Cluster Bahntechnik

CNA Fachausschuss

Abschlussbericht der Arbeitsgruppe Schritte zum generischen IT Security Architekturmodell von Schienenfahrzeugen

Stand: 26. Mai 2021

Inhaltsverzeichnis

1 Einleitung

Im Rahmen des CNA (Center for Transportation & Logistics Neuer Adler) in Nürnberg hat sich in 2019 ein Arbeitskreis IT-Sicherheit in der Bahntechnik gebildet. Die Mitglieder setzen sich aus Vertretern aus Industrie, Betreibern, Zulassungsbehörden, Gutachtern und der Wissenschaft zusammen. Der Arbeitskreis entwickelt eine generische Security Architektur für Schienenfahrzeuge.

In der AK-Sitzung am 18.02.2020 in Nürnberg wurden zwei Vertiefungsfelder identifiziert, die in Arbeitskreis-Kleingruppen weiter ausgearbeitet werden. Ziel dieser Arbeitsgruppe ist, ausgehend von den rechtlichen und normativen Vorgaben eine anwendbare Security-Architektur für Schienenfahrzeuge zu erarbeiten. Dieser Bericht fasst die erarbeiteten Ergebnisse zusammen.

Die Mitglieder der Arbeitskreis-Kleingruppe sind:

- Friedrich Feistle (ANNAX/Wabtec, Koordinator),
- Jürgen Sept (Siemens Mobility GmbH),
- Martin Kursawe (DB Systemtechnik GmbH),
- Dr. Daniel Lüdicke (DLR) und
- Paolo Fanuli (Selectron/Knorr-Bremse).

2 Regulatorische Rahmenbedingungen

Die Digitalisierung ist ein allgemeiner Trend in allen Bereichen der Industrie und Gesellschaft. Durch eine stetig wachsende Digitalisierung von Funktionen und Vernetzung erlangt die IT- bzw. Cyber-Sicherheit (Security) als Teil der allgemeiner gefassten Informationssicherheit [1] eine wachsende Bedeutung. Im Zuge eines steigenden Digitalisierungsgrades entstehen für den Staat, die Industrie und Gesellschaft auch steigende Abhängigkeiten von der Funktionsfähigkeit und Verfügbarkeit dieser Systeme. Die für die Volkswirtschaft besonders wichtigen Systeme werden als „Kritische Infrastruktur“ bezeichnet und stehen unter einer besonderen Aufmerksamkeit. So zählen auch Teile der Eisenbahn zur kritischen Infrastruktur.

Die gesetzlichen Rahmenbedingungen zur IT-Sicherheit für den Schienenverkehr in Deutschland leiten sich zum Einen bereits von EU-Recht ab und zum Anderen aus den Sicherheitsanforderungen der eisenbahnspezifischen Gesetze (siehe Abbildung 1).

Die EU-Richtlinie 2016/1148 [2] „…über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen…“ (NIS-Richtlinie) und deren Umsetzungsgesetz in Deutschland [3] fordert eine nationale Strategie für die Sicherheit von Netz- und Informationssystemen sowie Kooperationsgruppen für die strategische Zusammenarbeit. Interessanter für den Eisenbahnsektor sind Sicherheitsanforderungen und Meldepflichten für die Betreiber/Anbieter „wesentlicher“ Dienste sowie die Schaffung von Computer-Notfallteams (CSIRTs-Netzwerk — Computer Security Incident Response Teams Network). Die in der NIS-Richtlinie für Deutschland zuständige Behörde ist das Bundesamt für Sicherheit in der Informationstechnik (BSI) [4].

In Deutschland ist das Bundesamt für Sicherheit in der Informationstechnik (BSI) [4] eine zentrale Stelle im Bereich IT-Sicherheit. Seine Aufgaben beschreibt das BSI-Gesetz (BSIG) [5]. So ist das BSI die zentrale Meldestelle für IT-Sicherheit, stellt technische Informationen bereit, gibt Warnungen aus und definiert Sicherheitsstandards. Einen besonderen Schwerpunkt bildet die Absicherung der „Kritischen Infrastrukturen“. Welche Institutionen zur kritischen Infrastruktur gehören beschreibt die Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-KritisV) [6]. Darin wird dem Sektor Transport und Verkehr eine besondere Bedeutung für das Funktionieren des Gemeinwesens und die Versorgung der Allgemeinheit mit Leistungen zum Transport von Personen und Gütern bescheinigt (BSI-KritisV §8). Für den Schienenverkehr sind Personen-, Güter- und Zugbildungsbahnhöfe, das Schienennetz, Stellwerke und Leitzentralen (Anhang 7, Teil 1b) Teil der kritischen Infrastruktur wenn sie eine (nach Anhang 7, Teil 2/3) bestimmte Größe, Zugehörigkeit oder Kapazität besitzen. (Vernetzte) Schienenfahrzeuge werden hier jedoch bisher nicht explizit erwähnt. In ähnlicher Weise wird der ÖPNV betrachtet. Das BSI-Gesetz macht in §8 umfangreiche Vorgaben an Betreiber digitaler Dienste und Kritischer Infrastrukturen, die indirekt durch Betreiberanforderungen auch auf Fahrzeughersteller wirken.

Der rechtliche Bezug der IT-Sicherheit für die verschiedenen Schienenverkehrsbereiche leitet sich aus dem allgemeineren Sicherheitsbegriff der jeweils gültigen Rechtsvorschriften ab. Für den öffentlichen Verkehr von Vollbahnen beschreibt das Allgemeine Eisenbahngesetz (AEG) [7] in §4, dass Eisenbahninfrastrukturen und Fahrzeuge den Anforderungen der öffentlichen Sicherheit genügen müssen. Auch die Eisenbahn-Bau- und Betriebsordnung (EBO, §2) [8], die Verordnung über den Bau und Betrieb der Straßenbahnen (BOStrab, §2 Satz 1) [9] sowie die Verordnung über den Bau und Betrieb von Anschlussbahnen (BOA, §1a) [10] weisen bereits zu Beginn darauf hin, dass Bahnanlagen und Fahrzeuge so beschaffen sein müssen, dass sie den Anforderungen der Sicherheit und Ordnung genügen.

Für Nebenbahnen die dem Verband Deutscher Verkehrsunternehmen (VDV) angehören entwickelt sich gerade der branchenspezifische Standard (B3S) nach dem BSI-Gesetz (§8a (2)): die VDV-Schrift 440 Branchenanforderungen an

die IT-Sicherheit [11] mit VDV-Mitteilung 4400 Maßnahmenkatalog zur VDV-Schrift 440 - Maßnahmen für personelle, organisatorische und bauliche/physische Sicherheit sowie branchenspezifische Technik [12].

In Abbildung 1 sind die grundsätzlichen rechtlichen Zusammenhänge der IT-Security für Schienenfahrzeughersteller und –Betreiber, wie gerade beschrieben, dargestellt.

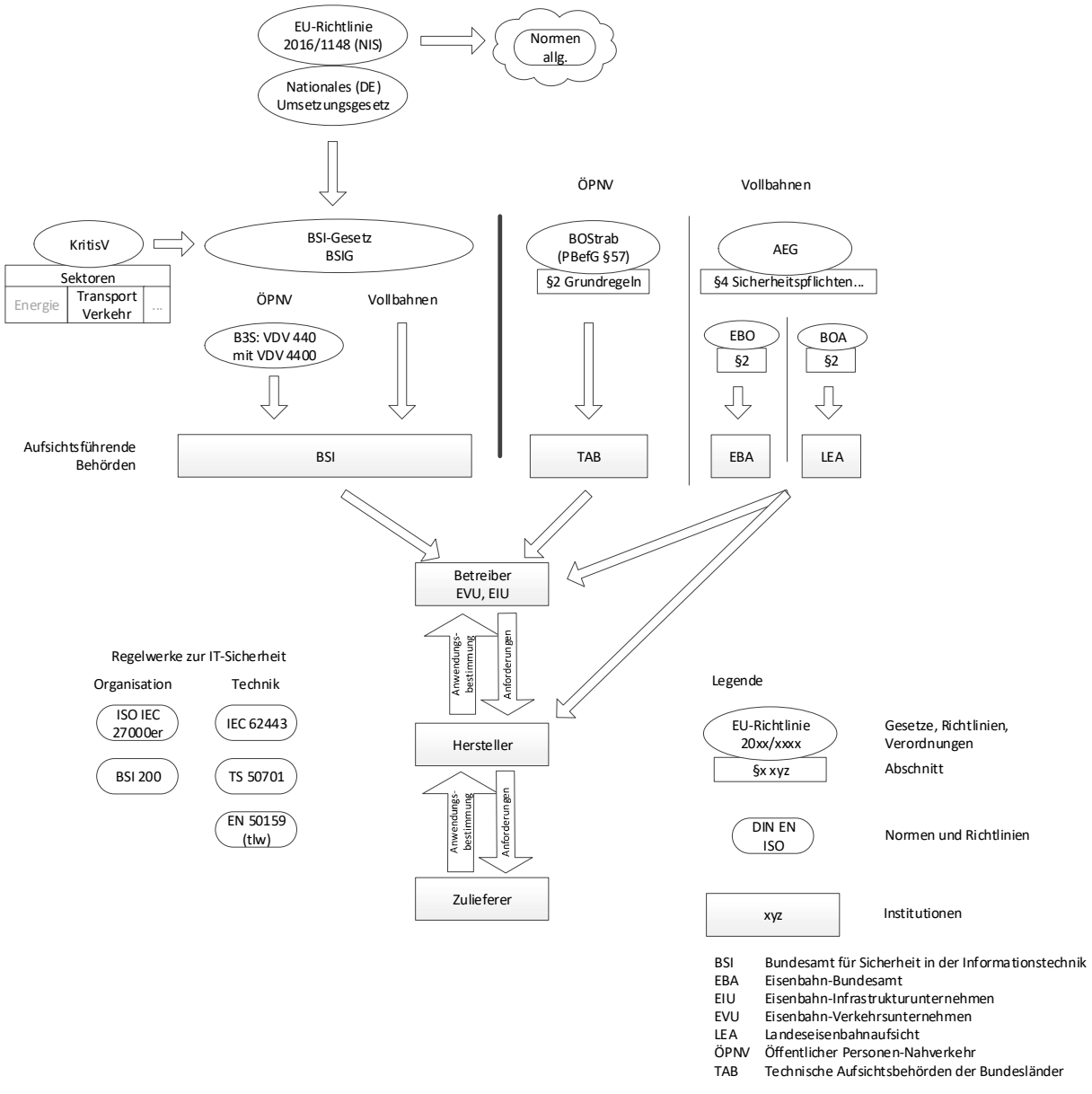

Abbildung 1: IT-Sicherheitsanforderungen an Schienenfahrzeugbetreiber und -hersteller

Als Grundstruktur wie IT-Sicherheit initiiert, gesteuert und überwacht werden kann, wird ein Informationssicherheitsmanagement (ISMS) eingeführt, für deren Umsetzung es unterschiedliche, zum Teil harmonisierte, Grundlagen gibt.

Die Normenreihe ISO/IEC 27000ff fasst die Normen mit den allgemeinen sowie branchenspezifischen Leitfäden zur Informationssicherheit zusammen, die teilweise in deutscher Übersetzung als DIN-Normen vorliegen. Die Norm ISO/IEC 27001 [13, 14] zum Management von Informationssicherheit gibt Vorgaben von der Einführung über den Betrieb bis zur Verbesserung eines Informationssicherheitsmanagementsystems.

Das BSI stellt mit dem IT-Grundschutz eine ganzheitliche Methode vor, die es Organisationen ermöglicht stufenweise eine angemessene IT-Sicherheit zu erreichen. Als Vorgehensweisen wird eine Basis-, Standard- oder Kernabsicherung vorgeschlagen, der modular eingeführt und erweitert werden kann. Der IT-Grundschutz ist als sogenannter BSI-Standard [1, 15 bis 17] und im IT-Grundschutz-Kompendium [18] erschienen.

Als weiterer sektorspezifischer Umsetzungsleitfaden beschreibt die Technische Spezifikation TS 50701 Railway applications – Cybersecurity [19] Anforderungen und Leitlinien/Unterstützung an Betreiber, Integratoren und Hersteller/Zulieferer bezüglich IT-Sicherheit während des gesamten Produkt-Lebenszyklusses. Diese technische Spezifikation setzt auf der Normenreihe IEC 62443 auf und soll die branchenspezifischen Besonderheiten abdecken.

Die im Anschluss vorgestellt Normenreihe IEC 62443 zur IT-Sicherheit hat im Schienenfahrzeugbereich größere Verbreitung gefunden.

2.1 Die Normenreihe IEC 62443

Die branchenunabhängige Normenreihe IEC 62443 Industrial communication networks - Network and system security [20] beschäftigt sich mit der IT-Sicherheit von, sehr allgemein gefassten, industriellen Automatisierungssystemen (“Industrial Automation and Control Systems” (IACS)). Die Norm wurde ursprünglich für die stationäre Prozessindustrie entwickelt und deckt heute als Grundnorm für IT-Sicherheit allgemein Automatisierungssysteme aller Industriebereiche ab.

In der Normenreihe sind vier allgemeine Strukturebenen definiert. Der erste Teil fasst die grundlegenden Definitionen, Konzepte und Modellvorstellungen der Normenreihe zusammen. Der Teil 1-1 [20] liegt bereits seit Juli 2009 vor. Im zweiten Teil sind organisatorische Themen wie Informationssicherheitsmanagementsysteme [21] und Patchmanagement [22] enthalten. Weiter technisch orientiert beschäftigen sich der dritte Teil mit einer Gesamtsystemsicht und der vierte Teil mit einzelnen Komponenten. Aus dieser Normenreihe sind bereits sieben der 13 geplanten Teile veröffentlicht. Die Abbildung 2 zeigt alle Teile der Normenreihe:

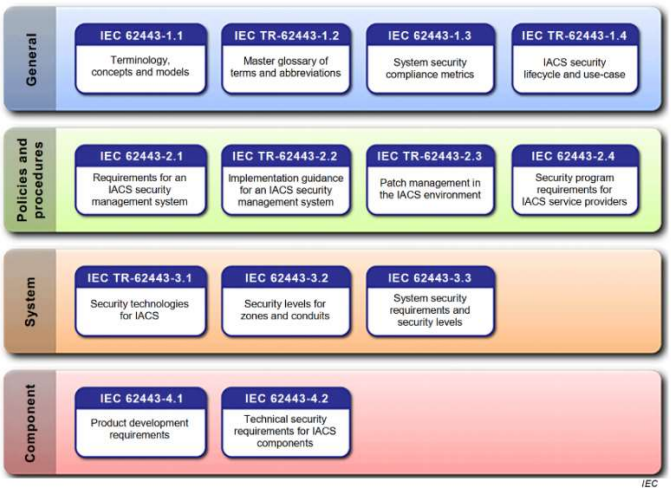

Abbildung 2: Normenreihe IEC 62443 (Bild aus [23])

Neben der technischen Sicht lassen sich auch organisatorisch orientierte Rollen in einem Lebenszyklus beschreiben, die verschiedene Teile der Normenreihe nutzen:

Rolle	Normteile IEC 62443	Beschreibung
Hersteller	2-3, 3-3, 4-1, 4-2	Entwickelt und stellt ein Automatisierungssystem aus Hardware- oder Softwareprodukten (selbst und aus Subkomponenten) her
Integrator	2-3, 2-4, 3-2, 3-3	Fügt ein Automatisierungssystem zusammen, und nimmt es in Betrieb
Betreiber	2-1,2-3, 2-4, 3-2, 3-3	Nutzt ein Automatisierungssystem

2.1.1 Allgemeine Konzepte nach IEC 62443-1-1

Die Norm fasst allgemeine/sinnvolle/hilfreiche Konzepte der IT-Sicherheit zusammen und wendet sie auf Automatisierungssysteme an.

Betrachtungsobjekt (System under consideration)	Bestimmung des Untersuchungsobjektes
Sicherheitskontext (Security Context)	Bestimmung des Umfelds des Betrachtungsobjektes und dessen betrieblichen Einsatzes Definition der Risikobeeinflussung durch das äußere Umfeld
Sicherheits-/ Schutzziele (Security Objectives)	Vertraulichkeit, Integrität und Verfügbarkeit, nach Anwendung in unterschiedlicher Reihenfolge
Minimale Rechte (Least Privilege)	Einschränkung von Rechten auf ein notwendiges Minimum (könnte die Verfügbarkeit reduzieren)
Gestaffelte Verteidigung (Defense in Depth)	Mehrere Maßnahmen hintereinander, aufeinanderfolgende Barrieren
Risikoanalyse (Threat-Risk-Assessment)	Risikoermittlung aus Inventarwert, Bedrohung und Schwachstellen Ermittlung des Restrisikos mit Schutzmaßnahmen
Richtlinien und Prozesse (Policies and Procedures)	Informationssicherheitsmanagementsystem (ISMS)
Sicherheit der Lieferkette (Supply Chain Security)	Abgeleitete Anforderungen an Zulieferer

2.1.2 Grundkonzepte (Fundamental Concepts) nach IEC 62443-3-2

Die Grundkonzepte sind methodische Werkzeuge sowie Themengebiete, die ein Sicherheitskonzept bilden:

<table>
<tr><td>Sicherheit-Lebenszyklus
(Security Life Cycle)</td><td>Lebenszyklus von Security-Anforderungen und -Maßnahmen</td></tr>
<tr><td>Reifegrad
(Maturity level)</td><td>Bewertung des Entwicklungsstandes von Prozessen</td></tr>
<tr><td>Zonen und Kommunikations-kanäle
(Zones and Conduits)</td><td>Einteilung des Gesamtsystems in Sicherheitszonen gleichen Schutzbedarfs (Zones) und kontrollierter Zonenübergänge (Conduits).</td></tr>
<tr><td>Sicherheitsniveau
Security level (SL)</td><td>Bewertung der Bedrohungsstärke nach Eigenschaften des Angreifers. Die qualitative Einstufung muss organisationsweit kalibriert werden.
<table>
<tr><th>SL</th><th>Mittel</th><th>Ressourcen</th><th>Fähigkeiten</th><th>Motivation</th></tr>
<tr><td>SL-0</td><td colspan="4">keine Gefahr der Beeinträchtigung oder Manipulation</td></tr>
<tr><td>SL-1</td><td colspan="4">zufällige/beiläufige Beeinträchtigung oder Manipulation</td></tr>
<tr><td>SL-2</td><td>einfach</td><td>begrenzt</td><td>allgemein</td><td>niedrig</td></tr>
<tr><td>SL-3</td><td>ausgefeilt</td><td>mittel</td><td>domänensp.</td><td>mittel</td></tr>
<tr><td>SL-4</td><td>ausgefeilt</td><td>umfangreich</td><td>domänensp.</td><td>hoch</td></tr>
</table>
Bewertung des Sicherheitsniveaus:
<table>
<tr><td>Security-Level – Capability (SL-C)</td><td>Erreichbares Sicherheitsniveau</td></tr>
<tr><td>Security-Level – Target (SL-T)</td><td>Vorgegebenes/zu erreichendes Sicherheitsniveau aus der Risikoanalyse</td></tr>
<tr><td>Security-Level – Achieved (SL-A)</td><td>Bereits erreichtes Sicherheitsniveau</td></tr>
</table></td></tr>
</table>

2.1.3 Basisanforderungen (Foundational Requirements) nach IEC 62443-3-3

Konkrete Systemanforderungen an Automatisierungssysteme setzen sich aus Basis- und Systemanforderungen sowie Erweiterungen zusammen. Für den Integrator sind die Anforderungen in Teil -3-3 [24] beschrieben.

Nr.	Abk.	Foundational Requirements	Basisanforderungen
1	IAC	Identification and Access Control	Identifizierung und Zugangskontrolle
2	UC	Use Control	Nutzungskontrolle
3	SI	System Integrity	Systemintegrität
4	DC	Data Confidentiality	Vertraulichkeit der Daten
5	RDF	Restricted Data Flow	Beschränkter Datenfluss
6	TRE	Timely Response to Events	Rechtzeitige Reaktion auf Ereignisse
7	RA	Resource Availability	Ressourcenverfügbarkeit

Zu den Basisanforderungen gibt es konkrete Anforderungen die an die Maschine oder Anlage gerichtet sind. Diese Systemanforderungen (SRs – System Requirements) sind im Anhang C der IEC 62443-3-3 [24] abgelegt. Um unterschiedlichen Sicherheitsniveaus (SL's) Rechnung zu tragen gibt es daran angepasste Anforderungserweiterungen (RE's – Requirement Enhancements).

2.1.4 Anforderungen an Subsysteme und Komponenten

Für den (Komponenten-) Hersteller gelten z.B. die Anforderungen an den Lebenszyklus für eine sichere Produktentwicklung nach -4-1 sowie die Technischen Sicherheitsanforderungen an Komponenten nach -4-2 als Ableitung aus den Systemanforderungen. Letztere werden auch als Zertifizierungsgrundlage für Komponenten verwendet (vgl. TeletrusT-Prüfschema [25] für Konformitätsbewertungen).

3 Vorgehensmodell nach IEC62443-3-2

Der Systementwurf zur DIN EN 62443-3-2 [23] definiert die Anforderungen an

- die Festlegung eines Betrachtungsobjekts (System under Consideration, SUC),
- die Aufteilung dieses Betrachtungsobjekts in Zonen und Zonenübergänge (Conduits),
- die Beurteilung für Zonen und Zonenübergänge,
- die Feststellung des Schutzbedarfs und daraus ggf. die Festlegung des zu erreichenden Security-Levels für Zonen und Zonenübergänge sowie
- die Dokumentation der Sicherheitsanforderungen.

In **Abbildung 3** ist der generische Arbeitsablauf dargestellt, der auch Grundlage für die Arbeiten dieser Arbeitsgruppe war. Mit dem Ziel, die Schritte zu einem generischen Security Architekturmodell von Schienenfahrzeugen zu beschreiben, beschränkten sich dabei die Arbeiten auf die folgenden Schritte:

- Definition des Betrachtungsobjekts „Schienenfahrzeug“ (Kapitel 4) entsprechend ZCR 1 (Zone and Conduit Requirement)
- Gruppierung der Funktionsgruppen eines Schienenfahrzeuges unter dem Blickwinkel des Schutzbedarfs entsprechend ZCR 2
- Zuordnung der Funktionsgruppen zu Zonen (Kapitel 4.2) entsprechend ZCR 3
- Festlegung und Beschreibung der Zonenübergänge (Kapitel 4.1 und 5) entsprechend ZCR 3

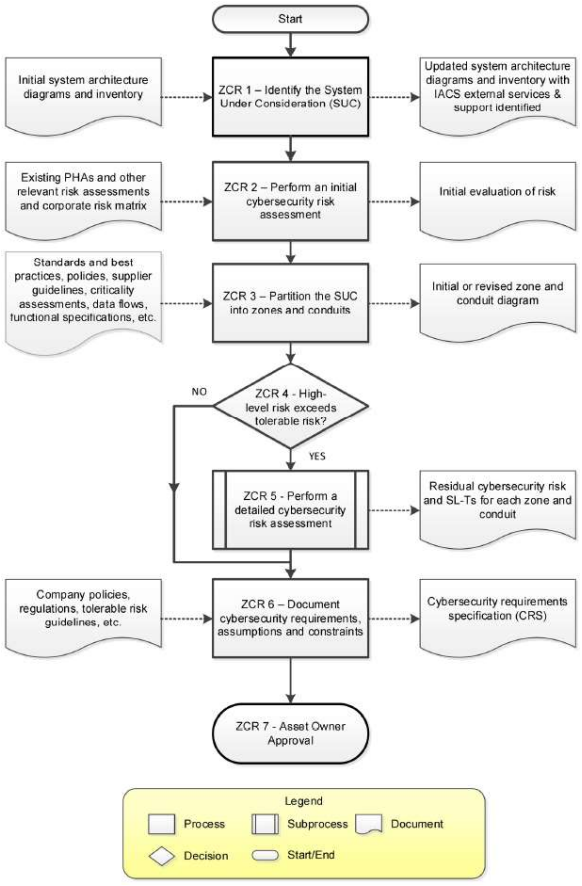

Abbildung 3: Arbeitsablaufdiagramm zur Festlegung der Zonen und Zonenübergänge sowie zur Beurteilung des Risikos (aus [23])

4 Grundlagen zur Definition des Betrachtungsobjektes „Schienenfahrzeug“

Um ein System bzgl. Security behandeln zu können ist es erforderlich, dieses Betrachtungsobjekt (System under Consideration SUC) und seinen Kontext so zu beschreiben, dass es möglichst alle Security Belange darstellt. Im Folgenden werden zunächst die Grundlagen unter Einbeziehung der einschlägigen Normen dargestellt.

4.1 Zonen und Zonenübergänge

Die Definition von Zonen und Zonenübergängen (Conduits) soll das Betrachtungsobjekt (System under Consideration SUC) vollständig beschreiben und stellt deshalb eine Teilaufgabe der Risiko Analyse dar, die dazu dient, Gefährdungen für das betrachtete System zu erkennen. Sind die Security Zonen einmal festgelegt, kann man die Conduits als Verbindungen zwischen jeweils zwei Zonen definieren.

4.1.1 Zonen

Gemäß dem IEC62443 Standard ist es erforderlich, das betrachtete Referenzsystem im Zug in Zonen zu unterteilen. Das Ziel, welches man damit verfolgt ist, Geräte mit ähnlichem Schutzbedarf und ähnlichen Risiken in dieselbe Zone zu gruppieren, aus dem Schutzbedarf der Zone lassen sich dann Security Eigenschaften ableiten, die diesen Schutzbedarf gewährleisten.

Im Abschnitt 4.2 wird beschrieben, welches Referenz Modell dazu angewendet wurde und welche Zonen daraus abgeleitet wurden. Neben dem Referenz Modell für die Zonen wurde auch ein Modell für die Conduits verwendet, welches diesem angepasst ist. Man muss stets im Auge behalten, dass es sich hier um Modelle handelt, die es erlauben generelle Aussagen zu machen. Wenn man reale Architekturen eines Zuges betrachtet wird man sehen, dass diese im Detail abweichen können.

Die Steuergeräte im Zug, die der Steuerung einer Funktion des Zugs gewidmet sind, können als Endgeräte der Zugsnetzwerke betrachtet werden. Diese finden sich in den verschiedenen Security Zonen wieder, denen sie – in Anlehnung an die TS 50701 - gemäß Funktionsgruppe, Kritikalität, gemeinsamer Security Eigenschaften oder anderer Merkmale zugeordnet werden.

4.1.2 Zonenübergänge

In den Conduits finden sich die Geräte, die die Übergänge zwischen den verschiedenen Zonen bilden, z.B. Switches, Routers, Firewalls, Gateways, Wireless Modems usw. Diese Netzwerkgeräte dienen primär dazu, die Kommunikation zwischen den Funktionen zu ermöglichen und den Datenfluss zu steuern. Für die Security übernehmen sie innerhalb des Conduits zusätzlich die Rolle, den Datenfluss zwischen den Zonen auch zu überwachen und Zugriffsregeln (Access Policies) zwischen den Zonen durchzusetzen.

Netzwerkgeräte können sich auch in einer Zone befinden, statt in einem Conduit. Ein Switch kann z.B. statt für die Regelung des Datenflusses zwischen den Zonen auch „nur“ dazu eingesetzt werden, unnötigen Datenverkehr in Netzwerk-Segmenten zu verhindern, z.B. durch Bilden von Broadcast Domains. Sind die Security Anforderungen dann für alle Broadcast Domains identisch, bildet dieser Switch dann aus Security Sicht kein Conduit, wird sich also in derselben Zone wie die anderen Geräte befinden, die über den Switch kommunizieren. Gemäß IEC62443 ist es deshalb auch nötig, für jede Zone und jedes Conduit genau zu definieren, welche Geräte darin enthalten sind.

In modernen Zügen findet man für Netzwerke immer mehr Ethernet Technologie, aber in bestehenden Flotten gibt es oft nur ältere oder ein Gemisch diverser Technologien. Deshalb werden spezifische Endgeräte oft an mehrere Netzwerke angeschlossen, je nach gewählter Architektur und Topologie (siehe **Abbildung**).

Vehicle Bus

- CAN (CANopen, J1939)
- Ethernet (z.B. Ethernet Consist Network nach IEC61375)
- MVB (z.B. im TCN verwendet)
- RS-485, RS-232, RS-422

Train Bus

- Ethernet (z.B. Ethernet Train Backbone nach IEC61375)
- CAN Powerline
- WTB

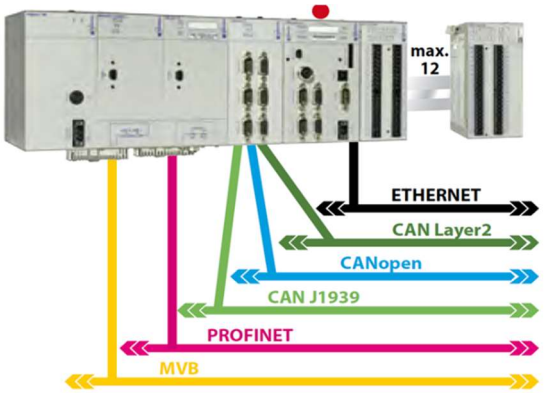

Abbildung 4 Verschiedene Netzwerktechnologien (Beispiel)

Typische Situationen:

Haben diese Netzwerke dann unterschiedliche Security Levels, stellt sich die Frage, wo die Zonengrenzen und die Conduits zu definieren sind. Im einfacheren Fall befindet sich ein solches Gerät innerhalb eines Conduits, weil es Zonenübergange mit Sicherungsmaßnahmen (z.B. mit Flusskontrolle) realisieren kann (z.B. ein Gateway, Switch, Firewall…). Dieser Fall ist in **5** dargestellt.

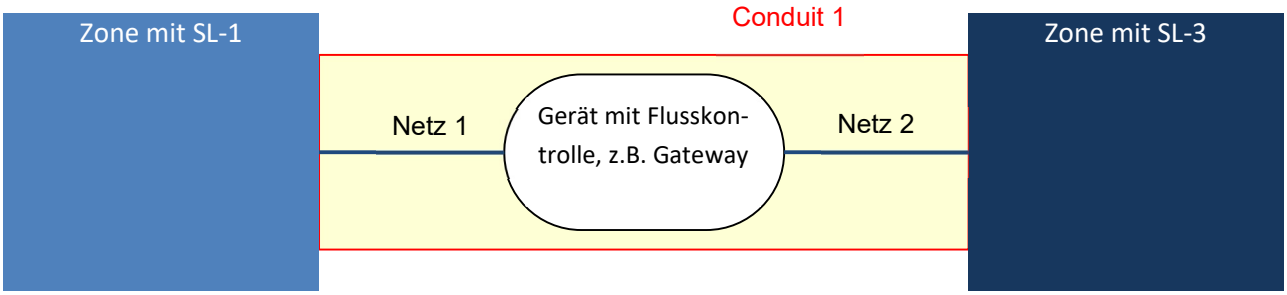

Abbildung 5: Zonengrenzen – Gerät mit Flusskontrolle

Kann ein solches Gerät hingegen keine Flusskontrolle wahrnehmen, muss aber trotzdem mit mehreren Zonen kommunizieren (z.B. eine einfache Steuereinheit (PLC o.ä.)), würden sich potenziell Zonenübergänge, wie in **Abbildung 6** unten „innerhalb“ des Gerätes ergeben.

Abbildung 6: Zonengrenzen – Gerät ohne Flusskontrolle

Lösungsmöglichkeiten:
Die weitere Analyse wird durch ein solches Modell erschwert, weil man für die Risiko-Analyse in das Gerät „hinein“ schauen müsste. Es ist deshalb oft einfacher, in solchen Fällen, das betroffene Gerät in eine eigene Zone zu legen und von dort Conduits zu allen angeschlossenen Netzen zu bilden (z.B. über eine Firewall), wie **Abbildung 7** zeigt. Dann muss das Innere des Gerätes nicht mehr betrachtet werden.

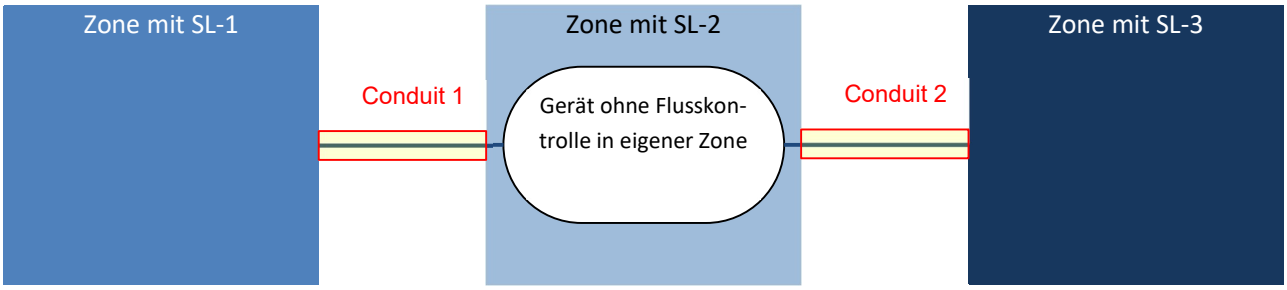

Abbildung 7: Zonengrenzen – Gerät ohne Flusskontrolle in eigener Zone

Bei gleichem Security Level wie eine der Zonen, kann es auch in diese Zone verschoben werden (siehe **Abbildung 8**).

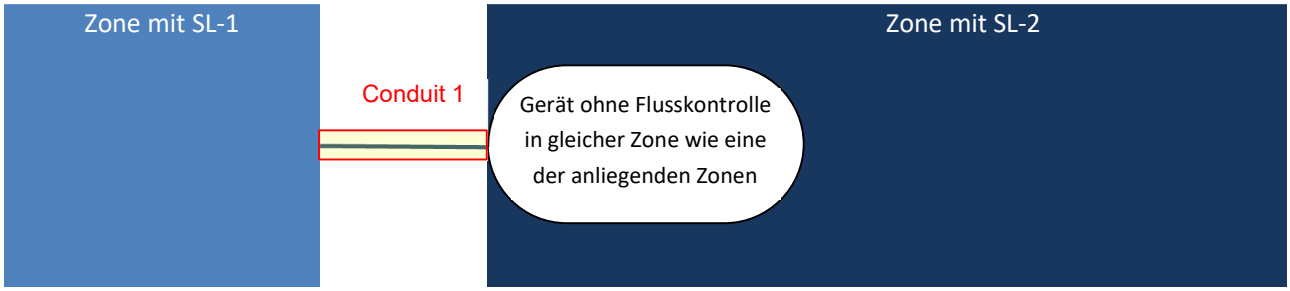

Abbildung 8: Zonengrenzen – Geräte ohne Flusskontrolle mit gleichem Security Level wie angrenzende Zone

Mit diesen Strukturen wird die weitere Analyse wieder möglich, ohne dass die innere Funktionalität und der Aufbau des Gerätes betrachtet werden muss.

Best Practice:
Ältere Technologien weisen u.U. geringere Risiken auf, da dafür weniger Angriffe und Werkzeuge bekannt sind. Diese Netzwerke sind zwar nicht gegen Abhören geschützt (fehlende Confidentiality im Standard), jedoch stellt das oft ein kleines Risiko dar. Das Security Level Target für ein Conduit muss sich am schwächsten Glied orientieren bzw. am größten Risiko ausrichten.

4.1.3 Aufbau der Security Architektur

Um die Komplexität einer Risiko Analyse zu reduzieren, ist es empfehlenswert zunächst logische Conduits zu betrachten. Diese sind der Einfachheit halber mit indiziertem Buchstaben Cx, also C1, C2, usw. durchnummeriert (siehe Abbildung 9). Dies ist deshalb nützlich, weil sie in einer ersten Übersicht die Beurteilung des Risikos erlauben, ohne zunächst auf technische Details der physischen Verbindungen einzugehen. In einer zweiten Iteration der Analyse kann dann jedes physische Netz eines Conduits individuell neu beurteilt werden. Diese Schritte entsprechen im IEC62443-3-2 Standard den High-Level und Detail-Level Risk Assessments.

In einer 1. Iteration wird man von den physischen Details eines Conduits abstrahieren und nicht berücksichtigen, welche Technologie eingesetzt wird. In der 2. Iteration wird man dann das Detail des Conduits anschauen und z.B.

feststellen, dass darin Ethernet, CAN und MVB Netze enthalten sind. Im Detail wird dabei die Angriffsfläche für Ethernet in diesem Beispiel grösser ausfallen als jene für CAN oder MVB, schon nur wegen der publizierten Schwachstelle (Vulnerability) wie auch der öffentlich zugänglichen Angriffswerkzeuge für diese Schwachstelle.

In der verwendeten Darstellung, welche als Matrix aufgebaut wurde, finden sich in den Spalten die Funktionsgruppen und Funktionen wieder. In den Zeilen sind die verschiedenen Netzwerkzonen aufgeführt, hier also z.B. das Train Control System (TCN) usw. (siehe **Abbildung 9**)

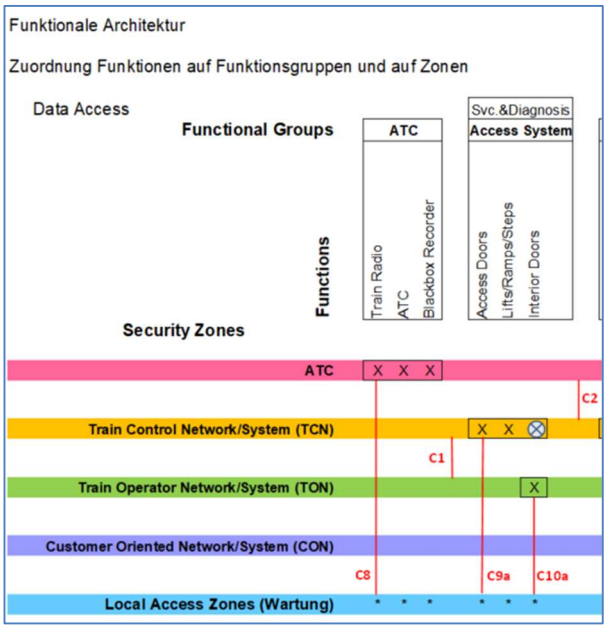

Abbildung 9: Zuordnung Funktionen auf Funktionsgruppen und auf Zonen

Befindet sich ein Endgerät (bzw. dessen Funktion) in einer Zone, dann wird dort im Schnittpunkt von Spalte (Funktion) und Zeile (Zone) ein «X» eingetragen. Funktionen, die einer übergeordneten Funktionsgruppe zugehören, werden mit einer Umrandung der Zellen markiert, so dass alle «X» sich dann in einem durch den Rahmen markierten Rechteck befinden. In einigen Fällen befindet sich das «X» innerhalb eines Kreises. Damit wurden Funktionen identifiziert, die sich in realen Architekturen oft physisch oder logisch in einer anderen Zone befinden als der Rest der Funktionen dieser Gruppe. Es kann in diesen Architekturen unter Umständen sinnvoll sein, diese Funktionen in der Folge in die jeweils andere Zone zu verlagern, um einen einheitlichen Schutz über die Zone zu erreichen.

In dieser Darstellung kann man die Conduits dann als, hier rot markierte und mit Cx beschriftete, vertikale Linien einzeichnen. Zwischen zwei Zonen (hier Zeilen), gibt es dann immer nur höchstens eine Linie, also ein logisches Conduit, wenn diese Zonen verbunden sind. Den Fluss des Datenverkehrs kann man sich innerhalb der Zone als horizontal (in der Zeile) vorstellen und im Übergang in die andere Zone dann vertikal in der roten Linie.

Will man in einer weiteren Analyse dann die physischen Netze betrachten und analysieren, kann es Sinn machen, diese weiter unten im Diagramm auch als hier grau unterlegte Zeilen aufzuführen. In diesen Linien markiert das «X» dann, ob die Funktion mit diesem physischen Netz verbunden ist. In unserem Beispiel sind jene physischen Technologien aufgelistet, die man heute in Schienenfahrzeugen am meisten vorfindet.

4.2 Ableitung der Zonen für Referenzmodell Schienenfahrzeug

Ein Schienenfahrzeug beinhaltet eine große Anzahl von Funktionsgruppen, die so unterschiedlichen Bereichen wie z.B. Fahren und Bremsen oder Fahrgastinformation zuzuordnen sind. Diese Bereiche sind bezüglich ihrer Sicherheitsrelevanz (Safety) sehr unterschiedlich einzustufen. Während Eingriffe in die Zugsteuerung naturgemäß besonders gefährlich sind, können Störungen der Fahrgastinformation in vielen Fällen als reine Unannehmlichkeit angesehen werden.

Für eine systematische Bewertung der Funktionsgruppen eines Schienenfahrzeuges musste zunächst eine umfassende Übersicht aller für die Funktion relevanten Funktionsgruppen gefunden werden. Basis war dafür die DIN EN 15380 [22], die einen Katalog der im Fahrzeug enthaltenen Funktionsbereiche enthält.

Die in der DIN EN 15380 aufgeführten Funktionsgruppen wurden unter dem Blickwinkel des Schutzbedarfs in fünf Sicherheitsbereiche entsprechend ZCR 2 (Security Zonen) gruppiert:

- Automatic Train Control (ATC)
- Train Control Network (TCN)
- Train Operator Network (TON)
- Customer Oriented Network (CON/Public)
- Wartung (Maintenance)

Diese Sicherheitsbereiche orientieren sich an der Erfahrung der Experten aus dem Bereich Schienenfahrzeuge sowie ähnlichen Definitionen internationaler Gremien (z.B. CENELEC AK 50701).

Ausgangspunkt war die interne Definition der Sicherheitsbereiche eines großen deutschen Fahrzeughersteller, der die vier Kernbereiche ATC, TCN, TON und CON betrachtet.

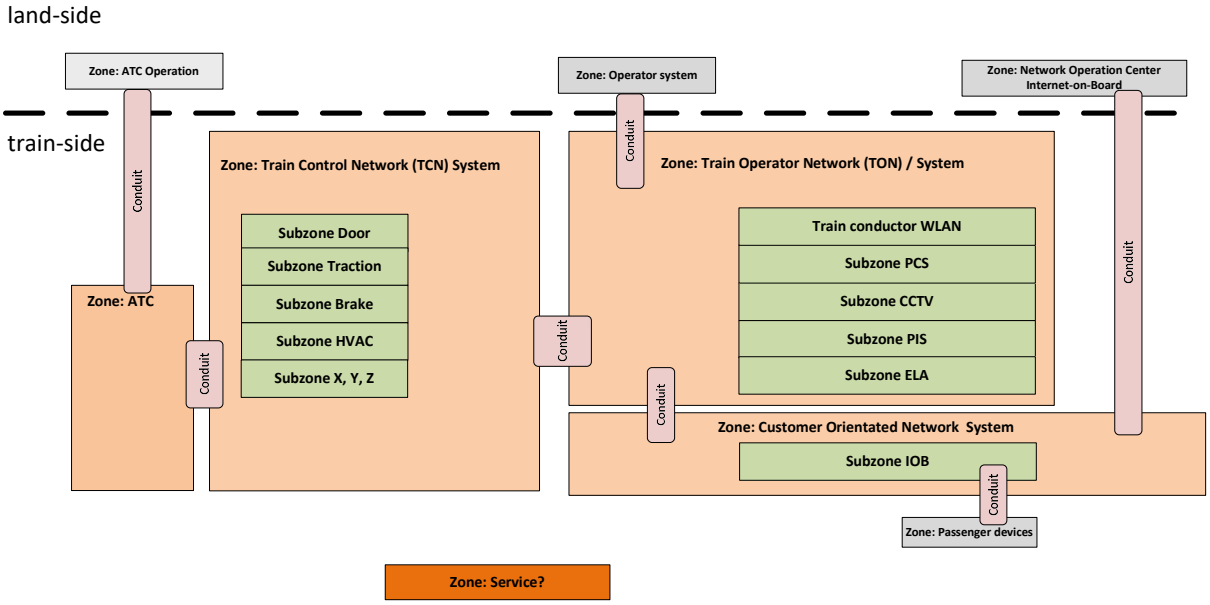

Abbildung 10 Zuordnung der wesentlichen Funktionsgruppen eines Fahrzeuges zu den genannten Security Zonen

In Abbildung 10 ist die in der Arbeitsgruppe gefundene Zuordnung der wesentlichen Funktionsgruppen eines Fahrzeuges zu den genannten Security Zonen dargestellt. Diese Darstellung bezieht sich auf moderne Triebzüge. Für andere Zugkonfigurationen kann sie im Detail abweichen.

Die Security Zonen sind - in der Rangfolge ihrer Kritikalität - wie folgt definiert:

- **Automatic Train Control (ATC)**
  Beschreibt die Fahrzeug-seitigen Zugsicherungssysteme (z.B. ETCS, LZB) und zusätzlich die Automatic Train Operation (ATO).
- **Train Control Network (TCN)**
  Mit allen Funktionsgruppen, die für Fahren und Bremsen erforderlich sind zusammen mit der Energieversorgung des Fahrzeuges und dem System der äußeren Zugangstüren. Ebenfalls hier zugeordnet sind die Brandschutzanlagen. Im Arbeitskreis wurde daneben – anders als in anderen Studien - die Klimaanlage inklusive Druckschutzsystem hier eingeordnet. Die genannten Systeme sind für den Zugbetrieb unbedingt erforderlich (sicherheitsrelevant). Bei einem Ausfall kann die Fahrt nicht fortgesetzt werden.
  Neben den obengenannten Funktionsgruppen wurden diesem Bereich weitere für den Betrieb des Fahrzeuges wichtige Funktionsgruppen zugeordnet. Das umfasst u.a. die Innentüren und die Beleuchtung. Im

Unterschied zu anderen Studien wurden im Arbeitskreis außerdem die Toiletten und die Beschallungs- und Kommunikationsanlagen diesem Bereich zugeordnet. Bei Ausfall eines dieser Systeme kann der Zugbetrieb nur mit erheblichen Einschränkungen fortgeführt werden.
In anderen Studien werden diese beiden Bereiche unterschieden und in eigene Sicherheitszonen zugeordnet. Nach Ansicht der Mitglieder des Arbeitskreises hat eine solche Unterteilung auf die erforderlichen Security-Anforderungen aber keine relevanten Auswirkungen, so dass sie hier keine Unterscheidung vorgenommen wurde.

- **Train Operator Network (TON)**
  Mit allen Funktionsgruppen, die für die Betreuung der Fahrgäste erforderlich sind. Im Einzelnen sind dies die Fahrgastinformationssysteme ergänzt um die mobilen Geräte der Zugbegleiter für die Fahrgastbetreuung sowie Videoüberwachungs- und Fahrgastzählsysteme. Ein Ausfall dieser Systeme ist betriebsbehindernd, die Zugfahrt kann aber meist – mit Einschränkungen – fortgeführt werden.
- **Customer oriented Network (CON/Public)**
  Mit allen Funktionsgruppen, die für die Anbindung und Stromversorgung der privaten Geräte der Fahrgäste erforderlich sind. Hierzu gehören Mobilfunk-Repeater, Internetzugänge über Wireless LAN und auch die 230V Steckdosen im Sitzbereich. Ein Ausfall dieser Systeme kann die Möglichkeiten der Fahrgäste zur persönlichen Kommunikation und Unterhaltung einschränken, behindert aber nicht direkt die Fahrt.
- **Wartung (Maintenance)**
  Hier sind alle Wartungszugänge zu den diversen steuernden Systemen im Zug zusammengefasst. Da praktisch jede Steuereinheit einer Funktionsgruppe über einen Wartungszugang verfügt, sind diese über alle Sicherheitsbereiche des Zuges verteilt. Während der Fahrt werden die Wartungszugänge üblicherweise nicht genutzt, so dass ein Ausfall keine unmittelbaren Auswirkungen auf den Zugbetrieb hat. Aufgrund der Möglichkeit über einen Wartungszugang auf kritische Systeme einwirken zu können, ist ihr Schutz aber von besonderer Bedeutung.

Während viele der obigen Zuordnungen von Funktionsgruppen zu Sicherheitsbereichen selbsterklärend sind, bedürfen andere Zuordnungen einer näheren Erläuterung:

Zuordnung betriebswichtiger Funktionen zum Train Control Network

- **Klimaanlage (HVAC)**
  Hintergrund ist, dass in modernen Triebzügen mit versiegelten Fenstern bei Ausfall der Klimaanlage die Frischluftversorgung zum Erliegen kommt und die Fahrt in vielen Fällen – z.B. bei hohen Außentemperaturen - abgebrochen werden muss.
- **Druckschutz (Pressure Protection)**
  Der Druckschutz dient speziell bei Tunnelfahrten dazu die Passagiere vor gefährlichen Druckstößen zu schützen. Ein Ausfall kann zum Abbruch der Fahrt führen.
- **Küche (Galley)**
  Speziell aus Hygieneerwägungen können Ausfälle im Bereich der Küche – wie z.B. die Wasserdesinfektion – unmittelbar gesundheitsgefährdende Folgen haben.

Zuordnung stark betriebsbehindernder Funktionen zum Train Control Network

- **Toilettensystem**
  Im Fernverkehr ist - besonders bei langen Fahrtabschnitten ohne Halt eine Mindestausstattung mit funktionsfähigen Toiletten obligatorisch. Ein umfassender Ausfall des Systems kann deshalb unter bestimmten Umständen den Abbruch der Fahrt erfordern.

- **Beschallungsanlage (PA)**
  Für die Warnung der Passagiere vor Gefahren, wie z.B. Bränden ist es erforderlich, dass das Zugpersonal die Möglichkeit hat, Durchsagen spezifisch für den jeweiligen Gefahrenfall zu machen und ggf. Anweisungen zu einer geregelten Evakuierung zu geben. Wenn diese Möglichkeit entfällt, muss die Fahrt in vielen Fällen abgebrochen werden.
- **Betriebliches Kommunikationssystem**
  Um den betrieblichen Ablauf – speziell in Fernverkehrszügen, in denen mehrere Zugbegleiter an Bord sind, – zu organisieren, wird ein betriebliches Kommunikationssystem benötigt, an dem das gesamte Zugpersonal einschließlich des Triebfahrzeugführers angebunden ist. Auch hier führt eine Nichtverfügbarkeit in vielen Fällen zum Abbruch der Fahrt.
  Ebenfalls Teil des Kommunikationssystems sind Sprecheinrichtungen in PRM-Toiletten, an Rollstuhlplätzen usw. Fallen sie aus, so muss in vielen Fällen Zugpersonal zur Überwachung dieser Einrichtungen abgestellt werden.

Zuordnung betriebseinschränkender Funktionen zum Train Operator Network

- **Fahrgastinformationssystem**
  Speziell in komplexen Situationen, wie z.B. einer Zugteilung im Laufe der Fahrt kann der Betrieb des Zuges nur mit großem persönlichen Einsatz des Zugpersonals aufrechterhalten werden, wenn diese Systeme ausfallen, so dass sie heute zum Grundbestandteil für den Zugbetrieb gehören.
- **Mobilgerät für Zugbegleiter**
  Inzwischen sind Mobilgeräte für die Zugbegleiter und ihre Anbindung an stationäre Systeme aus dem täglichen Betrieb nicht mehr wegzudenken. Ein Ausfall beeinträchtigt die Servicequalität erheblich.
- **CCTV**
  Um die persönliche Sicherheit der Fahrgäste speziell in Zügen ohne Zugbegleiter zu gewährleisten und die Beweissicherung bei Straftaten zu ermöglichen werden heute in vielen Zügen Videoüberwachungsanlagen eingesetzt. Ein Ausfall kann die Strafverfolgung erschweren.
- **Fahrgastzählsysteme**
  Fahrgastzählsysteme dienen zur Steuerung der Auslastung. Eine Störung kann mittelbar zu einer Überbelegung von Zügen führen. Kurzfristige Auswirkungen sind dagegen nicht zu erwarten.

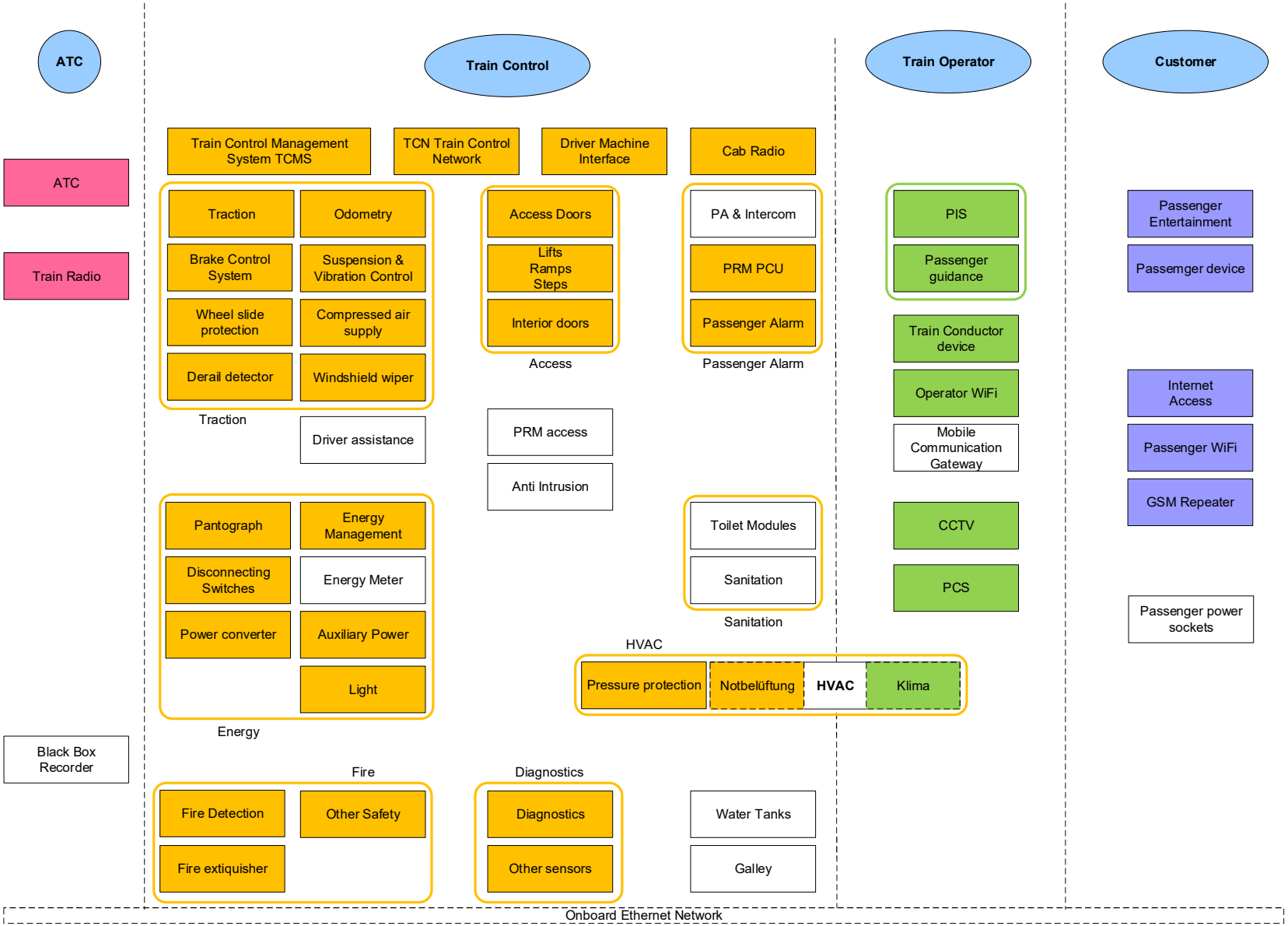

Abbildung 11: Zuordnung von Komponenten zu Sicherheitsbereichen (Zonen)

5 Generische Security Architektur Modell

Anhand von 2 sollen hier die wesentlichen Betrachtungen für das Security Architektur Modell eines Beispiel Fahrzeuges dargestellt werden.

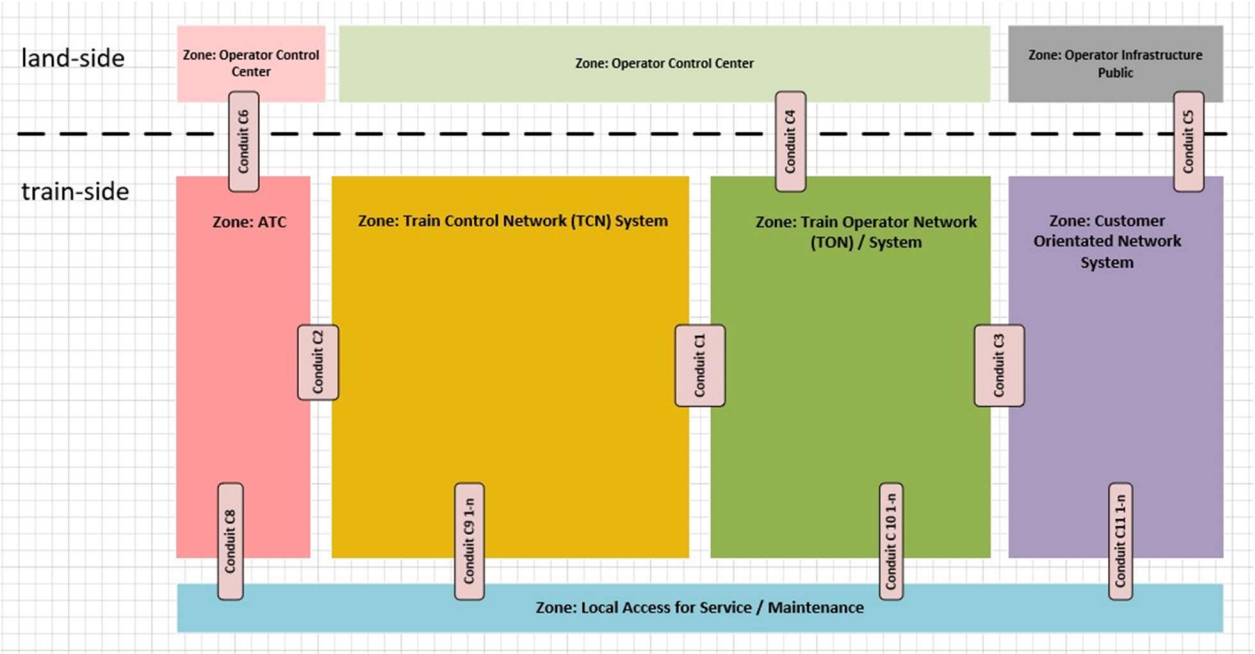

Abbildung 12: Security Architektur Modell am Beispiel eines Fahrzeuges

Es sind acht Zonen dargestellt, nämlich einerseits jene, die in Kapitel 4.2 beschrieben sind. Dies sind zum einen Zonen auf dem Zug und zum anderen zwei weitere Zonen „Operator Control Center Zone OCC“ und „Operator Infrastructure Public Zone OIP“, die sich außerhalb des Zuges befinden.

Bei der Definition des „System under Consideration“ SuC wird also davon ausgegangen, dass die Zonen aus Abschnitt 4.2 zum SuC gehören, OCC und OIP hingegen die umgebenden Systeme darstellen.

Gefährdungen können über die umgebenden Systeme oder die Wartungszonen eingeschleust werden. Diese Zonen müssen betrachtet werden, um mögliche Angriffspfade zu beurteilen.

Um das SuC weiter zu beschreiben ist es nötig, für jede Zone die darin enthaltenen Geräte („Assets“) aufzulisten und deren Funktion kurz zu beschreiben. Ein erster Ansatz ist in Abschnitt 4.2 sichtbar, um alle Systeme systematisch und strukturiert aufzulisten und zu beschreiben. Diese Listen helfen, die Risiko Analyse ebenso strukturiert durchführen zu können und darüber eine Vollständigkeit zu erreichen.

Sind die Zonen festgelegt, müssen auch die Conduits beschrieben werden. Ein Conduit verbindet immer zwei Zonen und wird deshalb durch diese zwei Zonen definiert. In der generischen Architektur wurden folgende logische Conduits identifiziert:

- **Conduit C1:** verbindet Zone TCN und TON
- **Conduit C2:** verbindet Zone ATC und TCN
- **Conduit C3:** verbindet Zone CON und TON
- **Conduit C4:** verbindet Zone TON und OCC

- **Conduit C5:** verbindet Zone OCC und CON
- **Conduit C6:** verbindet Zone ATC und OCC
- **Conduit C7:** verbindet Zone(n) Wartung und OCC (speziell handelt es sich hier um das Conduit für Fernwartung)
- **Conduits C8, 9, 10 und 11:** verbinden die Geräte mit der Zone (bzw. den Zonen) Wartung
- **Conduit C12:** verbindet Zone OIP mit CON (zentraler Internetzugang)

Auch für die Conduits sollen die darin enthaltenen Geräte aufgelistet werden. Oft findet man hier Netzwerkgeräte, Switches, Gateways, Firewalls, usw.

Stellt man in **Abbildung 12** die Zusammenhänge dar, sieht man schnell, dass die «Local Access Zones» generell ein bedeutendes Risiko darstellen. Hier findet man meistens die lokalen, auf Ethernet, IP und Web-Browser basierenden Schnittstellen für die Wartung der Geräte. Gemäß IEC62443 Standard muss jedes externe Gerät, das temporär am Zug angeschlossen wird, also z.B. der Wartungs-PC, in einer eigenen, separaten Zone angesiedelt werden und die Schnittstelle muss ein eigenes Conduit zu dieser Zone haben. Da in jedem Zug Geräte von vielen unterschiedlichen Herstellern vorhanden sind, muss der Betreiber für die Risikobetrachtung und für die Schutzmaßnahmen für jeden Geräte-Hersteller mindestens eine solche Zone planen (deshalb steht hier Zones auch in der Mehrzahl).

Um das Bild nicht zu überlasten, musste bei den Conduits zu diesen «Local Access Zones» die Darstellung etwas vereinfacht werden. Wie oben erwähnt, muss man für jedes Gerät eines anderen Herstellers eine separate Zone für die Wartungsschnittstelle definieren. Diese ist mit einem Asterisk (*) in der «Local Access Zones» markiert. Statt ein Conduit für jede Funktion in diese Zone einzutragen, ist hierfür nur einmal pro Funktionsgruppe ein Conduit eingezeichnet. Diese Conduits sind zusätzlich mit einem kleinen Buchstaben indexiert. Dieser Buchstabe markiert dann unterschiedliche Funktionsgruppen. Dies soll an folgendem Beispiel verdeutlicht werden: C9a markiert das Conduit zwischen der Funktionsgruppe «Access System» und der «Local Access Zones». Die «9» markiert dabei die Verbindung zwischen den Zonen, das «a» hingegen die Funktionsgruppe. Alle Wartungs-Conduits der Funktionsgruppen, die sich in der Zone TCN befinden, tragen die Nummer 9.

Man sieht also, dass das Fehlen einer einheitlichen Wartungsschnittstelle sowohl die Analyse der Risiken wie auch deren Minderung stark erschwert.

5.1 Tabelle Zuordnung Funktionen auf Funktionsgruppen und Zonen unter Berücksichtigung der Zonenübergänge (Conduits)

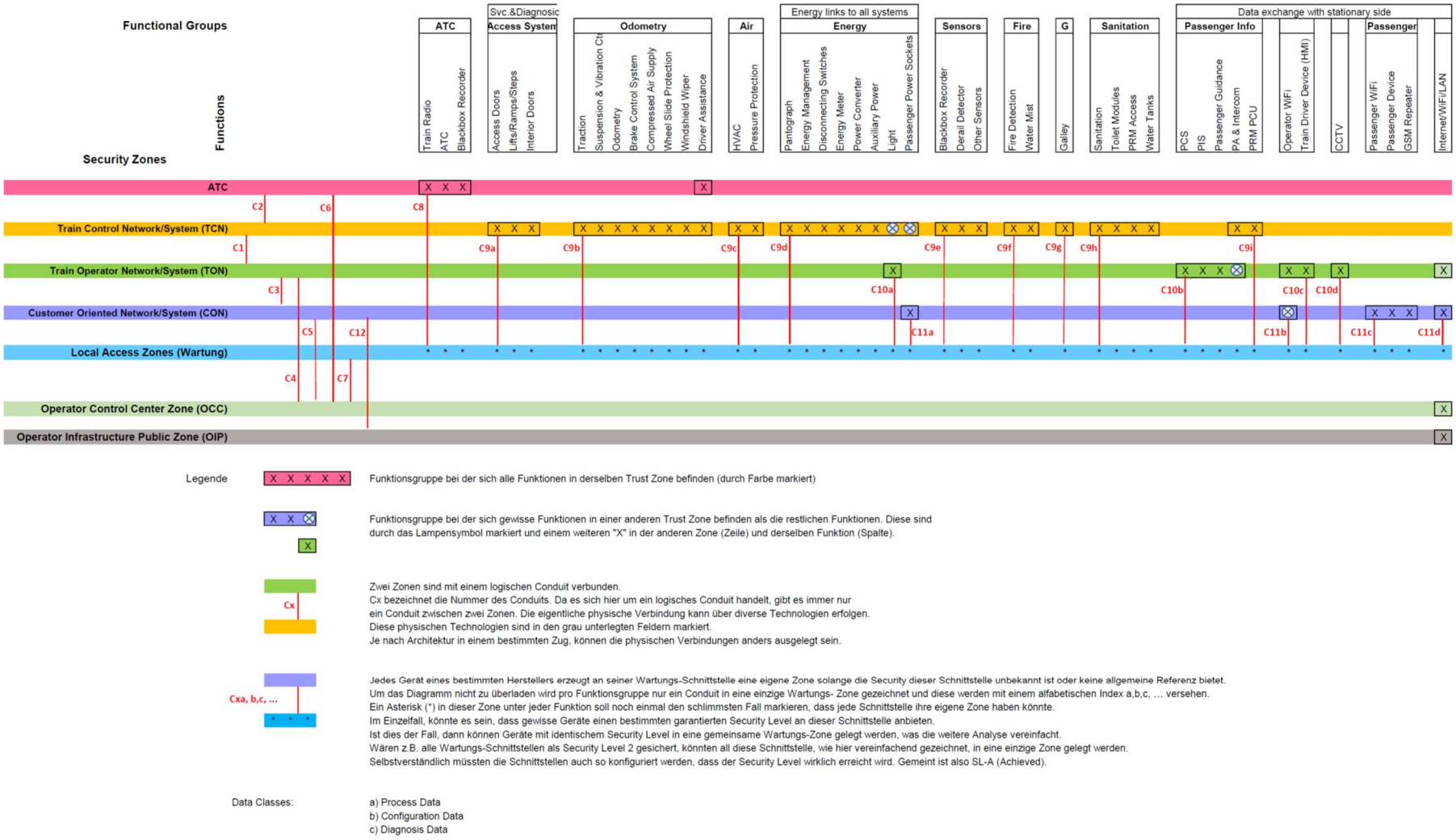

Abbildung 13 Tabelle Zuordnung Funktionen auf Funktionsgruppen und Zonen unter Berücksichtigung der Zonenübergänge (Conduits)

6 Zusammenfassung und Ausblick

Dieser Bericht erarbeitet ein generisches IT Security Architekturmodell von Schienenfahrzeugen in dem er die Schritte des Arbeitsablaufdiagramms zur Festlegung der Zonen und Zonenübergänge sowie zur Beurteilung des Risikos aus der DIN EN 62443-3-2 [23] auf einen typischen Triebzug anwendet.

Als Ergebnis entstand eine Tabelle mit der Zuordnung der typischen Funktionen des Triebfahrzeuges auf Funktionsgruppen und Zonen unter Berücksichtigung der Zonenübergänge (Conduits). Diese Tabelle ist als Handreichung für die praktische Analyse von Schienenfahrzeugen gedacht.

Um deren Anwendung zu erleichtern wird im Bericht die Herleitung der Tabelle beginnend mit der gesetzlichen und normativen Einbettung über das Vorgehen bei der Ermittlung der Zonen und Zonenübergänge im Detail dargestellt.

Bei der Erarbeitung der genannten Tabelle wurde deutlich, dass eines der größten Risiken für eine Gefährdung der IT-Sicherheit in den Wartungszugängen liegt. Hier bietet sich eine Vertiefung im Rahmen einer weiterführenden Untersuchung an – speziell im Hinblick auf eine Standardisierung.

7 Verzeichnisse

7.1 Abbildungsverzeichnis

7.2 Literaturangaben

[1] BSI 200-1:2017-10. *BSI-Standard 200-1: Managementsysteme für Informationssicherheit (ISMS)*. https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzStandards/Standard201/ITGStandard201_node.html, abgerufen am: 02.12.2020

[2] Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union. NIS. In: Amtsblatt der Europäischen Union

[3] Der Bundestag: Gesetz zur Umsetzung der Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union, Bd. 2017. 2017

[4] Bundesamt für Sicherheit in der Informationstechnik: Homepage des Bundesamt für Sicherheit in der Informationstechnik (BSI). https://www.bsi.bund.de, abgerufen am: 04.12.2020

[5] Der Bundestag: Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz - BSIG). BSIG

[6] Bundesministerium des Innern: Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-Kritisverordnung - BSI-KritisV). BSI-KritisV. Ausfertigungsdatum: 2016

[7] Allgemeines Eisenbahngesetz. AEG. 1993 (2020)

[8] Eisenbahn-Bau- und Betriebsordnung. EBO. 1967 (2019)

[9] Verordnung über den Bau und Betrieb der Straßenbahnen(Straßenbahn-Bau- und Betriebsordnung - BOStrab). BOStrab. 1987 (2019)

[10] Bundesländer: Verordnung über den Bau und Betrieb von Anschlussbahnen. BOA

[11] VDV 440:2020-07. *VDV-Schrift 440 Branchenanforderungen an die IT-Sicherheit*. https://www.beka-verlag.info/VDV-Schriften/Informationstechnik-Informationsverarbeitung/Nachrichtentechnik/VDV-Schrift-440-Branchenanforderungen-an-die-IT-Sicherheit-Print::1029.html, abgerufen am: 02.12.2020

[12] VDV-Mitteilung 4400:2020-07. *VDV-Mitteilung 4400 Maßnahmenkatalog zur VDV-Schrift 440 - Maßnahmen für personelle, organisatorische und bauliche/physische Sicherheit sowie branchenspezifische Technik*. https://www.beka-verlag.info/VDV-Mitteilungen/Informationstechnik-Informationsverarbeitung/Nachrichtentechnik/VDV-Mitteilung-4400-Massnahmenkatalog-zur-VDV-Schrift-440-eBook::487.html, abgerufen am: 02.12.2020

[13] ISO IEC 27001:2013-09. *Information technology -- Security techniques -- Information security management systems -- Requirements*. https://webstore.iec.ch/publication/11286, abgerufen am: 07.12.2020

[14] DIN EN ISO / IEC 27001:2017-06:2017. *Informationstechnik –Sicherheitsverfahren –Informationssicherheitsmanagementsysteme – Anforderungen (ISO/IEC 27001:2013 einschließlich Cor 1:2014 und Cor 2:2015);Deutsche Fassung EN ISO/IEC 27001:2017*. https://www.beuth.de/de/norm/din-en-iso-iec-27001/269670716, abgerufen am: 27.10.2020

[15] BSI 200-2:2017-10. *BSI-Standard 200-2: IT-Grundschutz-Methodik*. https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzStandards/Standard202/ITGStandard202_node.html, abgerufen am: 02.12.2020

[16] BSI 200-3:2017-10. *BSI-Standard 200-3: Risikomanagement. BSI 200-3*. https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzStandards/Standard203/ITGStandard203_node.html, abgerufen am: 02.12.2020

[17] BSI 100-4:2008-11. *Notfallmanagement. BSI-Standard 100-4 zur Business Continuity*. http://deposit.d-nb.de/cgi-bin/dokserv?id=3099909&prov=M&dok_var=1&dok_ext=htm

[18] Bundesanzeiger Verlag GmbH u. Deutschland: IT-Grundschutz-Kompendium. Unternehmen und Wirtschaft. Köln: Reguvis Bundesanzeiger Verlag; Bundesanzeiger Verlag 2018

[19] prEN TS CEN 50701. *prEN TS 50701 Railway applications - Cybersecurity*

[20] IEC TS 62443-1-1:2009-07:2009-07. *Industrial communication networks. Network and system security*. https://webstore.iec.ch/publication/7029, abgerufen am: 13.10.2020

[21] IEC 62443-2-1:2010-11:2010-11. *Industrial communication networks – Network and system security – Part 2-1: Establishing an industrial automation and control system security program. Network and system security*. https://webstore.iec.ch/publication/7030, abgerufen am: 26.10.2020

[22] IEC TR 62443-2-3:2015-06:2015-06. *Security for industrial automation and control systems - Part 2-3: Patch management in the IACS environment*. https://webstore.iec.ch/publication/22811, abgerufen am: 26.10.2020

[23] IEC 62443-2-4:2017-08:2017-08. *Security for industrial automation and control systems – Part 2-4: Security program requirements for IACS service providers*. https://webstore.iec.ch/publication/61335, abgerufen am: 26.10.2020

[24] IEC 62443-3-3:2013-08:2013-08. *Industrial communication networks –Network and system security –Part 3-3: System security requirements and security levels*. https://webstore.iec.ch/publication/7033, abgerufen am: 26.10.2020

[25] TeleTrusT - Bundesverband IT-Sicherheit e.V.: TeleTrusT zu IEC 62443-4-2, 2021. https://www.teletrust.de/publikationen/teletrust-iec-62443-4-2/, abgerufen am: 27.02.2021

7.3 Abkürzungsverzeichnis

AEG	Allgemeines Eisenbahn Gesetz
ATC	Automatic Train Control
BOStrab	Betriebsordnung Straßenbahn
BSI	Bundesamt für Sicherheit in der Informationstechnik
CAN	Controler Area Network
CCTV	Closed Circuit TV (Videoüberwachung)
CON	Customer Oriented Network
EBA	Eisenbahn Bundesamt
EBO	Eisenbahn Betriebsordnung
EIU	Eisenbahn Infrastrukturunternehmen
EVU	Eisenbahn Verkehrsunternehmen
FIS	Fahrgastinformationssystem
LEA	Landeseisenbahnaufsicht
MVB	Multi Vehicle Bus
ÖPNV	Öffentlicher Personen-Nahverkehr
PA	Public Address
PCU	Passenger Communication Unit
PRM	People with reduced mobility
SUC	System under Consideration
TAB	Technische Aufsichtsbehörde der Bundesländer
TCN	Train Control Network
TON	Train Operator Network
WTB	Wire Train Bus