# 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.

## Impressionen vom Gründungssymposium am 25. Januar 2016

Prof. Mira Mezini, Vizepräsidentin für Wissens- und Technologietransfer, TU Darmstadt, und Frank Sennhenn, Vorstandsvorsitzender der DB Netz AG, unterzeichnen den Kooperationsvertrag für CYSIS

Auf dem Programm des Symposiums standen zahlreiche Fachvorträge aus Wirtschaft und Industrie

Die Organisation des Gründungssymposiums wurde unterstützt von CYSEC, dem Profilbereich Cybersecurity der TU Darmstadt

Get Together in der Bibliothek des Georg-Christoph-Lichtenberg-Haus in Darmstadt

Fotos: Claus Völker / Ann-Kathrin Braun / TU Darmstadt

## 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://www1.deutschebahn.com/innovationsallianz/start/forschung/AG_CYSIS.html