reduzierten Betriebsart arbeiten können.

Die Komponenten müssen die Kommunikationslast – z.B. durch Reduzierung der Übertragungskapazität an einer Netzwerkschnittstelle – managen können.

DOS-/DDOS-Attacken über die Fernwartungsschnittstelle können auf verschiedenen Ebenen des OSI-Schichtenmodells erfolgen:

- MAC-Adressen
- UDP-Telegrammen
- TCP-Verbindungsanfragen
- http-Anfragen

Eine Überflutung mit **MAC-Adressen** zielt darauf ab, ein Überlaufen der „Source Address“ Tabellen (speichern alle MAC-Adressen, mit denen der Switch kommuniziert) in einem Switch zu bewerkstelligen. Der Switch kann dann in eine Rückfallebene fallen, in der seine Funktion auf die eines Hubs reduziert wird, so dass alle Daten an alle Teilnehmer weitergeleitet werden. Dies muss durch eine entsprechende Konfiguration verhindert werden.

Eine Überflutung mit **UDP-Telegrammen** zielt darauf ab, die Verarbeitungs- und Reaktionsmöglichkeiten eines Applikations-Systems und ggf. einer vorgeschalteten Firewall zu überlasten. Sie nutzt den Mechanismus einer automatischen Rückmeldung (ICMP) für Ports aus, an denen keine Applikation angebunden ist. Ein Schutz dagegen kann eine Beschränkung der Anzahl möglicher ICMP-Pakete oder ein Ausfiltern von UDP-Telegrammen bestimmter Sender sein.

Eine Überflutung mit **TCP-Verbindungsanfragen** zielt darauf ab, die im Speicher eines Applikationssystems gehaltenen Informationen zu noch nicht vollständig aufgebauten TCP-Verbindungen überlaufen zu lassen, in dem der Vorgang des Verbindungsaufbaus vom anfragenden System nicht zu Ende geführt wird. Da eine Erhöhung der zugehörigen Speicherkapazität immer nur temporär eine Entlastung bieten kann, gibt es für solche Situationen spezielle Vorgehensweisen, wie z.B. das Löschen der Einträge in der Verbindungstabelle bei Überlastung und deren Rekonstruktion nach dem ggf. erfolgenden Eintreffen der finalen Bestätigung durch das anfragende System.

Bei einer Überflutung mit **http-Anfragen** werden so lange http-Verbindungen zu einem Applikationssystem aufgebaut, bis dessen Kapazität für solche Verbindungen überschritten ist und keine neuen Anfragen mehr bearbeitet werden können. Abhilfe können Maßnahmen zur SPAM-Abwehr (z.B. über Einträge zu verdächtigen Anfragenden in einer sogenannten Reputations-Datenbank) bringen. Eine Alternative ist eine Web Application Firewall (WAF) die den Zugriff über

Accesslisten (Whitelist: nur mit vordefinierten Teilnehmern bzw. Blacklist: mit explizit gesperrten Teilnehmern) steuert.

5.2.2 T028 Bedrohung Software-Schwachstellen oder -Fehler

Die Erfahrung zeigt, dass keine SW – auch wenn sie noch so gut geprüft wurde - fehlerfrei ist. Sicherheitslücken können unter Umständen von Angreifern ausgenutzt werden, um Schadsoftware einzuschleusen, unerlaubt Daten auszulesen oder Manipulationen vorzunehmen.

Die Gegenmaßnahmen setzen sich aus zwei Teilen zusammen: Zum einen dem Erkennen und Beheben solcher Sicherheitslücken, zum anderen der Erhöhung der Widerstandsfähigkeit (Resilienz) gegenüber der Ausnutzung solcher Schwachstellen. Ersteres muss über einen SW-Pflegeprozess geregelt werden, letzteres durch technische Maßnahmen.

Zu einem Softwarepflegeprozess gehören Prozesse, wie sie von der IEC 62443 im Teil 4-1 gefordert werden, um auch über zumindest einen Teil der Lebenszeit IT-Security zu gewährleisten. Hierzu gehören zum Beispiel auch Anforderungen an „Maintenance-Geräte“, die an der Wartungsschnittstelle angeschlossen werden dürfen. Ein Teil dieser Maßnahmen werden auch gesetzlich gefordert werden, sobald der Cyber Resilience Act (CRA) verabschiedet werden wird. Hierzu gehören unter anderem die Reaktion auf Schadensmeldungen und die Realisierung von Security Patches.

Im Rahmen der technischen Maßnahmen müssen im vorliegenden Beispiel einer Türsteuerung zwei Zugänge zum Applikationssystem betrachtet werden: Zum einen über die lokale Wartungsschnittstelle, zum anderen über das Netzwerk und die Fernwartungsschnittelle.

Bedrohung	Gefährdung 0.28 Software-Schwachstellen oder -Fehler	
Kurzerläuterung der Bedrohung	Erlangung von Zugriff auf Hard- oder Software und Manipulation der Informationen und damit des Systemverhaltens.	
Annahmen zur Bewertung	Annahme: Keine SW ist fehlerfrei; auch durch Prozesse im SIL-Bereich können Fehler nicht ausgeschlossen werden (Prozesse fokussieren hier hauptsächlich auf Safety Aspekte, weniger auf Security Kontext) Als zu betrachtendes System wurde die Türsteuerung mit ihrer Wartungsschnittstelle betrachtet, der evtl. Service-Laptop wurde nicht in die Betrachtung einbezogen. (SW-Fehler einer potentiellen Update-SW sind nicht Teil der Betrachtung)	
Risikobetrachtung	**Ergebnis**	**Erläuterung**
Einstufung Exposure	3	Ohne Security-Maßnahme direkter physischer Zugriff auf die Systeme möglich. Es ist kein Schutz gegen Malware irgendeiner Art vorhanden.
Einstufung Vulnerability	2	Die erfolgreiche Ausnutzung der Schwachstelle erfordert Kenntnisse über das Türsteuersystem. Mehrstufiger Angriff mit hoher Vorbereitungszeit.
Einstufung Likelihood	4	Exposure+Vulnerability-1 (entspr. TS 50701)
Einstufung Impact	C	Es kann zur Verfälschung der Daten kommen. Es ist möglich, dass Fehlhandlungen aufgrund von

		Fehlinformationen ausgeführt werden. Bei Änderung von Konfigurationsdaten der Türsteuerung kann es im schlimmsten Fall zur unzeitigen Öffnung oder zum Einklemmen von Reisenden kommen.
Resultierendes Risiko	Hoch	entspr. Risikomatrix
Risiko-Differenz	**3**	Ggü. Target-Risk: Low
Maßnahmen IEC 62443-3-3 System-Requirements	SR 3.4 SR 3.5 SR 3.6 SR 3.7 SR 5.1 RE 1 SR 5.2 RE 1 SR 6.2	
Maßnahmen IEC 62443-4-2 Komponenten-Requirements *Konkreter Vorschlag der Umsetzung*	Siehe nachfolgende Ausführungen	
Kompensierende Maßnahmen	-	
Note: Bericht aus der Praxis	Zusätzlich physischer Zugriff vermeiden	
Risikobetrachtung *mit implementierten Maßnahmen*	**Ergebnis**	**Erläuterung**
Einstufung Exposure	2	Zugriff eingeschränkt. Maximale physische Absicherung nachträglich ohne Tausch nicht möglich.
Einstufung Vulnerability	1	Konfigurationen angepasst und Dokumente nicht mehr einfach zugänglich.
Einstufung Likelihood	2	Exp+Vuln-1
Einstufung Impact	C	Es kommt zu Einschränkungen der Nutzung der Wartungsschnittstelle. Maximal finanzielle und Reputationsschäden können auftreten. Keine Absenkung Impact möglich.
Resultierendes Risiko	Medium	Entspr. Risikomatrix
Risiko-Differenz	**0**	Das ermittelte Risiko entspricht nicht dem Ziel-Risiko (Low), jedoch Medium (+1). Es kann akzeptiert werden. Weitere kompensierende, verhältnismäßige Maßnahmen (KRITIS Gesetz) konnten nicht identifiziert werden.
Weitere kompensierende Maßnahmen	-	

5.2.2.1 Lokale Wartungsschnittstelle

Im Falle der lokalen Wartungsschnittstelle sind folgende Maßnahmen zur Erhöhung der Resilienz gegenüber einer Attacke auf SW-Schwachstellen empfehlenswert:

CR3.4 Software- und Informationsintegrität

- Zugangsschutz durch Authentifikation der Benutzer (Wartungspersonal) über ein personengebundenes Passwort
- Integritätscheck im Ruhezustand und bei Übertragung (z.B. durch Zertifikate und HMAC)
- Ausgabe und Protokollierung einer von Mensch und Maschine verifizierbaren Prüfsumme, die einen Software- und Konfigurationsstand eindeutig identifiziert

CR 3.5: Eingabevalidierung

- Applikationssysteme sollten das Format und den Inhalt aller Benutzer-Eingaben validieren, um sicherzustellen, dass die Werte innerhalb der vorgesehenen Bereiche liegen und gültige Werte enthalten. Wird eine problematische oder ungültige Eingabe erkannt, sollten die Programme entweder einen vorbestimmten sicheren Wert verwenden oder in einen bekannten sicheren Zustand übergehen und gleichzeitig das Ereignis protokollieren.

CR 3.6: Vorbestimmte Zustände der Ausgänge

- Wechselt das Applikationssystem in einen sicheren Zustand, sollten die Ausgänge definierte Rückfallwerte annehmen.

CR 3.7: Fehlerbehandlung

- Wenn vom Applikationssystem ein Fehler erkannt wird, stellt es öffentlich keine Informationen zur Verfügung, die genutzt werden könnten, um das Gerät anzugreifen. Zum Auslesen solcher Fehlermeldungen sind spezielle Berechtigungen erforderlich, damit nicht authentifizierte Benutzer keine kritischen Informationen erhalten.

CR 6.2: Kontinuierliche Überwachung

- Das Applikationssystem protokolliert alle relevanten Aktionen und Ereignisse und übermittelt sie auf einem sicheren Weg (vgl. Maßnahmen aus Kap. 5.2.3.2) an einen zentralen Logging-Server.

Ergänzend sollte ein geeigneter physischer Zugangsschutz den Zugriff durch Unbefugte auf die betroffenen Systeme verhindern.

5.2.2.2 Fernwartungsschnittstelle

Neben den im Vorhergehenden bereits genannten Maßnahmen zur Erhöhung der Resilienz von Applikationssystemen gegenüber Attacken auf Sicherheitslücken in der SW sind für Fernwartungszugänge weitere Maßnahmen im Bereich des Netzwerkes erforderlich.

Dies sind im Einzelnen:

CR 5.1 Netzaufteilung

- Die eingesetzten Netzwerkkomponenten (Switche, Router, Firewalls etc.) müssen in der Lage sein, die logische Segmentierung des Netzwerkes zur Abschottung der Funktionsbereiche zu gewährleisten

CR 5.2 Schutz der Zonengrenze

- Die eingesetzten Netzwerkkomponenten (Switche, Router, Firewalls etc.) müssen in der Lage sein, die Kommunikation an den Zonengrenzen zu überwachen und zu steuern, um die im Zonen- und Conduits-Modell definierte Trennung zu gewährleisten.

5.2.3 T030 Unberechtigte Nutzung oder Administration von Geräten und Systemen

Der Zugriff auf Systeme darf grundsätzlich nur von dazu berechtigten Personen erfolgen. Dies gilt insbesondere für Systeme mit Safety-Bezug, wie die Türsteuerung und damit auch für die Wartungsschnittstelle. Wie eingangs erwähnt, dient diese nicht nur zum Auslesen von Diagnosedaten, sondern auch zum Update der Software, konfigurieren oder zur Behebung von Fehlern. Eine unberechtigte administrative Benutzung könnte die Konfiguration der Türsteuerung derart manipulieren, dass sich Türen beispielsweise nicht mehr öffnen, verzögert öffnen, die Öffnungszeiten verkürzt werden oder Türen nicht mehr schließen.

Als Grundschutz sollte ein geeigneter physischer Zugangsschutz den Zugriff durch Unbefugte auf die betroffenen Systeme verhindern. Wartungsarbeiten sollten nur auf geschütztem Betriebsgelände durchgeführt werden. Im Fahrzeug sind die Komponenten Zugriffsgeschützt zu verbauen. Generalschlüssel, wie z.B. Vierkantschlüssel, sind für sicherheitsrelevante Komponenten zu vermeiden.

Bedrohung	Gefährdung 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen	
Kurzerläuterung der Bedrohung	Administration der Türsteuerung über die Wartungsschnittstelle durch unberechtigte Personen	
Annahmen zur Bewertung	Annahme: administrativer Zugriff auf die Wartungsschnittstelle ist sowohl lokal vor Ort als auch über Fernwartungslösungen möglich.	
Risikobetrachtung	**Ergebnis**	**Erläuterung**
Einstufung Exposure	3	Ohne Security-Maßnahme direkter physischer Zugriff auf die Systeme durch anstecken eines Laptops oder Fernwartungszugang möglich.
Einstufung Vulnerability	3	Ohne Schutz gegen unberechtigte Nutzung oder Administration besteht hohe Verwundbarkeit. Das Anschließen eines Laptops oder die Eingabe der IP-Adresse ist ausreichend.
Einstufung Likelihood	5	Exposure+Vulnerability-1 (entspr. TS 50701)
Einstufung Impact	B	Da die Türsteuerung safety-relevant ist und über die Wartungsschnittstelle Konfigurationen geändert werden können, könnte es im Falle einer sich bei voller Fahrt öffnenden Tür zu vereinzelten Todesfällen kommen.
Resultierendes Risiko	Sehr hoch	entspr. Risikomatrix
Risiko-Differenz	**4**	Ggü. Target-Risk: Low
Maßnahmen IEC 62443-3-3 System-Requirements	SR 1.1; SR 1.1 RE 1; SR 1.1 RE 2; SR 1.1 RE 3; SR 1.2; SR 1.2 RE 1; SR 1.3; SR 1.5; SR 1.5 RE 1; SR 1.7; SR 1.7 RE 2; SR 1.8; SR 1.10;	

	SR 1.11; SR 1.13; SR 1.13 RE 1; SR 2.1; SR 2.1 RE 1; SR 2.1 RE 2; SR 2.1 RE 4; SR 2.6; SR 2.8; SR 2.8 RE 1; SR 5.1 RE 3; SR 5.2; SR 5.2 RE 1; SR 5.2 RE 2; SR 6.1; SR 6.2	
Maßnahmen IEC 62443-4-2 Komponenten-Requirements *Konkreter Vorschlag der Umsetzung*	Siehe nachfolgende Ausführungen	
Kompensierende Maßnahmen	Physischer Zutrittsschutz + zugriffsgeschützte Verbauung der Komponenten im Fahrzeug	
Note: Bericht aus der Praxis		
Risikobetrachtung *mit implementierten Maßnahmen*	**Ergebnis**	**Erläuterung**
Einstufung Exposure	1	Nach Umsetzung der Maßnahmen starker Zugriffsschutz gegeben
Einstufung Vulnerability	1	Bei vollständiger Umsetzung sind gute Hacking-Kenntnisse erforderlich, um Zugriff auf die Wartungsschnittstelle zur erhalten.
Einstufung Likelihood	1	Exp+Vuln-1
Einstufung Impact	B	Durch den Zugriff von nur noch berechtigten und entsprechend geschulten Personen ist die Gefährdung durch unberechtigte Nutzung zum Herbeiführen eines Personenschadens maximal reduziert.
Resultierendes Risiko	Medium	Entspr. Risikomatrix
Risiko-Differenz	**1**	Das ermittelte Risiko entspricht nicht dem Ziel-Risiko (Low), jedoch Medium (+1). Es kann akzeptiert werden.
Weitere kompensierende Maßnahmen	Umsetzen eines speziellen Werkstatt Modus, sodass nur in diesem über die Wartungsschnittstelle auf die Türsteuerung zugegriffen werden kann.	

5.2.3.1 Lokale Wartungsschnittstelle

Im Falle der lokalen Wartungsschnittstelle sind folgende Maßnahmen zur Vermeidung von unberechtigter Nutzung oder Administration empfehlenswert:

CR 1.1 Identifizierung und Authentifikation von menschlichen Nutzern

Die Komponente mit Wartungsschnittstelle muss die Fähigkeit haben, alle menschlichen Nutzer nach IEC 63443-3-3 SR 1.1 zu identifizieren und zu authentifizieren. Dabei muss das Prinzip der minimal erforderlichen Rechte unterstützt werden.

- Für die Verwendung der Wartungsschnittstelle ist eine eindeutige Identifizierung und Authentifikation erforderlich. Sofern Benutzername und Passwort eingesetzt werden, müssen diese personenbezogen sein.

- Auf Grund der Kritikalität des lokalen Zugriffs sollte nach Möglichkeit ein zweiter Faktor zur Identifizierung und Authentifikation eingesetzt werden.

CR 1.2 Identifizierung und Authentifikation von Softwareprozessen und Geräten

Komponenten müssen die Fähigkeit haben, sich selbst zu identifizieren und sich gegenüber anderen Komponenten zu authentifizieren. Bei der Wartungsschnittstelle steht hier insbesondere der Wartungslaptop im Fokus. Bei diesem muss es sich um ein bekanntes Gerät handeln, welches zum Anschluss berechtigt ist. Dies sollte durch ein Zertifikat realisiert werden.

Andere, unbekannte Geräte dürfen seitens der Wartungsschnittstelle nicht zur Übertragung von Daten akzeptiert werden, um Safety-Funktionen nicht zu gefährden.

CR 1.3 Nutzerkontenverwaltung

Die Komponenten müssen die Fähigkeit bieten, die Verwaltung aller Nutzerkonten direkt zu unterstützten oder in ein System (z.B. zentrales Service Gateway – siehe Abbildung 6) zu integrieren, dass Nutzerkonten nach IEC 62443-3-3 SR 1.3 verwaltet.

CR 1.5 Verwaltung der Authentifizierer

Neben einer Kennung ist zum Nachweis der Identität ein Authentifizierer notwendig (z.B. Token, symmetrische Schlüssel, PKI, Passwörter, Schlüsselkarten).

- Authentifizierer müssen ausgetauscht werden können, Standardpasswörter sind nach Inbetriebnahme zu ändern.
- Für Übertragung und Speicherung sind geeignete kryptografische Schutzmechanismen einzusetzen.

CR 1.7 Stärke der Authentifikation durch Passwörter

Komponenten, die Passwörter zur Authentifikation verwenden, müssen die Fähigkeit habe, eine konfigurierbare Stärke von Passwörtern gemäß international anerkannten und bewährten Passwortleitlinien zu bieten.

- Komponenten müssen die Fähigkeit haben, eine minimale und eine maximale Lebensdauer von Passwörtern für alle Nutzer durchzusetzen.

CR 1.8 PKI-Zertifikate

Falls eine für die betrachtete Komponente relevante Public-Key-Infrastruktur (PKI) zum Einsatz kommt, muss die Komponente die Fähigkeit haben, eine solche PKI entsprechend bewährter Verfahren zu betreiben oder öffentliche Schlüsselzertifikate von einer bestehenden PKI beziehen zu können. Im Falle der Komponente mit Wartungsschnittstelle muss diese in der Lage sein, ein Schlüsselzertifikat anzufordern (z.B. nach X.509).

Anmerkung: Der Vertrauensgeber der Zone sollte über eine vertrauenswürdige Chain-of-trust an Wartungsschnittstellen angeschlossene Geräte zertifizieren.

CR 1.10 Rückmeldung vom Authentifizierer

Die Komponente muss die Fähigkeit bieten, während des Authentifikationsvorganges die Rückmeldungen von Authentifikationsinformationen zu verdecken, z.B. durch Anzeigen von Sternchen bei Eingabe des Passworts.

CR 1.11 Erfolglose Anmeldeversuche

Es sollen nicht unbegrenzt fehlerhafte Anmeldeversuche an der Wartungsschnittstelle möglich sein.

CR 2.1 Durchsetzung der Autorisierung

Die Komponente muss einen Mechanismus für die Durchsetzung der Autorisierung aller identifizierten und authentifizierten Nutzer bereitstellen. Nur die Personen, denen entsprechende Rollen (z.B. Wartung) zugewiesen wurden, dürfen durch das System berechtigte Wartungsarbeiten durchführen. Jemand, dem diese Rolle nicht zugewiesen ist, wird seitens der Wartungsschnittstelle abgewiesen.

Bei besonders kritischen Handlungen wie z.B. die Veränderung der Dauer der Türöffnung ist ggf. eine doppelte Zustimmung / vier-Augen-Prinzip zu implementieren.

CR 2.8 Prüfbare Ereignisse

Die Komponente muss die Fähigkeit haben, Zugriffe zu protokollieren. Die Protokolle sollten dabei beinhalten, wer wann wie auf die Wartungsschnittstelle zugegriffen hat und welche Handlung ausgeführt wurde.

Die Ereignisdaten sollten an ein zentrales System zur Auswertung übergeben werden können.

CR 6.1 Zugriffsmöglichkeit auf Ereignisprotokolle

Der Zugriff auf die Ereignisprotokolle sollte in Aufgabentrennung erfolgen, sprich, derjenige, der Wartungsaufgaben durchführt sollte keinen Zugriff auf die Protokolle haben, um Manipulationen vorzubeugen.

5.2.3.2 Fernwartungsschnittstelle

Neben den im Vorhergehenden bereits genannten Maßnahmen zum Schutz der lokalen Wartungsschnittstelle vor unberechtigter Nutzung sind für die Fernwartungszugänge weitere Maßnahmen im Bereich des Netzwerkes erforderlich.

Dies sind im Einzelnen:

CR 1.1 RE 2 Multifaktor-Authentifikation für nicht vertrauenswürdige Netze

Die Fernwartung muss mit einem zweiten Faktor, z.B. Token geschützt werden. Die Authentifikation muss nicht durch die Komponente selbst erfolgen, sondern kann an den Netzaußenbereich an ein Security Gateway ausgelagert werden. Sinnvoll wären hier der Einsatz von PAM-Lösungen (Privileged Access Management) zur Fernwartung.

CR 1.13 Zugriff über nicht vertrauenswürdige Netze

Da eine Fernwartung im Regelfall von außerhalb des Schienenfahrzeugs erfolgt und dafür Zugriff über das Internet erforderlich ist, ist diese Kommunikation-Verbindung kryptografisch abzusichern. Auch

dies muss nicht durch die Komponente erfolgen, sondern kann an ein Security Gateway ausgelagert werden.

CR 1.13 RE 1 Genehmigung ausdrücklicher Anmeldebegehren

Eine Fernwartung darf nur nach ausdrücklicher Zustimmung zugelassen werden. Dies kann über die Komponente geregelt werden, in dem ein bestimmter Zustand (technische wie betriebliche Vorgaben) vorherrschen muss, um überhaupt Zugriff erlangen zu können (z.B. Werkstattmodus). Dann wird der Zugriff nach Identifizierung und Authentifikation genehmigt. Ein dauerhafter Zugriff ist zu vermeiden.

Die Komponente muss die Fähigkeit bieten, die Fernzugriffssitzungen entweder automatisch, z.B. durch Ablauf der gewährten Wartungszeit oder manuell zu beenden, z.B. durch Umschalten von Werkstattmodus in Betrieb.

CR 5.1 Netzaufteilung

Die eingesetzten Netzwerkkomponenten (Switche, Router, Firewalls etc.) müssen in der Lage sein, die logische Segmentierung des Netzwerkes zur Abschottung der Funktionsbereiche zu gewährleisten.

Die Wartungsschnittstelle sollte isoliert sein und keine weiteren Verbindungen innerhalb des Netzwerkes zulassen.

CR 5.2 Schutz der Zonengrenze

Die eingesetzten Netzwerkkomponenten (Switche, Router, Firewalls etc.) müssen in der Lage sein, die Kommunikation an den Zonengrenzen zu überwachen und zu steuern, um die im Zonen- und Conduits-Modell definierte Trennung zu gewährleisten.

SR 5.2 RE 1 standardmäßig verweigern, zulassen von Ausnahmen (Deny by default, allow by exception)

In der Fernwartungskette muss sichergestellt sein, dass Netzwerkverkehr standardmäßig abgelehnt und nur in Ausnahmefällen zugelassen wird.

Im vorangegangenen Kapitel 5.2 wurden am konkreten Beispiel der Wartungsschnittstelle der Prozess der Risikobewertung und Maßnahmendefinition durchgeführt und anhand dreier Beispiele dargestellt. Es wurden weitere Bedrohungen mit Relevanz auf die Wartungsschnittstelle analysiert. Die Bewertung ist aus Gründer der Lesbarkeit des Dokuments im Anhang zu finden.

6 Anwendung abgeleiteter Maßnahmen

Aufbauend auf der Risikoanalyse für das gewählte Beispiel der Wartungsschnittstelle mit Fokus Türsteuerung wurden mehrere relevante Maßnahmen zur Risikobeherrschung identifiziert. Allen Maßnahmen liegen einerseits die IEC 62443-3-3 sowie -4-2 Maßnahmen zugrunde, anderseits wurden kompensierende, d.h. ergänzende Maßnahmen hinzugefügt. Der Nachweis einer vollständigen Übereinstimmung mit der IEC 62443-4-1 und 4-2 für Komponenten bzw. IEC 62443-3-* für Betreiber von Systemen setzt die Erfüllung sämtlicher Maßnahmen der Norm voraus.

Dieses Kapitel fasst die Maßnahmen zur Beherrschung der IT Security kompakt zusammen und beleuchtet neben den technischen Maßnahmen, die in Kapitel 5.2 erarbeitet wurden, auch Maßnahmen für die Organisation. Darüber hinaus nennt der Bericht ergänzende allgemeingültige Empfehlungen und geht auf die Beschränkungen für Bestandsfahrzeuge ein.

6.1 Übergreifende Maßnahmen in der Organisation

Grundsätzlich betrachten wir folgenden Maßnahmen als vergleichsweise einfach umsetzbar und besonders relevant:

1. Awareness
2. Secure Procedures
3. Assetmanagement
4. Vulnerability Managementprozess Hersteller und Betreiber
5. Physische Security
6. Secure Configuration
7. Security Monitoring

Die Maßnahmen sind in der Reihenfolge der schnellsten Umsetzbarkeit und Wirkung aufgeführt. Gleichzeitig bauen sie teilweise aufeinander auf und erfordern daher diese Reihenfolge. Folgend sind die Maßnahmen und ihre Wirkung kurz beschrieben.

Awareness aller Mitarbeiter, insbesondere jedoch der Mitarbeiter mit Zugriff und Arbeiten an den Wartungsschnittstellen und Türsteuerungen, bildet eine Grundlage für alle weiteren Maßnahmen. Dadurch werden einerseits das Risiko und die möglichen Auswirkungen (Impact) adressiert. Hierüber entstehen Sensibilität und Verständnis für die kommenden Maßnahmen. Gleichzeitig wird sofort die Aufmerksamkeit für mögliche bösartige Akteure oder ungewöhnliche Veränderungen am Fahrzeug erhöht.

Auf Basis einer Grund-Sensibilisierung können **sichere Prozeduren** eingeführt werden, die im Ablauf z.B. die physische Manipulationsfreiheit der Systeme, aber auch andere Arbeitsschritte wie Multi-Control-Prinzipien etc. umfassen. Damit werden die handelnden Personen maximal in den Erhalt des Security-Levels einbezogen.

Als wichtigste Grundlage für technische Maßnahmen wird ein **Assetmanagement** eingeführt, das auch ein Konfigurationsmanagement umfasst. Weiterhin sind Netzstrukturpläne erforderlich, die die Verbindungen und Abhängigkeiten zueinander dokumentieren. Darüber lassen sich u.a. Policies an den Schnittstellen dokumentieren. Hier ist auch die Kritikalität je Asset aufzunehmen, um darzustellen, inwiefern dieses Asset für das zentrale Ziel – ein Schienenfahrzeug sicher (safe und secure) zu betreiben – relevant ist. Das heißt, häufig vorhandene, kaufmännische Assetmanagement-Systeme sind meist nicht ausreichend, da sie nicht die notwendige Aktualität und Detailtiefe zur Erfassung von Software- und Firmware-Ständen usw. erlauben. Es ist jedoch stark zu empfehlen das

kaufmännische System mit dem IT-Asset-Management System zu verbinden, um eine gemeinsame „Wahrheit“ (single source of truth) hinsichtlich Anzahl und Ort von Systemen zu haben.

Vulnerability Management beschreibt das koordinierte Vorgehen, Sicherheitslücken in Systemen aufzudecken, zu bewerten und dokumentieren sowie entsprechend der Bewertung zu beheben. Dies kann im einfachsten Teil aus einer Suche nach Updates während einer regulären Wartung bestehen. Ist ein höheres Maß an Aktualität erforderlich, können Security-Updates auch neue Wartungstermine erfordern, oder je nach Fähigkeit und Kritikalität der Systeme auch Over The Air Updates nötig machen.

Als nächsten Schritt können die einfachsten, technischen Maßnahmen hinzugefügt werden. Dies sind **physische Schutzmaßnahmen**. Diese Schutzmaßnahmen können die Nachrüstung einfacher Abdeckungen sein, die mindestens mit Werkzeug entfernt werden müssen. Kritische Schnittstellen sollten hinter verschlossenen Türen/Klappen/Abdeckungen liegen, die durch einen Schließmechanismus geschützt sind. Dies erlaubt einerseits einen schnellen Zugriff, andererseits zusätzlichen Schutz. Das Schließsystem sollte ein Schlüssel sein, der nur den Personen mit notwendigem Zugriff ausgehändigt wird. Vierkant, Dreikant, etc. stellen keine Erhöhung des Schutzes dar.

Die meisten Systeme sind **konfigurierbar**. Es lassen sich Einstellungen hinsichtlich Logging, Zugriffsrechten, Schutz von Daten, Schnittstellen usw. treffen. Wenn bisher nur der Hersteller des Produkts diese Rechte hat, dann sollte dies geändert werden. Die Hoheit über die Konfiguration sollte beim Betreiber liegen. Auch für zukünftige Cloud-basierenden Wartungs- und Konfigurationszugriffe muss ein Zugriff immer durch den Betreiber genehmigt werden. Die Konfigurationen sind nach dem „least privilege“ Prinzip einzustellen, d.h. möglichst wenige Rechte einräumen, so dass der Zugriff und die Möglichkeit zur Veränderung nur durch eine möglichst geringe Anzahl von Personen und vorher definierten Schritten möglich sind. Dies erhöht die Zugriffsschwelle.

Security-Monitoring erlaubt dem Anwender, Angriffe in der Entstehung und vor dem Eintreten der Auswirkung zu erkennen. Grundlage für Security-Monitoring legt ein Assetmanagement, welches die Übersicht über relevante Systeme und die zu überwachenden Kommunikationsbeziehungen gibt. Für das Security Monitoring muss zentral ein Auswertesystem – Security Incident und Event Monitoring (SIEM) – und lokal jeweils eine Möglichkeit zum Generieren der Informationen implementiert werden.

Die Integration eines Security Monitorings verlangt darüber hinaus eine Datenmanagementstrategie, d.h. eine Konzeption an welchen Stellen ggf. Datenvorverarbeitung erfolgt, um das Netzwerk nicht zu überlasten. Zudem müssen Use-Cases geschrieben und Onboarding-Prozesse ausgeführt werden.

Üblicherweise werden die Assets nach ihrer Relevanz in das SIEM aufgenommen. Zunächst werden dann einfache, regelbasierte Use-Cases umgesetzt, die z.B. Brute-Force Angriffe erkennen können. Erst mit zunehmender Systemreife (Maturität) sind weitere Angriffserkennungen über z.B. künstliche neuronale Netze, Deep-Learning oder Machine-Learning sinnvoll.

6.2 Besonderheiten Bestandstechnik

Häufig war diese Compliance allerdings nicht explizit gefordert und ist für im Bestand befindliche Fahrzeuge und Systeme ohne komplette Neuentwicklungen nicht umsetzbar. Für diese Fälle sind mindestens folgende allgemeinen Maßnahmen anzuwenden:

In der praktischen Anwendung sind für die meisten Betreiber vor Allem die Bestandsfahrzeuge im Fokus. Selbst wenn in naher Zukunft neue Fahrzeuge beschafft werden sollen, wird nur sukzessive auf neue Fahrzeuge umgestellt und die Bestandsflotte häufig noch sehr lange mitgeführt. Gleichzeitig verlangen teils gesetzliche Vorgaben, in jedem Fall aber die tatsächliche Bedrohungssituation ein Handeln auch im Bestand.

Für Bestandsfahrzeuge ist es unter dem Gesichtspunkt der Verhältnismäßigkeit in der Regel nicht möglich, alle als relevant identifizierten Maßnahmen zur Risikobeherrschung wie in einem Neufahrzeug umzusetzen. In diesem Fall müssen dem Risiko angemessene, alternative Maßnahmen ergriffen werden. Daraus kann ein erhöhtes Restrisiko verbleiben, welches bewusst eingegangen werden kann.

Um trotzdem eine adäquate Risikobehandlung zu erlauben, werden folgende Schritte empfohlen:

1. Prüfung der Maßnahmenliste auf Maßnahmen, die nachträglich unter dem Gesichtspunkt der Verhältnismäßigkeit hinzugefügt werden können
2. Priorisierung der Maßnahmen nach dem größten Nutzen zur Beherrschung der Risiken
3. Identifikation der offenbleibenden Risiken und Einschätzung des jeweiligen Restrisikos
4. Definition der Risikoakzeptanz oder des Risikotransfers, z.B. auf Versicherungen oder andere Verfahren

Im Bestand sind also besonders Grundlagenmaßnahmen der Prozesse und IT-Systeme im Unternehmen zu schaffen. Diese Maßnahmen legen für alle Bestandssysteme und Neuanschaffungen die Grundlage, ein sicheres (secure) System aufbauen zu können. Technisch beschränken sich die weiteren Maßnahmen vor Allem auf die Detektion und Planung einer Reaktion. Das nachträgliche Hinzufügen von IT-Security Fähigkeiten in bestehender Software und Hardware ist dagegen technisch oft nicht möglich und/oder unverhältnismäßig.

7 Bestands-Beispiel aus der Praxis

Als Praxisbeispiel für die Netzwerkumgebung in einem Schienenfahrzeug und die dazugehörige Wartungsschnittstelle wird eine Straßenbahn angenommen, in deren Netzwerk die typischen Subsysteme und Komponenten in verallgemeinerter Form dargestellt sind.

Ausgehend von der Netzwerkarchitektur und unter Berücksichtigung der obengenannten theoretischen Herleitung der IT-Security an Wartungsschnittstellen, kann man in einem allgemeingültige Zwischenfazit zusammenfassen, mit welchen Herausforderungen die Verantwortlichen für die Sicherung der Schnittstelle konfrontiert sind und wie der Lösungsweg aussieht.

7.1 Security-Zonen typischer Schienenfahrzeuge

Die Kommunikationssysteme auf einem Straßenbahnfahrzeug lassen sich grob in die Teile Fahrzeugtechnik, Betreibersysteme und Fahrgastbereich einteilen, was in Abbildung 5 dargestellt ist. Dies kann man auch als die drei großen IT-Security Zonen auffassen. Hinzu kommen noch Strukturen auf der Landseite, die hier jedoch nur bis zu den verbindenden Conduits betrachtet werden. Für die technische Auslegung und Funktion der Systeme im Bereich der Fahrzeugtechnik sind typischerweise die FZ-Hersteller zuständig. Betreibersysteme werden vom Betreiber verantwortet und vom diesem beeinflusst, wohingegen der Fahrgast ausschließlich mit Systemen im Fahrgastbereich interagiert.

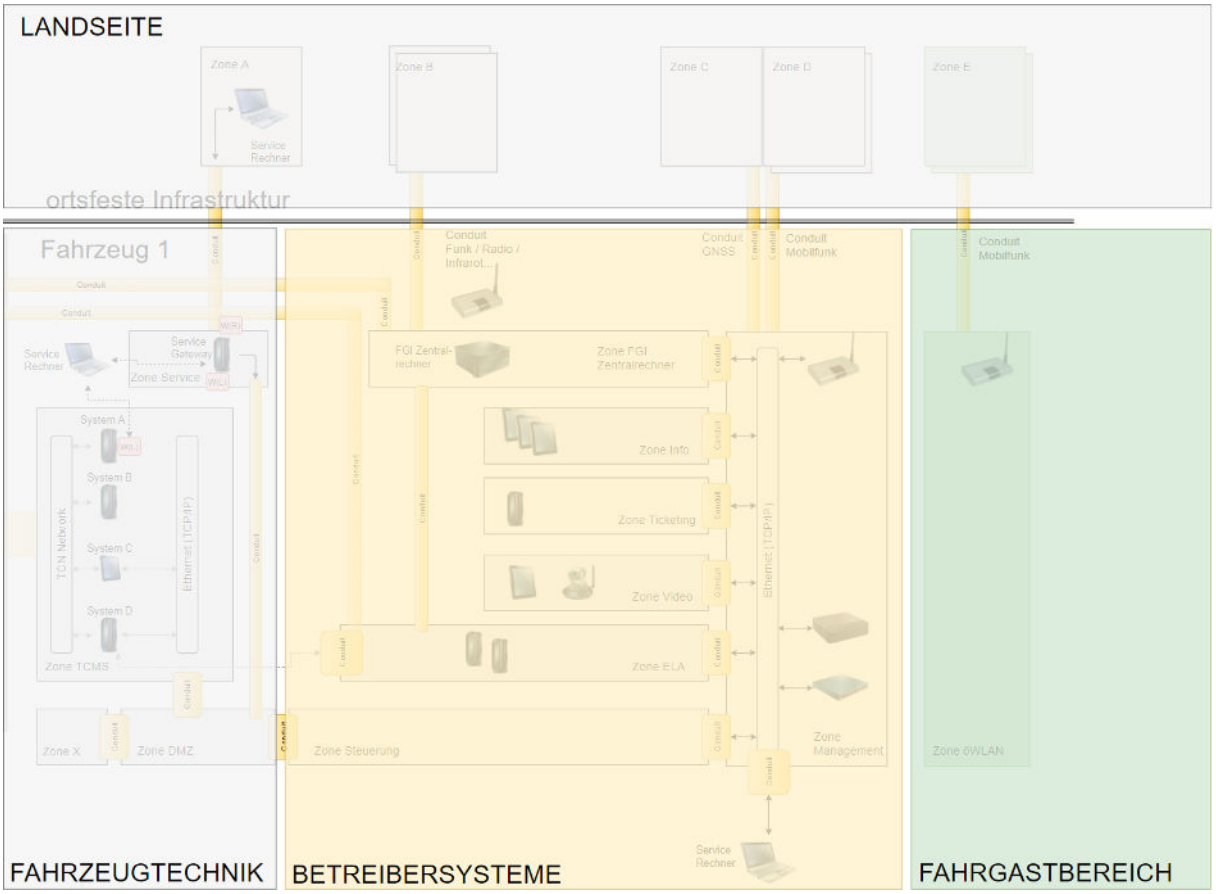

Abbildung 5: Schematische Einteilung der Kommunikationsebenen im Straßenbahnfahrzeug

Bei einem eingehenderen Blick in die Architektur des Fahrzeugs zeigen sich innerhalb der übergeordneten Kommunikationsbereiche vielfältige Subsysteme. Die Abbildung 6 Abbildung 6:

Kommunikationsstruktur und IT-Security Zonen einer verallgemeinerten Straßenbahnzeigt wesentliche Details der Kommunikationsstruktur und die Einteilung in IT-Security-Zonen für eine verallgemeinerte Straßenbahn.

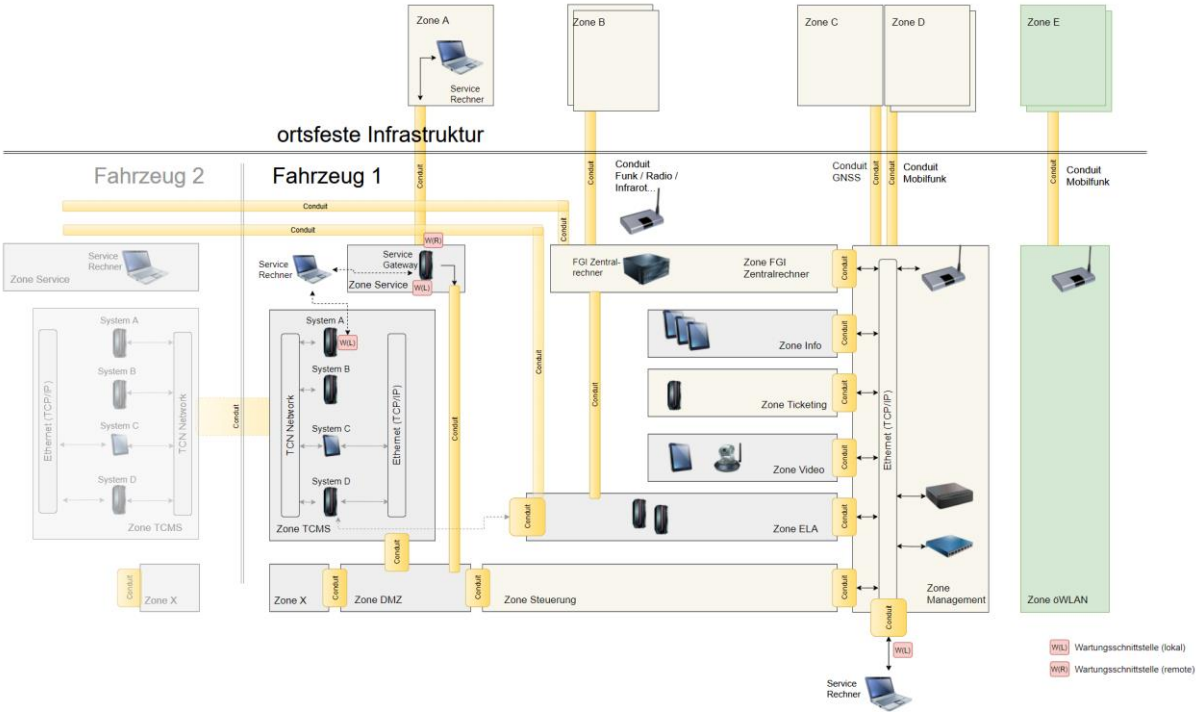

Abbildung 6: Kommunikationsstruktur und IT-Security Zonen einer verallgemeinerten Straßenbahn

Bevor tiefer auf die verschiedenen Zonen eingegangen wird, soll an Abbildung 6 die verschiedenen Gruppen von Wartungsschnittstellen in unserer verallgemeinerten Straßenbahn aufgezeigt werden. Wie an System A der TCMS-Zone in der Grafik exemplarisch dargestellt, verfügen viele Systeme über physische lokale Wartungsschnittstellen, hier gekennzeichnet durch „W(L)“. Auch heute schon gängiger ist die Wartung der Systeme über eine Remote-Schnittstelle ggf. unter Einbeziehung eines Security Gateways (hier mit „W(R)“ dargestellt). Für Systeme im Betreiber- oder Fahrgastbereich ist es zusätzlich möglich, Wartung über das Netzwerk durch Anschließen eines Wartungs-PCs lokal an das Ethernet-Netzwerk (auch hier „W(L)“) durchzuführen.

7.1.1 Zone Fahrzeugtechnik

Die Kommunikation zwischen den Systemen der Fahrzeugtechnik bzw. deren Steuergeräten z.B. Bremse, Klima oder Tür ist in einer TCMS IT-Security Zone gekapselt. Darin liegt ein echtzeitfähiges TCN-Bussystem (WTB/MVB) für den operativen echtzeitfähigen Datenverkehr. Zur Erhöhung Ihrer Bandbreite haben manche Steuergeräte eine zusätzliche Ethernet-Schnittstelle; Bestandsysteme verfügen meist noch über eine lokale Wartungsschnittstelle.

Diese lokale Wartungsschnittstelle ist oft als RS232-, USB- oder CAN-Interface ausgeführt. Wenn lokale Wartung an einem System (wie in unserem Beispiel der Türsteuerung) durchgeführt werden soll, schließt ein ausgebildeter Techniker des Betreibers oder des Herstellers einen Wartungs-PC direkt an diese Schnittstelle an. Dies wird in der Regel in Werkstattumgebung durchgeführt; der Zugang zu dieser Wartungsschnittstelle ist im Betrieb oft nur durch physische Abschottung gesichert.

Ein aus Wartungssicht effizienterer Weg ist die Wartung über eine Fernwartungsschnittstelle („W(R)“). In Werkstatt- oder Büroumgebung können berechtigte Mitarbeiter des Betreibers oder des Herstellers unter bestimmten Voraussetzungen (z.B. Abstellung in der Werkstatt) über Fernwartung

Wartungsschnittstellen ansprechen, welche hinter einem Security Gateway zugänglich sind. Die Kommunikationskette besteht aus einem Conduit der Zug-Land-Kommunikation, dem Security Gateway, einem Conduit zur DMZ bis hin zum zu wartenden System z.B. in der TCMS-Zone (in unserem Beispiel die Ethernetschnittstelle der Türsteuerung).

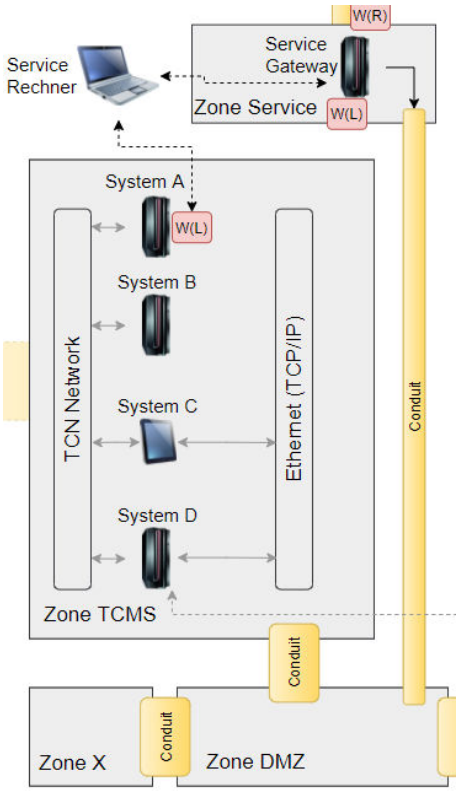

Abbildung 7: Detaildarstellung Zone Fahrzeugtechnik

Die TCMS-Zone wird als betrieblich sehr wichtig erachtet und enthält sicherheitsrelevante (Safety) Funktionalitäten. Das im Bestand weitestgehend verwendete TCN-Bussystem (WTB/ MVB) ist sehr bahnspezifisch. In diesem werden, wie in Feldbussystemen der 1990er Jahre üblich, die Daten unverschlüsselt übertragen. Verschlüsselung auf Applikationsebene sind ebenfalls unüblich bzw. in der zugehörigen Norm EN 61375 [4] nicht vorgesehen. Die Kabel sind hinter der Verkleidung durch das gesamte Fahrzeug verlegt und für Fahrgäste nicht direkt zugänglich. Teilweise jedoch sind Kabel und Stecker durch leicht mit dem Bahnvierkant zu öffnende Klappen erreichbar. Für den Zugriff auf das TCN sind hohe Expertenkenntnisse nötig und der Einfluss ist lokal auf eine Bahn begrenzt. Ein Fernzugriff ist nicht möglich. Ein Angriff erfordert daher spezifisches Wissen.

Weiterhin sind üblicherweise lokale Wartungszugänge an den Steuergeräten wie in Kapitel 5.1 dargestellt, vorhanden.

Jede Änderung der TCN-Konfiguration ist aufwändig, da sie mit den Herstellern der Steuergeräte abgestimmt werden muss und eine (mindestens teilweise) Erneuerung der Fahrzeugzulassung nach sich zieht. Solche Änderungen werden i.d.R. über die Zone “Service” mittels eines speziellen Service-Rechners im Fahrzeug durchgeführt. Ein Anschluss fremder Rechner wird heute typischerweise durch Abschottung, sowie Authentifikation und Autorisierung, ausgeschlossen.

Ein Update von Steuergeräten führt, besonders bei sicherheitsrelevanten Systemen, zu hohem Aufwand in Zertifizierungs- und Zulassungsprozessen. Deshalb sind Updates bei Steuergeräten teuer und deren Anlass sind eher zwingende fahrzeugtechnische Gründe. Der Patch von

Softwareschwachstellen ist heute noch unüblich, wodurch nicht nur die Netzwerke, sondern auch die daran angeschlossenen Steuergeräte durch Eindringlinge stärker gefährdet sind.

Die Trennung der TCMS-Zone von der Zone Betreibersysteme erfolgt durch eine sog. Demilitarisierte Zone, über die weitere Zonen erreichbar sind.

Die Demilitarisierte Zone (DMZ) bezeichnet einen Netzwerkbereich, der die Zugriffsmöglichkeiten daran angeschlossener Teilnetze durch Firewalls kontrolliert. Die DMZ leitet isolierte Datenströme zwischen die Teilnetze durch und kann Dienste, nach angeschlossenem Netzbereich isoliert, anbieten. Dies ist eine übliche Netzwerkarchitektur, um verschiedenen, aus Sicherheitsgründen voneinander getrennten Netzwerkbereiche, mit einem zentralen Zugangspunkt und Servern für zentrale Dienste zu verbinden.

7.1.2 Zone Betreibersysteme

In der Zone Betreibersysteme häufig anzutreffende Ethernet-Netzwerke stellen eine potenziell größere Gefahr dar, da sie standardisierte Schnittstellen und Protokolle anbieten. Das Betreibernetzwerk wird als eigene Zone angesehen, das durch Conduits verschiedene weitere Betreibersubzonen miteinander verbindet. Die Conduits werden an den Zonengrenzen durch Paketfilter realisiert. Die Betreibersubzonen sind typischerweise:

- Steuerung: Dient der Datenübernahme aus der Fahrzeugtechnik und dem Datenaustauch bzgl. servicerelevanter Informationen.
- Infotainment: Enthält die Fahrgastanzeigen außen und innen
- Ticketing: Enthält den Fahrkartenautomat, Entwerter
- Video: Enthält die Kameras zur Fahrgastüberwachung und Fahrzeug-Umfeldbeobachtung sowie den Videorekorder
- ELA: Elektronische Lautsprecher-Anlage, akustische Fahrgastinformation und Fahrgastsprechanlage, mit eigenem Conduit zu den anderen Teilzügen

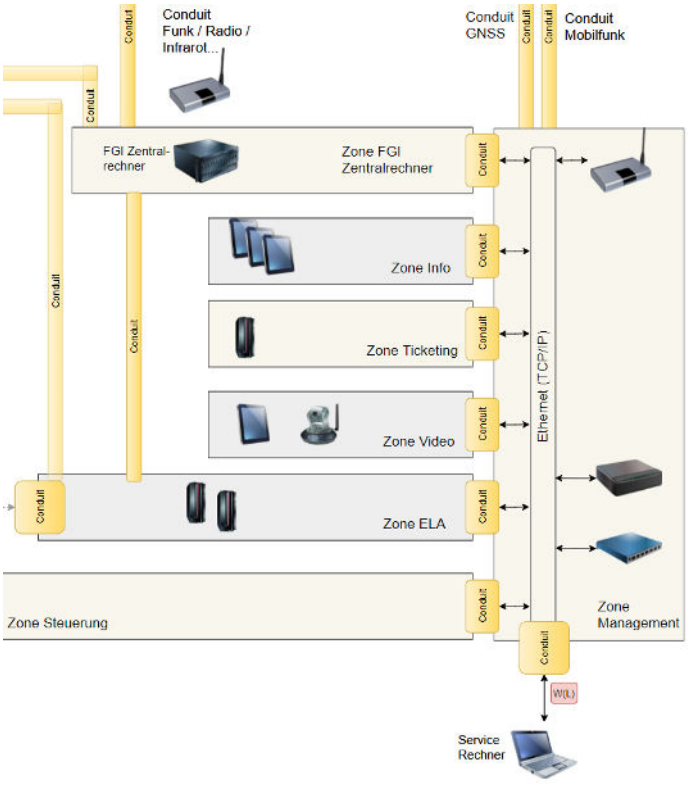

Abbildung 8: Detaildarstellung Security-Zone Betreiber

Die größte und wichtigste Betreiber-Sub Zone umfasst den Zentralrechner, der viele Funktionen zur Fahrzeugführung konzentriert und dem Triebfahrzeugführer eine Benutzeroberfläche zur Verfügung stellt (im konkreten Beispiel ITCS-Bordrechner). Der Zentralrechner benutzt durch Direktverdrahtungen und weitere direkte Verbindungen viele Conduits zu anderen Fahrzeugsystemen. Von dieser Zone gehen auch die Conduits der Leittechnik über die Luftschnittstelle zu den ortsfesten Fahrweg-Anlagen aus. Ein Sensor zur Satellitennavigation hat, zur Vollständigkeit, auch ein Conduit zu Navigationssatelliten.

Die Betreiber-Zone unterhält ein Conduit in das ortsfeste Betreibernetzwerk. Die Daten sind für die Übertragung gemäß Stand der Technik kryptografisch gesichert. Der Betreiber überträgt durch das Conduit Streckeninformationen auf das Fahrzeug und kann Diagnoseinformation abrufen.

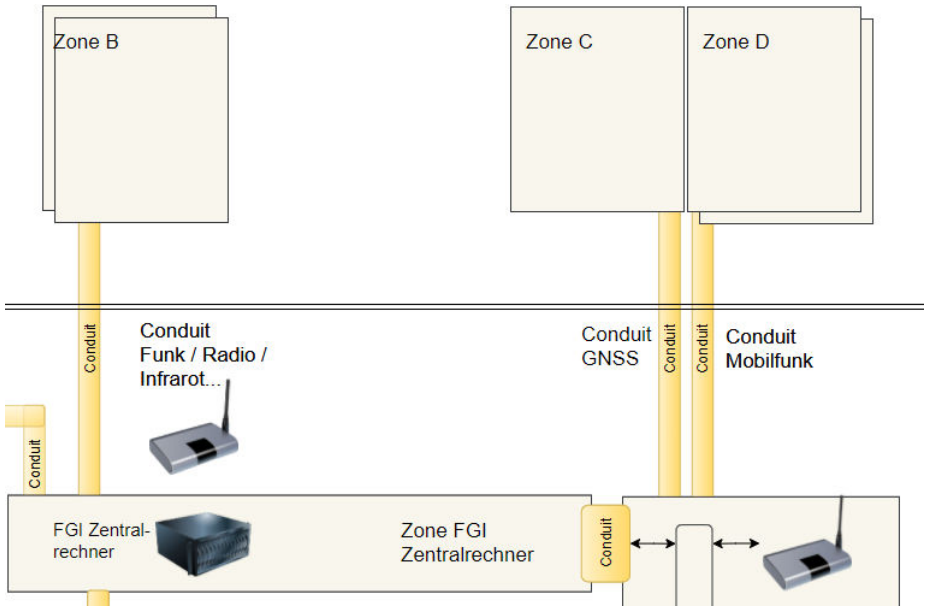

Abbildung 9: Detaildarstellung Übergang Landseite

Die Verbindung der Zonen durch das offene Netz, repräsentiert durch die Conduits, sind an den Zonengrenzen zu sichern. Die Übergänge der Zonen zu den Conduits sind durch Firewalls bzw. Paketfilter umgesetzt. Damit wird sichergestellt, dass der Netzwerkverkehr nur von/zu definierten IP-Adressen, Ports und in eine bestimmte Richtung akzeptiert wird. Damit wird die Angriffsfläche in den dahinter liegenden Netzwerken (der Zonen) reduziert. Weitere Schutzmaßnahmen wie datenbezogene Einbruchserkennung (IDS), Malware-Detektion und applikations-basierte Firewall-Fähigkeiten (Application layer firewalling) sind im betrachteten Beispiel (noch) nicht vorgesehen, da sie heute nicht dem Stand der Umsetzung in der Praxis entsprechen.

Der Switch in der Betreiberzone hat oft mehrere unbenutzte Ports, an die weitere Systeme angeschlossen werden können. Über die Ports (Conduit zur Zone *temporär verbundenen Geräte*) ist das Betreibernetzwerk erreichbar. Einzelne Funktionen sind durch Authentifikation an den Zielsystemen gesichert. Durch Anschluss eines Service-Rechners an dieses Betreibernetzwerk (siehe „W(L)“) ergibt sich hier die Möglichkeit, Wartung für die Betreibersysteme durch autorisierte Mitarbeiter des Betreibers durchzuführen. Der Zugang ist durch eine mechanische Klappe und einen Verschluss (z.B. mit Bahn-Vierkant) geschützt. Jedoch ist die Erfahrung der Betreiber, dass sich die Fahrgäste gegenseitig überwachen und von unautorisierten Handlungen abhalten. Bei Straßenbahnen ist die Entfernung zum Triebfahrzeugführer meist gering, sodass hier auch eine indirekte Überwachung/Kontrolle noch wirkt.

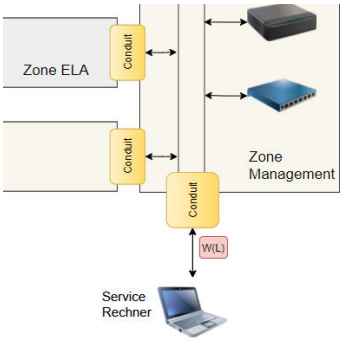

Abbildung 10: Detaildarstellung Management Zugang

7.1.3 Zone Fahrgastbereich

Die **Fahrgastzone** ist gänzlich von den restlichen Fahrzeugnetzwerken getrennt und verfügt über einen Conduit zu einem eigenen Uplink via Mobilfunk pro Consist. Der möglichst leichte Zugang durch unbekannte Fahrgäste ist hier gewollt und der Zugang für potentielle Angreifer besonders leicht. Der Datenverkehr ist vergleichsweise hoch. Einem Conduit zu den Fahrzeugnetzwerken würde man eine hohe Wahrscheinlichkeit eines Angriffes und hohes Schadenspotential zuordnen, was ein besonders hohes Risiko ergäbe. Dieses Risiko wird durch den Wegfall des Conduits minimiert.

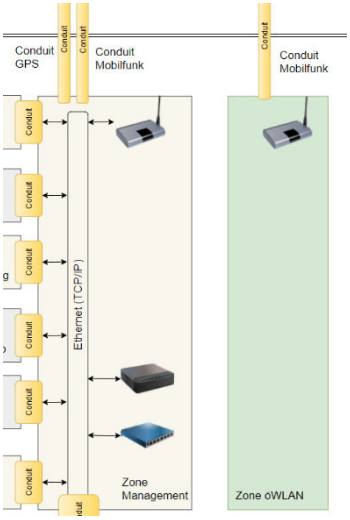

Abbildung 11: Detaildarstellung Security-Zone Fahrgastfunktionen

7.1.4 Kopplung von Fahrzeugen

Sind mehrere Wagen (Consists) miteinander gekoppelt, dann werden mehrere Conduits zwischen den Consists/Teilzügen aktiv.

- Über den TCN-Backbone (WTB) und einen Conduit ist zwischen den Fahrzeugtechnik-Zonen der Teilzüge eine Verbindung vorhanden.
- Das Zentralsteuergerät des aktiven Fahrerstands übernimmt die Kontrolle der einzelnen Subsysteme, auch in benachbarten Consists.
- Die ELA-Zonen verbinden sich über Conduits und können nun auf den Gesamtzug wirken.

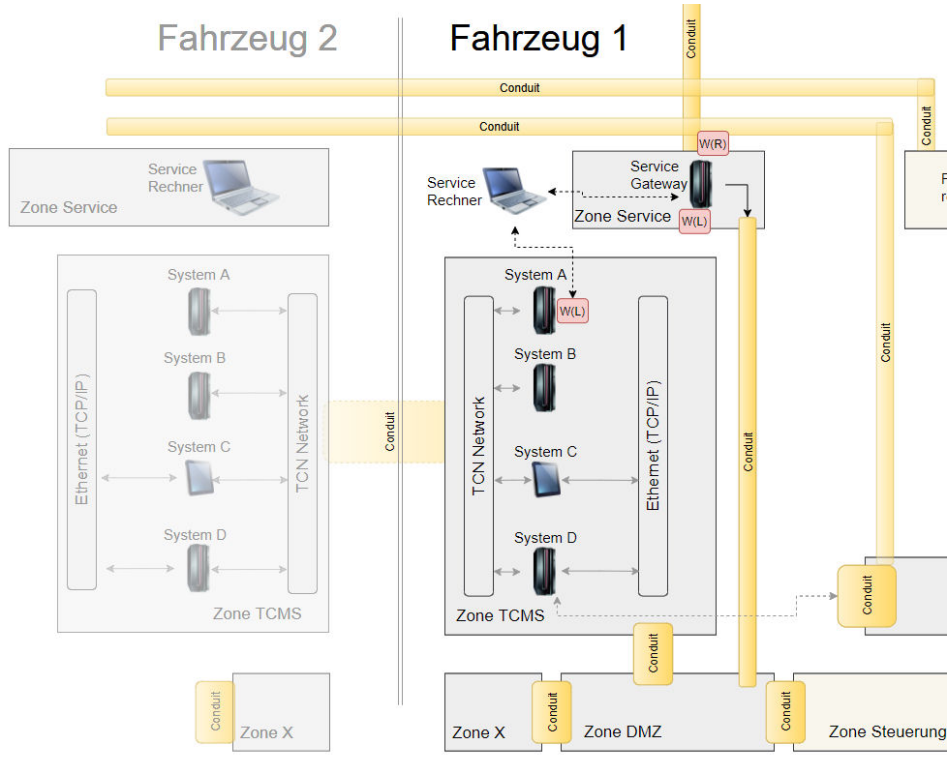

Abbildung 12: Detaildarstellung Security-Zonenübergänge zu weiteren Fahrzeugen

7.2 Zwischenfazit

Das dargestellte Praxisbeispiel zeigt, dass im betrachteten Schienenfahrzeug grundsätzliche Anforderungen an die IT-Sicherheit wie die Netzwerksegmentierung zur Kapselung unterschiedlicher Security-Anforderungen erfüllt sind. Diese ergibt sich jedoch eher aus der Anordnung der Geräte und der "Hoheit" über die Geräte und das Lifecycle-Management als aus der Norm IEC 62443.

Manche Steuergeräte haben eine lokale Wartungsschnittstelle, die über eine physische Schnittstelle angesprochen wird. Für den Fall einer Fernwartung wird häufig eine Ethernet Schnittstelle genutzt. Auch wenn es eine DMZ gibt, welche als Bindeglied für Wartungs- und Servicerechner für Wartungszwecke dienen soll, gibt es aus der Historie heraus nicht immer eine zwingende systematische Beschränkung, dass nur dieser Weg gewählt werden kann.

Der Patch von Softwareschwachstellen stellt Hersteller und Betreiber heute noch vor große Herausforderungen, da ein Update von Steuergeräten, besonders bei sicherheitsrelevanten Systemen, zu hohem Aufwand in Zertifizierungs- und Zulassungsprozessen führt. Deshalb sind Updates bei Steuergeräten teuer und deren Anlass sind eher zwingende fahrzeugtechnische Gründe. Dadurch sind nicht nur die Netzwerke, sondern auch die daran angeschlossenen Steuergeräte durch Eindringlinge stärker gefährdet. Dies gilt insbesondere für eigentlich längst bekannte Schwachstellen der IT-Security, deren Beseitigung aus Angst vor dem Verlust der Zulassung nicht adressiert werden.

Das Patchen von Software wird basierend nach Inkraftsetzung des EU-Cyber-Resilience-Act [4] jedoch verpflichtend. Weiterhin ist anzumerken, dass im Bestand heute oft ein Konflikt besteht zwischen

[4] https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52022PC0454

unangreifbarer IT-Sicherheit und der Benutzbarkeit von Systemen. Vollumfängliche Security-Maßnahmen führen oft dazu, speziell Wartungsschnittstellen komplett abzuschalten, dies wiederrum verhindert die sinnvolle Wartung durch Mitarbeiter der Wartung und Instandhaltung. Zukünftig müssen deshalb zwingend die Bedürfnisse der Wartung in der Security Konzeption / Architektur berücksichtigt werden; vor allem auch, um die Akzeptanz für Sicherheitsmaßnahmen auch bei Wartungspersonal zu erhöhen.

Fazit: Unvollständige und ungeeignete Security-Mechanismen sind ein technisches und wirtschaftliches Risiko. Deren Behandlung stehen oft finanzielle Aspekte entgegen. Dies schließt auch die Wartungsschnittstellen mit ein.

8 Zusammenfassung und Empfehlungen

IT-Security ist keine wählbare Option, sondern normative und gesetzliche Vorgabe.

Wettbewerbsnachteile dürfen nicht entstehen, da alle Hersteller und Betreiber daran gebunden sein müssen. Das in erster Linie wirtschaftliche Risiko eines IT-Vorfalls trägt vorranging der Betreiber, wenngleich alle beteiligten Stakeholder in ihrem jeweiligen Einflussbereich ihrer Verantwortung gerecht werden müssen. Daher hat der Betreiber, der die Fahrzeuge aktuell im Einsatz hat, ein besonderes Interesse, die Robustheit und Resilienz der Fahrzeuge in Bezug auf aktuelle und zukünftige Herausforderungen der IT-Security zu erhalten bzw. zu steigern.

Für Neufahrzeuge, Redesign oder Serienbetreuung kann der Betreiber die Anforderungen/Aufgaben teilweise an den Hersteller weiterleiten oder gemeinsam bearbeiten.

Aus Sicht der IT-Security ist daher für jede Neuentwicklung die Anwendung der IEC 62443 von Beginn an (Security by Design) zwingend erforderlich. Hierbei muss explizit auch die Wartungsschnittstelle betrachtet werden. Dies gilt für die Anforderungsseite (Betreiber) und die technische Entwicklung (Hersteller), wie für den Betrieb (Betreiber und Hersteller) der Anlagen.

Die Betreiber und Hersteller sollten darüber hinaus das Framework der ISO 27001 als Grundlage im Unternehmen etablieren, um die Unternehmensstruktur auf die Anforderungen der lebenslangen Aufrechterhaltung der IT-Sicherheit vorzubereiten.

Für die Handlungssicherheit bei Betreiber und Hersteller ist eine Vereinheitlichung der Zulassungsprozesse zu empfehlen. Dies vermeidet unterschiedliche lokale Anforderungen, die zwangsläufig zu einer hohen Variantenvielfalt führen. Dies hat hohe Aufwände in der Entwicklung, in der Aufrechterhaltung der IT-Sicherheit sowie im Betrieb zur Folge. Im Ergebnis nimmt die Etablierung eines adäquaten Niveaus der IT-Sicherheit eine deutlich höhere Zeitspanne in Anspruch.

Durch die Vereinheitlichung der Genehmigungs- und Zulassungsanforderungen der IT-Sicherheit für Schienenfahrzeuge im Allgemeinen und Wartungsschnittstellen im Spezifischen, beschleunigt die erfolgreiche Einführung der IT-Sicherheit.

Obgleich die Komplexität bei der Einführung und Umsetzung von Maßnahmen zur IT-Sicherheit hoch ist und die Stakeholder vor Herausforderungen stellt, entstehen auch Chancen. Neben der Minimierung der Risiken, innerhalb der Prozesskette für einen Security-Bruch verantwortlich zu sein, ermöglicht vollständig umgesetzte IT-Security auch die Sicherung des zukünftigen Geschäfts, da sie die Grundlage für die Teilnahme an Ausschreibungen darstellt. Darüber hinaus schafft Klarheit im Bereich der IT-Sicherheit Vertrauen beim Kunden und ermöglicht Transparenz bei der Bewertung von Lieferanten; für die eigene Lösung steigen die Wettbewerbsvorteile.

9 Definitionen

Die **Sicherheit** ist in der Eisenbahn das höchste zu schützende Ziel. Bis vor nicht allzu langer Zeit wurde mit dem Begriff Sicherheit jedoch nahezu ausschließlich die Betriebssicherheit verbunden, also dem Schutz von Menschen und Umwelt vor physischen, nicht vorsätzlich herbeigeführten Schäden. In den letzten Jahren hat jedoch auch eine andere Facette der Sicherheit an Bedeutung gewonnen, nämlich den Schutz und die Abwehr von vorsätzlichen, durch bestimmte Interessengruppen verübten Schäden. Im englischen Sprachgebrauch werden diese beiden Facetten von Sicherheit auch durch verschiedene Begriffe unterschieden, „**Safety**“ und „**Security**“. Im Deutschen wird manchmal versucht, diese Unterscheidung über "funktionale Sicherheit" (Safety) und "Informationssicherheit" (Security) abzubilden, was jedoch den jeweiligen Bereichen nicht immer gerecht wird. In diesem Bericht wird daher oft der jeweilige englische Begriff angeführt, wenn insbesondere auf eine der beiden Varianten verwiesen werden soll.

Safety (Funktionale Sicherheit) ist die Freiheit des Systems von inakzeptablem Risiko für Mensch und Umwelt.

Dem gegenüber grenzt sich die **Security** ab durch:

* die Maßnahmen, die getroffen wurden, um ein System zu schützen,

* den Zustand eines Systems als Resultat von Schutzmaßnahmen,

* die Eigenschaft von Systemressourcen, frei von versehentlicher oder absichtlicher Veränderung, Zerstörung oder Verlust zu sein,

* die Fähigkeit der Daten und Funktionen eines Systems, sich unautorisierten Personen und Systemen zu verweigern und autorisierten Personen und Systemen verfügbar zu sein oder

* die Verhinderung illegalen oder unerwünschten Eindringens oder Manipulation an dem beabsichtigten Betrieb eines Systems.

9.1 Begriffsdefinitionen im Security-Kontext

Authentication (Authentisierung): Prozess der Nachweismethode auf Seite des zu Identifizierenden; Vorzeigen des Nachweises der Identität gegenüber einem Authentifizierer.

Authenticity (Authentizität): Bereitstellung der Sicherstellung, dass ein angegebenes Charakteristikum einer Identität korrekt ist.

Authentification (Authentifizierung): Die Authentifizierung beschreibt in Anlehnung an [5] die Verifizierung der Echtheit der Identität einer Entität, zum Beispiel eines Nutzers oder eines IT-Systems. Sie erfolgt üblicherweise durch ein Passwort (Wissen), ein biometrisches Merkmal wie den Fingerabdruck (Eigenschaft) oder durch Hardware-Sicherheitsmodule (Besitz).

Authentifier (Authentifizierer): System (Hardware / Software), welches die Authentifizierung durchführt.

Authorization (Autorisierung): Wenn die Echtheit der digitalen Identität eines Nutzers erfolgreich verifiziert werden konnte, kann das IT-System (Endgerät, Server, IT-Dienst, Cloud, …) dem Nutzer für ihn oder seine Rolle definierte Rechte einräumen.

Availability (Verfügbarkeit): Einsatzbereitschaft einer bestimmten Funktion und der Verfügbarkeit von Daten über einen bestimmten Zeitraum.

Conduit: Logische Gruppierung von Kommunikationskanälen. Diese verbindet zwei oder mehr Zonen, die definierte Security Anforderungen haben. Das Conduit muss sicherstellen, dass die Security-Anforderungen der kritischeren Zone nicht kompromittiert werden. [6]

Confidentiality (Vertraulichkeit): Geheimhaltung des Inhalts sowie Schutz der Privatsphäre.

DMZ (Demilitarisierte Zone): Entkoppeltes und isoliertes Teilnetzwerk, das zwei oder mehrere Zonen mit unterschiedlichem Schutzbedarf miteinander verbindet, um den Datenfluss zwischen diesen kontrollieren zu können. [7]

Exposure (Anfälligkeit): Bezeichnet die Angriffsfläche bzgl. der Zugänglichkeit bzw. Erreichbarkeit für einen Angreifer.

Impact (Auswirkung): Bewertete Auswirkung eines bestimmten Ereignisses.

Integrity (Integrität): Sicherstellung der Korrektheit (Unversehrtheit) von Daten und der korrekten Funktionsweise der Systeme. Der Begriff Integrität wird im Bereich der Bahn jedoch auch im Sinne Zugvollständigkeit, die Integritätsüberwachung in diesem Zusammenhang die Überwachung der Zugvollständigkeit verwendet. Hier gibt es ein gewisses Verwechslungspotential. Diese Interpretation wird in diesem Bericht jedoch nicht aufgegriffen.

Likelihood (Eintrittswahrscheinlichkeit): Gewichteter Faktor auf der Grundlage einer subjektiven Analyse der Wahrscheinlichkeit, dass eine bestimmte Bedrohung in der Lage ist, eine bestimmte Sicherheitslücke oder eine Reihe von Sicherheitslücken auszunutzen.

Sicherheitsstrategie: Die Sicherheitsstrategie ist ein ganzheitliches Konzept, welches Aspekte der Safety und Security umfasst, um die wesentlichen Funktionen des Systems über den gesamten Lebenszyklus mit der notwendigen Verfügbarkeit und Qualität aufrecht zu erhalten. Dies sind üblicherweise Maßnahmen von der Planung, über die Beschaffung, verwendete Technologien und Architekturen, Lieferanten, Prozesse bis hin zu den Komponenten, dem operativen Betrieb sowie der Außerbetriebnahme.

PKI: Public Key-Infrastrukturen (PKI) dienen zum Verwalten von Zertifikaten mit öffentlichen Schlüsseln und weiteren Attributen über deren gesamten Lebenszyklus, von der Erstellung über die Aufbewahrung und Verwendung bis hin zur Löschung. Dabei kommt es neben der sicheren Erstellung und Speicherung gültiger Schlüssel auch auf die organisatorische Maßnahme der Verifizierung der ursprünglichen Identität ihrer Inhaber – der PKI-Nutzer – an. Public Key-Infrastrukturen bestehen aus Hardware, Software und einem abgestimmten Regelwerk, der Leitlinie. Diese definiert, nach welchen Sicherheitsregeln die Dienstleistungen um die Zertifikate erbracht werden. Dazu zählen das Betriebskonzept der PKI, die Nutzerrichtlinien sowie Organisations- und Arbeitsanweisungen. [5]

Resilience (Resilienz): Resilienz bezeichnet die Fähigkeit eines Systems, auf Bedrohungen, Störungen und allgemein unerwartete Ereignisse angemessen zu reagieren, sich anzupassen und sich zu erholen. Dies kann durch Maßnahmen zur Redundanz, Fehlertoleranz und Wiederherstellbarkeit erreicht werden.

SuC (System under Cosideration / betrachtetes System): Eine Sammlung von Anlagen, die für die Bereitstellung und den Betrieb einer Bahnanwendung notwendig sind, einschließlich aller relevanten Netzwerkinfrastrukturanlagen.

Vulnerability (Verwundbarkeit): Ein Fehler oder eine Schwachstelle in der Gestaltung, Implementierung, oder dem Betrieb und Management eines Systems, der / die ausgenutzt werden könnte, um die Integrität oder Sicherheitsstrategie des Systems zu verletzen.

(Security)-**Zone**: Die Gruppierung logischer oder physikalischer Anlagen auf der Grundlage des Risikos, oder anderer Kriterien wie etwa der Kritikalität der Anlagen bzgl. der Betriebsfunktion, des physikalischen oder logischen Standorts, des erforderlichen Zugangs (z.B. Prinzip der geringsten Rechte), oder der verantwortlichen Organisation.

9.2 Begriffsdefinitionen Bahntechnik

Consist: Ein Wagen oder eine feste Kombination von Wagen, die über ein abgeschlossenes, statisches TCN-Bussystem oder -Netzwerk (Wagenbus) im TCMS-Kontext miteinander kommunizieren. Kommunikation über ein Consist hinaus ist i.d.R. nur über den Zugbus (WTB, ETB) möglich.

Consist-Network (Wagenbus / Fahrzeugbus): Es repräsentiert ein statisches, vorkonfiguriertes Kommunikationssystem innerhalb eines Consists. Als Bussysteme sind MVB und das Ethernet-basierende Switch-Netzwerk ECN standardisiert. Darüber hinaus werden weitere Kommunikationssysteme verwendet.

MVB (Multifunction Vehicle Bus): Eine in der IEC 61375-1 [4] bzw. IEC 61375-3-1 [8] definierte Ausprägung eines Consist-Bussystems (Wagenbus / Fahrzeugbus) mit hoher Verbreitung in Bestandsfahrzeugen.

TCMS (Train Control Management System): Ein Train Control Management System (TCMS) ist ein computergestütztes Steuerungssystem, das verschiedene Subsysteme der Fahrzeugtechnik verwaltet, die für die Steuerung des Zuges notwendig sind. Hierzu gehören typischerweise das Antriebssystem, die Bremsen, Türen, Klimaanlagen, Beleuchtung und Kommunikationssysteme. I.d.R. sind die Steuerkomponenten des TCMS funktional sicher auszulegen, was dadurch auch einen hohen Schutzbedarf im Sinne der IT-Security folgen lässt.

TCN (Train Communication Network): In der Normenreihe IEC 61375 definierte Kommunikationssysteme für den Einsatz auf Schienenfahrzeugen, über dass die TCMS-Fahrzeugelemente miteinander verbunden sind. TCN-Kommunikationssysteme bestehen aus zwei Netzwerkebenen, dem zugweiten und dynamischen Train-Backbone (Zug-Bus), sowie dem statischen Consist-Network (Wagenbus / Fahrzeugbus), die mittels verschiedener Bus-/Netzwerktechnologien umgesetzt werden.

Train-Backbone (Zug-Bus): Zugweites Kommunikationssystem zur Verbindung aller Consists und zur Kommunikation über Consist-Grenzen hinweg.

WTB (Wire Train Bus): Eine in der IEC 61375-2-1 [9] definierte Ausprägung des Train-Backbones (Zug-Bus) als Bussystem mit hoher Verbreitung in Bestandsfahrzeugen.

Train (Zug): Ein Zug besteht aus einem oder mehreren Consists.

10 Literaturverzeichnis

[1] C-NA, „Generisches IT Security Architekturmodell von Schienenfahrzeugen," 26 05 2021. [Online]. Available: https://www.c-na.de/wp-content/uploads/2021/06/210420_CNA_IT-Sec_Abschlussbericht_210521_oB.pdf. [Zugriff am 14 03 2024].

[2] ERTMS, „ERTMS SECURITY CORE GROUP," 11 8 2023. [Online]. Available: https://ertms.be/activities/ertms-security-core-group. [Zugriff am 14 03 2024].

[3] International Electrotechnical Commission, „IEC 62443-3-2," *IT-Sicherheit für industrielle Automatisierungssysteme - Teil 3-2: Sicherheitsrisikobeurteilung und Systemgestaltung,* 2020.

[4] International Electrotechnical Commission, „IEC 61375-1:2012," *Electronic railway equipment - Train communication network (TCN) - Part 1: General architecture,* 2012.

[5] N. Pohlmann, Cyber-Sicherheit, Springer Vieweg, 2022.

[6] International Electrotechnical Commission, „IEC 62443-3-3:2013," *Industrielle Kommunikationsnetze - IT-Sicherheit für Netze und Systeme - Teil 3-3: Systemanforderungen zur IT-Sicherheit und Security-Level,* 2013.

[7] International Electrotechnical Commission, „IEC 62443-2-1," *IT-Sicherheit für industrielle Automatisierungssysteme - Teil 2-1: Anforderungen an ein IT-Sicherheitsprogramm für IACS-Betreiber,* 2009.

[8] International Electrotechnical Commission, „IEC 61375-3-1:2012," *Electronic railway equipment - Train communication network (TCN) - Part 3-1: Multifunction Vehicle Bus (MVB),* 2012.

[9] International Electrotechnical Commission, „IEC 61375-2-1:2012," *Electronic railway equipment - Train communication network (TCN) - Part 2-1: Wire Train Bus (WTB),* 2012.

11 Anhang

Nachfolgend finden sich weitere Beispiele einer detaillierten Risikoanalyse bezogen auf relevante Bedrohungen aus dem BSI-Katalog [2]. Dieser Anhang stellt somit eine Ergänzung zu Kap. 5.2 dar.

11.1 T016 Diebstahl

Bedrohung	**T 016 Bedrohung Diebstahl Geräte, Speichermedien, Dokumente**	
Kurzerläuterung der Bedrohung	Erlangung von Zugriff auf Informationen, die einen Angriff erleichtern/ermöglichen (Reconnaissance) oder Unterbindung Nutzbarkeit durch fehlende Systemstücke.	
Annahmen zur Bewertung	Im Status quo sind die Systeme, Speichermedien und Dokumente nicht oder nicht ausreichend gegen Kopie, Löschen, Entwenden gesichert.	
Risikobetrachtung	**Ergebnis**	**Erläuterung**
Einstufung Exposure	3	Ohne Security-Maßnahme direkter physischer Zugriff auf die Systeme möglich. Medien sind gegen Löschen und Entfernen nicht gesichert. Dokumente werden nicht klassifiziert und entsprechend geschützt.
Einstufung Vulnerability	3	Die Entwendung ist ohne weitere Kenntnisse möglich.
Einstufung Likelihood	5	Exposure+Vulnerability-1 (entspr. TS 50701)
Einstufung Impact	B	Es kommt zu Einschränkungen der Nutzung der Wartungsschnittstelle oder es können auf den Informationen aufbauend Angriffe geplant werden. Maximal finanzielle und Reputationsschäden können auftreten.
Resultierendes Risiko	Hoch	entspr. Risikomatrix
Risiko-Differenz	**3**	Ggü. Target-Risk: Low
Maßnahmen IEC 62443-3-3 System-Requirements	SR 1.1 SR 1.5 SR 4.1 RE 1	
Maßnahmen IEC 62443-4-2 Komponenten-Requirements *Konkreter Vorschlag der Umsetzung*	-	
Kompensierende Maßnahmen	Prozessuale Regelung zum Schutz des Zugriffs auf den Maintenance-Laptop; physische Absicherung des Werkgeländes bei Abstellung; Erschwerung des Zugriffs im Betrieb durch entsprechenden Einbau, soziale Hemmung und Vorhandensein des Fahrers	
Note: Bericht aus der Praxis	- Abgestellte FZ: Abschottung des Zugangs zum Gelände, Abschottung Zugang zum Gewerk über Sechskant + Schlüssel, - FZ im Betrieb: Fahrgäste + Fahrer + Videoüberwachung reichen aus, um Bedrohung zu minimieren	

Risikobetrachtung *mit implementierten Maßnahmen*	**Ergebnis**	**Erläuterung**
Einstufung Exposure	2	Zugriff eingeschränkt. Maximale physische Absicherung nachträglich ohne Tausch nicht möglich.
Einstufung Vulnerability	1	Konfigurationen angepasst und Dokumente nicht mehr einfach zugänglich.
Einstufung Likelihood	3	Exp+Vuln-1
Einstufung Impact	B	Es kommt zu Einschränkungen der Nutzung der Wartungsschnittstelle. Maximal finanzielle und Reputationsschäden können auftreten. Keine Absenkung Impact möglich.
Resultierendes Risiko	Low	Entspr. Risikomatrix
Risiko-Differenz	**0**	Das ermittelte Risiko entspricht dem Ziel-Risiko (Low)
Weitere kompensierende Maßnahmen	-	

11.2 T021 Manipulation

Bedrohung	T0.21 Manipulation von Hardware oder Software	
Kurzerläuterung der Bedrohung	Erlangung von Zugriff auf Hard- oder Software und Manipulation der Informationen und damit des Systemverhaltens.	
Annahmen zur Bewertung	Im Status quo sind die Systeme, Hard- und Software nicht oder nicht ausreichend gegen Manipulation gesichert. Die Systeme und ihre Software sind nicht im Netz frei zugänglich. Im Beispiel wurde die Wartung für Türsteuerungen betrachtet. Türsteuerung verarbeitet ein Embedded SW-Image, das über Embedded Entwicklungs-Umgebungen beim Hersteller erstellt wird. Die Türsteuerung besitzt i.d.R. kein weitverbreitetes Betriebssystem (Windows / Linux), sondern oft ein Embedded-Echtzeit (ggf. sogar funktional sicheres) OS, bei dem die Anwendungslogik im Build-Prozess mit einkompiliert wird. Dazu sind Embedded EW-Umgebungen notwendig.	
Risikobetrachtung	**Ergebnis**	**Erläuterung**
Einstufung Exposure	2	Ohne Security-Maßnahme direkter physischer Zugriff auf die Systeme möglich. Manipulation bedarf Vorkenntnisse – mind. 2-stufiger Angriff – da die Software nicht Open Source oder anderweitig verfügbar ist.
Einstufung Vulnerability	2	Die Software ist nicht gegen Manipulation geschützt. Es sind keine Standardprotokolle. Eine Vorbereitung ist notwendig. 2-Stufiger Angriff.
Einstufung Likelihood	3	Exposure+Vulnerability-1 (entspr. TS 50701)

Einstufung Impact	C	Es kann zur Verfälschung der Daten kommen. Es ist möglich, dass Fehlhandlungen aufgrund von Fehlinformationen ausgeführt werden. Bei Änderung von Konfigurationsdaten der Türsteuerung kann es im schlimmsten Fall zur unzeitigen Öffnung oder zum Einklemmen von Reisenden kommen.
Resultierendes Risiko	Signifikant	entspr. Risikomatrix
Risiko-Differenz	**2**	Ggü. Target-Risk: Low
Maßnahmen IEC 62443-3-3 System-Requirements	SR 3.4, SR 3.5, SR 3.3, SR 3.8, SR 4.3, SR 7.7, SR 1.5	
Maßnahmen IEC 62443-4-2 Komponenten-Requirements *Konkreter Vorschlag der Umsetzung*	-	
Kompensierende Maßnahmen	-	
Note: Bericht aus der Praxis	Zusätzlich physischer Zugriff vermeiden (VAG)	
Risikobetrachtung *mit implementierten Maßnahmen*	**Ergebnis**	**Erläuterung**
Einstufung Exposure	1	Zugriff eingeschränkt. Maximale physische Absicherung nachträglich ohne Tausch nicht möglich.
Einstufung Vulnerability	1	Konfigurationen angepasst und Dokumente nicht mehr einfach zugänglich.
Einstufung Likelihood	3	Exp+Vuln-1
Einstufung Impact	C	Es kommt zu Einschränkungen der Nutzung der Wartungsschnittstelle. Maximal finanzielle und Reputationsschäden können auftreten. Keine Absenkung Impact möglich.
Resultierendes Risiko	Low	Entspr. Risikomatrix
Risiko-Differenz	**0**	Das ermittelte Risiko entspricht dem Ziel-Risiko (Low)
Weitere kompensierende Maßnahmen	-	