# Resiliente Architekturen in der Eisenbahn-Signaltechnik

**Arbeitsgruppe CYSIS**

## Einleitung

Die Eisenbahn-Leit- und Sicherungstechnik ist in einem konstanten Wandel begriffen. Während in der Vergangenheit ausschließlich auf proprietäre Systeme sowie geschlossene Kommunikationsinfrastruktur zurückgegriffen wurde, rückt in der Zukunft die Nutzung kommerzieller Geräte („commercial off-the-shelf devices“, COTS) sowie offener Netze in den Vordergrund. Während in der Leit- und Sicherungstechnik bereits ein hohes Niveau an funktionaler Sicherheit erreicht wurde, stellen diese neuen Umgebungen hohe Anforderungen an die IT-Sicherheit. Um auf die wachsende Bedrohungslage – durch die gestiegene Qualität und Quantität von Angriffen gegen Kommunikationsnetze – vorbereitet zu sein, wird eine „resiliente“ Infrastruktur benötigt, die trotz Angriffen ihre wichtigsten Funktionen aufrechterhalten kann. Hierzu reicht ein reiner Perimeterschutz nicht mehr aus. Vielmehr ist eine "defense in depth"-Strategie vorteilhaft, bei der mehrere Schutzschichten vorgesehen sind, die mit Erkennungs- und Reaktionsmechanismen kombiniert sind.

Das Projekt "Resiliente Architekturen" der Arbeitsgruppe Cybersecurity für sicherheitskritische Infrastrukturen (CYSIS) hat sich intensiv mit Konzepten der Resilienz im Umfeld der Eisenbahn-Leit- und Sicherungstechnik befasst. Das vorliegende Whitepaper enthält Empfehlungen, wie Resilienz gegen IT-Sicherheitsvorfälle in der Leit- und Sicherungstechnik erreicht werden kann. Es ist das Ergebnis intensiver Diskussionen zwischen der Wissenschaft, den Betreibern sowie den Herstellern. Das Dokument erhebt keinen Anspruch auf Vollständigkeit, sondern beschreibt vielmehr Eigenschaften, die von der Arbeitsgruppe als wichtig für ein resilientes System erachtet werden, und die zur Härtung von künftigen Systemen der Leit- und Sicherungstechnik angewendet werden können.

## Definition Resilienz

Der Fokus im vorliegenden Kapitel zur Definition des Begriffs Resilienz liegt auf technischen Systemen und hier vor allem auf dem Merkmal der IT-Sicherheit. Hierzu wird zuerst eine generelle Definition von Resilienz gegeben, die sich zum Großteil an bestehenden Definitionen orientiert, um eine begriffliche Konsistenz zu den Festlegungen von Resilienz der übrigen Literatur zu gewährleisten. Diese generelle Begriffsbestimmung wird dann zum einen auf den Infrastrukturbereich der Bahn, in Form der Leit- und Sicherungstechnik (LST), und zum anderen auf den IT-Sicherheitsbereich hin konkretisiert.

### Allgemeine Definition von Resilienz im Rahmen von CYSIS

Es wird folgende Definition von Resilienz im Rahmen der Arbeitsgemeinschaft Cybersecurity für sicherheitskritische Infrastrukturen (CYSIS) angegeben, welche sich im Wesentlichen auf die Definition des NIST (National Institute of Standards and Technology, 2013) bezieht:

Die Resilienz eines informationstechnischen Systems in Bezug zur IT-Sicherheit ist durch folgende Fähigkeiten gekennzeichnet:

a) Das System und die Organisation sollen auf ungünstige Bedingungen und/oder außergewöhnliche Beanspruchungen vorbereitet sein.
b) Das System soll auf ungünstige Bedingungen und/oder außergewöhnliche Beanspruchung reagieren können und seine wesentlichsten Funktionen, trotz einer möglichen eingeschränkten Funktionalität, aufrechterhalten können.
c) Das System soll innerhalb eines akzeptierbaren Zeitintervalls wieder in einen definierten Systemzustand zurückkehren können.

## Spezifizierungen von *Resilienz* für den Bereich Infrastruktur Bahn (LST)

Die in dem vorangegangenen Kapitel angegebene Definition von *Resilienz* ist bewusst allgemein gehalten und soll in diesem Kapitel für den Bereich Infrastruktur Bahn, d.h. speziell für den Bereich Leit- und Sicherungstechnik, im Rahmen der CYSIS Arbeitsgruppe geschärft werden.

Die Definition von *Resilienz* für ein System basiert auf der Funktionsfähigkeit des Systems unter dem Einfluss einer ungünstige Bedingung und/oder einer außergewöhnlichen Beanspruchung. Diese generelle Aussage muss für sicherheitstechnische Systeme beschränkt werden, denn eine Verminderung der Funktionalität eines Sicherungssystems ist nur dann akzeptabel, wenn dadurch die funktionale Sicherheit des Gesamtsystems nicht unzulässig beeinträchtigt wird. Das bedeutet für *Resilienz* bei Sicherungssystemen, dass die zusätzliche und selbstverständliche Anforderung bzgl. der funktionalen Sicherheit des Gesamtsystems ebenfalls erfüllt sein muss.

Unter der Formulierung **„ungünstige Bedingungen und/oder außergewöhnliche Beanspruchungen“** werden nur für die IT-Sicherheit relevante Ereignisse betrachtet, d.h. Angriffe im Sinne der Norm IEC 62443.

Als **„eingeschränkte Funktionalität“** wird verstanden, dass das System in einer Rückfallebene mit verminderter Leistungsfähigkeit arbeitet, wobei jedoch die funktionale Sicherheit des Gesamtsystems gewahrt bleibt.

Die Einstufung einer Funktion als **„wesentliche Funktion“** sollte der Organisation, der Behörde oder dem Sektor obliegen. Generell sollten folgende Funktionen als *„wesentliche Funktion“* eingestuft werden:

- *„wesentliche Funktionen“* im Sinne der Definition der IEC 62443-3-3: *„zur Erhaltung der Gesundheit, der Sicherheit, der Umwelt sowie der Verfügbarkeit der zu überwachenden Einrichtung erforderliche Funktion oder Fähigkeit“*
- Alle Funktionen die notwendig sind, um die Ausführung einer wesentlichen Funktion im Sinne der IEC 62443-3-3 zu gewährleisten z.B. Stromversorgung, Lüftung etc.
- Funktionen, die Mitigationsfunktionen zur Gewährleistung der Resilienz sind: Identify, Protect, Detect, Respond, Recover

Ebenso sollte die Definition des **„definierten Zustands“** der Organisation, der Behörde oder dem Sektor obliegen. Generell kann jedoch festgestellt werden, dass auch nach einem Angriff auf Systeme der LST das Gesamtsystem Bahn in der Lage sein muss, die Anforderungen des IT-Sicherheitsgesetzes bzw. die der entsprechenden Verordnung zu erfüllen.

## Anforderungen an resiliente Architekturen

### Ende-zu-Ende Sicherung der Kommunikation

Da große und komplexe Netzwerke in der Regel nicht vollständig in der Hand des Betreibers sind und damit nicht alle Eigenschaften und Netzwerkübergänge bekannt sind, ist es sinnvoll davon auszugehen, dass unautorisierter Zugriff nicht mehr ausgeschlossen werden kann.
Daher wird eine Ende-zu-Ende Sicherung des Kommunikationsweges zwischen Teilnehmern notwendig, um die Authentizität und Integrität der Daten sicherzustellen. Vertraulichkeit ist kein vorrangiges Ziel in der Leit- und Sicherungstechnik.

### Adaptierbarkeit

Speziell COTS-Systeme (z.B. Betriebssysteme) unterliegen einem starken Wandel. Aus diesem Grund wird der Bedarf zum Nachjustieren, Patchen und Substituieren von Verfahren bestehen. Dem gegenüber stehen Zertifizierungs- und Zulassungsprozesse, die deutlich schwergängiger sind, als das bisher im IT-Umfeld üblich ist. Daraus lassen sich drei Grundprinzipien der Adaptierbarkeit ableiten:

- Safety-relevante Anteile sollten nach Möglichkeit gekapselt und langlebiger sein.
- Komponenten mit größerer Änderungshäufigkeit (z.B. COTS-Anteile, kryptografische Verfahren) sollten so aufgebaut sein, dass Änderung und der Nachweis der Rückwirkungsfreiheit (im Sinne der EN 50129) nach Möglichkeit ohne substantielle Änderung von Sicherheitsnachweisen möglich sind.
- Es sollten nur Features, Dienste oder Komponenten verwendet werden, die für die Bereitstellung der Funktionalität notwendig sind. Nicht benötigte Features, Dienste oder Komponenten sollten abgeschaltet, deaktiviert oder deinstalliert sein.

Bei Verwendung von COTS-Anteilen ist davon auszugehen, dass Schwachstellen auch von Dritten mit einer relativ kurzen Vorlaufzeit veröffentlicht werden. Maßnahmen zur Behebung und Mitigation sowie Reaktionszeiten im Eisenbahnumfeld müssen zwischen Herstellern, Betreibern und Aufsichtsbehörden abgestimmt werden.

### Analysefähigkeit und Beobachtung

Komponenten und Netzwerk einer Eisenbahnsicherungsanlage müssen zukünftig beobachtbar und analysierbar sein. Hierzu sind ggf. Schnittstellen zu Managementsystemen zu vereinbaren und Sensoren im Netzwerk vorzusehen.

### Datenaggregation und Reaktion

Ein wesentlicher Aspekt wird zukünftig der Diagnostizierbarkeit, Beobachtung, Analyse und Reaktion auf kritische Ereignisse zukommen. Daher ist zu ermöglichen, dass die verfügbaren Informationen über den Zustand des Netzwerks (durch Sensoren) und der Integrität des Systems (Code und Konfiguration) aggregiert, an einer zentralen Stelle verfügbar gemacht und auf Anomalien untersucht werden. Es muss ein Prozess definiert werden, wie auf Anomalien reagiert wird.
Die Abhängigkeit zu Diagnosesystemen bzw. Lagezentren sind dabei festzulegen.

### Datenfilterung

Innerhalb des Übertragungssystems der LST-Anlage sind Möglichkeiten der Datenfilterung vorzusehen. Idealerweise befinden sich Einrichtungen zur Datenfilterung an Gefahrenübergangspunkten. Diese sind Grenzen von Integritätsbereichen oder zukünftig sogenannte Points of Service (PoS). Wichtig hierbei ist, dass das Versagen der Datenfilterung zeitnah offenbart werden muss. Die Filterung selbst erfolgt nach vorgegebenen Regeln, die idealerweise einem Whitelisting genügen. Die Verletzung von Sicherheitsregeln muss kommuniziert werden.

### Laufzeitprüfung der Integrität der Systeme

Bei modernen Systemen ist die Funktionalität in großen Teilen von Code und Konfiguration bestimmt, deren Integrität von zentraler Bedeu-

tung ist. Daher muss festgestellt werden können, ob der auf dem System befindliche Code und die Konfiguration dem Abnahmezustand entsprechen. Die Integrität einer Komponente muss nachweislich geprüft werden können. Die Qualität der Integritätsprüfung muss auch bei einem kompromittieren System gewährleistet sein.
Eine zuverlässige Laufzeitprüfung kann beispielsweise durch die Verwendung von Trusted Boot, Trusted Platform Modules (TPM) oder ähnlichen Konzepten geschehen.

### Attestierbarkeit der Integrität gegenüber Dritten

Die Integrität des Systems, von Code und Konfiguration, muss extern prüfbar sein. Es muss sichergestellt sein, dass der tatsächliche Integritätsstand attestiert wird. Es muss ein Prozess definiert sein, der die Integrität aller relevanten Systeme regelmäßig überprüft. Die Prüfzyklen müssen, basierend auf dem Anwendungsgebiet und IT-Sicherheitsniveau, definiert sein.

### Protokollierung kritischer Ereignisse

Um die Nachverfolgbarkeit von Angriffen zu erleichtern, müssen kritische Ereignisse, wie z.B. Konfigurationsänderungen, protokolliert werden. Basierend auf dem Anwendungsgebiet und dem Sicherheitsniveau muss definiert sein, welche Ereignisse als kritisch angesehen werden. Nachträgliche Veränderungen des Logs müssen verhindert oder zumindest erkannt werden.

### Einfache Übertragbarkeit der Konfiguration auf Ersatzgeräte

Um im Störungsfall eine Komponente schnell und sicher ersetzen zu können, genügt es i.a. nicht, die Hardware zu tauschen sondern es müssen auch die Konfigurationsdaten übertragen werden (bspw. durch Smart-Card oder Download). Eine einfache, schnelle und sichere Übertragbarkeit der Konfiguration soll sichergestellt sein. Die Reaktions- und Behebungszeiten sind abhängig vom jeweiligen Gerät/System.

### Warnung bei schwachen Konfigurationen der IT-Sicherheit

Schwache Einstellungen (bspw. veraltete Kryptographie-Algorithmen) sollen erkannt werden können. Dafür müssen die Konfigurationen der Komponenten auslesbar sein. Eine geeignete Stelle zur Bewertung der Konfiguration muss definiert werden und ggf. eine Warnung erzeugen. Ein geeignetes Intervall muss für den Abstand zwischen zwei Überprüfungen festgelegt werden. Die Notwendigkeit einer bewussten Akzeptanz von schwachen Konfigurationen, um bspw. erforderliche Kompatibilität zu erreichen, ist zu prüfen.

### Modulare Architektur zur Begrenzung einer Kompromittierung

Eine modulare Architektur des Systems soll die Isolierung von Einheiten ermöglichen, wobei die Funktionalität des Systems nicht mehr als nötig eingeschränkt werden soll. Eine Isolierung dient dazu, die Auswirkungen einer Kompromittierung zu begrenzen. Ebenso kann eine diversitäre Infrastruktur zur Isolierung einer Kompromittierung beitragen. Dabei ist zu beachten, dass der Ort der Auswirkung der Kompromittierung nicht zwingend das Einfallstor für den Angriff war und dass möglicherweise nicht alle kompromittierten Einheiten erkannt wurden.

### Erkennung von physischen Zugriffen

Der physische Zugriff auf kritische Komponenten muss erkennbar sein. Dadurch sollen unberechtigte Zugriffe und damit mögliche Kompromittierungen aufgedeckt werden. Kritische Objekte können bspw. durch Einbruchmeldeanlagen geschützt werden. Ein Zugriff wird sofort bemerkt. Weniger kritische Objekte können bspw. verplombt werden. Ein Zugriff ist später nachvollziehbar.

### Kryptographische Schlüssel müssen sicher erzeugt und aufbewahrt werden

Die Sicherheit eines kryptographischen Systems beruht ausschließlich auf der sicheren Erzeugung und Geheimhaltung der kryptographischen Schlüssel. Ein geheimer Schlüssel, der

durch einen Unbefugten gelesen werden kann ist kompromittiert und gefährdet die IT-Sicherheit des Systems. Kryptographische Schlüssel sollen in sicherer Hardware gespeichert sein und dann das Hardwaremodul nicht verlassen.

### Herstellen des Urzustandes bzw. des Ersatzzustandes

Eine große Herausforderung ist es, sicherzustellen, dass nach erfolgter Herstellung eines Ersatzzustandes nicht sofort wieder ein kompromittierter Zustand entsteht. Hierzu muss betrieblich und/oder technisch ein Responseplan erstellt werden.
Das System muss für das Gesamtsystem oder Teilsysteme einen sicheren Zustand zur Verfügung stellen können, dazu ist eine verstärkte Beobachtung notwendig. Nach Kompromittierung sind Daten für Analysen/Forensik zur Verfügung zu stellen.

### Verfahren zum sicheren Schlüsselaustausch muss unterstützt werden

Es muss ein Schlüsselaustauschverfahren unterstützt werden, um geheimes Schlüsselmaterial sicher und entfernt austauschen zu können. Das Verfahren kann bspw. für eine regelmäßige Erneuerung der Schlüssel, beim Upgrade auf bessere kryptographische Verfahren oder bei Kompromittierung des Systems eingesetzt werden.

### Störungszustand realisierbar

Im Fall einer Kompromittierung eines Teilsystems soll dieses vom Gesamtsystem getrennt werden können. Dies bietet die Möglichkeit, Analysen durchführen zu können, ohne das Gesamtsystem zu gefährden. Die Wiedereingliederung nach Herstellen des Urzustandes sollte nur nach Bedienhandlungen möglich sein. Danach erfolgt zusätzlich die Beobachtung der Komponente.

### Systemreserven

Das System ist zukunftsfähig zu gestalten. Daher sind ausreichende Reserven für das höchste verfügbare Log-Level, Analysen und Updates vorzusehen. Dies betrifft sowohl neue Versionen als auch grundsätzlich neue Schlüssel und verbesserte Schlüsselverfahren.

### Asset- und Configuration-Management

Kenntnisse über Zustand und Integrität des Gesamtsystems sind zwingend erforderlich, um Veränderungen feststellen und bewerten, Änderungsrisiken einschätzen und Störungen diagnostizieren zu können. Hierzu ist ein Asset- und Configuration-Management entsprechend dem aktuellen Standard (derzeit ITIL V3) aufzubauen und zu betreiben. Das beinhaltet ein Modell des Systems, das sämtliche Komponenten samt ihrem Sollzustand (u.a. Softwarestand, Version, Zertifikat, Prüfsumme) sowie deren gegenseitige Beziehungen beinhaltet. Das Systemmodell muss kontinuierlich geprüft und ggf. angepasst werden. Schnittstellen zum automatisierten Feststellen des Istzustandes sind in den Komponenten soweit möglich vorzusehen.

## Anhang

# I. Anmerkungen zur Definition von Resilienz

Der Begriff *Resilienz* findet seine Verwendung in unterschiedlichen Bereichen der Wissenschaft, Gesellschaft und Technik und bezeichnet generell die Widerstandskraft eines Systems gegen außergewöhnliche Belastungen und/oder ungünstige Umgebungsbedingungen. Der Umfang der betrachteten Systeme umfasst sozio-ökologische Systeme genauso wie auch technische Systeme beispielsweise der Regelungs- und Steuerungstechnik in verschiedenen Ingenieursbereichen. Aus diesem Grund existiert eine Vielzahl von spezifischen Definitionen von *Resilienz*, die vom jeweiligen Fachgebiet beeinflusst worden sind. Aus der umfangreich verfügbaren Literatur zu dem Thema sei exemplarisch und ohne Anspruch auf Vollständigkeit, auf die beiden Dokumente (Petit, Phillips, Verner, & Whiteld, 2012) (Community & Regional Resilience Institute (CARRI), 2013) verwiesen, die einen Überblick über die gebräuchlichsten Definitionen von *Resilienz* in unterschiedlichen Disziplinen geben.
Zur Definition von *Resilienz* wurden Definitionen aus verschiedenen Quellen bewertet, wobei sich die folgenden Begriffsbestimmungen als geeignete Basis für die weitere Bearbeitung herauskristallisiert haben.

- Glossar der Internetplattform zum Schutz Kritischer Infrastrukturen (Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) und Bundesamt für Sicherheit in der Informationstechnik (BSI), 2016):
  ***Resilienz***
  *Resilienz ist die Fähigkeit eines Systems, mit Veränderungen umgehen zu können. Resilienz bedeutet Widerstandsfähigkeit gegen Störungen jeder Art, Anpassungsfähigkeit an neue Bedingungen und eine flexible Reaktion auf Veränderungen mit dem Ziel, das System – z. B. einen Betrieb oder einen Prozess – aufrecht zu erhalten.*

- Publikation des NIST (National Institute of Standards and Technology (NIST), 2013):
  ***Information System Resilience***
  *The ability of an information system to continue to: (i) operate under adverse conditions or stress, even if in a degraded or debilitated state, while maintaining essential operational capabilities; and (ii) recover to an effective operational posture in a time frame consistent with mission needs.*

- Übersichtsdokument des ANL (Petit, Phillips, Verner, & Whiteld, 2012):
  ***Resilience***
  *The ability of an entity — asset, organization, community, region — to anticipate, resist, absorb, respond to, adapt to, and recover from a disturbance.*

Zusammenfassend lässt sich als Kernaussage der genannten Definitionen *Resilienz* als Systemeigenschaft verstehen, welche der Erhaltung, Verteidigung und Wiederherstellung der Funktionsfähigkeit bzw. Verfügbarkeit des betrachteten Systems im Falle von außergewöhnlichen Belastungen und/oder ungünstigen Umgebungsbedingungen dient.
Die ANL detailliert diese übergeordnete funktionale Anforderung durch Aufteilung des *Resilienz*-Begriffes in die folgenden sechs Teilfunktionen (*to anticipate, resist, absorb, respond to, adapt to, recover*), welche man dem typischen zeitlichen Ablauf eines Ereignisses zuordnen kann (siehe folgende Abbildung 1).

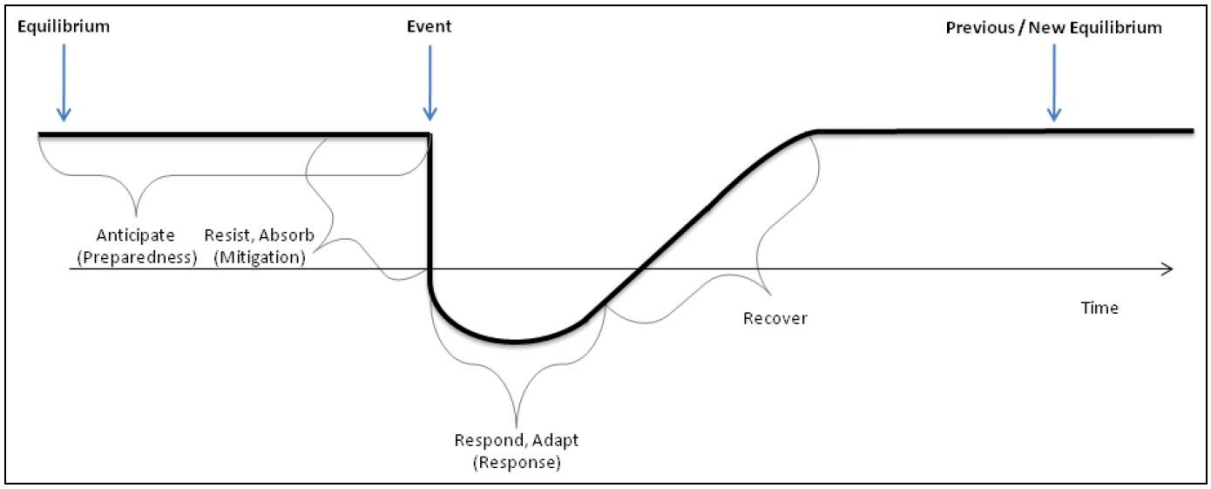


Abbildung 1: Teilbereiche von Resilienz vor dem Hintergrund eines Ereignisszenarios (Argonne National Laboratory (ANL), 2012)

Im ANL Dokument (Petit, Phillips, Verner, & Whiteld, 2012) werden die genannten Teilfunktionen zu vier Maßnahmengruppen zusammengefasst:

- ***Preparedness*** *(anticipate):* **(Vorbereitung)**
  Activities taken by an entity to define the hazard environment to which it is subject
- ***Mitigation measures*** *(resist, absorb)**:*** **(Beschränkung der Auswirkungen)**
  Activities taken prior to an event to reduce the severity or consequences of a hazard
- ***Response capabilities*** *(respond, adapt):* **(Einleitung von Gegenmaßnahmen)**
  Immediate and ongoing activities, tasks, programs and systems that have been undertaken or developed to manage the adverse effects of an event
- ***Recovery mechanisms*** *(recover):* **(Rückkehr in einen definierten Zustand)**
  Activities and programs designed to effectively return conditions to a level that is acceptable to the entity

Die im ANL Bericht genannten Maßnahmengruppen sind gleichartig zu den im NIST Dokument (National Institute of Standards and Technology (NIST), 2013) definierten Kernfunktionen zur Behandlung von IT-Sicherheitsrisiken. Diese sind:

- ***Identify*** *– Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities*
- ***Protect*** *– Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.*
- ***Detect*** *– Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.*
- ***Respond*** *– Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.*
- ***Recover*** *– Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event*

Werden die ANL Maßnahmen „*Beschränkung der Auswirkungen*“ und „*Einleitung von Gegenmaßnahmen*“ formal zu der übergeordneten Maßnahmengruppe „*Reaktion auf das Ereignis*“ zusammengefasst, so ergeben sich die nachfolgend aufgeführten vier Maßnahmengruppen, welche zur Etablierung einer *Resilienten Architektur* berücksichtigt werden sollen:

I. **Vorbereitung** auf ein mögliches bzw. zu erwartendes Ereignis
Diese Eigenschaft umfasst neben technischen Designanforderungen an ein System auch organisatorische Maßnahmen z.B. Aufbau und Pflege eines IT-Sicherheits-Managementsystems, eines Asset-Managementsystems, Erstellung einer „*Risk Tolerance Policy*“, Durchführung von IT-Sicherheits-Risikoanalysen etc. umfasst.

II. **Erkennung** einer Gefährdung
Die Erkennung eines kompromittierten Systems, ebenso wie die Erkennung von sog. *Passiven Angriffen,* also Angriffen die gerade unentdeckt bleiben sollen, stellt mit eine der wesentlichsten Herausforderungen der IT-Sicherheit dar.

III. **Reaktion** auf eine Ereignis:

   a. **Beschränkung der Auswirkungen** eines möglichen Ereignisses

   b. **Einleitung von Gegenmaßnahmen** als Reaktion auf ein eingetretenes Ereignis

IV. **Rückkehr** in einen akzeptierbaren Zustand
Das wesentlichste Ziel nach der Reaktion auf ein Ereignis stellt die mittel- bis langfriste Rückkehr in den Normalbetrieb des Systems da.

Mit der allgemeinen Definition von Resilienz ergibt sich die in folgender Tabelle dargestellte Verknüpfung zu den o.g. Maßnahmengruppen und zu den entsprechenden NIST Kernfunktionen:

Tabelle 1: Zuordnung der identifizierten Maßnahmen und NIST Kernfunktionen zur allgemeinen Definition von Resilienz

<table>
<tr><th>Allgemeine Definition von Resilienz</th><th>Maßnahmengruppe</th><th>NIST Kernfunktionen</th></tr>
<tr><td>1</td><td>2</td><td>3</td></tr>
<tr><td>Die Resilienz eines informationstechnischen Systems in Bezug zur IT-Sicherheit ist durch folgende Fähigkeiten gekennzeichnet:</td><td colspan="2"></td></tr>
<tr><td rowspan="2">a) Das System und die Organisation sollen auf ungünstige Bedingungen und/oder außergewöhnliche Beanspruchungen vorbereitet sein.</td><td>Vorbereitung</td><td>Identify<br>Protect</td></tr>
<tr><td>Erkennung eines Ereignisses</td><td>Detect</td></tr>
<tr><td rowspan="3">b) Das System soll auf ungünstigen Bedingungen und/oder außergewöhnlicher Beanspruchung reagieren können und seine wesentlichsten Funktionen, trotz einer möglichen eingeschränkten Funktionalität, aufrechterhalten können.</td><td>Reaktion auf das Ereignis:</td><td></td></tr>
<tr><td>Beschränkung der Auswirkungen</td><td rowspan="2">Respond</td></tr>
<tr><td>Einleitung von Gegenmaßnahmen</td></tr>
<tr><td>c) Das System soll innerhalb eines akzeptierbaren Zeitintervalls wieder in einen definierten Systemzustand zurückkehren können.</td><td>Rückkehr in einen definierten Zustand</td><td>Recover</td></tr>
</table>

Der Vorteil dieses direkten Abgleichs der Definition von Resilienz mit den entsprechenden Maßnahmengruppen und NIST Kernfunktionen ist, dass mit dem NIST Dokument (National Institute of Standards and Technology (NIST), 2013) ebenfalls direkte Verknüpfungen der Kernfunktionen mit

Anforderungen aus anderen Regelwerken z.B. ISO/IEC 27001, IEC 62443 gegeben sind. Dieser Zusammenhang kann später für die Ableitung von spezifischen technischen Designanforderungen und organisatorischen Maßnahmen einer Resilienten Architektur vorteilhaft verwendet werden.

## II. Detaillierung einiger Anforderungen

Wo nötig, werden zu einigen der im Whitepaper genannten Anforderungen an resiliente Architekturen in den folgenden Abschnitten noch weitere Informationen gegeben.

### Ende-zu-Ende Sicherung der Kommunikation

Die Rahmenbedingungen für den Austausch von sicherheitsrelevanten Daten regelt hierfür die Norm EN 50159. Weitere Schutzziele, wie Integrität, Rechtzeitigkeit etc. werden mit Maßnahmen in der benannten Norm aufgeführt.
Die Norm EN 50159 unterscheidet zwischen 3 Netzwerkkategorien, wobei hier nur Rahmenbedingungen für sicherheitsrelevante Daten genannt werden. Je Kategorie werden Gefährdungen aufgeführt und entsprechende Maßnahmen beschrieben. Für den Fall eines Kategorie-3-Netzes – sprich nichtautorisierter Zugriff kann nicht mehr ausgeschlossen werden – werden kryptographische Verfahren zur Datenwegsicherung vorgeschrieben. Diese gliedern sich in die Maßnahmen nach B0 bzw. B1, d.h. kryptographische Sicherung zuzüglich eines adäquaten Safety-Codes bzw. Verwendung eines kryptografischen Safety-Codes. Damit sind sowohl Tunnel als auch kryptographische Anhänge möglich. Kryptographische Anhänge bieten den Vorteil, dass Aufzeichnung und Auswertungen an beliebiger Stelle möglich sind. Bei Verwendung von Tunneln ist dieses nur an Tunnelendpunkten möglich. Bei der Verwendung kryptographischer Verfahren müssen ggf. separate Safety-Codes bzw. auch weitere kryptographische Verfahren aufeinander abgestimmt werden, da Fehlerzustände (Bitkipper, etc.) geeignet offenbart werden müssen.
Es wird davon ausgegangen, dass anzuwendende Verfahren anerkannten Regeln der Technik genügen müssen. Mindestvorgaben erfolgen durch europäische Gesetzgebung bzw. die Aufsichtsbehörde (EBA) bzw. via Amtshilfe durch das BSI.

### Adaptierbarkeit

Die Adaptierbarkeit der Systeme erlaubt u.a., dass z.B. eine Software Anteile enthalten darf, die für den konkreten Einsatz nicht notwendig sind und daher auch nicht projektiert wurden. Auf diese Weise kann eine Software für verschiedene betriebliche Rahmenbedingungen geschaffen werden, ohne für jede Situation ein angepasstes System entwickeln und zulassen zu müssen.

### Analysefähigkeit und Beobachtung

Dies wird gefordert, weil die Voraussetzung für eine zeitgerechte Reaktion (siehe folgenden Absatz "Datenaggregation und Reaktion" im Whitepaper) auf IT-Sicherheits-Ereignisse ist, dass das System kontinuierlich überwacht wird (Siehe IEC 62443-3-3 Kap. 10.4 Continuous monitoring).

### Datenfilterung

Datenfilterung wird gefordert, um die Ausbreitung einer Kompromittierung eingrenzen zu können. Laut IEC 62443-3-3 Kap. 9.4.2 ist dies ein Bestandteil der Defense-in-Depth-Strategie. Durch die Einteilung des Systems in Zonen mit verschieden hohen Sicherheitsanforderungen, im Sinne der IEC 62443, ist eine Abgrenzung an den Zonengrenzen durch Datenfilterung erforderlich, damit eine Zone mit hohen Anforderungen nicht durch die Verbindung zu einer Zone mit geringeren Anforderungen angreifbar wird.

Geeignete Architekturen für Filterlösungen findet man in der Literatur bzw. auch in Regelwerken, wie z.B. dem BSI Grundschutzkatalog. Heutige Lösungen sind z.B. das Security-Translator-System gemäß LH 415.9104 bzw. Firewalls mit Überwachung.
Die Offenbarung muss an Systemen erfolgen, die 7x24 besetzt und beobachtet werden. In heutigen LST Anlagen ist das der Fdl[1]-Arbeitsplatz bzw. das KISA[2] Sicherheitscenter (KSC).

### Attestierbarkeit der Integrität gegenüber Dritten

Die Attestierbarkeit wird gefordert, um die korrekte IT-Sicherheit-Konfiguration bei Inbetriebnahme, auch bei Wiederinbetriebnahme nach einem IT-Sicherheitsvorfall, zur Laufzeit oder bei Erweiterung/Umbau des Systems gegenüber Dritten, z.B. dem Abnahmeprüfer oder Verantwortlichen für die IT-Sicherheit nachweisen zu können.

### Warnung bei schwachen Konfigurationen der IT-Sicherheit

Nach der Bewertung der Konfiguration und der Erzeugung der Warnung müssen Systeme oder Prozesse vorhanden sein, um angemessen auf die Warnung reagieren zu können.

### Herstellen des Urzustandes bzw. des Ersatzzustandes

Bei den Systemzuständen ist es notwendig zwischen einem kompromittierbaren und einem kompromittierten Zustand zu unterscheiden. Bei einem kompromittierbaren Zustand ist eine Sicherheitslücke bekannt geworden, die potentiell ausgenutzt werden kann, aber bei dem betrachteten System noch nicht ausgenutzt wurde. Mit dem Ausnutzen der Lücke geht das System in den kompromittierten Zustand über. Erst in diesem Zustand kann eine Beeinträchtigung stattfinden.
Es sind Fälle denkbar, bei denen nach einer Kompromittierung ein Zustand ohne Sicherheitslücke (nicht kompromittierbar) nicht in akzeptabler Zeit hergestellt werden kann. Ein solcher kompromittierbarer Zustand kann als funktional sicherer Ersatzzustand nach einem Angriff geeignet sein, wenn Maßnahmen zur Überwachung seiner Kompromittierung getroffen werden.

[1] Fahrdienstleiter
[2] Kommunikationsinfrastruktur für sicherheitsrelevante Anwendungen

## III. Zuordnung der Anforderungen zu NIST-Kernfunktionen

Die folgende Tabelle ordnet den Phasen des NIST-Frameworks die vom Whitepaper aufgestellten Anforderungen zu.

| Function | Category | Subcategory | Anforderung |
|---|---|---|---|
| Identify (ID) | Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy. | ID.AM-1: Physical devices and systems within the organization are inventoried<br>ID.AM-2: Software platforms and applications within the organization are inventoried<br>ID.AM-3: Organizational communication and data flows are mapped<br>ID.AM-4: External information systems are catalogued<br>ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value<br>ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established | Asset- und Configuration-Management |
| | Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions. | ID.BE-1: The organization's role in the supply chain is identified and communicated<br>ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated<br>ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated<br>ID.BE-4: Dependencies and critical functions for delivery of critical services are established<br>ID.BE-5: Resilience requirements to support delivery of critical services are established | |
| | Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk. | ID.GV-1: Organizational information security policy is established<br>ID.GV-2: Information security roles & responsibilities are coordinated and aligned with internal roles and external partners<br>ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed | |

| | | | |
|---|---|---|---|
| | | ID.GV-4: Governance and risk management processes address cybersecurity risks | |
| | Risk Assessment (ID.RA): The organization understands the cybersecurity risk the organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals. | ID.RA-1: Asset vulnerabilities are identified and documented<br>ID.RA-2: Threat and vulnerability information is received from information sharing forums and sources<br>ID.RA-3: Threats, both internal and external, are identified and documented<br>ID.RA-4: Potential business impacts and likelihoods are identified<br>ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk<br>ID.RA-6: Risk responses are identified and prioritized | |
| | Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions. | ID.RM-1: Risk management processes are established, managed, and agreed to by organizational stakeholders<br>ID.RM-2: Organizational risk tolerance is determined and clearly expressed<br>ID.RM-3: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis | |
| **Protect (PR)** | Access Control (PR.AC): Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions. | PR.AC-1: Identities and credentials are managed for authorized devices and users<br>PR.AC-2: Physical access to assets is managed and protected<br>PR.AC-3: Remote access is managed<br>PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties<br>PR.AC-5: Network integrity is protected, incorporating network segregation where appropriate | Laufzeitprüfung der Integrität der Systeme (AC1)<br>Datenfilterung (AC4, AC5) |
| | Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements. | PR.AT-1: All users are informed and trained<br>PR.AT-2: Privileged users understand roles & responsibilities<br>PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities | |

| | | | |
|---|---|---|---|
| | | PR.AT-4: Senior executives understand roles & responsibilities<br>PR.AT-5: Physical and information security personnel understand roles & responsibilities | |
| | Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information. | PR.DS-1: Data-at-rest is protected<br>PR.DS-2: Data-in-transit is protected<br>PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition<br>PR.DS-4: Adequate capacity to ensure availability is maintained<br>PR.DS-5: Protections against data leaks are implemented<br>PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity<br>PR.DS-7: The development and testing environment(s) are separate from the production environment | Laufzeitprüfung der Integrität der Systeme (DS1)<br>Attestierbarkeit der Integrität gegenüber Dritten (DS6)<br>Ende-zu-Ende Sicherung der Kommunikation (DS2)<br>Kryptografische Schlüssel müssen sicher erzeugt und aufbewahrt werden (DS1)<br>Systemreserven (DS4) |
| | Information Protection Processes and Procedure (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets. | PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained<br>PR.IP-2: A System Development Life Cycle to manage systems is implemented<br>PR.IP-3: Configuration change control processes are in place<br>PR.IP-4: Backups of information are conducted, maintained, and tested periodically<br>PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met<br>PR.IP-6: Data is destroyed according to policy<br>PR.IP-7: Protection processes are continuously improved<br>PR.IP-8: Effectiveness of protection technologies is shared with appropriate parties<br>PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery an Disaster Recovery) are in place and managed<br>PR.IP-10: Response and recovery plans are tested<br>PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening) | Einfache Übertragbarkeit der Konfiguration auf Ersatzgeräte (IP4) |

| | | | |
|---|---|---|---|
| | | PR.IP-12: A vulnerability management plan is developed and implemented | |
| | Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components is performed consistent with policies and procedures. | PR.MA-1: Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools<br>PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access | |
| | Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements. | PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy<br>PR.PT-2: Removable media is protected and its use restricted according to policy<br>PR.PT-3: Access to systems and assets is controlled, incorporating the principle of least functionality<br>PR.PT-4: Communications and control networks are protected | Protokollierung kritischer Ereignisse (PT1)<br>Warnung bei schwachen Konfigurationen der IT-Sicherheit (PT4)<br>Modulare Architektur zur Begrenzung einer Kompromittierung (PT3)<br>Verfahren zum sicheren Schlüsseltausch muss unterstützt werden (PT4) |
| **DETECT (DE)** | Anomalies and Events (DE.AE): Anomalous activity is detected in a timely manner and the potential impact of events is understood. | DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed<br>DE.AE-2: Detected events are analyzed to understand attack targets and methods<br>DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors<br>DE.AE-4: Impact of events is determined<br>DE.AE-5: Incident alert thresholds are established | Analysefähigkeit und Beobachtung (AE2, AE3) |
| | Security Continuous Monitoring (DE.CM): The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures. | DE.CM-1: The network is monitored to detect potential cybersecurity events<br>DE.CM-2: The physical environment is monitored to detect potential cybersecurity events<br>DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events<br>DE.CM-4: Malicious code is detected<br>DE.CM-5: Unauthorized mobile code is detected<br>DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events | Analysefähigkeit und Beobachtung (CM1 bis 7)<br>Erkennung von physischen Zugriffen (CM2) |

| | | | |
|---|---|---|---|
| | | DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed<br>DE.CM-8: Vulnerability scans are performed | |
| | Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events. | DE.DP-1: Roles and responsibilities for detection are well defined to ensure accountability<br>DE.DP-2: Detection activities comply with all applicable requirements<br>DE.DP-3: Detection processes are tested<br>DE.DP-4: Event detection information is communicated to appropriate parties<br>DE.DP-5: Detection processes are continuously improved | |
| **RESPOND (RS)** | Communications (RS.CO): Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies. | RS.CO-1: Personnel know their roles and order of operations when a response is needed<br>RS.CO-2: Events are reported consistent with established criteria<br>RS.CO-3: Information is shared consistent with response plans<br>RS.CO-4: Coordination with stakeholders occurs consistent with response plans<br>RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness | |
| | Analysis (RS.AN): Analysis is conducted to ensure adequate response and support recovery | RS.AN-1: Notifications from detection systems are investigated<br>RS.AN-2: The impact of the incident is understood<br>RS.AN-3: Forensics are performed<br>RS.AN-4: Incidents are categorized consistent with response plans | |
| | Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident. | RS.MI-1: Incidents are contained<br>RS.MI-2: Incidents are mitigated<br>RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks | Modulare Architektur zur Begrenzung einer Kompromittierung (MI1, MI2)<br>Störungszustand realisierbar (MI2, MI2) |
| | Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities. | RS.IM-1: Response plans incorporate lessons learned<br>RS.IM-2: Response strategies are updated | |

| | | | |
|---|---|---|---|
| RECOVER (RC) | Recovery Planning (RC.RP): Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events | RC.RP-1: Recovery plan is executed during or after an event | Herstellen des Urzustandes bzw. des Ersatzzustandes (RP1) |
| | Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities. | RC.IM-1: Recovery plans incorporate lessons learned<br>RC.IM-2: Recovery strategies are updated | |
| | Communications (RC.CO): Restoration activities are coordinated with internal and external parties, such as coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors. | RC.CO-1: Public relations are managed<br>RC.CO-2: Reputation after an event is repaired<br>RC.CO-3: Recovery activities are communicated to internal stakeholders and executive and management teams | |

## IV. Umgang mit IT-Sicherheits-Vorfällen in Bahn-Systemen

Im Folgenden wird ein Vorschlag unterbreitet, wie Aktivitäten gemäß Normung (Bsp. NIST) zu Aktivitäten und Technologie im Bahnumfeld führen. Dabei findet die Aktivitäten/Technologie Zuordnung in den Varianten klassische LST vs. IT-Technologie statt. Bein Einführung eines Prozesses mit IT Verfahren ist dann noch zu überlegen, inwiefern heutige LST-Prozesse nach Regelwerk 892 dann durch z.B. ITIL ergänzt werden müssen.

| **NIST Kernfunktion** | **Technologie/Aktivität LST Variante 1 (Vorgehen analog heutiger Grundprinzipien)** | **Technologie/Aktivität LST Variante 2 (Vorgehen unter Verwendung von IT-Prozessen)** |
|---|---|---|
| **IDENTIFY** | Prozess: Prüfung und Anlagenabnahme nach RiLi 892 und VV BAU STE (gilt auch für TK Anlagen mit Sicherheitsverantwortung); Pläne, Planlage Zukünftig Identifikation von KE (Konfigurationseinheiten) über Bezeichner und weitere Merkmale (z.B. Zertifikationen). Planprüfung wird um Zertifikatsprüfung ergänzt.<br><br>Technologie: Neben den reinen Technikbezeichnern (für Pläne) werden Zertifikate verwendet. Diese Zertifikate zum Identitätsmanagement werden im KISA Sicherheitscenter hinterlegt. Das Zertifikat dient auch zur Zugangskontrolle (Verfahren z.B. 802.1X). Damit ist in KISA die Inventory Database hinterlegt. Das Management obliegt LST. Eigenschaften von KE sind Prüfsummen und ggf. Zertifikate. Diese gehen weiterhin in Eigenprüfungen ein. Zertifikate werden im KSC geprüft und ggf. zurückgezogen.<br>Verwendung von Secure Boot. | Prozess: Prozess nach RiLi 892 und VV BAU STE wird um ITIL Prozess ergänzt. Hierzu wird ein Anlagenkonfigurations-Management aufgesetzt. Zusätzlich befinden sich im Bereich LST sowohl Signalwerker als auch IT-Administratoren. Ergänzend zur baulichen Abnahme gemäß RiLi 892/VV BAU STE wird ein Soll-Range aufgenommen. Dazu sind während der Abnahme Lastgeneratoren zu verwenden. Der Soll-Range dient als Input z.B. für IDS[3] Systeme.<br><br>Technologie: Zusätzlich zur Meldungsoffenbarung auf dem Fdl-Arbeitsplatz wird ein Managementsystem verwendet. Zu klären ist, inwiefern das Managementsystem auch in den Abnahmeprozess eingebunden ist. Das Managementsystem ist auch gleichzeitig Inventory Database und eine Kopplung zu IDS Systemen. Die IDS Systeme detektieren Abweichungen vom Soll-Bereich. Zu klären ist die Betreiberverantwortung, Herstellerverantwortung für die Definition des Sollbereiches. Der Grundzustand installiert ist via Secure Boot immer wieder erreichbar. Zusätzlich wird danach der Sollzustand überwacht. Das Management System kann für Patch Rollouts für Betriebssysteme und Firmware verwendet werden. Nach erfolgtem Rollout ist per Abnahme wieder der Sollzustand zu prüfen. Die Gültigkeit von Zulassungen und Nachweise der Rückwirkungsfreiheit ist zu klären. Ebenso das Thema Responsible Disclosure Time. Patchlevel werden auch durch das Management System überwacht. |

[3] Intrusion Detection System

| | | |
|---|---|---|
| **PROTECT** | Prozess: Schutz vor unautorisiertem Zutritt nach 50159 ist durch LST zu überwachen. Abweichungen von der Planlage werden auf dem Fdl-Arbeitsplatz offenbart und dokumentiert (alter Sprachgebrauch – gedruckt).<br><br>Technologie: tw. s. oben. Anschluss an die LST Anlage wird über Zertifikate geregelt. Zertifikate werden im KSC verwaltet. Es wird eine Passwort-Policy verwendet oder es wird ein zentraler Login über einen Verzeichnisdienst eingeführt (wo die Policy geregelt wird). Signaltechnisch sichere Systeme bzw. weitere geeignete und abgenommene Prüfpartner sind für die Integrität der Anlage verantwortlich. Netzwerke haben eine geeignete Segmentierung (Adressen, logische Konfigurationen). Grundprinzipien sind im Regelwerk zu hinterlegen (z.B. 819.0705, 861.xxxx). Kryptografische Verfahren werden zur Übertragung generell verwendet. Die Prüfverfahren beziehen auch Systemparameter mit ein (White Listing). Systeme sind auf minimal notwendige Konfiguration gehärtet. | Prozess: Schutz vor unautorisiertem Zutritt und Sollzustände des Konfigurationsmanagements werden überwacht und im Managementsystem offenbart.<br><br>Technologie: tw. s. oben. Anschluss an LST Anlage erfolgt gemäß Zertifikaten und der im Konfigurationsmanagement (inventory management) des Management Systems hinterlegten Sollkonfiguration. Passwortpolicy wird im Managementsystem überwacht, ggf. Bereitstellung einen zentralen Verzeichnisdienstes. Prüfsysteme der LST prüfen nur Anwendungsspezifisch. Ggf. werden auch anwendungsbezogene Parameter /Prüfsummen / Zertifikate im Managementsystem hinterlegt und mit überwacht. Netzwerksegmentierung liegt in der Verantwortung der IT Administratoren. Grundprinzipien sind im Managementsystem hinterlegt. Das Managementsystem ist als Umbrellasystem ausgelegt. Verletzungen werden hier offenbart und den zuständigen Administratoren gemeldet. Die LST-Anlage läuft, wenn im Soll-Bereich, weiter. Systeme sind gehärtet, erforderliche Mechanismen für Patch-Management und Überwachung durch das Managementsystem sind freigeschaltet. Es werden generell kryptografische Verfahren zur Datenübertragung eingesetzt. |
| **DETECT** | Prozess: Überwachung der Planlage erfolgt am Fdl-Arbeitsplatz und im KSC. Mit Störungen verbunden sind Sammelmelder. Hier müssen ggf. weitere und ggf. feingranularere Sammelmelder kreiert werden. Vorgehen danach gemäß Regelwerk 892. Ggf. sind auch Ergänzungen zum Regelwerk 482.9001 hinsichtlich des Themas ASB notwendig.<br><br>Technologie: Selbstprüfungen zur Überwachung der Integrität der Systeme, sowie Mechanismen zur Sicherstellung der Integrität und Authentizität von Nachrichten werden gemäß Normenlage umgesetzt. Abschaltungen von Anlagenteilen werden direkt offenbart. Bestimmte Störungsmeldungen werden ggf. auch dokumentiert. Ggf. erfolgt Offenbarung ohne direkte Abschaltung der Systeme selbst, sondern Rückziehung von Zertifikaten im KSC und damit Isolierung der betreffenden Systeme. | Prozess: Überwachung erfolgt im Management System gemäß Eigenprüfung von LST Systemen verbunden mit Sollzustand und KM-Vorgaben (Patch-Level, Konfiguration, Prozessüberwachung). Unklare Ereignisse, trotz System im Sollzustand werden gemeldet und gehen zur Bewertung in ein Lagezentrum. Lagezentrum entscheidet mit dem Eisenbahnbetriebsleiter (EBL) über Fortführung des Betriebes und Zeitdauer der Fortführung. Überwacht werden auch Verbindungsbeziehungen, Login-Versuche, Datenverkehr-Anomalien, unübliche Ports, Eventlogs, Systemparameter.<br><br>Technologie: Im Management System laufen Daten von Überwachungsagenten, IDS zusammen und werden analysiert und korreliert. Bei Abweichung werden die Daten ins Lagezentrum weitergegeben und es erfolgt eine Alarmierung. LST Systeme müssen Überwachungsagenten hosten können bzw. es sind geeignete Messpunkte für IDS festzulegen. Es sind Vorkehrungen zu treffen, um ggf. vor Ort forensische Daten zu gewinnen (Tools für LST Administratoren). Kurzfristige Wiederherstellung mittels Secure Boot ist möglich. Abstimmung hinsichtlich Häufigkeit und Prozess ist erforderlich. Die Integritätsprüfung sicherheitsrelevanter Nachrichten erfolgt gemäß Norm. |

| | | |
|---|---|---|
| **RESPOND** | Prozess: Bei Abweichungen von der Planlage bzw. Abschaltung (Störung) zu vieler Systeme greifen Betriebsverfahren, wie heute festgelegt. Lagezentren sind zu besetzen. Betrieb wird entsprechend Verfahren und räumlicher Ausdehnen fortgeführt. Weiteres s. oben.<br><br>Technologie: log-Dateien und Konserven rückwirkungsfreier Diagnosesysteme können abgezogen und ausgewertet werden. Klärung: Wer, Zeitraum? Rückzug von Zertifikaten im KSC. | Prozess: Bei Abweichungen vom Sollzustand bzw. Konfigurationszielzustand erfolgen Isolationsmaßnahmen bzw. Abschaltungen. Bei Lage im Sollzustand und längerer beobachteter Unregelmäßigkeiten erfolgen ggf. betriebliche Maßnahmen nach Abstimmung s. oben oder Einleitung von Recovery Maßnahmen.<br><br>Technologie: Abzug von Daten der Management und IDS Systeme. Log Daten Sammlung. Forensische Maßnahmen auf den identifizierten anomalen Systemen. Isolation identifizierter Systeme. Erforderliche Netzwerkresegmentierung, ggf. Kappen unnötiger oder verzichtbarer Verbindungen gemäß Notfallkonzept. Vorbereitung ggf. erforderlicher Patch Rollouts mit Rolloutplanung gemäß Notfallkonzept (Abstimmung mit betrieblicher Planung). |
| **RECOVER** | Prozess: Wiederherstellung des Planlagezustandes unter der Voraussetzung, dass:<br>• Ursache des Fehlverhaltens geklärt und Verstanden ist.<br>• Gegenmaßnahmen (ggf. auch betriebliche Kompensationsmaßnahmen) erfolgt sind und für ggf. temporär akzeptable Schwachstellen (nach Risikobewertung) eine Behebung terminiert ist (RPZ Verfahren z.B. nach 0831-103)<br>• Ggf. erforderlicher Neudurchlauf von NTZ Phasen (ggf. verkürzt), CSM Bewertungen oder erneute Verfügbarkeitsbetrachtung.<br>• Abgestimmte Beobachtungsphase.<br><br>Technologie: Intensivierung von Diagnose, log-Datenanalyse. Nutzung von Secure Boot Technologie. Neuerstellung von Zertifikaten und ggf. Berücksichtigung weiterer Parameter. Ggf. Planänderung mit Neuerstellung Daten und/oder kurzfristiger Anpassung mit Brauneinbesserung. Änderung von Beziehungen über KSC. | Prozess: Neudefinition des Sollzustandes bzw. des Konfigurationszielzustandes. Ggf. temporär akzeptierte einfache Wiederherstellung.<br>Patch-, Konfigurationsplanung, Netzwerkresegmentierung (nach Analyse). Analyse Änderungen gemäß SLA und Spiegelung an Zielen. Einspielen der Änderungen über Managementsystem nach betrieblich abgestimmter Rolloutplanung.<br>Ursachen müssen verstanden sein, Wirksamkeit der Maßnahmen ist nachzuweisen. Abstimmung zusätzlicher Beobachtungsmaßnahmen. Ggf. organisatorische Maßnahmen.<br><br>Technologie: zentralisiertes Patchmanagement. Neuherausgabe von Zertifikaten und/oder Signaturen. Änderungsmanagement über zentralisierte Management Systeme. Nutzung von Secure Boot und zentralen Policy Vorgaben. Netzwerkmanagement. |

## V. Literaturverzeichnis

Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) und Bundesamt für Sicherheit in der Informationstechnik (BSI). (1. Dezember 2016). Von http://www.kritis.bund.de/SubSites/Kritis/DE/Servicefunktionen/Glossar/Functions/glossar.html?lv2=4968608 abgerufen

CENELEC. (2010). EN 50159: Railway applications – Communication, signalling and processing systems – Safety-related communication in transmission systems.

Community & Regional Resilience Institute (CARRI). (2013). Definitions of community resilience: An analysis.

International Electrotechnical Comission. (kein Datum). IEC 62443 Industrial communication networks – Network and system security.

National Institute of Standards and Technology (NIST). (2013). Security and privacy controls for federal information systems and organizations. *NIST Special Publication, 800*, S. 53.

Petit, F., Phillips, J., Verner, D., & Whiteld, R. (2012). Resilience: theory and applications. *Decision and Information Sciences Division, Argonne National Laboratory*. Von http://www.dis.anl.gov/pubs/72218.pdf abgerufen

## Kontakt

Björn Zimmer, DB Netz AG, Mainzer Landstraße 201, 60326 Frankfurt a.M.
Telefon: 069 265 304 16 | Mail: Bjoern.Zimmer@deutschebahn.com

## Weitere Informationen

Die Arbeitsgruppe „Cybersecurity für sicherheitskritische Infrastrukturen – CYSIS“ wurde am 25. Januar 2016 von der Deutschen Bahn AG und der TU Darmstadt im Rahmen der Innovationsallianz und des bestehenden DB RailLab gegründet. Ziel der AG ist es, den durch die Digitalisierung im Eisenbahnsektor gestiegenen Herausforderungen der Cybersecurity in sicherheitskritischen Infrastrukturen wirksam begegnen zu können.

Die AG Cybersecurity ist eine Basis für intensiven Informationsaustausch zwischen Industrie und Wissenschaft im Eisenbahnsektor, um von den gegenseitigen Erkenntnissen profitieren zu können. Mit Hilfe der Partner aus dem wissenschaftlichen Bereich, u.a. CYSEC, dem Profilbereich für Cybersicherheit an der TU Darmstadt, können effektive Abwehrtechniken und Gegenmaßnahmen erforscht und weiterentwickelt werden. Angestrebter Effekt ist die Vernetzung des Eisenbahnsektors mit der akademischen Forschung zum Thema Cybersecurity.

## Webseite

http://www.cysis.eu