IT-Sicherheit auf Schienenfahrzeugen – Vom gesetzlichen Kontext zur generischen Architektur

Der Arbeitskreis IT-Sicherheit des CNA (Center for Transportation & Logistics Neuer Adler) hat, ausgehend von den rechtlichen und normativen Vorgaben, eine praxistaugliche generische IT-Sicherheitsarchitektur für Schienenfahrzeuge entwickelt.

Einleitung

Durch aktuelle technologische Weiterentwicklungen im Bereich der Digitalisierung bieten sich auch für Schienenfahrzeuge neue Potenziale. Die immer stärker werdende Vernetzung der Systeme ermöglicht neue Funktionen für Betrieb und Instandhaltung, die einen deutlichen Mehrwert versprechen. Diese Tendenz erleichtert es aber auch potenziellen Angreifern auf diese Systeme im Fahrzeug zuzugreifen.

Während die funktionale Sicherheit (Safety) bei Schienenfahrzeugen seit Langem ein wichtiger Faktor ist, bekommt nun auch die IT-Sicherheit (Security) eine zunehmende Relevanz. Vor diesem Hintergrund fordert der Gesetzgeber im Bereich der kritischen Infrastrukturen Maßnahmen zur Reduzierung des Risikos bezüglich IT-Sicherheit. Aber auch in allen anderen Bereichen ergeben sich durch die IT-Sicherheit selbst und deren Rückwirkungen auf die funktionale Sicherheit vielfältige neue Anforderungen für Betreiber und Hersteller von Schienenfahrzeugen.

Aus dem Bereich der Automatisierungstechnik findet die Norm DIN EN 62443, unter Einbeziehung der TS 50701, auch im Schienenfahrzeugbereich zunehmend Anwendung. Der Untersuchungsgegenstand ist hier das Schienenfahrzeug mit vernetzten Systemen, deren Schnittstellen und Kommunikationseinrichtungen, sowie deren äußeren Schnittstellen zur Integration in das Gesamtsystem Bahn.

Der vorliegende Artikel macht basierend darauf einen Vorschlag für eine ganzheitliche IT-Sicherheitsarchitektur für Schienenfahrzeuge. Im folgenden Abschnitt fasst er die regulatorischen Rahmenbedingungen der betreffenden Gesetze und Normen zusammen und beschreibt die organisatorische Einbettung der beteiligten Organisationen. Anschließend wird das Schienenfahrzeug, am Beispiel eines modernen Triebzuges, als Untersuchungsgegenstand aus IT-Security-Sicht definiert. Der Hauptteil des Artikels entwickelt ein ganzheitliches IT Security Architekturmodell für einen generischen Triebzug. Dies soll als Leitfaden und Vorgehensmodell die praktische Anwendung der IT-Sicherheit auf Schienenfahrzeugen unterstützen und die Handhabung des Industriestandards EN 62443 für Schienenfahrzeuge erleichtern. Weiterführende Fragestellungen (z.B. die Wartungsschnittstelle) werden im Ausblick aufgegriffen.

Gesetze & Normen

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 Bild 1). So fordert die EU-Richtlinie 2016/1148 [1] „… Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen…“ (NIS-Richtlinie) und deren Umsetzungsgesetz in Deutschland eine nationale Strategie für die Sicherheit von Netz- und Informationssystemen, sowie Sicherheitsanforderungen und Meldepflichten für die Betreiber und Anbieter „wesentlicher“ Dienste.

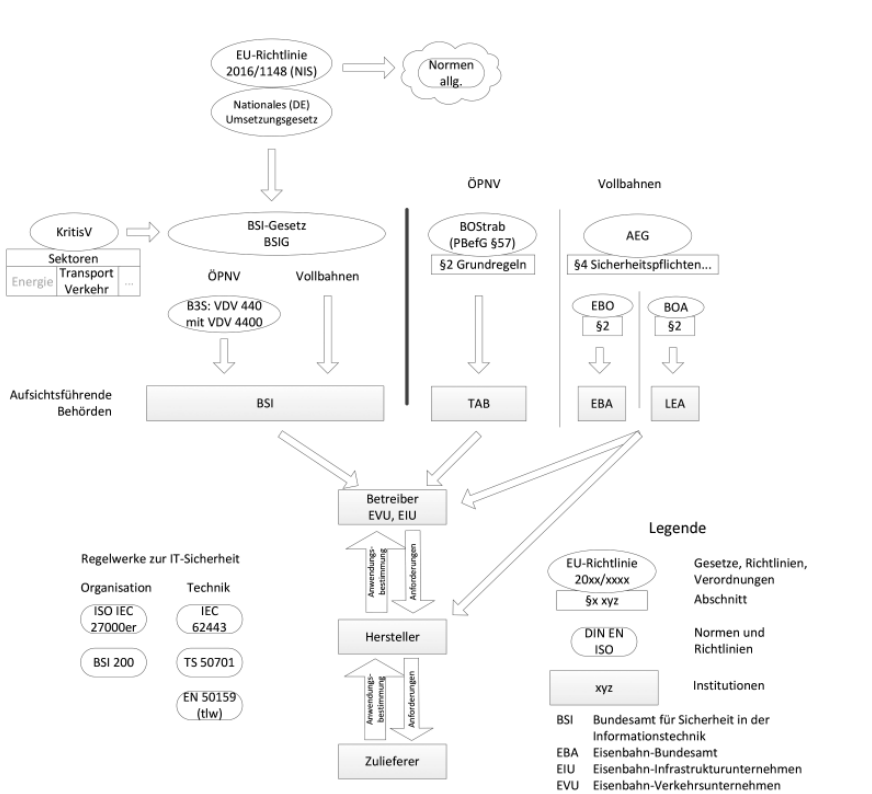
Friedrich Feistle
Business Development für Fahrgastinformationssysteme in Schienenfahrzeugen bei ANNAX mit Schwerpunkt Systemtechnik
friedrich.feistle@Wabtec.com

Martin Kursawe
Leiter Fahrzeugsoftware, Informationstechnik in der Business Line Engineering innerhalb der DB Systemtechnik GmbH. Beim Eisenbahn-Bundesamt anerkannter Gutachter für Fahrzeuge, Prüfung der Fahrzeugleittechnik, Schwerpunkt: Erstellung und Änderung von Software
martin.kursawe@deutschebahn.com

Daniel Lüdicke
Wissenschaftlicher Mitarbeiter am Institut für Systemdynamik und Regelungstechnik des Deutschen Zentrums für Luft- und Raumfahrt. Mit dem Forschungsschwerpunkt auf kommunikationsbasierten Schienenfahrzeug-Fahrwerksanwendungen
daniel.luedicke@dlr.de

Jürgen Sept
Product and Solution Security Officer und damit verantwortlich für IT-Sicherheit für alle Schienenfahrzeugprojekte der Siemens Mobility GmbH Rolling Stock
juergen.sept@siemens.com

Paolo Fanuli
Leiter Knorr Bremse SfS Kompetenzzentrum für Produkt Cyber Security
paolo.fanuli@selectron.ch



1: IT-Sicherheitsanforderungen an Schienenfahrzeugbetreiber und -hersteller

In Deutschland ist das Bundesamt für Sicherheit in der Informationstechnik (BSI) eine zentrale Stelle im Bereich IT-Sicherheit. Seine Aufgaben beschreibt das BSI-Gesetz (BSIG) [2]. Welche Institutionen zur besonders schützenswerten kritischen Infrastruktur gehören, benennt die „Verordnung zur Bestimmung Kritischer Infrastrukturen" nach dem BSI-Gesetz (BSI-KritisV) [3]. Für den Schienenverkehr sind Personen-, Güter- und Zugbildungsbahnhöfe, das Schienennetz, Stellwerke und Leitzentralen Teil der kritischen Infrastruktur, wenn sie eine besondere Zugehörigkeit haben oder eine bestimmte Größe und Kapazität übersteigen. Für Nebenbahnen, die dem Verband Deutscher Verkehrsunternehmen (VDV) angehören, entwickelt sich mit der VDV-Schrift 440/4400 gerade der branchenspezifische Standard (B3S) nach dem BSI-Gesetz.

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), dass Eisenbahninfrastrukturen und Fahrzeuge den Anforderungen der öffentlichen Sicherheit genügen müssen. Ähnlich formulieren es auch die EBO, BOStrab und BOA.

Die gesetzlichen Rahmenbedingungen überwachen die jeweils (für ihren Bereich zuständigen) Aufsichtsführenden Behörden und wirken hauptsächlich auf die Betreiber (EVU, EIU) von Eisenbahneinrichtungen ein. Die Betreiber geben ihre Randbedingungen in Form von Anforderungen an Hersteller weiter, die Hersteller brechen diese als Integratoren für ihre Zulieferer herunter. Umgekehrt geben die Hersteller und deren Zulieferer die Anwendungsbestimmungen für den sicheren Betrieb ihrer Produkte an den Betreiber weiter.

Als Grundstruktur wie IT-Sicherheit initiiert, gesteuert und überwacht werden kann, wird ein Informationssicherheitsmanagementsystem (ISMS) eingeführt, für dessen Umsetzung es unterschiedliche, zum Teil harmonisierte, Grundlagen gibt. Die Normenreihe ISO/IEC 27000ff fasst zum Beispiel die Normen mit den allgemeinen sowie branchenspezifischen Leitfäden zur Informationssicherheit zusammen. Das BSI stellt mit dem IT-Grundschutz eine ganzheitliche Methode vor, die es Organisationen ermöglicht, stufenweise eine angemessene IT-Sicherheit zu erreichen.

Als weiterer sektorspezifischer Umsetzungsleitfaden setzt die Technische Spezifikation TS 50701 (Railway applications – Cybersecurity) [4] auf der Normenreihe IEC 62443 auf und adaptiert diese Industrienorm für den Bahnsektor.

Die branchenunabhängige Normenreihe IEC 62443 „Industrial communication networks – Network and system security" [5] 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. Im zweiten Teil sind organisatorische Themen enthalten. Weiter technisch orientiert beschäftigen sich der dritte Teil mit einer Gesamtsystemsicht und der vierte Teil mit einzelnen Komponenten.

Arbeitsschritte zur Entwicklung eines generischen IT-Security Architekturmodells

Das Vorgehen beim Systementwurf eines generischen IT-Security Architekturmodells von Schienenfahrzeugen beschreibt die DIN EN 62443-3-2 mit den folgenden Arbeitsschritten:

- Definition des Betrachtungsobjekts „Schienenfahrzeug" 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 entsprechend ZCR 3
- Festlegung und Beschreibung der Zonenübergänge entsprechend ZCR 3

Anhand dieser vier Arbeitsschritte entwickeln die folgenden Abschnitte ein gene-

risches IT-Security Architekturmodell für einen verallgemeinerten modernen Triebzug bzw. Schienenfahrzeug.

Beschreibung des Betrachtungsobjekts mit Zonen und Zonenübergängen

In jeder Domäne, in der es um den Schutz eines wertvollen Gutes geht, kommt man auf abstrakter Ebene zu einem ähnlichen Vorgehensmodell, das sich darauf reduziert, den Schutzbedarf zu ermitteln und je nachdem wie hoch dieser ist, geeignete Maßnahmen zu finden, um diesen Schutz sicher zu stellen.

Vereinfacht kann man das sehr gut am Beispiel einer mittelalterlichen Befestigungsanlage visualisieren: Je höher der Schutzbedarf eines Gutes war, desto mehr Burgmauern und/oder Wassergräben wurden zum Schutz vor Angreifern errichtet.

Für den reibungslosen Betrieb einer Burg in Friedenszeiten war es allerdings erforderlich, diese Befestigungsanlagen für diejenigen, die dazu autorisiert waren, möglichst leicht überwindbar zu gestalten. Hierzu gab es z. B. Zugbrücken, die heruntergelassen wurden, wenn das richtige Losungswort genannt wurde und falls nicht, wurde die Befestigungsanlage verschlossen, damit der Schutz gewährleistet blieb. Vom Prinzip her ähnliche Verfahren finden sich auch in aktuellen Normen zur IT-Sicherheit.

Wie in den vorherigen Abschnitten bereits dargestellt, ist die Normenreihe IEC 62443 das führende Regelwerk in der IT Sicherheit für OT-Systeme (Operational Technology) und damit auch für Schienenfahrzeuge. Der elementare Schritt der Norm IEC 62443 ist die Beschreibung des Betrachtungsobjektes (hier das Schienenfahrzeug als „System under consideration"). Aus der o. g. Burg-Metapher lässt sich das erforderliche Zonenmodell und der „Defense in Depth" Ansatz gut erklären. Er bedeutet nichts anderes, als dass verschiedene Sicherungsebenen (Burgmauern) für die schützenswerten Assets je nach ihrem Schutzbedarf definiert und errichtet werden. In der modernen IT-Welt wird dabei von den drei Ebenen Physical Security, Network Security sowie System- und Software-Integrity als Basis für einen adäquaten Schutz gesprochen.

Ein weiterer wichtiger Faktor ist die umfassende Beschreibung des Betrachtungsobjekts in Form von Zonen und Zonenübergängen um den „Defense in Depth" Ansatz anwenden zu können. Hierbei ist es für die spätere Risikobetrachtung entscheidend, den Kontext des Betrachtungsobjekts so genau wie möglich zu erfassen. Kontext bedeutet in diesem Zusammenhang, wie das Betrachtungsobjekt in sein Umfeld eingebettet ist und die vorgesehene Betriebsumgebung aussieht bzw. welche Risiken auf das Betrachtungsobjekt hieraus resultieren.

Ableitung der Zonen für das Referenzmodell Schienenfahrzeug

Für eine systematische Analyse der IT-Sicherheit muss ein System als ein abstraktes Modell mit Zonen und Übergängen zwischen diesen Zonen dargestellt werden. Die IEC 62443 sieht hierzu ein mehrstufiges Vorgehen zur Identifizierung des in der weiteren Analyse zu betrachtenden Systems vor.

Nach einer strukturierten Beschreibung des Betrachtungsobjekts und seines Kontexts, wird eine initiale Risikoanalyse durchgeführt, um Funktionsbereiche mit gleichem Schutzbedarf zu identifizieren und das System dann in entsprechende Security Zones („Zonen") aufzuteilen.

Für eine systematische Bewertung der Funktionsgruppen eines Schienenfahrzeuges ist eine umfassende Übersicht aller für den Betrieb eines Schienenfahrzeuges relevanten Funktionsgruppen erforderlich. Eine solche Übersicht bietet die DIN EN 15380 (Teil 4 Funktionsgruppen), die einen Katalog aller im Fahrzeug enthaltenen Funktionsgruppen enthält.

Ein Schienenfahrzeug besteht gemäß dieser Norm aus 18 Hauptbaugruppen und insgesamt 106 Unterbaugruppen. Bei der Durchsicht der zugehörigen Unterbaugruppen werden insgesamt knapp 60 Funktionsgruppen mit IT-Bezug identifiziert.

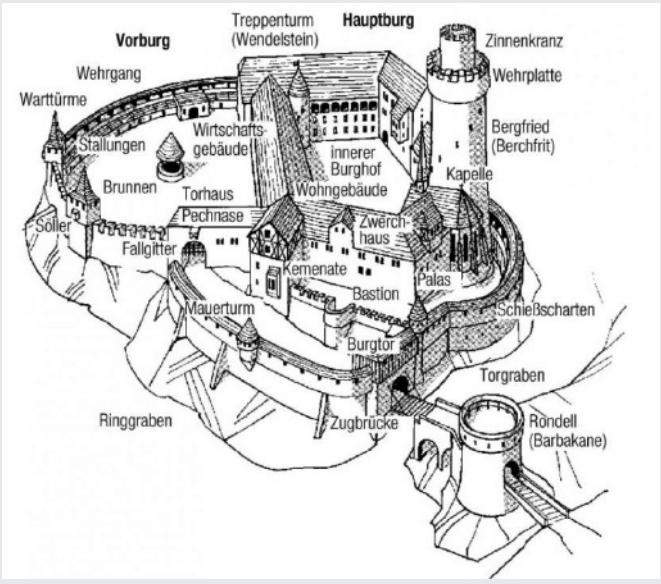
Diese Funktionsgruppen werden unter dem Blickwinkel des Schutzbedarfs in fünf Sicherheitsbereiche (Zonen) entsprechend der DIN EN 62443 gruppiert:

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

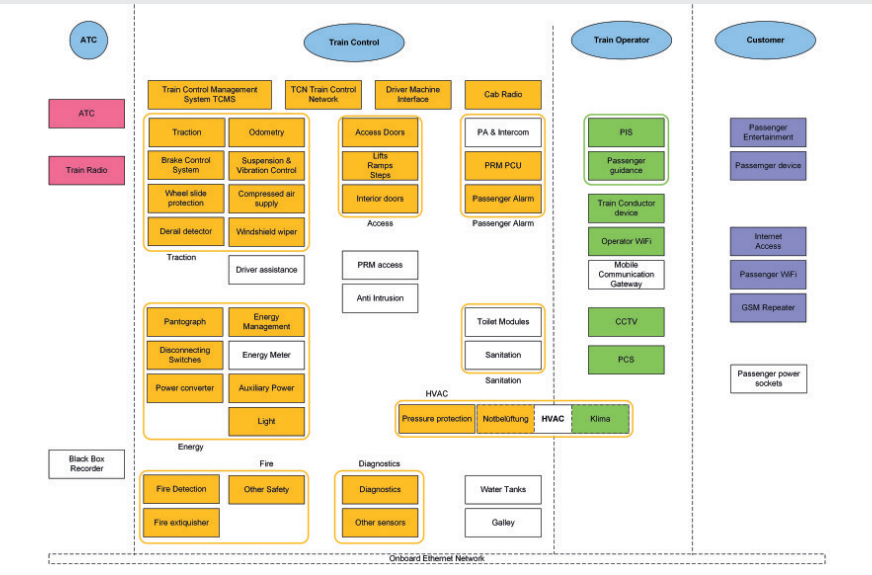
Diese Zonen orientieren sich an der Erfahrung von Experten aus dem Bereich Schienenfahrzeuge sowie ähnlichen Definitionen internationaler Gremien (z. B. CENELEC TC 9X/WG 26). Die Zuordnung der Funktionsgruppen zu den Sicherheitszonen bezieht sich auf Architekturen moderner Triebzüge. Für andere Zugkonfigurationen kann diese im Detail abweichen.

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

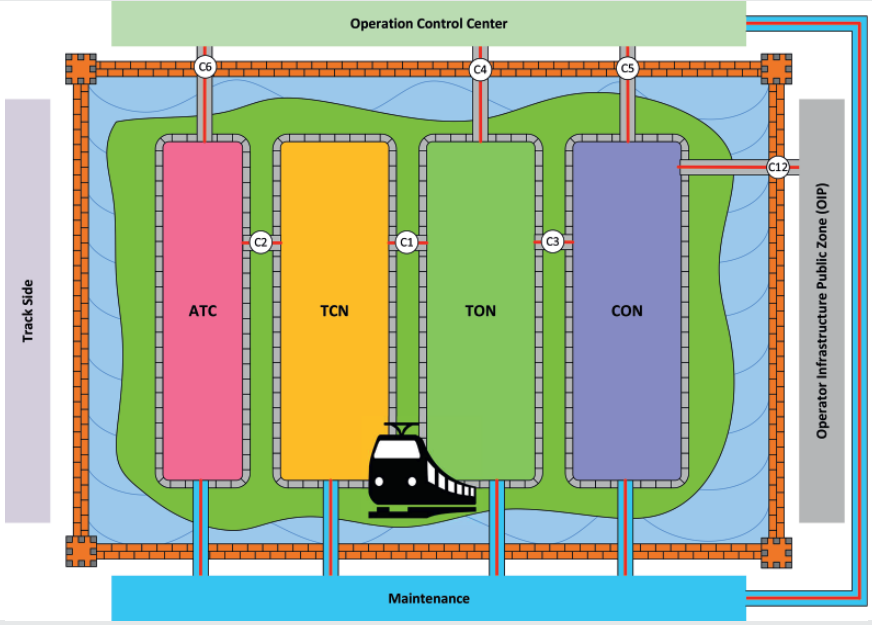
- **Automatic Train Control (ATC)**
  Die ATC beschreibt die fahrzeugseitigen Zugsicherungssysteme (z. B. ETCS, LZB) und zusätzlich die Automatic Train Operation (ATO). Diese Systeme sichern den



2: Zonen und Übergänge in einer Burganlage



3: Zuordnung von Komponenten eines Triebzuges zu Sicherheitsbereichen (Zonen)



4: Zonen und Zonenübergänge eines Triebzuges

Zugbetrieb, d.h. eine Nichtverfügbarkeit dieser Systeme führt dazu, dass die Fahrzeuge nicht oder nur unter besonderen Bedingungen betrieben werden dürfen.

- **Train Control Network (TCN)**
  Dem TCN sind alle Funktionsgruppen zugeordnet, 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. Bei modernen Triebzügen gehört zu diesem Bereich auch die Klimaanlage inklusive Druckschutzsystem. Die Verfügbarkeit der genannten Systeme ist für den Zugbetrieb von großer Bedeutung. Außerdem ist hier das Schutzziel der Integrität (Safety) dieser Funktionen besonders hervorzuheben.
  Neben den oben genannten Funktionsgruppen wurden diesem Bereich weitere für den Betrieb des Fahrzeuges wichtige Funktionsgruppen zugeordnet. Dies sind u.a. die Innentüren, die Beleuchtung, die Toiletten und die Beschallungs- und Kommunikationsanlage. Bei Ausfall eines dieser Systeme kann der Zugbetrieb nur mit erheblichen Einschränkungen (Mindertauglichkeitsfall) fortgeführt werden.
- **Train Operator Network (TON)**
  Das TON beinhaltet alle 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)**
  Das CON umfasst alle 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 abgeschaltet, 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.

Aus Bild 3 ist die genannte Zuordnung von Funktionsgruppen zu Sicherheitsbereichen im Einzelnen ersichtlich.

Aus dieser Gruppierung ergibt sich ein erstes Zonenmodell auf Fahrzeugebene, das auch die Verbindung zur Landseite (Kontext) mit einbezieht.

Eine geschickte Definition der einzelnen Zonen kann die Risikoanalyse der möglichen Angriffspfade bedeutend vereinfachen. Anderenfalls kann diese Analyse unnötig erschwert werden.

Bei der Analyse wird klar, dass die Sicherheitsfunktionen (Safety) beim sicheren Betrieb des Fahrzeuges hierbei einen besonderen Stellenwert einnehmen. Ein

durch einen Angriff gestörtes Zugsicherungssystem könnte fatale Folgen für den Betrieb mit sich bringen. Deshalb werden diese Funktionen als besonders schützenswert erachtet und einer eigenen Zone (ATC) zugewiesen. Die übergeordnete Fahrzeugsteuerung (TCMS) mit ihren Subsystemen (z. B. Antrieb, Bremse, Türen usw.) wird mit ihrer Sicherheitsrelevanz (Safety) ebenfalls in eine eigene Zone (TCN) gruppiert, die einen ähnlich hohen Schutzbedarf aufweist. Geht man im Bild 4 von links nach rechts, so nimmt der Schutzbedarf bzgl. Software-Integrität ab. In der Zone TON und CON befinden sich keine Safety-relevanten Funktionen. Diese Zonen sind von ihrem Schutzbedarf gesehen weit weniger kritisch, allerdings bieten sie durch ihre Exponiertheit (aufgrund des Passagier-WLANs) im CON und den existierenden Zonenübergängen ein nicht zu vernachlässigendes Angriffspotenzial.

Besonderen Stellenwert nimmt der Wartungsbetrieb ein. Dieser exponiert nahezu alle Komponenten im Fahrzeug und führt dazu, dass über diese Pfade der o.g. Schutz ggf. aufgehoben oder deutlich herabgesetzt wird. Auf die Burgmetapher bezogen bedeutet das, dass alle Tore geöffnet und alle Zugbrücken heruntergelassen sind. Das System Fahrzeug wäre ohne weitere organisatorische Maßnahmen in diesem Zustand dem Angreifer schutzlos ausgeliefert. Deshalb muss an den Wartungsbetrieb ein anderer Maßstab (bezüglich des Angreifertyps) angelegt werden als an den Fahrgastbetrieb. Dieser Ansatz führt uns zur Zone Wartung, die nur während des Wartungsvorgangs aktiv ist und während des Fahrgastbetriebs als nicht vorhanden betrachtet werden kann. Diese Zone wird heute meist lokal physisch geschützt, damit ein entsprechend hoher Schutz erreicht wird.

Zonenübergänge

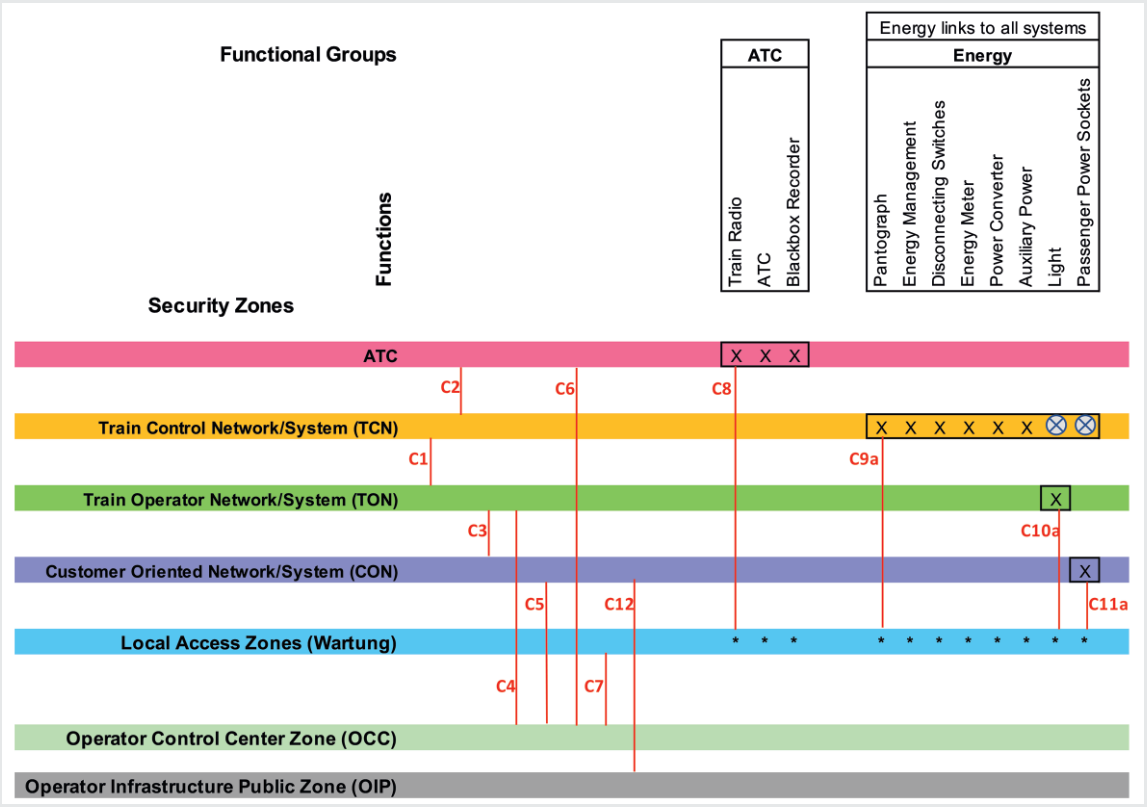
Zonenübergänge, im englischen als Conduits bezeichnet, verbinden nach Definition zwei Zonen miteinander. Für die initiale Risikobetrachtung ist es einfacher, logische Zonenübergänge zu definieren, denn damit reduziert sich die Komplexität der Analyse. Da sich in einem Zonenübergang meistens auch Geräte (i. d. R. Netzwerkgeräte) befinden, empfiehlt es sich zur weiteren Reduktion der Komplexität, immer mindestens eines dieser Geräte mit einer Flusssteuerung der Daten auszurüsten.

Beispiele dafür können Router, Gateways, Datendioden u. ä. sein. Mit dieser Maßnahme kann ein definierter Übergang zwischen den Zonen erzielt werden. Ein definierter Übergang ist dadurch gekennzeichnet, dass nur der autorisiert ist, die Grenze in die nächste Zone zu überschreiten, der sich authentifizieren kann, d. h. – in der Burgmetapher – das Losungswort kennt.

Moderne Losungsworte sind Zertifikate, die aus dem Alltag für die Verschlüsselung von Webseiten-Inhalten bekannt sind und sich dort bewährt haben. Solche Zertifikate enthalten verschlüsselte Signaturen (digitale Unterschriften), die eine Fälschung verhindern können. Man kann sie deshalb für viele unterschiedliche Schutzmaßnahmen verwenden, z. B. zur Verschlüsselung eines Passwortes, aber auch zur fälschungssicheren Identifikation eines Gerätes.

Beschäftigt man sich im Detail mit jeder Einzelfunktion, jeder Zone und jedem Übergang, wird deutlich, wie umfangreich eine anschließende Risikobetrachtung ausfallen wird. Deshalb soll im Folgenden eine Möglichkeit dargestellt werden, wie im Einzelnen vorgegangen werden kann, um zu einer systematischen Analyse zu gelangen.

Bild 5 zeigt einen Ausschnitt einer Darstellung von Zonen mit farblich unterschiedenen waagrechten Bändern. Jede Farbe entspricht hierbei einer Zone, die links bezeichnet wird (z. B. ATC, TCN, usw.).



5: Ausschnitt aus beispielhaft ausgefülltem praktischen Analysewerkzeug

An der Oberseite sind in den vertikal beschrifteten Spalten die Funktionen und Funktionsgruppen nach DIN EN 15380 aufgeführt (hier zur Vereinfachung nur zwei). Befindet sich eine Funktion in einer bestimmten Zone, so wird dies mit einem X im entsprechenden farbigen Band unten markiert. Die Kommunikation zwischen Funktionen innerhalb derselben Zone kann man sich als horizontalen Fluss innerhalb dieser Bänder vorstellen. Mit dieser Darstellung wird ein vorhandenes Datenflussmodell für die IT-Sicherheitsrisikobetrachtung austariert. Es ist dann möglich, die Zonenübergänge mit den senkrechten roten Strichen darzustellen, die jeweils immer nur zwei Zonen verbinden. Diese sind im Bild zur einfacheren Referenz mit einem C und Index bezeichnet, also z. B. C1, C2, usw..

C1 ist also der Übergang, der die Zonen TON und TCN verbindet. Die Kommunikation zwischen zwei Zonen kann man sich dann als vertikalen Fluss innerhalb dieser Übergänge vorstellen. Weil es sich um logische Übergänge handelt, gibt es jeweils nur einen Übergang zwischen zwei Zonen, in dem alle physischen Übergänge zusammengefasst sind.

Ein logischer Zonenübergang stellt dabei ein einfaches Modell dar, das alle physischen Übergänge in einen logischen Übergang zusammenfasst. In einer initialen Risiko-Analyse ist diese Vereinfachung zulässig und vereinfacht die Analyse sehr.

In realen Architekturen befinden sich Geräte teilweise in anderen Zonen als andere Geräte derselben Funktionsgruppe. Dies ist im Bild beispielhaft mit dem Lampensymbol dargestellt. In diesen Fällen kann eine Architekturänderung, d. h. die Zuordnung solcher Geräte zu einer anderen Funktionsgruppe, die Zonenbildung und die daraus folgenden nötigen Schutzmaßnahmen bedeutend vereinfachen.

Der Arbeitskreis IT-Sicherheit des CNA (Center for Transportation & Logistics Neuer Adler) hat, ausgehend von den rechtlichen und normativen Vorgaben, eine praxistaugliche generische IT-Sicherheitsarchitektur für Schienenfahrzeuge entwickelt.

Die weiter oben bereits erwähnte Situation der Wartungszone ist im Bild mit „*“ unter jeder Funktion dargestellt. Das verdeutlicht, dass sich im Prinzip jede Wartungsschnittstelle in einer eigenen Zone befindet und jede dadurch auch einzeln geschützt werden muss, solange keine Einigung auf eine für alle Hersteller einheitliche Wartungsschnittstelle gefunden werden kann.

Risikobetrachtung

Über die beschriebenen Schritte ist ein generisches Architekturmodell entstanden, das eine solide Basis für die im – gemäß der DIN EN 62443 – nächsten Schritt durchzuführende Risikoanalyse bietet. Es stellt alle möglichen Eintritts-/Angriffswege dar und stellt damit sicher, dass die Vollständigkeit der Risikobetrachtung gegeben ist.

Mit Hilfe der im generischen Architekturmodell definierten Zonen und Übergänge kann dann z.B. mit der „ATT&CK for ICS“ Methodologie (siehe dazu: attackics (mitre.org)) jeder mögliche Pfad des Betrachtungsobjektes verfolgt werden und über die Bedrohung das Risiko bzgl. IT-Sicherheit ermittelt werden.

Dabei muss berücksichtigt werden, dass Angreifer meistens nicht den direkten Angriffspfad suchen, sondern zuerst das schwächste Glied ausfindig machen, weil sie dort am einfachsten eindringen können. Danach erkunden sie das gefundene System und bewegen sich horizontal durch dessen Zonen und vertikal durch die Conduits bis zu besonders schützenswerten Bereichen. Dort können sie dann kritische Geräte kompromittieren.

Es ist deshalb ein fataler Trugschluss, ein Gerät am Netzwerk mit geringem Schutzbedarf als unbedeutend in Bezug auf IT-Sicherheit einzustufen. Ein Angriff über dieses Gerät kann als Brücke genutzt werden, um ein Eindringen in ein viel kritischeres Gerät zu erwirken.

Zusammenfassung und Ausblick

Die Zuordnung der typischen Funktionen in Funktionsgruppen sowie die Schritte des Arbeitsablaufdiagramms zur Festlegung der Zonen und Zonenübergänge (Conduits) und zur Beurteilung des Risikos aus der DIN EN 62443-3-2 führten zu einem generischen Architekturmodell für die IT-Sicherheit, welches als Unterstützung für die praktische Analyse in Schienenfahrzeugprojekten dienen kann.

Auf Basis eines bewährten Schutzkonzepts ist eine Architektur entstanden, in welcher die Zonenübergänge nur für Daten durchgängig sind, deren Sender über die notwendigen Rechte/Krypto-Schlüssel verfügen (Prinzip des Zero Trust: „Glauben Sie nichts ungeprüft.“)

Das Modell zeigt auch, dass die Wartungszugänge eines der größten Risiken für die IT-Sicherheit darstellen, weil sie Zugänge in alle Zonen haben. Dieser Sachverhalt wird als Nächstes einer vertiefenden Betrachtung im Arbeitskreis IT-Sicherheit des CNA https://www.c-na.de unterzogen.

www.eurailpress.de/archiv/IT_Sicherheit/

Literatur

[1] 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

[2] 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

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

[4] prEN TS CEN 50701. prEN TS 50701 Railway applications – Cybersecurity

[5] 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

Summary

IT security on rail vehicles – from legal context to generic architecture

The IT-security working group of CNA (Center for Transportation & Logistics Neuer Adler) has developed a practicable generic IT-security architecture for rail vehicles based on legal and normative specifications.