AG CYSIS

Security for Safety – Anforderungen an eine digitalisierte Bahnwelt

Autor

AG CYSIS UG Security for Safety

31.01.2018

Inhaltsverzeichnis

1 Einleitung

Die zunehmende IT-Durchdringung und Vernetzung praktisch aller Lebensbereiche eröffnet ökonomische wie gesellschaftliche Potenziale, auf die ein hochentwickeltes und industrialisiertes Land wie Deutschland nicht verzichten kann. Gleichzeitig aber entstehen durch die zunehmende Digitalisierung neue Gefährdungslagen, auf die schnell und konsequent reagiert werden muss. Die besondere Gefahr durch gezielte Cyber-Angriffe auf die IT-Infrastruktur betrifft neben staatlichen Stellen auch Kritische Infrastrukturen.

Kritische Infrastrukturen sind Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden.

Das IT-Sicherheitsgesetz (IT-SiG) und die BSI-Kritisverordnung (BSI-KritisV) setzen unter anderem dort an, wo sich eine moderne Gesellschaft Ausfälle am wenigsten leisten kann: bei den IT-Systemen der Kritischen Infrastrukturen.
Betreiber Kritischer Infrastrukturen werden verpflichtet, die für die Erbringung ihrer wichtigen Dienste erforderliche IT nach dem Stand der Technik angemessen abzusichern und diese Sicherheit mindestens alle zwei Jahre überprüfen zu lassen.

Hier ist in der Branche Transport und Verkehr der Schienenverkehr nicht ausgenommen. Die DB Netz AG ist das Schieneninfrastrukturunternehmen der Deutschen Bahn AG. Sie ist für das rund 33.300 Kilometer lange Streckennetz inklusive aller betriebsnotwendigen Anlagen verantwortlich. Pro Tag fahren auf der Infrastruktur der DB Netz AG im Schnitt 40.000 Züge. Zentrale Aufgabe ist es, den rund 420 Eisenbahnverkehrsunternehmen eine Infrastruktur in hoher Qualität und Verfügbarkeit zur Verfügung zu stellen und den Betrieb der Infrastruktur zu managen.
Die Digitalisierung im Bereich Zugsteuerung, Zugsicherung und Signalgebung erfordert eine höhere Verzahnung zwischen der Leit- und Sicherungstechnik und der Telekommunikation sowie eine engere Partnerschaft mit Herstellern, um die IT-Sicherheit und die funktionale Sicherheit zu gewährleisten.

Für den Sektor Transport und Verkehr, und hier im Besonderen die Deutsche Bahn**,** wird die Versorgung der Allgemeinheit mit Leistungen zum Transport von Personen und Gütern (Personen- und Güterverkehr) als kritische Dienstleistung definiert. Erbracht wird der Personen- und Güterverkehr durch den Schienenverkehr und verkehrsträgerübergreifend durch den ÖPNV, sowie durch die Logistik. Personenbahnhöfe sind Kritische Infrastrukturen, soweit sie der jeweils höchsten Kategorie zuzuordnen sind. Erfasst sind dadurch zum Beispiel die Hauptbahnhöfe von Berlin, Dortmund, Dresden, Düsseldorf, Frankfurt am Main, Hamburg, Köln, Leipzig, München, Nürnberg und Stuttgart.

Die DB Netz AG wurde als Eisenbahninfrastrukturunternehmen per Rechtsverordnung 2017 zum Betreiber kritischer Infrastrukturen im Sinne des IT-SiG. Das IT-SiG bezieht jegliche Informationstechnologien ein, die erhöhten Anforderungen bzgl. Kritischer Infrastruktur wären ggf. auf die relevanten Systeme einschränkbar.

Diese gesetzlichen Anforderungen muss die DB Netz AG als das Eisenbahninfrastrukturunternehmen in Deutschland durch ein umfassendes Informationssicherheitsmanagement umsetzen. Die DB Netz reagiert auf diese gesetzliche Anforderung mit der Erweiterung ihres Sicherheitsmanagements und ergänzt dieses um die Vorgaben zum Informationssicherheitsmanagement in einem neuen Unterstützungsprozess. Das Informationssicherheitsmanagement dient dem Schutz der IT-gestützten Geschäftstätigkeiten der DB Netz AG vor Bedrohungen und Schäden und beinhaltet die Vorgaben und Maßnahmen für eine organisatorische, wirtschaftliche und technisch

effiziente und effektive Absicherung der IT-Systeme. Somit leistet das Informationssicherheits-management einen maßgeblichen Beitrag, dass die Informationssysteme die übergeordneten Geschäftsprozesse anforderungsgemäß unterstützen können.

2 Eigenschaften und Kennzahlen

Grundprämisse bisheriger Vorgaben und Aktivitäten im Umgang mit Safety-Systemen der Eisenbahnen war die Vernachlässigbarkeit unbefugten Zugriffs. Angesichts einer stärker zunehmenden Vernetzung sowie der Verwendung allgemein zugänglicher Standards, hat sich hier die Bedrohungslage geändert. Aus diesem Grund findet IT-Sicherheit auch im Eisenbahnumfeld eine stärkere Beachtung. Der wesentliche Unterschied zwischen funktionaler Sicherheit und IT-Sicherheit ist, das letztere weniger durch konkrete Eigenschaften oder einen Zustand gekennzeichnet ist. Die von hoher Veränderlichkeit geprägten Problemstellungen der IT-Sicherheit erfordern stattdessen einen kontinuierlichen Risiko-Managementprozess.
.

Dieser hat zwei wesentliche Hebel

1. Minimierung der Angriffsfläche – Defense in Depth Konzept (s. AG CYSIS Whitepaper RA)
2. Managementsystem mit Zielvorgaben gemessen an einem definierten Schutzbedarf

Letztlich ist, entsprechend der aktuellen Lage, der Umgang mit IT-Sicherheit ein flankierender Prozess, um die Ziele und Eigenschaften der funktionalen Sicherheit zu erreichen und zwar durch die Minimierung bzw. den Ausschluss absichtliche Veränderungen von Systemeigenschaften.

Es wird unmittelbar klar, dass sich durch Wissen, technische Möglichkeiten und große hierarchische, flache Vernetzung das Risiko mit der Zeit erhöht. Somit ist eine kontinuierliche Adaption und Nachjustierung erforderlich. Diese geschieht einerseits technisch und andererseits prozessual. Insbesondere spielt die Schulung und Wissensadaption von Mitarbeitern eine herausragende Rolle.

Zur Feststellung, Überwachung und Nachjustierung ist es ideal, wenn geeignete Kennzahlen definiert werden können. Diese orientieren sich an den grundlegenden zu sichernden Systemeigenschaften, dem Schutzbedarf, abgeleitet aus entsprechenden Schutzzielen, und an den Fähigkeiten und Ressourcen potentieller Angreifer. Dazu werden Aufwand und Ressourcenbedarf gegenübergestellt.

Geeignete Schutzziele sind z.B.

Ziel	Beschreibung
Vertraulichkeit	Information ist nur Berechtigten zugänglich
Unverkettbarkeit	Transaktionen sind nicht abhängig zuordenbar
Nicht-Verfolgbarkeit	Zuordnung und Chronologie können Urheber nicht zugeordnet werden
Unbeobachtbarkeit	Quelle und Empfänger sind Dritten nicht ermittelbar
Verdecktheit	Kommunikation ist Dritten nicht erkennbar
Anonymität	Schutz vor Identifizierung
Authentizität	Informationen stammen aus vertrauenswürdiger Quelle

Verfügbarkeit	Daten und Systeme sind in bestimmtem Maße zugreifbar
Integrität	Vollständigkeit und Korrektheit von Informationen
Zurechenbarkeit	Information kann Urheber zugeordnet werden
Kontingenz	Inhalte und Umstände von Technikeinsatz sollen bewusst offen gestaltet sein

Tabelle 1 Auswahl an Schutzzielen (Nach: Bedner, Ackermann, Schutzziele der IT-Sicherheit in DuD, 05/2010)

Am Beispiel der Verfügbarkeit soll das erläutert werden.
Bahnanlagen sind planmäßig auf ihre ordnungsgemäße Beschaffenheit zu untersuchen (gem. EBO §17).
Aus diesem Grund sollte in der Betriebsphase eine fortlaufende Überprüfung der Verfügbarkeit auf Veränderungen durchgeführt werden. Bei unzulässigen Veränderungen ist ein Verbesserungsprozess anzustoßen.
Für die Beurteilung der Qualität der Dienste (QoS) und des Netzwerkes – einschließlich der Übertragungswege – (QoN) wären im laufenden Betrieb geeignete Qualitätsparameter zu messen, zu erfassen, auszuwerten, in Berichten darzustellen und den Verantwortlichen für die Bewertung bereit zu stellen. Sie müssten Qualitätsaussagen zur Systemfunktionalität und zur Verfügbarkeit ermöglichen.
Sind Dienstleister ganz oder teilweise mit Durchführungsaufgaben beauftragt, sollen die Berichte für betreiberseitige Durchführungskontrollen geeignet sein und verwendet werden.

Die Verfügbarkeit des Dienstes kann als solche schon gemessen werden (hierzu dienen entsprechende Merkmale). Eine Beeinträchtigung der Verfügbarkeit kann z.B. durch eine Distributed Denial of Service Attacke (DDoS) erfolgen. Umfang und Häufigkeit solcher Attacken feststellen zu können, ist eine weitere wesentliche Kennzahl.
Eine mögliche erforderliche technische Maßnahme ist die Installation eines Netzwerksensors oder eines Intrusion Detection Systems (IDS). Die Verwundbarkeit des Dienstes durch solche Attacken wird bestimmt durch die Architektur der Lösung, Patch-Level sowie Kenntnisse und Fähigkeiten von System-Administratoren. Somit werden weitere Kennzahlen verfügbar. Beispiele hierfür sind Anzahl und Soll-Ist-Vergleich von System-Patches, Komplexität der Architektur, Anzahl und Größe von Sicherheitszonen und Anzahl offener Netzwerkports. Außerdem sind die Anzahl von Administratoren, die Verfügbarkeit von Notfallmaßnahmen sowie die Aktualität von Zertifizierungen und durchgeführten Schulungen zu bewerten.

So könnte man diesen Prozess weiter analysieren und weitere sinnfällige Kennzahlen und Metriken ableiten. Wichtig hierbei ist eine geeignete Priorisierung und Hierarchie. Denen werden dann Aufwände und Ressourcenbedarf gegenüber gestellt. Das Gleichgewicht zwischen diesen Größen wird wesentlich bestimmt durch Service-Level-Agreements (SLA), Schwere der Sanktionen und wirtschaftliche Vertretbarkeit und – wesentlich – das Vermögen potentieller Angreifer, gegen die man sich mit wirtschaftlich vertretbarem Aufwand (gemessen an SLA und Sanktionen) schützen möchte.

Kennzahlen und Eigenschaften von Produkten, Systemen und Prozessen müssen gegen Anforderungen vom Betrieb bezüglich des NeuPro-Systems gespiegelt werden.

Diese Anforderungen kommen innerhalb des DB-Konzerns aus unterschiedlichen Quellen:

In der DB AG gelten die Sicherheitsrichtlinien Ril 114, sowie die Managementprozesse des IT-Sicherheitsmanagements der DB Netz AG.

Daneben werden für Safety die Standards EN 50126, EN 50128, EN 50129 sowie EN 50159 verwendet.

Aus Security Sicht ist die Norm IEC 62443 eine zentrale Norm, sowie deren nationale Ausgestaltung, die DIN VDE V 0831-104. Seit 2017 plant CENELEC (SG 26) die Erstellung einer europäische Norm, zunächst für den gesamten Bahnsektor. Vermutlich werden anschließend drei Teilnormen für die Bereiche Energie / Fahrzeuge / Infrastruktur (LST) erstellt.

2.1 CMMI – Capability Maturity Model Integration

Das CMMI-Modell stellt eine Familie von Referenzmodellen für die Produktentwicklung, den Produkteinkauf und die Serviceerbringung zur Verfügung. Ein CMMI-Modell ist eine systematische Aufbereitung bewährter Praktiken, um die Verbesserung einer Organisation zu unterstützen.

CMMI für Entwicklung (CMMI-DEV) umfasst gute Praktiken für die Entwicklung und Pflege von Produkten und Dienstleistungen sowie Praktiken, die den gesamten Lebenszyklus eines Produkts von der Konzeption über die Lieferung bis hin zur Pflege abdecken.

CMMI-DEV umfasst 22 Prozessgebiete, die im Rahmen der CMMI durch Fähigkeitsgrade bzw. Reifegrade bewertet werden können.

Fähigkeitsgrade (Capability Levels)
Fähigkeitsgrade beziehen sich darauf, wie gut eine Organisation Prozessverbesserungen in einzelnen Prozessgebieten erreicht. Diese Grade dienen zur inkrementellen Verbesserung der Prozesse in einem gegebenen Prozessgebiet. Die Darstellung in Fähigkeitsgraden beschreibt den Zustand der Prozesse einer Organisation auf einem einzelnen Prozessgebiet.

Die vier Fähigkeitsgrade:

0. Unvollständig
Ein „unvollständiger Prozess“ wird entweder gar nicht oder nur teilweise durchgeführt.
1. Durchgeführt
Der Arbeitsablauf enthält alle notwendigen Schritte, um die Arbeitsergebnisse zu erstellen.
2. Geführt
Ein geführter Prozess ist ein durchgeführter Prozess, der in Einklang mit den Leitlinien geplant und durchgeführt wird
3. Definiert
Zu einem definierten Prozess gibt es eine Beschreibung, die fortlaufend weiterentwickelt wird. Aus dem definierten Prozess werden prozessbezogene Erfahrungen zur Verbesserung gewonnen.

Reifegrade (Maturity Levels)
Reifegrade beziehen sich darauf, wie gut eine Organisation Prozessverbesserungen auf mehreren Prozessgebieten erreicht. Die Darstellung in Reifegraden beschreibt den Gesamtzustand der Prozesse einer Organisation. Die fünf Reifegrade stellen jeweils eine Grundlage für eine weitergehende Prozessverbesserung dar.

Die fünf Reifegrade:
1. Initial
Arbeitsabläufe werden gewöhnlich ad hoc und chaotisch durchgeführt
2. Geführt
Es ist sichergestellt, dass die Arbeitsabläufe entsprechend der Leitlinien geplant und ausgeführt werden.
3. Definiert
Arbeitsabläufe gut charakterisiert und verstanden und werden in Form von Normen, Verfahren, Hilfsmitteln und Methoden beschrieben.
4. Quantitativ geführt
Es sind quantitative Ziele für die Qualitäts- und Prozessleistung etabliert und als Kriterien verwendet.
5. Prozessoptimierung

Eine Organisation verbessert kontinuierlich ihre Prozesse auf der Grundlage eines quantitativen Verständnisses ihrer Geschäftsziele und Leistungsbedürfnisse.

Softwareentwicklungsprozesse von Lieferanten können gegen die oben genannten Fähigkeitsgrade und Reifegrade bewertet werden.

2.2 QoS (Quality of Service) für Verfügbarkeit

Da die Verfügbarkeit eines Systems Rückwirkung auf die Safety hat, muss das System eine bestimmte Verfügbarkeit aufweisen. Einer der Wege für Gewährleistung der Verfügbarkeit ist Verwendung von Quality of Service (QoS) in Netzwerken und Systemen. QoS gewährleistet Verfügbarkeit der benötigten Bandbreite in Zeiten der Stauung von Datenpaketen.

Es müssen deshalb Anforderungen definiert werden, die die benötigten Bandbreiten in verschiedenen Teilen des NeuPro-Systems festlegen. Aufgrund der Anforderungen an Bandbreiten können NeuPro-Systeme zusätzlich bewertet werden.

2.3 CVSS – Schwachstellen-Schweregrad

Das Common Vulnerability Scoring System, CVSS, (auf Deutsch „Bewertungssystem für gängige Verwundbarkeiten“) ist ein Industriestandard zur Bewertung des Schweregrades von Sicherheitslücken in IT-Systemen.

Das CVSS Verfahren hat drei wichtige Vorteile:

a. Klar definierter und transparenter Algorithmus für Berechnung des Schwachstellen-Schweregrads. Das ermöglicht ein besseres Verständnis und Vergleichbarkeit von Schwachstellen.
b. Standardisierte Schwachstellenbewertungen. Wenn eine Organisation IT-Plattformübergreifend einen gemeinsamen Algorithmus für Schwachstellenbewertung benutzt, kann auch eine gemeinsame Schwachstellenmanagement-Richtlinie erstellt werden, die die maximal erlaubte Zeitspanne für Beseitigung von Schwachstellen definiert.
c. Priorisierung von Schwachstellen. Das ermöglicht ein besseres Verständnis der Risiken, die die gegebene Schwachstelle darstellt.

Systeme oder Softwareprodukte von Lieferanten können auf Schwachstellen getestet und aufgrund von gefundenen Schwachstellen durch CVSS-Schwachstellen-Schweregrade bewertet werden.

Für diese Zwecke können Vulnerability-Scanning-Produkte eingesetzt werden, welche die Identifikation der Schwachstellen automatisieren.

2.4 Bedrohungs- und Risikoanalyse gemäß ISO 27005 oder IEC 62443-3-2

Vor dem Entwurf eines Systems ist eine Bedrohungs- und Risikoanalyse gemäß ISO 27005 oder IEC 62443-3-2 durchzuführen.

Der Standard ISO 27005 behandelt unter anderem das Thema „Information Security Risikomanagement“. Der iterative Prozess gemäß ISO 27005 umfasst sieben zum Teil parallel ablaufende Aktivitäten (s. Abb. 1).

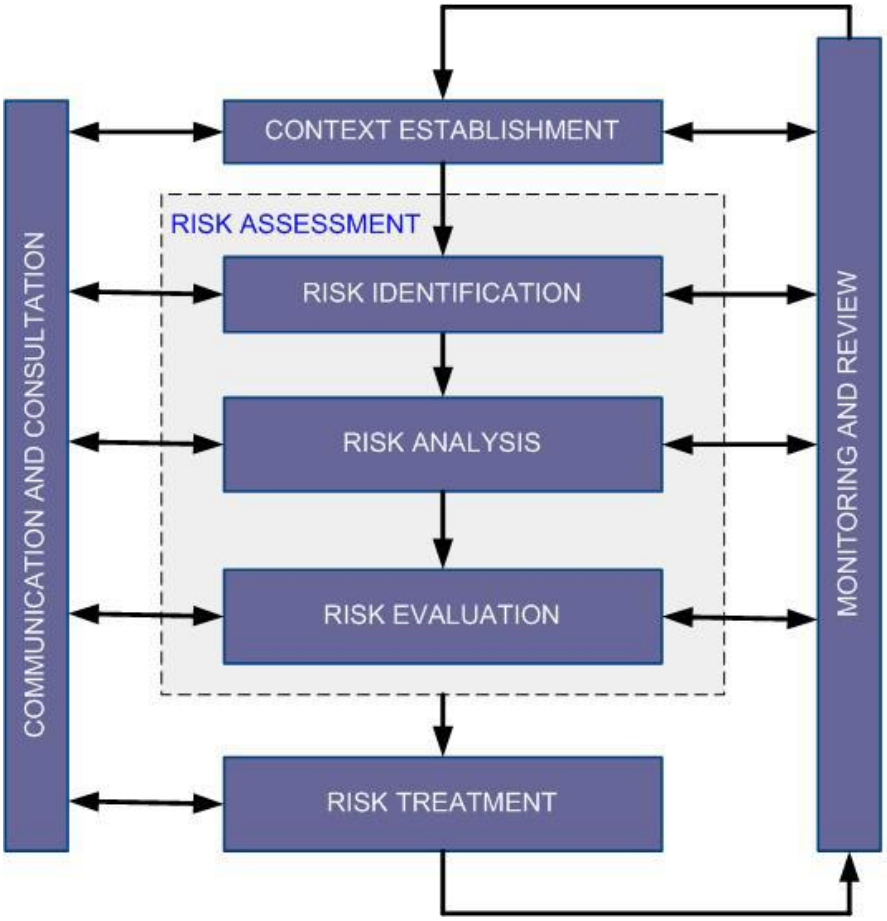


Abbildung 1: Risikomanagement Prozess gemäß ISO 27005

2.4.1 Verwendung von Security Levels gemäß IEC 62443

Im Rahmen einer IT-Risikoanalyse gemäß IEC 62443 sind für das bewertete System die zu erreichenden IT-Sicherheitslevels (Target Security Level, SL-T) abzuleiten, aus denen sich die zu erfüllenden Systemanforderungen (System Requirements, SR) und deren Erweiterungen (Requirement Enhancements, RE) ergeben. Diese sind über sieben grundlegende Anforderungen (Foundational Requirements, FR) gruppiert.

2.4.2 Die sieben grundlegenden Anforderungen

Die sieben Anforderungen gemäß IEC 62443 sind:

I. Identifizierung und Authentifizierung (identification and authentication control, IAC)
II. Nutzungskontrolle (use control, UC)
III. Systemintegrität (system integrity, SI)
IV. Vertraulichkeit der Daten (data confidentiality, DC)
V. Eingeschränkter Datenfluss (restricted data flow, RDF)
VI. Rechtzeitige Reaktion auf Ereignisse (timely response to events, TRE)
VII. Verfügbarkeit der Ressourcen (resource availability, RA)

Die IT-Sicherheitsanforderungen ergeben sich aus der Zuordnung der Security Levels zu den grundlegenden Anforderungen.

2.4.3 Security Levels gemäß IEC 62443:

Security Level 0, SL 0: keine spezifischen Anforderungen oder kein Security-Schutz nötig

Security Level 1, SL 1: Schutz vor gelegentlichem oder zufälligem Missbrauch

Security Level 2, SL 2: Schutz vor Missbrauch durch Personen mit einfachen Mitteln, mit geringen Ressourcen, gewöhnlichen Kenntnissen und geringer Motivation

Security Level 3, SL 3: Schutz vor Missbrauch durch Personen mit raffinierten Mitteln, mit mittleren Ressourcen, systemspezifischen Kenntnissen und mittlerer Motivation

Security Level 4, SL 4: Schutz vor Missbrauch durch Personen mit raffinierten Mitteln, mit erheblichen Ressourcen, systemspezifischen Kenntnissen und hoher Motivation

Die Target Security Levels (SL-T) und entsprechenden Systemanforderungen (SR x.y) werden während der Entwurfsphase auf Capability Security Levels (SL-C) abgebildet, die den vom System erreichbaren IT-Sicherheitslevel beschreiben. Abschließend ist der erreichte IT-Sicherheitslevel (Achieved Security Level, SL-A) mit dem zu erreichenden (SL-T) abzugleichen.

Für den Entwurf des NeuPro-Systems wird mindestens Security Level 3 empfohlen.

Grundsätzlich kann es aufgrund einer Risikobewertung sinnvoll sein, einzelne SL 4-Maßnahmen mit auszuwählen, die das System gegen einzelne Bedrohungen auf SL 4-Niveau schützen.

3 Designvorgaben

3.1 Vorüberlegungen

Geltungsbereich

Im Folgenden wird „Security for Safety“ ausschließlich für NeuPro-Systeme betrachtet.

Gegebenheiten bezüglich aktuell verwendeter Technik

NeuPro-Systeme setzen in ihrer ersten Anwendung auf bestehenden Stellwerks-Systemen auf. Es sind daher einige Randbedingungen für „Security for Safety“ zu beachten, die sich aus der Bestandstechnik ergeben:

- Bestehende Sicherheitsnachweise für Safety schließen die Betrachtung von systematischen Manipulationen und Angriffen durch „Innentäter“ aus.
- Der Bestand der Sicherheitsnachweise und damit einhergehend die Verwendung der gegenwärtigen Stellwerkstechnik ist nur dann möglich, wenn diese Annahme weiterhin gültig ist.
- Eine vollständige Neuentwicklung von Safety-Komponenten unter Berücksichtigung von Security-Aspekten ist derzeit mit den aktuellen Normen nicht möglich.

Es gilt daher, dass Security eine Manipulation von Safety verhindern muss. Safety muss unabhängig von gegebener Security nachweisbar sein. Der Nachweis kann aber hier nur für Angriffe von außen geführt werden.

Trennung von Security und Safety

Aus der Erfahrung mit derzeit bestehenden Security-Systemen lässt sich ableiten, dass eine zeitnahe Aktualisierung von Security-Komponenten möglich sein muss. Dies gilt sowohl für Software als auch Hardware. Die Annahme über die Lebenszeit von Security-Komponenten liegt bei einigen Jahren.

Ebenfalls kann aus der Erfahrung für Safety-Komponenten sofort abgeleitet werden, dass diese über Jahrzehnte im Feld bleiben und damit über ihren Lebenszyklus unverändert bleiben müssen.

Werden Funktionen von Safety und Security auf derselben Hardware realisiert, droht ein Zulassungsverlust für Safety-Komponenten, wenn die Security aktualisiert werden muss.

Die Kombination auf gleicher Hardware erzeugt darüber hinaus einen Zwang zur Reinvestition innerhalb des Lebenszyklus der Security. Ferner gäbe es einen Zwang zur Erstellung neuer Safety-Releases auf Basis neuer Hardware, die für Security-Funktionen erforderlich wird.

Da Safety und Security nach heutiger Sicht zudem von zwei Herstellern auf einer Komponente realisiert werden müsste, wäre der Marktaustritt eines Herstellers nicht beherrschbar und würde einen Austausch der gesamten Komponente erfordern.

Es folgt daraus, dass Security und Safety getrennt voneinander nachweisbar und aktualisierbar sein müssen.

Standardisierung der Security-Komponenten

Bei der Implementierung von Security-Komponenten muss darauf geachtet werden, dass diese ebenso wie die Safety-Komponenten standardisiert sind. Unterschiedliche, nicht kompatible Security-Systeme sind nicht beherrschbar. Die Komplexität des Managements des resultierenden Security-Systems wäre ansonsten zu hoch.

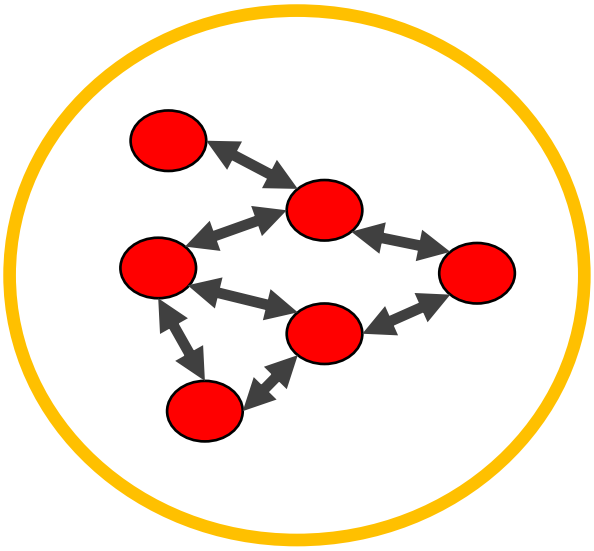
Dies ist aus Gründen der Verfügbarkeit von Fach-Ressourcen und ökonomisch weder sinnvoll noch darstellbar. In einem solchen Szenario wäre ein effizienter Schutz der Infrastruktur nicht sinnvoll möglich.

Daraus folgt, dass um die Safety-Komponenten herum eine für alle Techniken einheitliche „Security-Schale“ realisiert werden muss. Ein SOC muss alle dabei eingesetzten Techniken verwalten können.

3.2 Ansatz „Security-Schale“

Aus den Vorüberlegungen wird abgeleitet, dass die Lösung für NeuPro nur aus einer „Security-Schale“ bestehen kann. Um die weitgehend aus Bestandstechnik bestehende Safety-Welt wird eine standardisierte Security-Schale gelegt, die die genannten Anforderungen erfüllt.

Die Security-Schale kann man sich vereinfacht wie auf dem folgenden Bild vorstellen:



Es sind die folgenden Sicherheitsbereiche dargestellt:

Netzwerk (grau):	non-secure, non-safe
Security (orange):	secure, non-safe
Safety (rot):	non-secure, safe
Gesamtsystem:	secure + safe

Die Netzwerk-Komponenten sind dabei COTS-Komponenten beliebiger Hersteller (im Rahmen der Umweltbedingungen).

Die Security-Komponenten sind gegebenenfalls ebenfalls COTS-Komponenten, aber standardisiert, wie oben beschrieben. Die jeweiligen Hersteller müssen Langfristverfügbarkeit und Zertifizierung durch das BSI zusichern.

Die Safety-Komponenten werden wie bisher von den Signaltechnik-Herstellern geliefert.

Die oben abgeleitete Trennung von Security- und Safety-Komponenten darf nicht durch andere Teilsysteme (z.B. Diagnose, iBS, Ladeverfahren) umgangen werden.

Hieraus ergibt sich die Forderung, dass die Netzwerk- und Security-Schicht ein eigenes, gemeinsames Ladeverfahren für Konfigurationen und Updates haben.

Die Safety-Schicht hat ein eigenes, getrenntes Ladeverfahren für Konfigurationen, dies ist z.B. im Lastenheft der Objectcontroller aufzunehmen.

Langfristig ist eine weitergehende Lösung zu erforschen. Diese besteht nach gegenwärtigen Erkenntnissen dann aus einer komplett neuen Stellwerksarchitektur mit integrierten Security-Maßnahmen, die bei der Entwicklung von vorneherein berücksichtigt werden müssen.

3.3 Risiken

Die Betrachtung des Ansatzes mit getrennten Security-Komponenten „vor“ einer Safety-Komponente im Feldelement-Anschlusskasten (FeAk) zeigt, dass die Schnittstelle am Übergang Security zu Safety ein möglicher Angriffspunkt ist. Es wäre möglich, sich zwischen Security- und Safety-Komponenten aufzuschalten und von dort aus einen Angriff zu starten.

Die Verbindung dieser einen Safety-Komponente ist zwar grundsätzlich erst einmal auf den direkten Kontakt zu einer Zentraleinheit im Stellwerk limitiert und lässt auch nur bestimmte Protokolle durch, aber eine Schwachstelle in den Security-Komponenten könnte hier ausgenutzt und zur Kompromittierung des gesamten Netzes verwendet werden.

Aus diesem Grund wird eine unbeschränkte Bedienbarkeit aller Feldelemente aus jeder beliebigen Stellwerks-Zentraleinheit (ZE) im gesamten Einsatzgebiet der DB AG heraus verworfen.

Die Risiko-Minimierung erfolgt durch eine Segmentierung des Netzwerks, durch einen Einbruchschutz und ein verbessertes Schließsystem am FeAK bzw. Schalthaus.

Der Betreiber muss die Risikoabschätzung mit dem BSI abstimmen.

4 Aspekte der IT-Sicherheit und mögliche Umsetzung

Die Einbettung schützenswerter Komponenten in eine „Security- Schale“ ermöglicht die Aufrechterhaltung der Integrität sicherheitsrelevanter Daten und der Verfügbarkeit des Gesamtsystems. Dabei ist zu berücksichtigen, dass die IT- Sicherheit eines Systems nicht allein durch Technik gewährleistet werden kann. Ein Sicherheitsgateway schützt beispielsweise nicht gegen das physikalische Eindringen eines Angreifers in einen unzureichend abgesicherten Technikraum. Erst durch die Entwicklung und Umsetzung eines ganzheitlichen IT-Sicherheitskonzeptes können die IT-Grundwerte zuverlässig und nachhaltig geschützt werden.

Neben der implementierten Technik leisten insbesondere die zugrundeliegende Infrastruktur und der Betrieb im Unternehmen einen entscheidenden Beitrag zur IT-Sicherheit des Gesamtsystems Bahn. Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) sowie Anforderungen einschlägiger Standards wie den IEC 62443- und ISO 27000-Reihen lassen sich auf diese drei Bestandteile eines ganzheitlichen IT-Sicherheitskonzeptes abbilden.

So ist unter anderem der Schutz von Gebäuden und Anlagen primär durch die Infrastruktur zu gewährleisten. Andere Gruppen von Anforderungen sind nur durch ein Zusammenspiel mehrerer Aspekte erfüllbar. Eine restriktive und zugleich zweckmäßige Zutrittsbeschränkung erfordert beispielsweise eine Kombination infrastruktureller und organisatorischer bzw. betrieblicher Maßnahmen.

Abbildung 2 bietet eine Übersicht, wie Gruppen von IT-Sicherheitsanforderungen den beschriebenen Bestandteilen zugeordnet werden können.

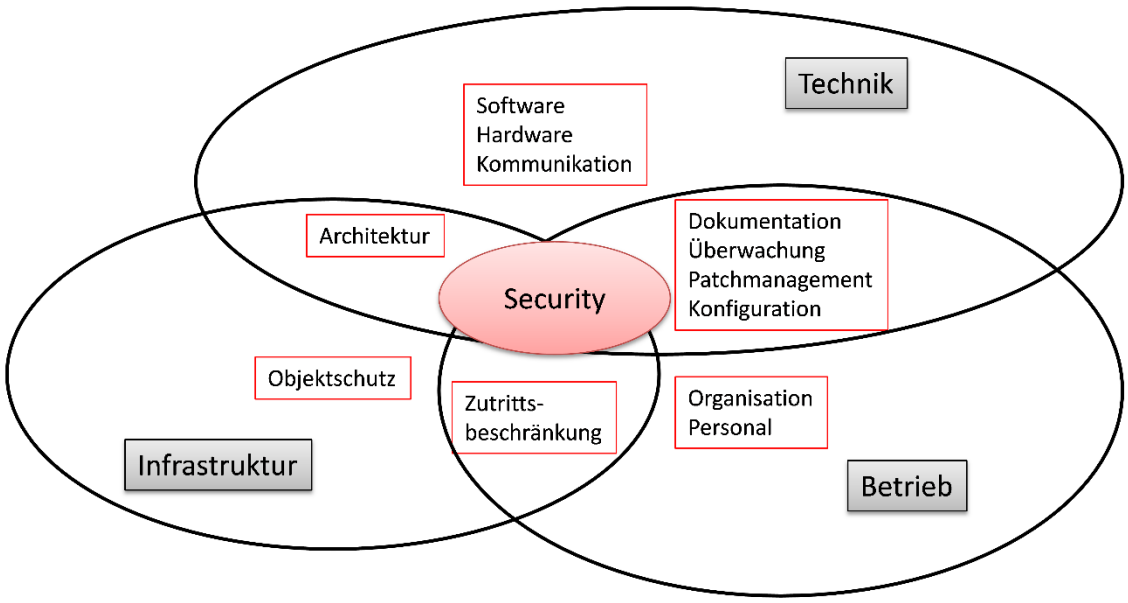


Abbildung 2: Ganzheitliche IT-Sicherheit durch infrastrukturelle, technische und betriebliche Maßnahmen

Sicherheitsrelevante Teilsysteme und Daten haben im Bahnsektor einen hohen Schutzbedarf, sodass sich aus IT-Sicherheitsanalysen ein umfassender Satz an Anforderungen technischer, betrieblicher und infrastruktureller Natur ergibt. Zum Teil sind diese Anforderungen durch bestehende Prozesse oder Objekte bereits umgesetzt, die durch entsprechende Nachweise auch bei

einer Systemzertifizierung nach neueren Standards geltend gemacht werden können. Insbesondere die Konformität zum Stand der Technik, die dem IT-Sicherheitsgesetz zufolge die Basis einer erfolgreichen Zulassung bildet, stellt Hersteller und Betreiber von Bahnsystemen aber vor neue Herausforderungen.

Die Zuordnung von effektiven Maßnahmen zu normativ verpflichtenden Anforderungen ist wesentlicher Bestandteil der Entwicklung einer „Security-Schale“, die rückwirkungsfrei den Schutzbedarf der sicherheitsrelevanten Teilsysteme erfüllt. Eine beispielhafte Auswahl derartiger Zuordnungen ist in Tabelle 2 enthalten.

Anforderungen	**Mögliche Maßnahmen**
Identifizierung & Authentifizierung, z.B.: • Eindeutigkeit • Passwortstärke	• Verbot von Gruppenaccounts, Verwendung technischer Signaturen bei bekannten Geräten, Multifaktor-Authentifizierung durch Security-Tokens • Passwortregeln und Anmeldelimitierung
Systemintegrität, z.B.: • Schutz vor Schadcode • Eingabevalidierung • Sitzungsintegrität	• „Whitelisting“ autorisierter Software und Versionen, Sicherheitsgateways an Netzübergängen • Paketfilter, vordefinierte Telegramminhalte • Sequenzierung von Telegrammen
Nutzungskontrolle, z.B.: • Durchsetzung der Autorisierung • Sitzungsmanagement • Zeitstempel, Nicht-Abstreitbarkeit	• Restriktive Rechtevergabe und regelmäßige Prüfung • Automatische Sitzungssperrung, Einzigartigkeit jeder Sitzung • Umfassende, nicht manipulierbare Dokumentation / Protokollierung aller Befehle
Überwachung und Reaktion, z.B.: • Überwachung des Netzwerks • Zugriff auf Logdaten • Verifizierung der Security Funktionalität • Patch- und Änderungsmanagement • Sichere Konfiguration	• 24/7 Überwachung durch Security-Center mit verschlüsseltem Zugang zu allen Teilnetzen • Auswertung d. Logdaten durch direkte Anbindung • Penetration-Tests vor Inbetriebnahme und Überprüfung auf neu entdeckte Schwachstellen • Bewertung entstehender Risiken → Stillstand o. planmäßige Distribution der Updates bei Bedarf • Zentrale Verwaltung und Pflege der Netzwerk- und IT-Sicherheitseinstellungen auf Basis der Herstellerempfehlungen und Sicherheitsrichtlinien (z.B. Deaktivierung nicht benötigter Dienste/Ports)

Eingeschränkter Datenfluss, z.B.: • Netzsegmentierung • Schutz der Netzübergänge • Kommunikationsbeschränkungen	• Physikalische und logische Trennung der Netze verschiedener Sicherheitsrelevanz; Unterbindung kabelloser Kommunikation • Sicherheitsgateway an Netzübergängen • Strikte Trennung des BKU-Netzes vom LST-Netz
Ressourcenverfügbarkeit, z.B.: • Backup & Recovery • DoS- Resistenz • Redundanz	• Sicherung kritischer Daten und kontrollierter Wiederanlauf in sicheren Zustand, geregelte Verfahren für Wiederinbetriebnahme • Aufrechterhaltung minimaler Funktionalität auch während DoS-Angriffen, Segmentierung der Netze • Verwendung von redundanten Komponenten und Kommunikationspfaden zur Umgehung von beeinträchtigten Netzsegmenten
Sichere Geländeaußengrenzen, z.B.: • Umfriedung • Zufahrten & Zugänge • Videoüberwachung	• Sicherung durch Stabgittermattenzaun • Personenvereinzelnde Türen, fahrzeugvereinzelnde Tore, Videotürsprechstellen mit Fernöffnung, Grundzustand immer geschlossen • Tag- und nachtfähige, lückenlose Aufnahme außen
Zutrittskontrolle, z.B.: • Sichere Zutrittsmechanismen • Sichere Türen & Fenster • Kontrollgänge • Begleitung von Fremdpersonen	• Transponderlesetechnik für dauerhaft Zutrittsberechtigte • Zustandsüberwachung o. Einbruchmeldeanlage, Durchwurfhemmung • Regelmäßige Überprüfung auf geschl. Fenster o.ä. • Betriebsfremde stets beaufsichtigen; Arbeitsplatz aufgeräumt und verschlossen/gesperrt hinterlassen
Sichere Technik, z.B.: • Sichere Technikräume • Kontrollierte Feldelemente	• Einbruchshemmende Türen und Massivbauweise • Kontinuierliche Überwachung netzfähiger Feldelemente und optionale Abschaltung/Isolation

Datenträgerkontrolle, z.B.: • Datenträgerverwaltung • Sicherer Austausch	• Führung eines Verzeichnisses, äußerliche Kennzeichnung, sichere Aufbewahrung • Personenbezogener Austausch mit Nachweis ohne Hinweise auf Inhalte
Personalmanagement, z.B.: • Fachliche Schulungen • Sensibilisierung für Risiken • Einstellung und Austritt • Beschäftigungsverhältnis	• Regelmäßige fachbezogene Unterweisungen mit Teilnahmenachweis • Regelmäßige Sensibilisierungsmaßnahmen zur Bedeutung der IT-Sicherheit für das Unternehmen • Sicherheitsüberprüfung vor Einstellung und geregelte Verfahren beim Austritt von Mitarbeitern • Verpflichtung auf Regelungen, Motivation d. Mitarbeiter

Tabelle 2: Umsetzungsmöglichkeiten verschiedener IT- Sicherheitsanforderungen

5 Verortung von Security Merkmalen

Um das Gesamtsystem effizient betreiben zu können, ist es notwendig festzulegen, an welchen Stellen bzw. in welchen Komponenten welche Security-Merkmale realisiert werden. In allen Komponenten alle Security-Merkmale umzusetzen ist aufwendig, komplex und damit schwer beherrschbar.

5.1 Security Merkmale

Grundsätzlich werden, ohne Anspruch auf Vollständigkeit, folgende Security-Merkmale betrachtet:

a) Datenfilterung (Layer 2 / Layer 3 / Layer 7)
b) Integritäts-Sicherung der Daten (Tunnel)
c) Priorisierung Daten (QoS, Layer 2 / Layer 3))
d) Protokollierung
e) Erfassung von Analysedaten
f) AAA: Authentifizierung, Autorisierung, Abrechnung
g) Integritäts-Sicherung der Komponenten
h) Patch- und Änderungsmanagement

Datenfilterung: Analyse der übertragenen Daten auf den unterschiedlichen Netzwerkebenen (Layern) und Verwerfen von Datenpaketen, die nicht den definierten Kriterien entsprechen.

Integritäts-Sicherung der Daten: Die übertragenen, sicherheitsrelevanten, Daten werden bei der Übertragung zwischen den Endpunkten durch kryptographisch sichere Verfahren gegen absichtliche Verfälschung gesichert.

Priorisierung der Daten: Die zu übertragenden Daten werden in unterschiedliche Prioritätsklassen eingeteilt, deren Verarbeitung und Weiterleitung nach Priorität gestaffelt erfolgt. Reicht die Verarbeitungs- oder Übertragungskapazität nicht für alle Daten aus, werden Daten niederer Priorität verworfen. Die Security-Funktion ergibt sich aus der Vermeidung von Denial-of-Service-Angriffen mit Daten niederer Priorität.

Protokollierung: Kontinuierliche Erfassung und wenn möglich zentrale Ablage der als relevant eingestuften Ereignisse in den Netzwerkkomponenten und auf den Endgeräten. Diese dienen als Grundlage für ein Security-Monitoring des Gesamtsystems.

Erfassung von Analysedaten: Bedarfsweise und ggf. auch simultane Erfassung des kompletten Netzwerkverkehrs an unterschiedlichen Stellen des Netzwerks zur Analyse komplexer Fehler oder der Ausbreitung von auf die Security ausgerichteten Angriffen im Netzwerk. Optimal wären die kontinuierliche Erfassung an vielen Stellen im Netzwerk und nur die bedarfsweise Übertragung an die zentrale Auswertungsstelle.

AAA: Kryptographisch sichere Authentifizierung der beteiligten Teilnehmer (Geräte, Benutzer etc.) und die davon abgeleitete Autorisierung nur zugelassene Aktionen durchführen zu können. In diesem Zusammenhang ist auch die Vertraulichkeit der übertragenen Informationen durch Verschlüsselung sicherzustellen. Das Thema Abrechnung ist in diesem Zusammenhang von untergeordneter Bedeutung.

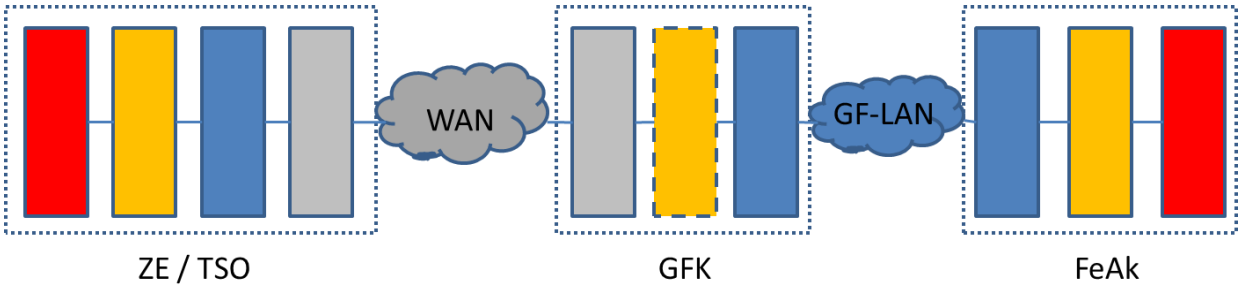
Integritätssicherung der Komponenten: Sicherstellung der Integrität der verwendeten Komponenten, hier primär der verwendeten Software, durch geeignete kryptographische Verfahren, gegen absichtliche Verfälschung.

Patch- und Änderungsmanagement: Zum einen die technische Möglichkeit, geänderte Software in unterschiedlichem Umfang in eine Komponente einspielen zu können, zum anderen der dazu notwendige betriebliche Prozess.

Die grundsätzlichen Security-Merkmale AAA, Integritätssicherung der Komponente und Patch- und Änderungsmanagement sollten grundsätzlich bei allen verwendeten Komponenten zum Einsatz kommen. Zu berücksichtigen ist hierbei, dass die aktuelle konkrete Ausprägung dieser Merkmale je nach üblichem Einsatzbereich der Komponenten (IT-Security, allgemeine IT, Automatisierungstechnik, Safety-Anwendung) sehr unterschiedlich ausfallen kann. Dies sollte bei der Definition der Anforderungen berücksichtigt werden, um die mögliche Anzahl der Anbieter nicht unnötig einzuschränken. Ungeachtet dessen ist eine kontinuierliche Verbesserung der Ausprägung dieser Merkmale, orientiert an einschlägigen Normen, zu fordern.

5.2 Topologie

Das folgende Bild zeigt die betrachteten Komponenten und die Topologie des Gesamtsystems.

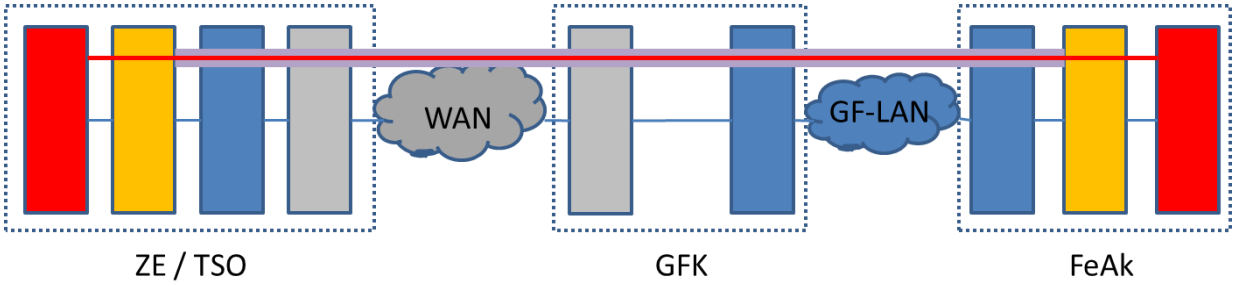


Dabei bedeuten:

ZE	Zentraleinheit
TSO	Technikstandort
GFK	Gleisfeldkonzentrator
FeAk	Feldelement-Anschlusskasten
WAN	Weitverkehrstransportnetz
GF-LAN	Gleisfeldnetz

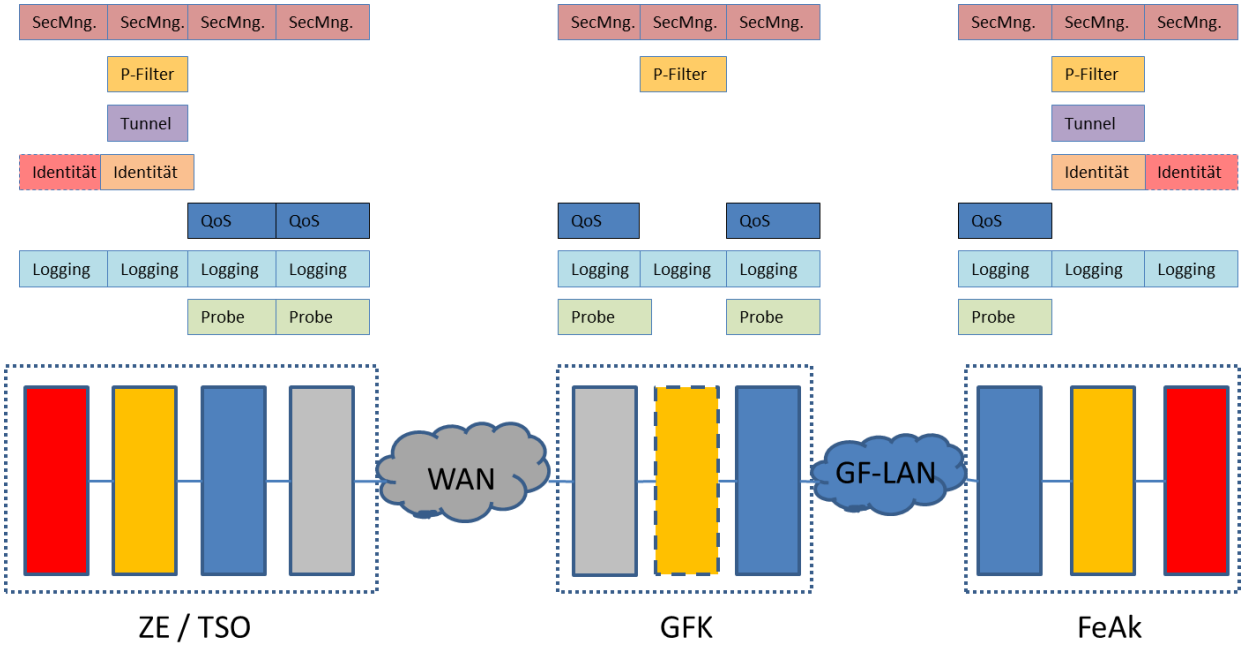
Unterschieden wird in diesem Zusammenhang grundsätzlich zwischen dem Weitverkehrsnetz und dem lokalen Gleisfeldnetz. Hintergrund sind die unterschiedlichen Einsatzbedingungen der Komponenten. Während die Weitverkehrs-Komponenten im Regelfall an zentralen Standorten mit kontrollierten Umgebungsbedingungen (Temperatur, Feuchte, EMV etc.) untergebracht sind, gelten für die Komponenten des Gleisfeldnetzes deutlich höhere Anforderungen, da sie sich teilweise in unmittelbarer Nähe des Gleises befinden. Auch funktional sind die Anforderungen in Teilbereichen unterschiedlich. Während die Komponenten des Gleisfeldnetzes in erster Linie grundlegende Netzwerk-Funktionen möglichst robust und aufgrund der sehr hohen Skalierungsfaktoren kosteneffizient realisieren sollen, müssen die Komponenten des Weitverkehrsnetzes auch höherwertige Netzwerk-Funktionalitäten bereitstellen. Sie weisen dafür aber nur ein Mengenverhältnis von 1:10 bis 1:100 gegenüber den Gleisfeld-Komponenten auf.

Eine zentrales Security Merkmal, der sichere Transport der Safety Daten (im Sinne von „Schutz gegen beabsichtigte Änderung“) durch einen Tunnel zwischen den beteiligten Endgeräten ist im Folgenden dargestellt.



Der schützende Tunnel besteht zwischen den Security-Komponenten, die unmittelbar zwischen den Safety- und den Netzwerk-Komponenten angeordnet sind. Er verbindet die beiden als sicher erachteten Safety-Zonen miteinander. Es besteht eine eindeutige1:1-Zuordnung eines Tunnels zu der Verbindung zwischen zwei Zonen.

Die Zuordnung der weiteren Security-Merkmale ist in folgendem Bild dargestellt:



Die dargestellten Security-Merkmale entsprechen weitgehend denen in Abschnitt 5.1 und sind hier noch einmal dargestellt.

Sicheres Management (Paketfilter, AAA, etc.)	SecMng.	Safety-Identität (Kennung)	Identität
Datenfilter (Paketfilter)	P-Filter	Priorisierung (QoS)	QoS
Integritätssicherung Daten (Tunnel)	Tunnel	Protokollierung	Logging
Security-Identität (Authentifizierung)	Identität	Erfassung Analysedaten	Probe

Wie zuvor beschrieben, werden die grundlegenden Security Merkmale, die für jede Komponente zutreffen sollten, hier unter dem Begriff „Sicheres Management“ zusammengefasst. Grundsätzlich sollten alle Komponenten das Merkmal „Logging“ bzw. „Protokollierung“ unterstützen um ein möglichst vollständiges Bild von den Zuständen im Gesamtsystem zu erhalten. Nicht gemeint ist hierbei die anwendungsspezifische Meldung von Fehlern und Zuständen z.B.

der Safety-Komponenten, sondern eine möglichst einheitliche Protokollierung und Übertragung von netzwerkrelevanten Ereignissen.

Alle Netzwerkkomponenten sollten darüber hinaus das Merkmal „QoS“ bzw. „Priorisierung“ beherrschen. Dabei kann berücksichtigt werden, dass eine Priorisierung im Regelfall nur beim Übergang zwischen Netzwerken mit deutlich unterschiedlichen verfügbaren Bandbreiten (LAN/WAN) erhebliche Vorteile bringt.

Ebenfalls vorteilhaft ist es, wenn die Netzwerkelemente das Merkmal „Erfassung von Analysedaten“ bzw. „Probe“ unterstützen, da dies die Fehlersuche im Netzwerk erheblich vereinfachen kann. Auch hier gilt, dass dieses Feature vor allem am Übergang zwischen zwei Netzwerken (LAN/WAN) besonders wichtig ist.

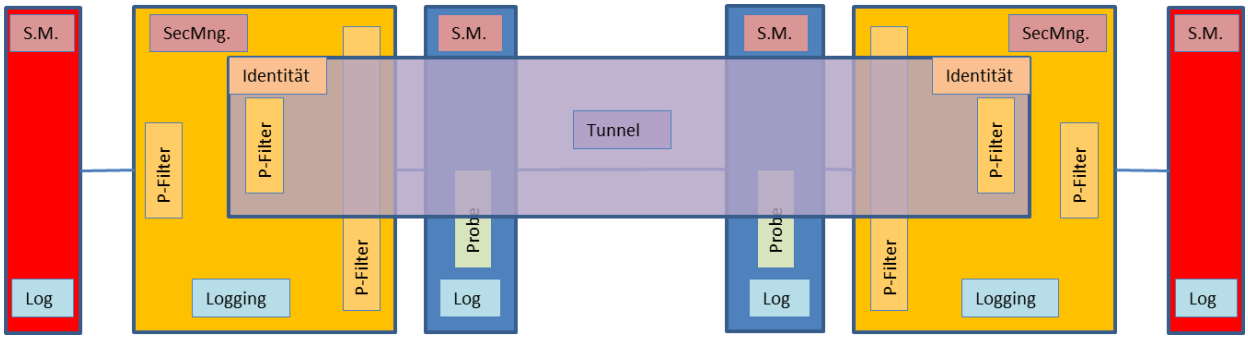
Die für die eigentliche Kontrolle der Datenverbindungen notwendigen Security-Merkmale sind dagegen nur in den Security-Komponenten erforderlich. Zum einen ist das Merkmal „Integritätssicherung“ bzw. Tunnel zu nennen. Es realisiert den kryptographisch gesicherten Transport der Daten zwischen den unterschiedlichen Zonen.

Das Merkmal „Security-Identität“ realisiert die sichere gegenseitige Authentifizierung der Kommunikationspartner. Hier kommt es besonders darauf an, dass die Identitätsinformationen einfach verwaltet und effizient in die Komponenten eingebracht werden können. Hier ist einer Public-Key-Infrastruktur (PKI) auf jeden Fall der Vorzug vor individuellen symmetrischen Schlüsseln zu geben.

Als weiteres wichtiges Security-Merkmal ist zuletzt noch der „Datenfilter“ bzw. „P-Filter“ zu nennen. Er stellt sicher, dass nur erlaubte Kommunikationsbeziehungen und -dienste oder auch Protokollinhalte transportiert werden. Eine zustandsorientierte Filterung von IP-Adressen und Diensten sollte auf jeden Fall vorhanden sein. An welchen Stellen zusätzlich eine inhaltsbasierte Protokollfilterung erforderlich ist, muss im Gesamtkontext festgelegt werden. Eine inhaltsbasierte Protokollfilterung der Safety-Protokolle scheint allerdings nur bedingt sinnvoll, da dann, je nach Realisierung, der Aufwand für den Nachweis der Rückwirkungsfreiheit sehr hoch werden kann.

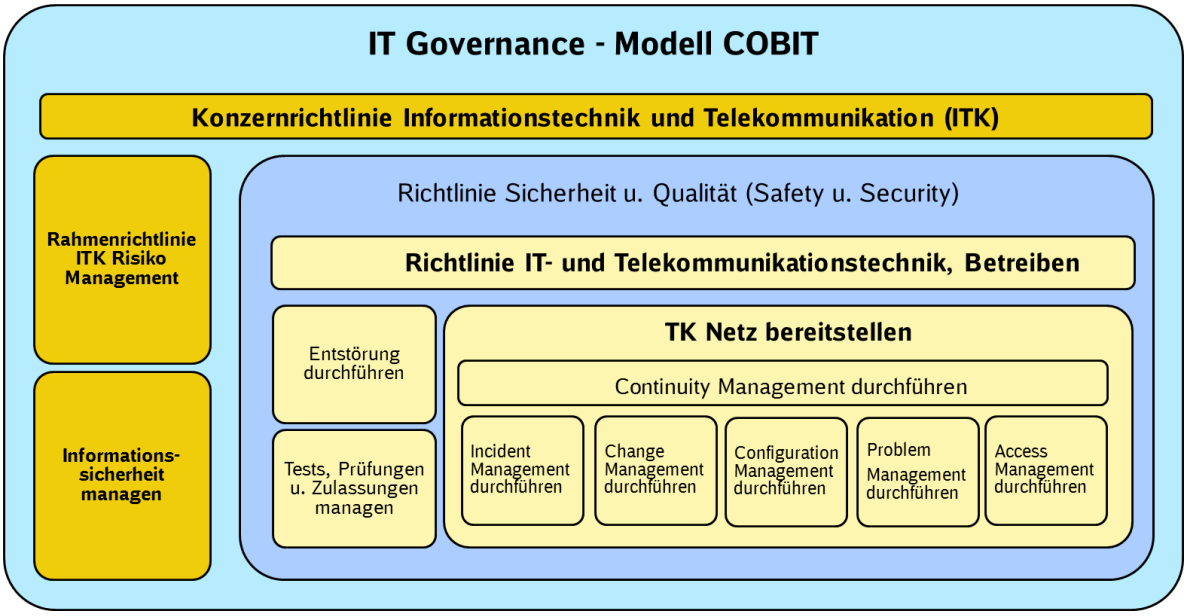
Der Vollständigkeit halber wurde noch das Merkmal „Safety-Identität“ mit aufgenommen. Es ist im eigentlichen Sinne kein Security-Merkmal, da es über keine kryptographischen Sicherheitsmerkmale verfügt, stellt aber eine zusätzliche Ebene der Identifizierung aller Teilnehmer dar, die an der sicheren Kommunikation beteiligt sind.

Das folgende Bild zeigt noch einmal, wo die unterschiedlichen Security-Merkmale angeordnet sind.



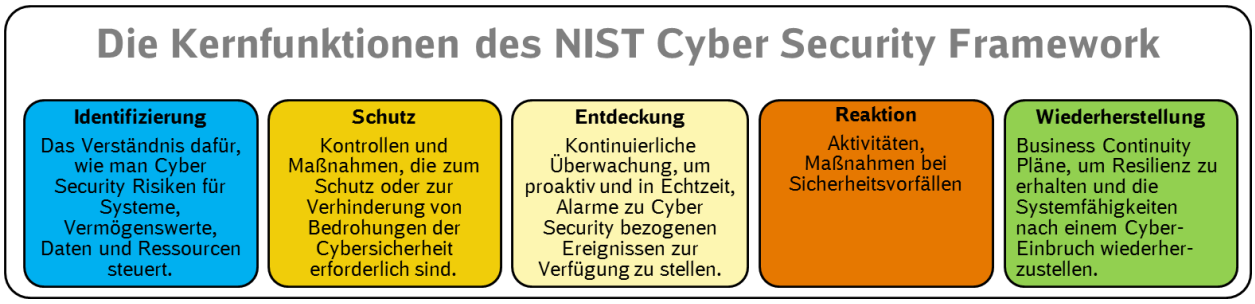
Wichtig ist in diesem Zusammenhang die Anordnung der Paketfilter. Diese regeln nicht nur, welche Datenpakete in die Security Komponente hinein oder aus ihr herauskommen, sie schränken weiterhin zusätzlich ein, welche Daten über den Tunnel transportiert werden können.

6 Betriebsführung und Security spezifische Regelungen



-Bestehende Regelwerkslandschaft der Telekommunikation und deren übergeordnete Vorgaben-

Die vorhandene TK-Betriebsführung der DB Netz sowie das Regelwerk besitzen nicht den notwendigen Reifegrad um den zusätzlichen Anforderungen für IT-Sicherheit gerecht zu werden und decken nur den BSI-Grundschutz ab.
Das im Konzern übergeordnete COBIT-Rahmenwerk (Control Objectives for Information and Related Technology) dient mehr der Steuerung der IT aus Unternehmenssicht und deckt nicht die Belange der IT-Sicherheit ab. Auch die sich am ITIL-Rahmenwerk (IT Infrastructure Library) orientierende TK-Prozesslandschaft mit ihren übergeordneten Richtlinien ist nicht für IT-Sicherheit ausgelegt. Das Whitepaper „Resiliente Architekturen in der Eisenbahn-Signaltechnik“ der Arbeitsgruppe CYSIS weist bereits auf das NIST (National Institute of Standards and Technology) Rahmenwerk zur IT-Sicherheit hin.
Die fünf zentralen Funktionen des Rahmenwerks: Identifizierung (Identify), Schutz (Protect), Entdeckung (Detect), Reaktion (Respond) und Wiederherstellung (Recover) werden unten dargestellt. Diese Funktionen sind nicht streng linear anzuwenden. Stattdessen können sie parallel und zeitgleich durchgeführt werden, um mit hoher Dynamik dem Thema IT-Sicherheit zu begegnen.



-Die Framework Core Functions des NIST Cyber Security Framework-

Das gesamte Rahmenwerk umfasst führende Praktiken aus verschiedenen Normungsgremien, die sich bei der Umsetzung der IT-Sicherheit als erfolgreich erwiesen haben, wenn Organisationen sie frühzeitig annehmen.

Der Rahmen stellt keine neuen Standards oder Konzepte vor. Vielmehr nutzt und integriert er branchenführende IT-Sicherheits-Praktiken, die von Organisationen wie NIST und der International Organization for Standardization (ISO) entwickelt wurden. Hierzu gehört auch der Inhalt der Norm IEC 62443.

Bestehende Regelungen zum Betrieb und zur Instandhaltung können mit Hilfe des o.g. Rahmenwerkes somit um Security-spezifische Regelungen ergänzt werden, die über die ereignisgetriebene Entstörung hinaus analytische und vorausschauende Komponenten notwendig machen.

Diese neuen Regelungen müssen ebenso technisch wie organisatorisch umgesetzt werden. Dies bedingt neben der Security Herausforderung auch einen hohen Anspruch an die verantwortliche Organisation. Ein neu zu gründendes Security Operations Center (SOC) ist mit dem herkömmlichen Network Operation Center nicht vergleichbar und hat allenfalls eine Schnittmenge der Aufgaben. Aber hauptsächlich sind neue Schnittstellen zwischen SOC, NOC und dem operativen Betrieb zu definieren, um den sicheren Betrieb zu gewährleisten.

7 Fazit

Bei der Entwicklung der Anforderungen wird ein Vorgehen nach IEC 62443 in jedem Fall empfohlen. Ergänzend können weitere Evaluationsverfahren eingesetzt werden. In jedem Fall handelt es sich immer um eine Momentaufnahme. Deshalb müssen einige Bewertungen wiederkehrend durchgeführt werden, um der zeitlichen Entwicklung der Produkt-, System- und Prozesseigenschaften sowie der Bedrohungslage zu folgen.

Eine grundlegende Voraussetzung für den Einsatz von Security und Safety-Komponenten ist derzeit deren Trennung bzgl. des Sicherheitsnachweises (Kapselung), um den unterschiedlichen Anforderungen zu notwendigen Aktualisierungen zu genügen. Ansonsten würde bei einem Upgrade der Security ein Zulassungsverlust für die Safety drohen. Die bestehende Safety-Architektur kann in diesem Falle übernommen werden. Die gesamten Anforderungen an die Security werden durch die Einbettung der Security-Technik in eine organisatorische Security-Schale erreicht.

Die Erfahrungen bei den Pilotvorhaben der NeuPro-Stellwerke werden wichtige Erfahrungen im Zusammenspiel Security mit Safety bringen. Neben den technischen Erfahrungen werden sich auch wichtige Erkenntnisse zu bisher nicht aufgetretenen Aufwänden für technische Security und für Organisationsaufbau und –betrieb ergeben.

Zukünftig werden Security und Safety in einem System integriert, was zusätzliche Herausforderungen für das Systemdesign und den Zulassungsprozess bedeutet. Die Anforderungen an Security und Safety müssen dann im Entwicklungsprozess des Gesamtsystems berücksichtigt werden. Hierzu sind sicher die Anpassung der Richtlinien und eine enge Abstimmung mit den Zulassungsbehörden notwendig.

8 Quellen

-DB Netz AG Internes Prozessportal
-https://fahrweg.dbnetze.com/fahrweg-de/unternehmen/db_netz_ag/wirueberuns.html
-Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz-ITSiG)
-Status quo, Zielbild und nächste Schritte bei der DB Netz AG, J. Antes, I.NVI 22.09.2016
-Bundesministerium des Innern: Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie) http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/Sicherheit/SicherheitAllgemein/kritis.html
-Bundesamt für Sicherheit in der Informationstechnik – BSI Das IT-Sicherheitsgesetz Kritische Infrastrukturen schützen BSI-ITSIG16/602
-CMMI® für Entwicklung, Version 1.3 (https://www.sei.cmu.edu/library/assets/whitepapers/10tr033de_v11.pdf)
-Common Vulnerability Scoring System v3.0: Specification Document (https://www.first.org/cvss/specification-document)
-Resiliente Architekturen in der Eisenbahn-Signaltechnik Arbeitsgruppe CYSIS, Whitepaper
-Why you should adopt the NIST Cybersecurity Framework, PwC Mai 2014, www.pwc.com/cybersecurity
-Rapid Security Assessments mittels NIST CSF, Rocco Gagliardi, 24. November 2016, https://www.scip.ch