Hochschule für Angewandte Wissenschaften Hamburg
Hamburg University of Applied Sciences

Masterarbeit

Torge Hinrichs

IT Sicherheit in künftigen digitalen Zugsicherungssystemen - Potentielle Risiken und Analyseansätze

Fakultät Technik und Informatik
Studiendepartment Informatik

Faculty of Engineering and Computer Science
Department of Computer Science

Torge Hinrichs

IT Sicherheit in künftigen digitalen Zugsicherungssystemen - Potentielle Risiken und Analyseansätze

Masterarbeit eingereicht im Rahmen der Masterprüfung

im Studiengang Master of Science Informatik
am Department Informatik
der Fakultät Technik und Informatik
der Hochschule für Angewandte Wissenschaften Hamburg

Betreuender Prüfer: Prof. Dr. Bettina Buth
Zweitgutachter: Prof. Dr. Kai von Luck

Eingereicht am: 29. August 2017

Torge Hinrichs

Thema der Arbeit
IT Sicherheit in künftigen digitalen Zugsicherungssystemen - Potentielle Risiken und Analyseansätze

Stichworte
Security Analyse, Risiko Analyse, Safety-kritische Systeme, Digitalisierung von Bahnsystemen, Modellbasiertes Testen, CENELEC, Cyber-Physical Systems

Kurzzusammenfassung
Im Laufe dieser Arbeit wurden einige mögliche Ausprägungen von zukünftigen digitalen Zugsicherungssystemen betrachtet und deren Risiken untersucht. Hierzu wurden zunächst die Grundlagen für die Domäne der Bahnanwendung und der IT Sicherheitsrisiken in aktuellen Bahnanlagen betrachtet. In einem nächsten Schritt wurden dann verschiedene Architekturen für zukünftige digitale Systeme vorgestellt. Im Folgenden wurden dann die Sicherheitsrisiken, die durch die Digitalisierung entstehen analysiert und Möglichkeiten aufgezeigt mit denen diese Risiken minimiert werden können.

Torge Hinrichs

Title of the paper
IT Security for future railway control systems - potential risks and analysis approaches

Keywords
Security Analysis, Risk Analysis, Safety-critical Systems, digitisation of railway control systems, modellbased testing, CENELEC, cyber-physical Systems

Abstract
In this thesis several characteristics of future railway control systems were considered and their risks were analysed. To prepere this scheme, the fundamentals of railways systems were introduced and analysed for potential security risks. In a next step various architecures for digitisation of railway control systems were presented. The security risks for these architectures were analysed and possible countermeasures were provided.

Inhaltsverzeichnis

Abbildungsverzeichnis

Listings

1 Einleitung

Der öffentliche Personenverkehr gewinnt in der mobilen Gesellschaft immer mehr an Bedeutung. Im Jahr 2016 wurden allein ca. 11 Milliarden Menschen mit öffentlichen Verkehrsmitteln befördert [Bun17a]. Der Großteil der Beförderten legte diese mit schienengebundenen Verkehrsmitteln zurück. Es ist notwendig, dass diese Verkehrsmittel zuverlässig betrieben werden; Das wird auch in der Umsetzung der EU Richtlinie zum Schutz kritischer Infrastrukturen „UP KRITIS“ [Bun16b] sichtbar zu der sich Deutschland im Juli 2015 verpflichtet. Zu diesen Infrastrukturen gehören unter anderem die Energie- und Wasserversorgung, dem Finanz- und Versicherungswesen und auch jede Form von Transport und Verkehr. Die Bahn nutzt zur Zeit noch vorwiegend analoge Technik. Diese ist jedoch deutlich veraltet und störanfällig, Verspätungen und Ausfälle aufgrund von Stellwerksschäden oder Weichenschäden sind die Folge. Einer Pressemitteilung der DB AG nach wird sich dies jedoch ändern [Bah17]. Demnach sollen bis zum Jahr 2018 eine Milliarde Euro in die Digitalisierung aller Bahnbereiche investiert werden. Mit diesem Geld sollen unter anderem die vorhandenen digitalen Angebote der Bahn verbessert werden, aber insbesondere auch die Betriebsinfrastuktur. Die Digitalisierung der Bahninfrastruktur bietet große Vorteile. Beispielsweise können digitale Sensoren im Stellwerksbetrieb die Störanfälligkeit reduzieren und somit Verzögerungen im Normalbetrieb verringern. Auf der anderen Seite birgt die Digitalisierung auch neue Risiken. Bahnsysteme, wie Stellwerke oder das Schienennetz in Deutschland basieren aktuell überwiegend noch auf analogen Komponenten. So kann in aktuellen Systemen nur durch die Stellwerkssteuerung auf Weichen und Sensoren auf der Strecke zugegriffen werden. Die Kommunikation dieser Geräte erfolgt ausschließlich über Kabelverbindungen und eigens für diesen Bereich konzipierte Protokollen. Mit der Digitalisierung dieser Komponenten entstehen völlig neue Risiken, die zuvor in klassischen Bahnsystemen keine Rolle spielten. Beispielsweise müssen diese Systeme robust gegen jede Form von Verbindungsverlust oder Ausfall sein. Werden diese Systeme beispielsweise internetfähig und agieren als Gerät im IOT (Internet of Things), müssen diese Systeme auch gegen unbefugte Zugriffe von außen geschützt werden. Besonders kritisch werden solche Eigenschaften, wenn nicht nur Daten von den Sensoren gelesen werden können, sondern auch aktiv die Aktorik des Systems beeinflusst werden kann. Betrachtet man zum Beispiel das

Zugunglück von Bad Aibling [Zei16] wird klar, welches Risiko durch Cyberangriffe entstehen kann. Auch wenn es sich hierbei um menschliches Versagen handelt ist es denkbar, dass ein solches Fehlverhalten durch einen Cyberangriff herbei geführt werden könnte. Dazu kommt das Ausmaß einer solchen Attacke noch deutlich verheerender ausfallen kann, da der Angreifer nicht nur einen einzelnen Streckenabschnitt manipulieren kann, sondern ortsungebunden agiert. Somit könnten viele Stellwerke gleichzeitig angegriffen und eine Tragödie wie in Bad Aibling könnte sich in ganz Deutschland zeitgleich an mehreren Orten ereignen.

Das Ziel dieser Arbeit ist die Identifizierung von Problemen und Risiken an ausgewählten Beispielen, die bei der Digitalisierung eines Bahnstellwerkes auftreten können. Zu diesem Zweck werden zunächst unterschiedliche Szenarien erstellt, welche als Studienobjekt für die nachfolgenden Analysen genutzt wird. Diese Szenarien werden genutzt um zunächst Probleme und Risiken für aktuelle Systeme zu untersuchen werden und dann in einem folgenden Schritt die zusätzlichen neuen Risiken herauszuarbeiten. Diese Szenarien können auf Grund des Umfangs dieser Arbeit nur in ausgewählten Punkten im Detail analysiert werden. Insbesondere wird diskutiert, welche Test und Analyseverfahren eingesetzt werden könnten, um Angriffe auf Bahnanwendungen vorzubeugen und welche Rolle Modelle dabei spielen.

1.1 Gliederung dieser Arbeit

Der folgende Abschnitt dieser Arbeit gibt eine Einführung in die Domäne der Bahnstellwerke. Des Weiteren werden existierende Risiken im Bahnbetrieb analysiert. Diese bilden die Grundlage für die Betrachtung eines digitalisierten Bahnbetriebs. Darauf folgt eine Einleitung in Cyber-Angriffe, die für die einen Angriff auf Bahnanlagen verwendet werden könnten. Das Kapitel 4 gibt eine Übersicht über die Architektur aktueller Bahnanlagen. Außerdem wird die Kommunikation der einzelnen Komponenten genauer betrachtet, sowie eine Analyse der Verwundbarkeiten durch Cyber-Angriffe durchgeführt. Darauf folgt eine Beschreibung, wie ausgewählte Komponenten eines Stellwerks digitalisiert werden könnten und wie sich das Zusammenspiel dieser Komponenten durch eine solche Modifikation verändert. Hierzu wird zunächst die bestehende Architektur in Frage gestellt. Aus dieser Betrachtung resultiert eine Architektur mit zwei Varianten, die als Betrachtungsobjekt für die weitere Arbeit verwendet wird. Mit der Digitalisierung entstehen neue Risiken, dabei handelt es sich überwiegend um Cyberangriffe. Weitergehend erfolgt die Analyse welche dieser Angriffe geeignet sind um das skizzierte digitale Stellwerk anzugreifen. Zugehörig dazu werden Gegenmaßnahmen betrachtet, die solche Angriffe verhindern können. Im Abschnitt 7 werden dann Methoden untersucht, mit

denen die Ursachen der Verwundbarkeiten im Vorfeld entdeckt werden können. Abschließend werden die Ergebnisse dieser Arbeit zusammengefasst und bewertet.

2 Einführung in die Domäne: Bahnanlagen

Um digitale Stellwerke zu verstehen und analysieren zu können, ist es notwendig den Aufbau der vorhandenen Systeme mit ihrer Funktionsweise zu betrachten. Als Grundlage für diese Betrachtungen dienen die Werke von Arnold „Eisenbahn-Sicherungstechnik“ [Arn87] und Kusche „Gleisbildstellwerke (Reihe Stellwerks- und Blockanlagen)“ [Kus84]. Außerdem wurde aktuellere Literatur von Fendrich „Handbuch Eisenbahninfrastruktur“ [Fen07] und Pachl „Systemtechnik des Schienenverkehrs“ [Pac13] für die Grundlagenarbeit verwendet.

Eine typische Bauform eines Stellwerks ist das sogenannte Gleisbildstellwerk. Dieses ist dadurch charakterisiert, dass es einen Stelltisch (Siehe Abbildung 2.1) besitzt, an dem der Fahrdienstleiter Weichen, Bahnübergänge und Signale steuern kann [Kus84]. Die folgende Abbildung zeigt einen solchen Stelltisch in der häufigsten Bauart, ein so genannter „Relais-/Drucktastenstelltisch“ (links). Die Abbildung rechts zeigt einen elektronischen Stelltisch.

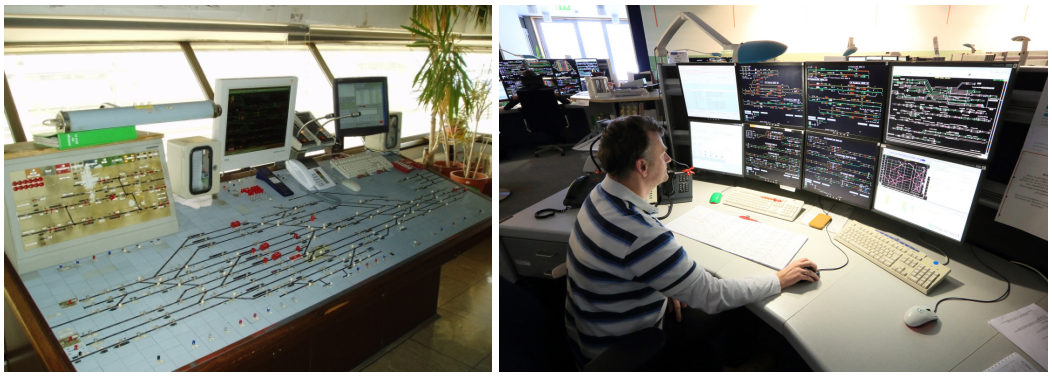

Abbildung 2.1: (links) Relais-/Drucktastenstelltisch Hütteldorf [M.A12] - (rechts) Betriebszentrale München [Mie17]

In Deutschland sind circa 45 % der Stellwerke Drucktastenstellwerke und etwa 13 % elektronische. Die restlichen Varianten sind mechanische und elektromechanische Stellwerke [Eic17]. Diese werden jedoch in dieser Arbeit nicht weiter berücksichtigt, da diese durch rein mechanische Steuerungen betrieben werden.

Die einzelnen Komponenten werden an dem folgenden Beispiel erläutert. Es handelt sich hierbei um das schematische Gleisbild des Stellwerkes „Hamburg-Schleswig-Holstein: Hamburg Eidelstedt“ [e.V17]. Dieses Stellwerk wurde gewählt, da es im Gegensatz zu den meisten anderen eine geringere Komplexität aufweist und somit überschaubarer ist. Die Abbildung 2.2 zeigt das komplette schematische Gleisbild des Stellwerks. Die Aufgabe des Stellwerks ist es die

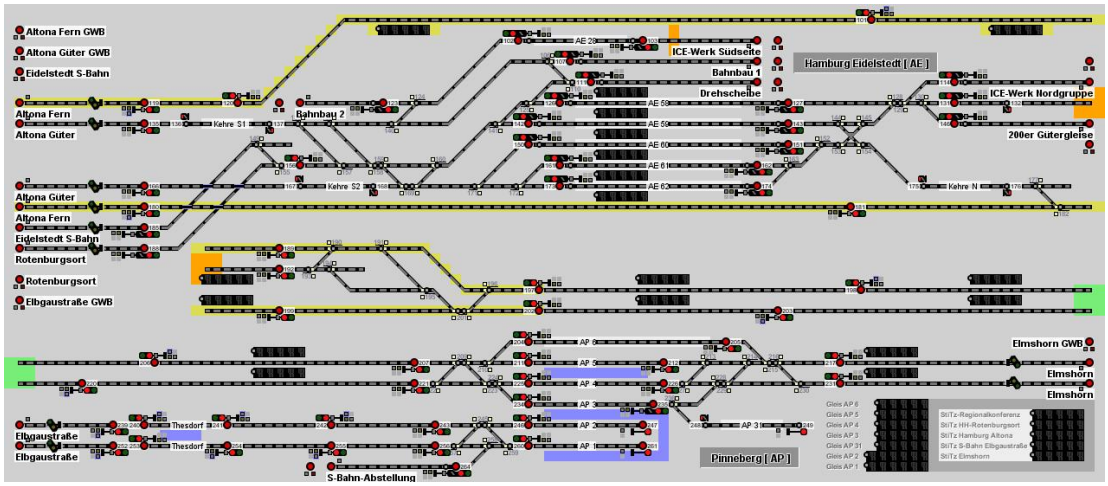

Abbildung 2.2: Schematische Darstellung eines Gleisbildes des Stellwerks „Hamburg-Schleswig-Holstein: Hamburg Eidelstedt “ [e.V17]

sichere Fahrt eines Zuges durch das Schienennetz zu gewährleisten. Der Triebfahrzeugführer im Zug muss sich auf die korrekte Signalbelegung und Weichenstellung verlassen können, da einem Zug durch das hohe Gewicht und die verhältnismäßig hohe Geschwindigkeit ein Fahren „auf Sicht“ durch den langen Bremsweg nicht möglich ist. Hierzu muss der Fahrdienstleiter einzelne Streckenabschnitte sperren bzw. wieder freigeben. Der folgende Abschnitt befasst sich mit den grundlegenden Elementen, aus denen ein Gleisbild zusammen gesetzt wird.

2.1 Überblick Bahnanlagen

Ein Gleisbildstellwerk besteht aus verschiedenen Komponenten, die in Kombination verschiedene Streckenabschnitte darstellen. Diese bestehen im Wesentlichen aus „Blockstrecken“ . Dabei handelt es sich um gesicherte Gleisabschnitte, die nur befahren werden dürfen, wenn diese frei

von Fahrzeugen sind. Innerhalb von Bahnhöfen wird dieser Begriff nur dann verwendet, wenn ein Bahnhofsgleis über besondere Sicherungsmaßnahmen verfügt. Bei den Sicherungsmaßnahmen handelt es sich um Sensoren, sogenannte Achszählern, die dem Fahrdienstleiter darüber Auskunft geben, ob ein Zug bzw. wie weit ein Zug einen bestimmten Bereich bereits passiert hat. Gleise, die planmäßig von Zügen befahren werden, müssen solche Sensoren vorweisen und werden als Hauptgleise bezeichnet. Außerhalb von Bahnhöfen werden diese auch als „freie Strecke“ bezeichnet. Alle weiteren Gleise werden als Nebengleise bezeichnet.

Zugehörig zu Blockstrecken sind „Blockstellen“ zu nennen. Dies sind Abschnitte, die nicht von mehreren Zügen zur gleichen Zeit befahren dürfen. Anders als Blockstrecken handelt es sich bei Blockstellen üblicherweise um Abzweigstellen (Weichen), Überleitstellen, Haltestellen oder Brücken. Alle Blockelemente, Blockstrecken, Abzweigstellen sind Abschnitte, in denen ein Zug von einer Blockstrecke auf eine andere wechseln kann. Wichtig hierbei ist, dass beim Übergang von einer Blockstrecke auf die Nächste nicht nur die beiden beteiligten Blockstrecken, sondern auch die angrenzende Blockstrecke gesperrt werden muss. Die folgende Abbildung 2.3 zeigt einen schematischen Aufbau einer Abzweigstelle.

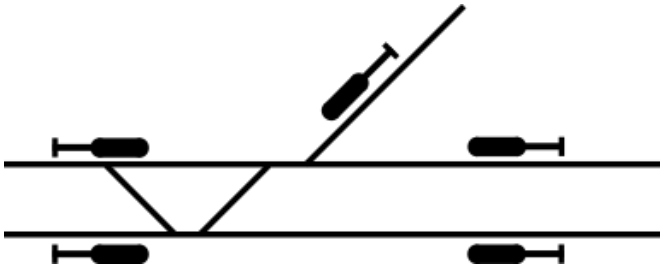

Abbildung 2.3: Schematische Darstellung einer Abzweigstelle

Überleitstellen sind Blockstellen, die von Zügen genutzt werden können, um von einem Gleis zum Anderen der gleichen Strecke zu wechseln. Dies ist nur bei mehrgleisigen Strecken möglich. Die Abbildung 2.4 zeigt eine schematische Darstellung einer solchen Überleitstelle. Wichtig hierbei, ähnlich zu den Abzweigstellen müssen die angrenzenden Blockstrecken gesperrt werden, um Zwischenfälle zu verhindern. Das Wechseln eines Gleises innerhalb einer Strecke kann über den weiteren Streckenverlauf entscheiden. Daher kann es notwendig sein, dass ein Zug auf ein anderes Gleis wechselt, um beispielsweise eine bestimmte Abzweigstelle zu erreichen.

Die Abbildung zeigt, die Notwendigkeit, dass nicht nur die abzweigende Blockstrecke sondern auch die angrenzenden Blockstellen gesperrt werden müssen. Geschieht dies nicht, kann

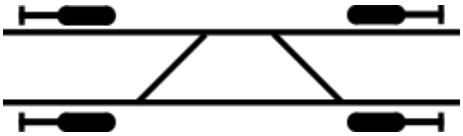

Abbildung 2.4: Schematische Darstellung einer Überleitstelle

aus einer anderen Richtung ein Zug in die Blockstelle einfahren und somit einen Zwischenfall verursachen.

Eine weitere Komponente des Gleisbildes sind Bahnhöfe. Bahnhöfe sind Bahnanlagen, die mit mindestens einer Weiche ausgestattet sind, in denen Züge beginnen, enden, ausweichen oder wenden können. Bahnhöfe sind im Allgemeinen durch Einfahrsignale oder Trapeztafeln von der restlichen Strecke abgegrenzt. Trapeztafeln sind weiße Tafeln mit schwarzem Rand, die an einem schwarz-weiß gestreiften Pfahl befestigt sind und grenzen in der Regel den Bahnhof von Blockstrecken ab. Die folgende Abbildung 2.5 zeigt schematisch den Aufbau eines Bahnhofs. Auffällig hierbei ist, dass obere und untere Fahrstrecke nur für den Betrieb in einer

Abbildung 2.5: Schematische Darstellung eines Bahnhofs

Richtung ausgelegt sind. Dies muss jedoch nicht zwingend so eingesetzt werden. Der Betrieb in beide Richtungen ist auch möglich.

Besonders in der Nähe von Bahnhöfen ist es notwendig, Züge auf andere Gleise zu verschieben oder die Fahrtrichtung zu ändern. Hierzu können sogenannte Nebengleise verwendet werden. Diese Gleise dazu genutzt werden Rangierfahrten durch zuführen oder einen Zug abzustellen. Die folgende Abbildung 2.6 zeigt eine schematische Darstellung eines solchen Gleises. In diesem Zusammenhang ist die „Anschlussstelle“ zu nennen. Hierbei handelt es sich

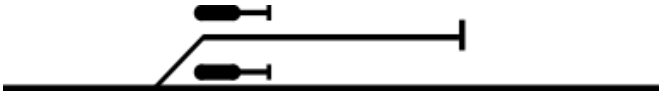

Abbildung 2.6: Schematische Darstellung eines Nebengleises

um eine freie Strecke, die auch für Rangierfahrten genutzt werden kann. Generell beschreibt dieser Begriff eine Zweigstelle innerhalb eines Streckenabschnittes, samt eines Nebengleises.

Hierbei muss in zwei Varianten unterscheiden: Auf der einen Seite Anschlussstellen, die während der gesamten Zeit inklusive des Hauptgleises gesperrt bleiben, bis der Zug den Bereich wieder verlassen hat. Auf der anderen Seite stehen Anschlussstellen, die obwohl sich noch ein Zug darin befindet wieder frei gegeben werden können. Hierbei handelt es sich üblicher Weise um sogenannte „Ausweichanschlussstellen“ bei denen der zuerst einfahrende Zug auf ein Nebengleis geleitet wird, sodass ein danach folgender Zug diesen überholen kann. Für diese Bereiche gelten besondere Regeln, damit mögliche Unfälle verhindert werden können.

Für die korrekte Ausführung solcher Manöver ist das Stellwerk zuständig. Der Fahrdienstleiter stellt hierzu Signale und Weichen so, dass ein reibungsloser Ablauf ermöglicht wird. Es lauern jedoch zahlreiche Risiken bei der fehlerhaften Bedienung des Stellwerks bzw. der falschen Beschaltung der Weichen und Signale. Der folgende Abschnitt befasst sich mit den Risiken, die allein durch das fehlerhafte setzen von Signalen oder stellen von Weichen entstehen können.

2.2 Analyse der Gefahren durch das Stellwerk

Durch den Betrieb des Stellwerks können Gefahren entstehen, die sogar katastrophales Ausmaß annehmen können. Hierbei ist es wichtig zu betrachten, dass nicht nur Materialermüdungen, beispielsweise an einer Weiche, oder fehlerhafte Teile, zum Beispiel in einem Signal, eine solche fatale Situation herbeiführen können, sondern auch Fehler in der Bedienung des Stellwerks. Wie in Abschnitt 1 beschrieben sorgte in Bad Aibling [Zei16] das Fehlverhalten eines Fahrdienstleiters dafür, dass zwei Züge auf einer eingleisigen Strecken zusammenstießen. Der folgende Abschnitt befasst sich mit einer Betrachtung ähnlicher Verstöße, die zu ähnlichen Konsequenzen führen können.

2.2.1 Gefährdung von vorn und hinten

Fährt ein Zug auf einer Blockstrecke so muss sich der Triebwagenführer darauf verlassen, dass der Fahrtweg für ihn gesichert ist. Dies geschieht dadurch, dass ein Signal, das die Einfahrt in eine Blockstrecke beschränken. Eine solche Blockstrecke soll nur von einem Zug zur Zeit befahren werden. Um dies zu gewährleisten muss sich zwischen 2 Zügen immer ein auf „Halt“ stehendes Signal befinden. Die Gefahrenquelle entsteht hierbei, wenn der Fahrdienstleiter diese Regel nicht einhält. Ein schnellerer Zug kann auf einen langsameren Zug auffahren. Geschieht dies beispielsweise hinter einer Kurve. Dort reicht der Bremsweg des schnelleren Zuges nicht aus, um den Zug zum Halten zu bringen und fährt auf den langsameren Zug auf. Ein Entgleisen des Zuges kann die Folge sein. Die folgende Abbildung 2.7

zeigt schematisch ein Szenario in dem ein Auffahren eines Zuges auf einen Anderen möglich ist.

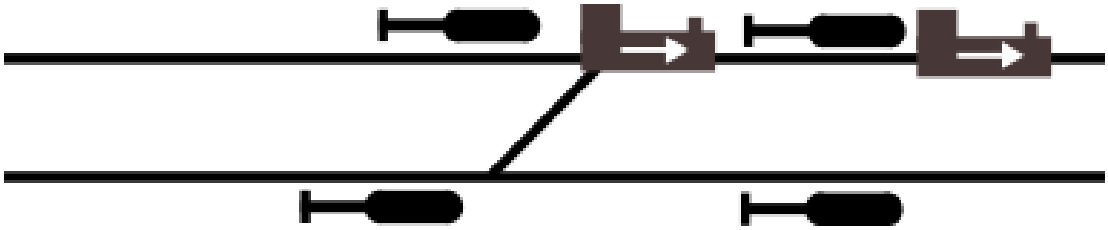

Abbildung 2.7: Schematische Darstellung einer Gefährung von vorn und hinten durch einen auffahrenden Zug

2.2.2 Gefährdung von der Seite

Eine weitere Gefährdung kann beim Wechseln einer Fahrstrecke entstehen. Der Fahrdienstleiter kann hierbei die Strecke bereits freigeben, obwohl sich noch ein anderer Zug in der Abzweigstelle befindet. Die Abbildung zeigt Situationen in denen der Zugverkehr durch je einen seitlich einfahrenden Zug gefährdet wird. Situation I zeigt einen Zug a, der auf von einem Gleis 3 über eine Wiche auf das Gleis 2 übergeleitet wird. Auf dem Gleis 2 befindet sich bereits ein Zug b. Fährt Zug a schneller als Zug b so liegt eine Situation vor wie in Abschnitt 2.2.1 beschrieben. Fährt Zug b langsamer liegt zwar eine Verletzung der Fahrdienstordnung vor, jedoch keine direkte Gefährdung durch eine Kollision. Situation II zeigt einen Zug b der auf einem Gleis 2 fährt und einen Zug c, der von Gleis 1 durch eine Weiche auf Gleis 2 umgeleitet wird. Befindet sich Zug b noch innerhalb der Abzweigstelle ist eine Kollision mit fatalen Folgen wahrscheinlich.

2.2.3 Gefährdung durch entgegenkommenden Zug

Die wohl schwerwiegendste Gefährdung entsteht dann, wenn zwei Züge auf dem gleichen Gleis auf einander zu fahren. Hierbei entsteht bei einem Zusammenstoß eine viel größere Wucht, als in den zuvor beschrieben Szenarien. Beide Züge fahren auf einander zu und addieren somit ihre Aufprallgeschwindigkeit. Anders als in den zuvor beschriebenen Gefährdungen, bei denen die Züge hintereinander fahren und sich ihre Aufprallgeschwindigkeit durch die Differenz der Züge ermitteln lässt. Das Ausmaß eines solchen direkten Zusammenstoßes wird beim Zugunglück von Bad Aiblingen deutlich. Die Abbildung 2.2.3 verdeutlicht diesen Sachverhalt. Wir beiden Zügen die Einfahrt in die Blockstrecke ist eine Kollision wahrscheinlich.

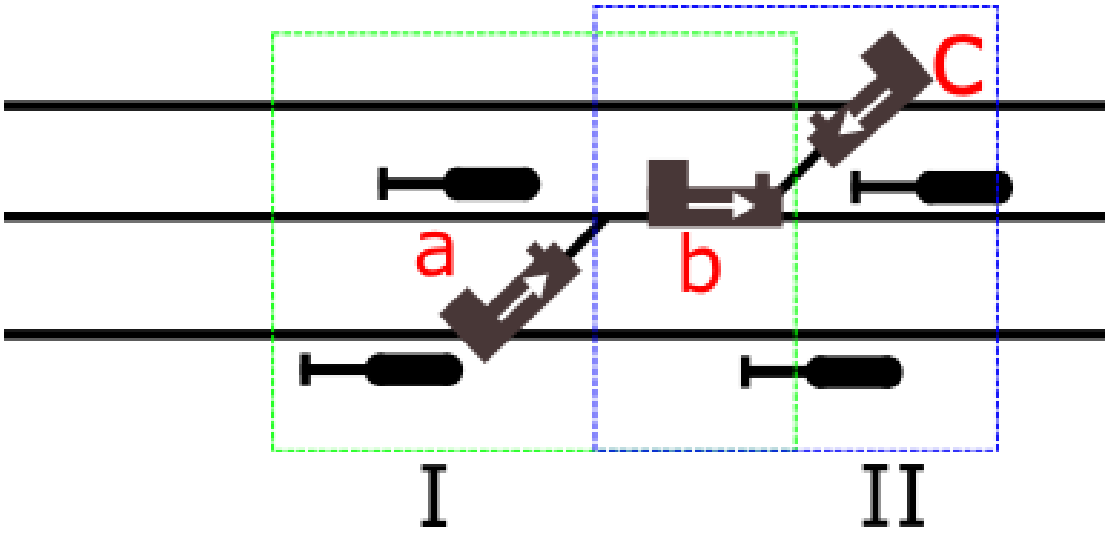

Abbildung 2.8: Schematische Darstellung einer Gefährung von der Seite. Situation I: Zug a schließt auf Zug b auf. Situation II Zug c fährt auf den in der Weiche befindlichen Zug b zu.

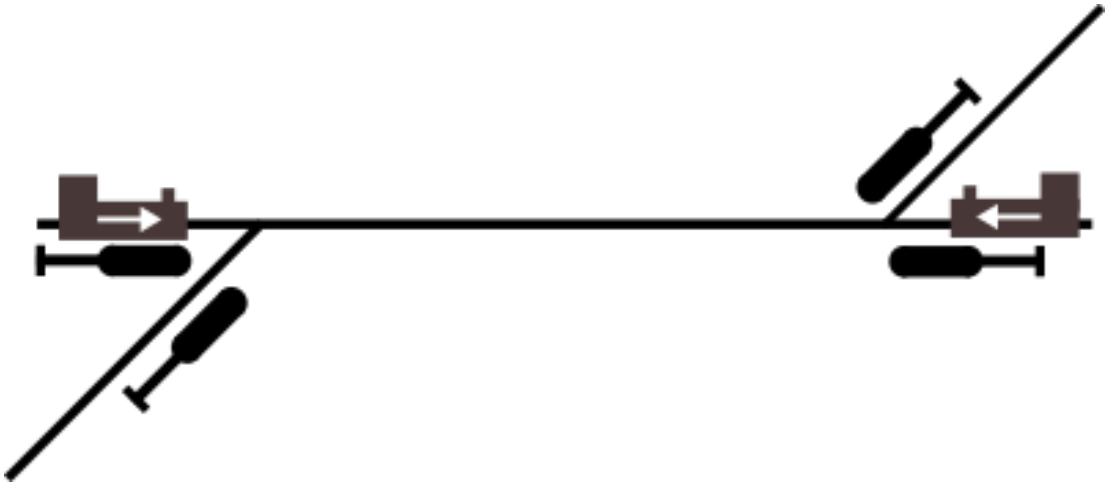

Abbildung 2.9: Schematische Darstellung einer Gefährung durch einen entgegenkommenden Zug auf eingleisiger Strecke.

2.2.4 Gefährdung durch Umstellen einer Weiche

Es kann auch mit nur einem Zug zu verehrenden Zwischenfällen kommen. Wie die Abbildung 2.10 zeigt. Die Abbildung zeigt, drei Wagons, die über eine Weiche fahren. Diese seien Teil eines Zugs, der von links nach rechts fährt. Die rot markierten Stellen verdeutlichen den

Schaltvorgang der Weiche. Die genaue Funktionalität einer Weiche wird in [Fen07] beschrieben. Wird eine Weiche umgestellt während sich noch ein Zug auf ihr befindet so fährt der vordere Teil des Zuges (rechts der Weiche) weiter auf den Schienen geradeaus, der hintere Teil hingegen wird abgelenkt und auf die abzweigenden Schienen geleitet. Dabei zieht jedoch der vordere Teil weiter an den Wagons und der Zug entgleist. Dies wird in der Regel durch Achszähler verhindert. Diese Zählen wie viele Achsen die Weiche passiert haben, stimmt die Anzahl nicht mit der erwarteten überein, so kann die Weiche nicht umgestellt werden. Jedoch ist ein manuelles Überschreiben dieser Sicherung durch das Stellwerk möglich. Es kann also auch zu solch einer Gefährdung kommen. Neben Versagen im Stellwerk kann es noch zu weiteren

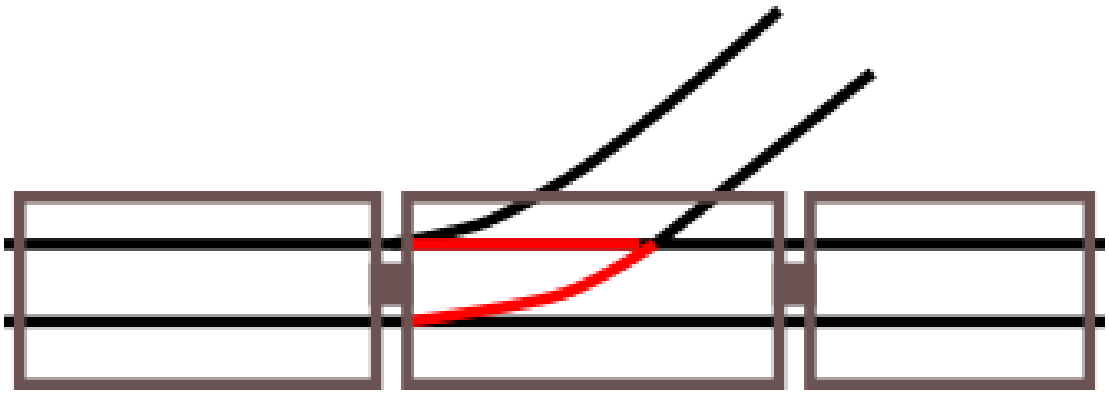

Abbildung 2.10: Schematische Darstellung einer Gefährung durch das verfrühte Umstellen einer Weiche.

Problemen im Bahnbetrieb kommen. Der folgende Abschnitt beschreibt Risiken, die zusätzlich zur Gefährdung durch das Stellwerk auftreten können.

2.3 Gefährdungen durch den Zug

Das Stellwerk stellt nicht die einzige Gefahrenquelle für den Zug betrieb dar. Dabei ist nicht nur das menschliche Versagen innerhalb des Stellwerkes zu betrachten, es muss demnach auch das menschliche Versagen des Triebfahrzeugführer betrachtet werden.

2.3.1 Gefährdung durch Missachten der Fahrbefehle oder Signale

Der Triebfahrzeugführer ist angewiesen den Signalen auf der Strecke folge zu leisten, um einen sicheren Ablauf einer Zugfahrt zu gewähren. Es kann jedoch zu Störungen im Normalbetrieb kommen. Für diese Fälle werden sogenannte Fahrbefehle verwendet [End03]. Diese

regeln besondere Situationen und weisen beispielsweise den Triebfahrzeugführer an, an einem bestimmten Signal zu stoppen oder sogar die Zugführung durch Signale zu ignorieren und „auf Sicht“ die Fahrt mit verringerter Geschwindigkeit fort zusetzten. Ein Risiko entsteht dann, wenn der Triebfahrzeugführer sowohl die Signale ohne einen gültigen Befehl missachtet, oder auch den ihm erteilten Fahrbefehl missachtet oder übersieht. Hierbei sind nun diverse Gefährdungen denkbar. Beispielsweise kann bei dem Missachten einer Geschwindigkeitsbeschränkung ein Zug den Halt auf den Schienen verlieren und entgleisen. Ein Beispiel für die Folgen eines solchen Fehlverhaltens ist das Zugunglück Santiago de Compostela, Spanien aus dem Jahr 2013. Am 24.03.2013 verunglückte ein Hochgeschwindigkeitszug aufgrund deutlich erhöhter Geschwindigkeit in einem Gleisbogen [ulz13]. Laut dem Untersuchungsbericht ERA/ADV/2015-6 der europäischen Eisenbahn Agentur [Car15] fuhr der Zug mit 199 Km/h auf einer Schnellfahrstrecke welche in einen alten nur langsam befahrbaren Streckenabschnitt mündet. Kurz vor dem Übergang in den alten Abschnitt wurde der Triebfahrzeugführer durch ein eingehendes Telefonat auf seinem Handy abgelenkt und verlor den Überblick darüber auf welchem Streckenabschnitt sich der Zug befand und fuhr mit gleicher Geschwindigkeit weiter. Laut Plan sollte dieser Abschnitt jedoch mit einer Geschwindigkeit von 80 Km/h befahren werden. Etwa 300 Meter vor erreichen eines Hauptsignals vor einem Gleisbogen bemerkte der Triebwagenführer seinen Fehler und leitete eine Schnellbremsung ein. Bei einer Geschwindigkeit von 153 Km/h entgleisten die ersten vier Wagen des Zuges und überschlugen sich. 80 Menschen starben und 152 Personen wurden verletzt. Dieser Zwischenfall ist klar auf menschliches Versagen zurückzuführen. Abseits dieser schwer kalkulierbaren Risiken müssen noch weitere Risiken berücksichtigt werden. Der folgende Abschnitt befasst sich mit einem Risikobereich, der zur Störung einer Zugfahrt führen kann.

2.3.2 Gefährdung durch Versagen von Bauteilen

Der Ausfall von Bauteilen an einem Zuges oder auf der Gleisanlage kann auch zu fatalen Situationen für eine Zugfahrt führen. Daher ist es wichtig, dass diese Teile in die Betrachtung einbezogen werden. Zunächst werden hierzu Komponenten identifiziert, die eine Gefährdung der Sicherheit darstellen. Die Hardwareanforderungen für solche Komponenten sind in der EN 50129 [DIN03] spezifiziert. Sind diese Systeme durch Software gesteuert, so sind die Safety Eigenschaften, die ein solches System erfüllen muss in der EN 50128 [DIN12] spezifiziert. Hierbei werden nicht nur Stellwerkskomponenten betrachtet, wie Weichen, Achszähler oder Signale, sondern auch kritische Bereiche am Zug, wie Kupplungen oder Bremsen. Beide Normen sind Spezialisierungen der übergeordneten IEC 61508, die sich mit dem Thema „Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer

Systeme“ befasst. In dieser Norm werden unter anderem auch Security-Richtlinien für die Schnittstellen aufgestellt. Alle Risiken, die bei einer Zugfahrt auftreten können, müssen analysiert und bewertet werden und von kontrollierenden Instanzen, wie zum Beispiel Behörden überprüft werden. Aus diesem Grund müssen umfassende Risikobewertungen vorgenommen werden. Der folgende Abschnitt zeigt exemplarisch, wie Risiken im Safety-kritischen Bereichen untersucht werden.

2.4 Analyse der Risiken

Für den Bahnbereich gilt, dass den Ablauf gefährdende Situationen im Betrieb vom Stellwerk erkannt werden müssen. Tritt eine solche Situation auf, so muss das Stellwerk dafür sorgen, dass das Gesamtsystem in einen sicheren Zustand überführt wird, damit das Problem behoben werden kann [Mas15]. Dieser Zustand wird als „failsafe state“ [Lap14] bezeichnet. Dieser Zustand dient dazu, dass das Gesamtsystem abgesichert ist und keine weiteren Gefährdungen auftreten können. Aus Sicht des Stellwerks können Weichen, sowie Signale in einen „failsafe state“ gebracht werden. Weichen sollten, wenn sie sich in diesem Zustand befinden nicht mehr geschaltet werden. Signale sollten das „STOP“ Signal anzeigen. Wenn diese Regeln befolgt werden ist es nicht mehr möglich weitere Gefährdungen, wie zum Beispiel in 2.2 dargestellt, zu verursachen.

Das Erkennen einer Gefährdung erfordert eine genaue Analyse der Situationen, die eine Gefahr darstellen und wie diese auftreten können hierbei müssen sowohl Fehler im Design als auch im tatsächlichen Betrieb berücksichtigt werden. Eine Gefährdung, auch „Hazard“ genannt, ist dabei wie folgt definiert: „a situation in which there is actual or potential danger to people or to the environment“ [Sto96]. Hierbei ist es unerheblich, ob der Hazard durch einen Softwarefehler, Hardwareversagen oder durch einen Menschen herbeigeführt wird. In den meisten Fällen müssen verschiedenen Kombinationen solcher Probleme auftreten, damit es zu einer potentiellen oder auch tatsächlichen Gefährdung kommen kann. Um diese Kombination von Ereignissen und deren Eintrittswahrscheinlichkeit zu bestimmen schlägt das Europäische Komitee für elektrotechnische Normung (Fr.: Comité Européen de Normalisation Électrotechnique) [CEN17], kurz CENELEC, die Verwendung von Fehlerbaumanalysen (FTA) [CEN07] vor. Hierbei handelt es sich um einen weit verbreitete und anerkannte Technik um eine Gefährdung in dafür notwendigen Ereignisse aufzuteilen und eine Abhängigkeit dieser Ereignisse bis hin zum tatsächlichen Ausfall des Systems aufzuzeigen. Die Vorgehensweise wird in dem IEC Standard 1025 festgelegt [STA90]. Grundsätzlich wird bei einer solchen Analyse ein Hazard

betrachtet und von dort aus werden rückwärts alle Ereignisse betrachtet, die zum auftreten des Hazards führen können. Die Abbildung 2.11 zeigt die Elemente, in einer Fehlerbaumanalyse verwendet werden können [VG81].

a) Ereignis Ein solches Ereignis entsteht durch die Kombination von einem oder mehreren logischen Gattern.

b) ODER-Gatter Der Ausgang dieses Gatters tritt auf, wenn mindestens ein der eingehenden Ereignisse auftritt.

c) UND-Gatter Der Ausgang dieses Gatters tritt auf, wenn alle eingehenden Ereignisse auftreten.

d) Sekundäres Ereignis Dieses Ereignis kann nicht weiter in Unterereignisse aufgeteilt werden. Grund dafür können fehlende Informationen oder nicht abschätzbare Konsequenzen sein.

e) Basisereignis Ein Basisereignis kann nicht weiter unterteilt werden. Hierbei handelt es sich üblicherweise um Bauteile bei denen die Ausfallwahrscheinlichkeiten bekannt sind oder Ausfallwahrscheinlichkeiten, die durch andere Analysen bestimmt wurden.

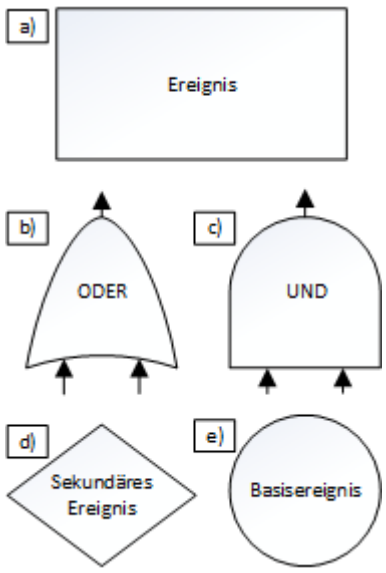

Abbildung 2.11: Elemente in einer Fehlerbaumanalyse

Um einen Überblick zu bekommen, wie solche Analysen aussehen werden im folgenden Abschnitt zunächst das Entgleisen eines Zuges und die Kollision an einem Bahnübergang

betrachtet.

Die folgende Abbildung 2.12 zeigt eine Fehlerbaumanalyse für das Entgleisen eines Zuges. Als Ausgangspunkt dient hierbei das Entgleisen des Zugs. Damit dieses Ereignis eintreten kann muss eines der darunter liegenden sechs Ereignisse eintreten. Dies wird durch die ODER Verknüpfung deutlich. Auffällig bei der Betrachtung der sechs Ereignisse ist, dass das Ereignisse wie: „Strecke beschädigt “ oder „Notbremse“ durch eine Raute modelliert sind. Diese Ereignisse werden als „sekundäre Ereignisse“ bezeichnet. Hierbei handelt es sich um Ereignisse, die nicht genauer aufgelöst werden können, oder über die keinen weiteren Informationen vorliegen. Die restlichen Ereignisse werden mit einem Rechteck modelliert. Diese beschreiben Ereignisse, die durch zusammensetzen von weiteren Ereignissen entstehen und daher weiter analysiert werden können. Beispielweise kann das Ereignis „Weiche falsch gestellt“durch eines der darunter liegenden Basisereignisse (als Kreis modelliert) ausgelöst werden. Basisereignisse beschreiben Ereignisse die nicht weiter aufgelöst werden können, oder für die Ausfallwahrscheinlichkeiten existieren. Die Wahrscheinlichkeiten können üblicherweise bei Bauteilen angegeben werden, da diese durch den Hersteller bestimmt werden. Es können aber auch Ereignisse auftreten, die erst durch die Verkettung mehrerer Ereignisse entstehen können. Dies ist bei dem Ereignis „Zug zu schnell“ der Fall. Das Ereignis tritt ein, wenn der Achszähler im Streckenabschnitt die falsche Position des Zuges meldet oder der Achszähler ganz defekt ist und zusätzlich dazu das Bremsen des Zuges keine Wirkung zeigt. Die Falschmeldung der Position durch den Achszähler kann weiter aufgelöst werden. Dies tritt ein, wenn der Achszähler defekt ist, dieser falsch gestellt wurde, oder der Streckenabschnitt zu früh frei gegeben wurde. Wichtig hierbei ist, dass es sich bei dem defekten Zähler um ein Materialversagen handelt, bei dem Freigeben des Streckenabschnittes und dem Nicht-umstellen der Weiche um menschliches Versagen. Das letzte zusammengesetzte Ereignis in diesem Fehlerbaum ist „Während Zug in Weiche, Weiche gestellt“ dieses Risiko wurde bereits in Abschnitt 2.2.4 genauer erläutert. Dieses Ereignis kann eintreten, wenn der Zug nicht korrekt in dem Streckenabschnitt erkannt wird oder die Weiche defekt ist. Die Erkennung des Zuges kann nicht korrekt funktionieren, wenn beispielsweise ein Sensor innerhalb der Weiche oder des Streckenabschnittes defekt ist oder zwei Züge zu dicht hinter einander fahren.

Weitere kritische Abschnitte bei der Sicherung einer Zugfahrt sind Bereiche in denen die Zugfahrt mit anderen Teilnehmern koordiniert werden muss. Dies ist beispielsweise an Bahnübergängen der Fall. Die Fehlerbaumanalyse in Abbildung 2.13 zeigt, welche Komponenten für die Kollision an einem Bahnübergang verantwortlich sein können. Eine Kollision findet dann

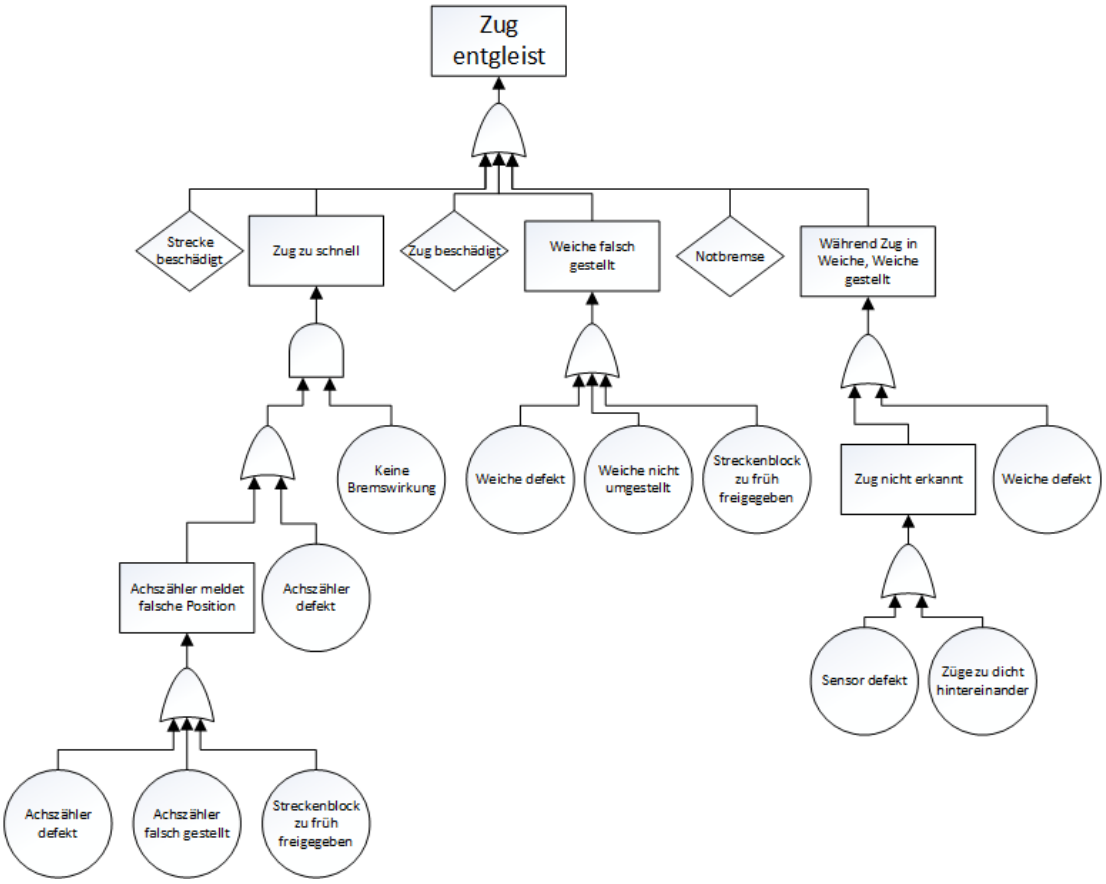

Abbildung 2.12: Fehlerbaumanalyse für das Entgleisen eines Zuges. Auf Basis von [Mew09]

statt, wenn sich ein Zug im Gleisabschnitt des Übergangs befindet und sich ein Gegenstand auf den Schienen befindet. Um dies zu verhindern verfügt ein Bahnübergang über verschiedene Sicherungsmaßnahmen. Grundsätzlich wird dabei in zwei verschiedene Bauformen unterschieden. Die erste Form ist der unbeschrankte Bahnübergang. Dieser zeichnet sich dadurch aus, dass er aus einem passivem Warnsignal, dem „Andreaskreuz“ besteht Zusätzlich dazu sind aktive Elemente in Form von blinkenden Warnleuchten angebracht. Die zweite Form erweitert die erste Form noch um Schranken, die den Fahrweg für die Straßenfahrzeuge und Fußgänger blockieren, wenn ein Zug durch den Bahnübergang fährt. Hierbei muss jedoch auch noch zwischen einem Bahnübergang mit „Halbschranke “, also eine Schranke auf der jeweiligen Fahrtrichtung und Bahnübergängen mit Schranken, also auf beiden Seiten auf jeder Spur eine Schranke, unterschieden werden. Wann welche Art verbaut wird ist in der Eisenbahn-Bau- und Betriebsordnung (EBO) [Bun67] geregelt. Aus Sicht des Zuges ist der Bahnübergang durch ein Haltesignal gesichert, dass dem Triebwagenfahrer signalisiert, wann der Bahnübergang befahrbar ist.

Eine Gefährdung entsteht, wenn eines der Sicherungsmaßnahmen ausfallen oder ignoriert werden. Der Zug ist die gefährdende Komponente, wenn beispielsweise der Triebwagenfahrer das Haltesignal ignoriert oder dieses Haltesignal defekt ist. Eine weitere Variante ist, dass der Zug nicht korrekt erkannt wird. Dies hat zur folge, dass der Zug an einer anderen Position erwartet wird, als er sich tatsächlich befindet. Dies entsteht, wenn beispielsweise der Achszähler der Strecke defekt ist oder die Strecke durch durch das Stellwerk zu früh frei gegeben wird. Damit es tatsächlich zu einer Kollision kommen kann muss zusätzlich zu dem Zug, der sich unerwartet in dem Streckenabschnitt befindet, noch ein Gegenstand auf den Schienen befinden. Ein solcher Gegenstand kann beliebig sein, von einem eingestürzten Baum, über verlorener Ladung, bis hin zu Personen oder Fahrzeugen. Ein solcher Gegenstand kann sich auf den Schienen befinden, wenn sich dieser trotz funktionierenden Sicherungsmechanismen im Schienenbereich aufhält. Eine andere Möglichkeit ist, dass sich der Gegenstand regelkonform verhält, aber die Sicherungsmaßnahmen versagen. Dies kann passieren, wenn beispielsweise die Warnleuchten des Bahnübergangs versagen. Bei unbeschrankten Übergängen ist damit keine aktive Sicherungsmaßnahme mehr funktionsfähig und die Chance für eine Kollision steigt. Handelt es sich um einen beschrankten Übergang, so bleibt diese Sicherung aktiv. Fallen auch die Schrankenanlagen aus, so ist auch bei einem beschrankten Bahnübergang keine aktive Sicherung mehr funktionsfähig und es kann zu einer Kollision kommen.

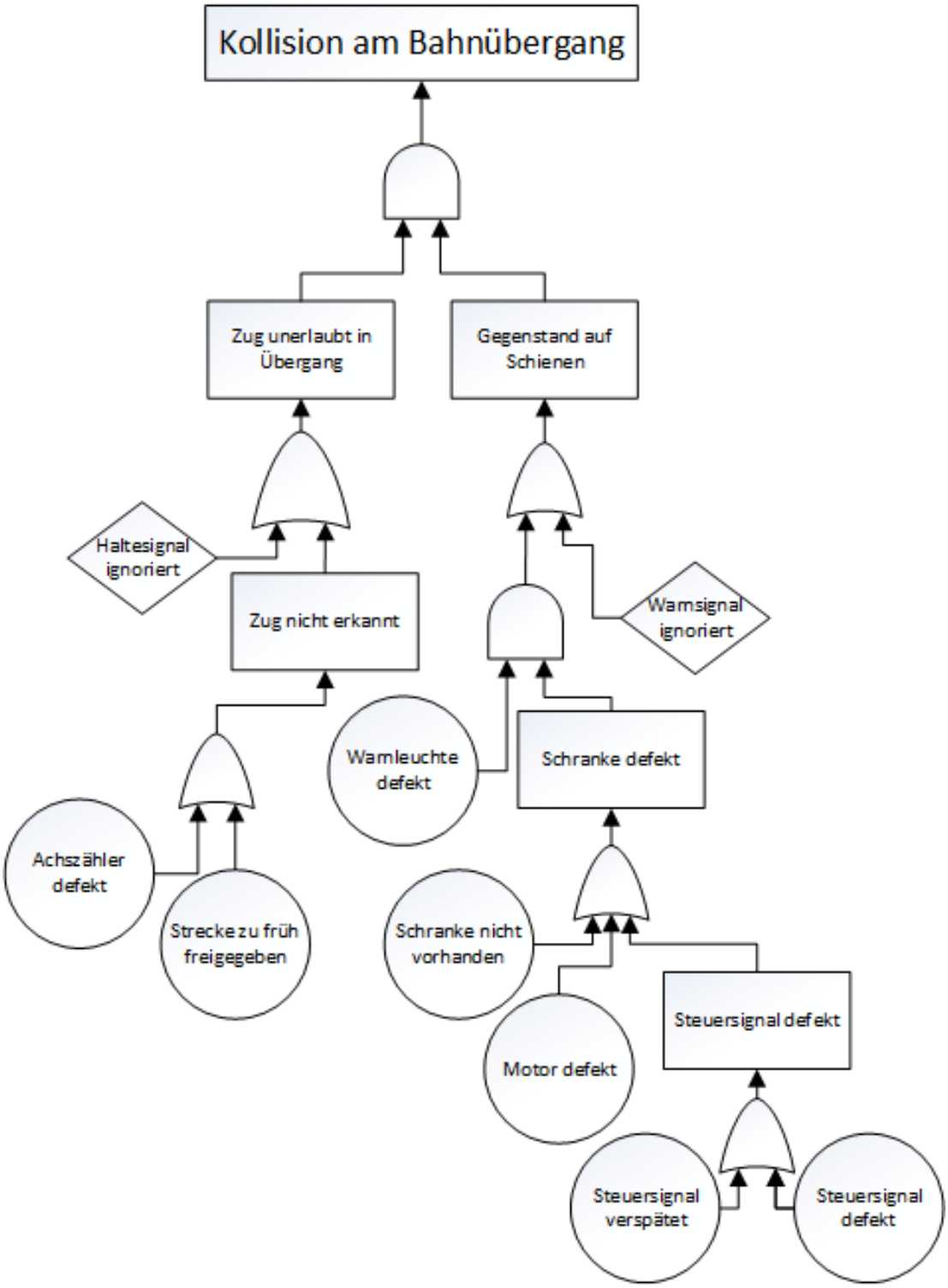

Abbildung 2.13: Fehlerbaumanalyse die Kollision eines Zuges an einem Bahnübergang. (Eigene Darstellung)

Dies sind nur Auszüge aus Risikoanalysen, die für die Sicherung einer Zugfahrt getätigt werden müssen. Jedoch beruhen diese Analysen darauf, dass die Bahnsysteme als in sich geschlossene Systeme eingesetzt werden und daher nur schwer durch äußere Einflüsse verändert werden können. Bei digitalen Stellwerken entstehen neue Schnittstellen mit von der Bahn unabhängigen Systemen. Aus diesem Grund ist es notwendig auch Cyberangriffe zu betrachten und diese in die Analyse eines digitalen Stellwerks mit einzubeziehen. Daher gibt der folgende Abschnitt einen Überblick über aktuell gängige IT-Angriffsszenarien und bezieht diese auf den Bahnbereich.

3 Einführung in Cyberangriffe

Um einen besseren Überblick über mögliche Angriffe und deren Szenarien zu bekommen betrachtet dieses Kapitel die zehn häufigsten It-Security Angriffe. Diese Liste wird von dem „Open Web Application Security Project “ (OWASP)[Kon17] erstellt. OWASP ist eine Non-Provit-Organisation, die sich zum Ziel gesetzt hat die Sicherheit von Anwendungen und Diensten im Internet zu verbessern. Dieses Projekt wird unter anderem auch von Großkonzernen wie Adobe oder Huawei unterstützt. Die Angriffsszenarien die in der Arbeit des OWASP vorgestellt werden beziehen sich nur auf Angriffe über das Internet. Dennoch lassen sich solche Angriffe leicht auf den Bahnbereich übertragen, wenn dieser digitalisiert und mit dem Internet verbunden ist.

3.1 Injections

Als „Injection Attacs“ [HVO06] werden Angriffe auf ein System bezeichnet, die durch das Modifizieren von Eingaben Zugriff auf ein System ermöglichen. Dieser Zugriff kann vom Ausspähen von Informationen bis hin zur vollständigen Kontrolle über ein System reichen. Dieser Art des Angriffes kann auf verschiedenen Ebenen durchgeführt und gegen unterschiedliche Teilsysteme gefahren werden. Gängige Vertreter sind hierbei Datenbanksysteme (SQL Injection), Betriebsysteme (Comandline Injection), XML Daten (XXE Injection) oder LDAP Systeme (LDAP Injection). Der Angriff wird in der Regel möglich, wenn die Eingaben in das System nicht korrekt oder gar nicht geprüft werden. Der Angriff erfolgt dann wenn es möglich ist Parameter eines Aufrufs oder einer Abfrage zu ändern und das Ergebnis dieses Aufrufs lesbar ist. Der folgende Abschnitt zeigt exemplarisch, wie ein solcher Angriff auf einer SQL Datenbank durchgeführt werden könnte.

Als Szenario für dieses Beispiel sei ein Onlineshop gegeben. Die Anzeige der Artikel erfolgt über eine angepasste URL für jeden Artikel, wie in Listing 3.1 dargestellt.

```
1 http://www.beliebigershop.de/artikel.php?nummer=1234
```

Listing 3.1: Beispiel-URL eines Onlineshops

Erfolgt der Aufruf dieser URL, so interpretiert üblicherweise ein PHP-Script die Adresse inklusive des Parameters „nummer=1234“. An dieser Stelle wird eine Variable nummer mit dem Wert 1234 erzeugt und dem PHP-Script zur Verfügung gestellt. Dieses Script erzeugt dann in der vorgesehenen Routine den in Listing 3.2 darstellen SQL-Ausdruck:

```
1 SELECT * FROM artikelNummern WHERE artikelNummer=1234;
```

Listing 3.2: Beispiel: gewollter korrekter SQL-Ausdruck

Der Ausdruck sammelt alle Spalteneinträge zu der gewünschten Artikelnummer und liefert diese Daten zurück an das Script. Das PHP-Script verarbeitet diese Daten und erstellt die gewünschte HTML-Seite mit den passenden Daten zu dem Artikel mit der Nummer „1234“. Vergisst der Programmierer im PHP-Script vor dem Verarbeiten der Variable den Wert zu bereinigen, so kann durch das Modifizieren der URL ein beliebiger weiterer Befehl ausgeführt werden. Das Listing 3.3 zeigt, wie eine solche modifizierte URL aussehen kann.

```
1 http://www.beliebigershop.de/artikel.php?nummer=1234;
2         UPDATE+benutzer+SET+passwort=123+WHERE+1=1;--
```

Listing 3.3: Beispiel: URL eines Onlineshops mit SQL-Injection

Wie im Listing 3.2 dargestellt wird auch diese Anfrage an den Shop in eine SQL Abfrage umgewandelt. Diese wird in Listing 3.4 dargestellt.

```
1 SELECT * FROM artikelNummern WHERE artikelNummer=1234;
2 UPDATE benutzer SET passwort=123 WHERE 1=1;--
```

Listing 3.4: Beispiel: korrumpierten SQL-Ausdruck

Die SELECT-Anweisung wird wie zuvor ausgeführt und liefert auch korrekte Ergebnisse. Jedoch wird zusätzlich noch die in Listing 3.4 dargestellte UPDATE-Anweisung ausgeführt. Diese ändert alle Passwörter aller Benutzer des Onlineshops auf „1234“. Die „- - “ am Ende der Anweisung stehen in der SQL-Syntax für einen Zeilenkommentar. Dieser wird am Ende der Anweisung eingesetzt, um mögliche weitere Anweisungen, die der Programmierer gewollt eingefügt haben könnte zu deaktivieren. Der Angreifer kann sich nun mit jedem beliebigen Benutzernamen in den Onlineshop einwählen und nach belieben ändern. Alle anderen Benutzer sind nun außerdem nicht mehr in der Lage den Shop zu nutzen.

Bezogen auf den Bahnbereich können solche Angriffe auf Stellwerke angewendet werden, sofern diese über APIs nach außen verfügen. Hierbei können sowohl Datenbanken als auch Betriebssysteme oder LDAP Systeme Ziel eines solchen Angriffs werden.

3.2 Broken Authentication and Session Management

Probleme mit der Authentifizierung oder der Session Verwaltung sind Probleme, die in erster Linie bei Webseiten auftreten können. Diese Art Angriff entsteht, wenn beispielsweise ein Online-Shop seine angemeldeten Kunden durch eine Session identifiziert [Mit17c]. Üblicherweise kann über die URL ermittelt werden, welchen Artikel innerhalb des Shops sich der Kunde ansieht. Zusätzlich kann nun auch die Session Id in der URL abgelegt werden. Das folgende Listing 3.5 zeigt eine URL in der unter dem Parameter session eine Session Id gespeichert wird.

```
1 http://www.beliebigershop.de/artikel.php?nummer=1234
2 ?session=2P0OC2JSNDLPSKHCJUN2JV
```

Listing 3.5: Beispiel: Session in einer URL gespeichert

Eine Gefährdung entsteht dann wenn der Kunde A diesen Link an eine weitere Person B sendet. Person B öffnet den Link und wird anhand der Session Id identifiziert. Diese verweist jedoch noch auf den Kunden A und somit gibt sich Person B als A aus und kann in seinem Namen einkaufen.

Eine weitere Möglichkeit diese Art Angriff durchzuführen ist, durch eine Unachtsamkeit des Anwenders. Muss der Anwender den Zugriff durch einen Login mit einer Session authentifizieren. Ist die Session nicht über einen timeout gesichert oder der Anwender vergisst sich auszuloggen. Ein Angreifer kann nun den gleichen Browser nutzen und ist mit der gleichen Session eingeloggt und authentifiziert. Diese Art Angriff wird als „Session Fixation“ bezeichet [Mit17d].

Für den Bahnbereich ist denkbar, dass überwachende Elemente, wie beispielsweise Statusanzeigen, über ein Interface bereit gestellt werden. Wird dieses Interface durch einen Login geschützt, dann müssen solche Angriffe in Betracht gezogen werden. Die Sicherung von kritischer Infrastruktur ist dabei in Abschnitt 6 des IEC 62443-3-3 [IEC13] geregelt. Der Standard fordert jedoch nur das Vorhandensein einer solchen Sicherung, nicht gesonderte Sicherung gegen Angriffe.

3.3 Security Misconfiguration

In vielen Anwendungen, besonders in Sicherheitskritischen, werden zwar Sicherungsmaßnahmen installiert. Diese aber oftmals nicht korrekt konfiguriert. Ein vermeintlich gesichertes System ist dann genau so verwundbar, wie ein ungesichertes System [SJT08]. Ein solches Problem kann verschiedene Ursachen haben.

Eine übliche Ursache Unachtsamkeiten bei der Installation des Systems. Gegeben ist folgendes Szenario:
Bei der Installation eines App-Servers wird automatisch eine Administrationskonsole installiert und aktiviert. Diese wird mit einem Standard Benutzernamen und Passwort als Administrator angelegt. Wird die Konsole nicht deaktiviert oder der Benutzername und oder das Password nicht geändert, kann ein Angreifer über eine solche Schnittstelle die Kontrolle über das System übernehmen [Zho17].

Als konkretes Beispiel ist „MySQL“. MySQL ist ein Open-Source relationales Datenbankverwaltungssystem und (Stand Juni 2017) auf dem zweiten Platz der meistgenutzten Systeme [sIg17]. Dieses Datenbanksystem erstellt mit der Installation einen Benutzer mit Adminitrationsrechten. Dieser Nutzer wird standardmäßig ohne Passwort erstellt [MyS17]. Wird das Passwort nicht geändert kann ein Angreifer ohne weitere Maßnahmen die volle Kontrolle über das System übernehmen.

Ein weiteres Szenario, in dem die Kontrolle über ein System erlangt werden kann, kann entstehen, wenn nach der Installation des Webserverdienstes „Apache“ [Gar17]die Verweise auf die mitgelieferten Beispiele nicht entfernt werden. Apache ist (Stand Juni 2017) der verbreitetste Webservice und wird von 49% der Anwender verwendet [W3T17]. Die mit der Installation mit gelieferten Beispiele liefern Informationen wie Versionsnummern und Verhalten über das gesamte System und somit nicht nur über die Apache Installation. Ein Angreifer kann diese Informationen nutzen um Angriffe speziell auf die verschiedenen Versionen der genutzten Software durchzuführen.

Für den Bahnbereich können solche Unachtsamkeiten auch kritisch werden, da es auf Grund ihrer Popularität wahrscheinlich ist, dass solche diese Software Systeme zum Einsatz kommen. Dieses Risiko muss besonders betrachtet werden, wenn digitalisierte Komponenten oder gar IoT Komponenten in ein Bahnsystem aufgenommen werden sollen. In der Praxis ist es üblich, dass

solche Komponenten über Web Protokolle wie HTTPs mit anderen Diensten kommunizieren dabei muss beachtet werden, dass diese Dienste korrekt konfiguriert sind. Wichtig hierbei ist, dass Standards für Verschlüsselung und generelle Sicherheitsrichtlinien eingehalten werden.

3.4 Sensitive Data Exposure

Angelehnt an Abschnitt 3.3 kann ein falsch konfigurierte Verschlüsselung für Benutzerkonten zu Problemen führen. Dies entsteht dann, wenn die Passwörter für die Benutzerkonten verschlüsseltet abgelegt werden, jedoch aber nicht durch „Salt“ zusätzlich erweitert werden. Ein Salt ist eine zufällige Zeichenfolge, die an das Passwort des Nutzers angehängt wird. Dadurch steigt die Länge und somit die Entropie des verwendeten Passworts. Außerdem evaluieren zwei gleiche Passwörter nicht mehr zu dem gleichen Hash-wert, da der Salt-wert zufällig gewählt wird [Kal00]. Fehlt die zusätzliche Sicherung durch einen Salt-wert kann ein Angreifer die Passwortdatei stehlen und mit Hilfe einer „Rainbow Table“, eine Tabelle, die die häufigsten genutzten Passwörter enthält, die gestohlene Passwortdatei entschlüsseln. Der Angreifer verfügt nun über alle im System gespeicherten Passwörter.

Bezogen auf den Bahnbereich kann dies kritische Auswirkungen haben. Sollte es einem Angreifer gelingen eine solche Passwortdatei zu stehlen ist es denkbar, dass sich dieser Zugang zum Steuerungssystem beispielsweise eines Stellwerks verschaffen kann und dort dann Signale und Weichen manipulieren. Aus diesem Grund muss sichergestellt werden, dass eine Prüfung der Zugriffsberechtigungen stattfindet. Diese Eigenschaft wird bereits von der IEC 62443-3-3 Norm Abschnitt 4.2 [IEC13] gefordert.

3.5 Underprotected APIs

In moderner Softwareentwicklung ist es Stand der Kunst Bibliotheken und Erweiterungen über ein „application programming interface“(API) anzubinden. Diese sind gekapselt und lose gekoppelt daher ermöglichen sie gute Wartbarkeit und hohe Flexibilität. Neue Versionen der Bibliothek können, solange das Interface nicht verändert wird einfach und direkt eingespielt werden. Um eine solche Bibliothek nutzen zu können muss diese nicht einmal auf System verfügbar sein. Bibliotheken wie: „JQuery“ [jT17], eine JavaScript Bibliothek zum erleichterten Erstellen von modernen Webseiten, kann zur Laufzeit auf dem Clientsystem über das Internet geladen werden.

Jedoch bietet diese Art der Entwicklung auch Nachteile:
Zum Einen ist der Quellcode bei vielen Bibliotheken nicht einsehbar. Der Entwickler muss darauf vertrauen, dass gängige Softwareentwicklungsstandards durch den API Entwickler eingehalten werden. Fehler oder Abbrüche, die durch die Bibliothek verursacht werden können nicht behoben werden und es muss auf eine korrigierte Version der Bibliothek gewartet werden.

Daraus resultiert ein weiterer Nachteil. Dadurch dass der Quellcode nicht einsehbar ist können Sicherheitsrisiken entstehen auf die kein Einfluss genommen werden kann. Beispielsweise kann eine Bibliothek anfällig für Injection-Angriffe sein. Durch das Verwenden der API ist es möglich, dass auch die eigene Anwendung angreifbar wird. Eine Studie der Aspect Securty, Inc [Asp12] zeigt, dass ca. 26% der überprüften 303,000 Versionen von 36,000 unterschiedlichen fehlerhaft sind. In der Analyse wurden nur Java-Bibliotheken betrachtet, die im Central Repository ("Central") angeboten werden. Darunter jedoch weit verbreitete Bibliotheken wie: GWT, Xerces oder Spring MVC. Aus der Analyse geht hervor, dass es wahrscheinlich ist, dass sich in einer durchschnittlichen Java-Applikation mindestens eine verwundbare Bibliothek befindet.

Im Bezug auf die Verwendung im Bahnumfeld muss sichergestellt werden, dass es Überprüfung von API Funktionalität gegeben ist. Diese kann durch statische und dynamische Tests und Analysen erfolgen, falls der Quellcode der Bibliotheken vorliegen. Außerdem können komplexere Verfahren verwendet werden wie beispielsweise Fuzzy-Testing [TDM08]. Hierbei werden die API Funktionen einer Bibliothek mit zufälligen Inputs aufgerufen und die Ergebnisse auf Plausibilität geprüft. Für externe Bibliotheken, solche deren Funktionsweise nicht einsehbar ist sind solche Prüfungen nicht möglich, dennoch müssen diese auf Sicherheitsaspekte überprüft werden. Eine Möglichkeit ist Security-Instrumentation [BM10]. Bei diesem Verfahren werden während der Ausführung einer Applikation Metadaten gesammelt, wie beispielsweise Zugriffe auf den Hauptspeicher oder Ressourcennutzung. Des Weiteren werden Regeln definiert, in der sich die Applikation bewegen muss. Werden diese Regeln verletzt werden wird ein Fehler gemeldet und es kann entsprechend reagiert werden. Eine Reaktion kann verschieden ausfallen von der Beendung der Applikation bis hin zum Vermerken in einem Log.

3.6 Using Components with Known Vulnerabilities

Nicht nur Bibliotheken können fehlerhaft sein, sondern auch komplette Softwarekomponenten oder Dienste. Viele Administratoren überprüfen jedoch nicht oder nur sehr selten die von ihnen genutzten Programme und Dienste auf Aktualisierungen oder Schwachstellen. Eine Folge daraus ist, dass ein Großteil der Angriffe auf ein System auf Fehler und Schwachstellen

zurück zu führen ist, die bereits in neueren Versionen des Dienstes oder der Komponente behoben wurde.

Beispielsweise zeigt der „Shodan Report“ [Mat17], dass auch im Jahr 2017, 2 Jahre und 9 Monate nach Beheben des Fehlers noch circa 200.000 Internetseiten verwundbar für einen Angriff über „Heartbleed“ [Mit17a] sind. Der Heartbleed-Fehler ermöglicht dem Angreifer durch Manipulation von Datenpaketen den Hauptspeicher des Ziels auszuspähen. Dadurch könnten kritische Informationen, wie Passwörter oder Geschäftsdaten, enthalten.

Im Bezug auf den Bahnbereich muss daher gesichert werden, dass eine ausreichende Aktualisierungsstrategie für die Software der Stellwerke und Züge verwendet wird. Angriffe mit bereits bekannten und behobenen Angriffsszenarien müssen verhindert werden.

3.7 Denial Of Service Attacks

Ein Denial-of-Service Angriff (DOS) beschreibt einen Angriff auf ein System in einem Netzwerk. Hierbei wird beispielsweise an einen Domain Name Service (DNS) eine Anfrage zum Auflösen eines Namens in eine IP Adresse gesendet. Auffällig hierbei ist, dass es sich bei der Anfrage um ein kleines Paket handelt (etwa 36 Bytes), die Antwort des Servers kann jedoch um ein vielfaches größer ausfallen (maximal 512 Bytes) [Moc87a] [Moc87b]. Wird nun die Absender Adresse dieser Anfrage gefälscht kann ein Angreifer mit kleinen Pakten an einen DNS-Server, große Antwortpakete erzeugen, die aber das „Opfer “erhält und verarbeiten muss. Die Abbildung 3.1 zeigt den Zusammenhang zwischen Angreifer DNS-Server und dem Opfer.

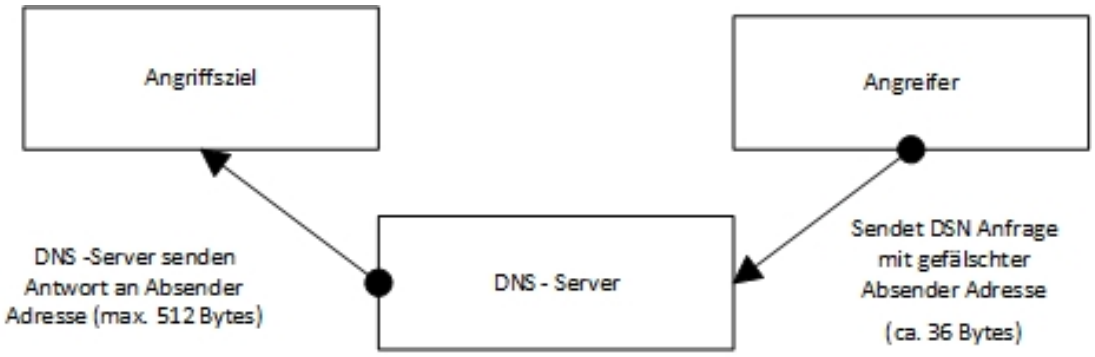

Abbildung 3.1: Vereinfachte Darstellung eines Denial-of-Service Angriffs über DNS-Sec

Werden zu viele Pakete über diese Methode an das Opfer umgeleitet, so ist das Opfer überlastet und kann keine Anfragen mehr bearbeiten, unabhängig an welchen Dienst diese gestellt werden. Das System bricht zusammen und alle Dienste sind blockiert. Moderne Server Systeme

besitzen genug Rechenleistung, um gewöhnliche DOS Angriffe abzufangen und keine größeren Schäden davon zu tragen. Jedoch können auch diese Systeme durch DOS Angriffe lahm gelegt werden. Bei „Distributed-Denail-of-Service“ (DDOS) Angriffen werden im Vorfeld mehrere tausend Computer mit Schadsoftware infiziert, diese können nach Wahl des Angreifers gesteuert werden. Mit dem Verbund an Computern (Botnetz) kann nun ein DOS Angriff mit allen Computern gleichzeitig durchgeführt werden. Die Last, die am Server entsteht, ist dem entsprechend größer und führt auch hier wieder zum Ausfall des Systems mit allen Diensten.

3.8 Jamming

Eine weitere Variante ein System in der Funktion zu stören kann bei drahtloser Kommunikation durchgeführt werden. Hierbei handelt es sich um das sogenannte „Jamming“ [GLY14]. Bei diesem Verfahren wird das wird das Funksignal so gestört, dass keine Kommunikation über diesen Kanal möglich ist. In der Praxis wird ein zweiter Sender (Störsender) in die Nähe der eigentlichen Sende- oder Empfangsvorrichtung gebracht. Dieser Störsender Überlagert den genutzten Frequenzbereich mit einem Rauschen, sodass keine nützlichen Funksignale das Ziel erreichen können. Diese Technik wurde beispielsweise bereits im zweiten Weltkrieg von deutschen Streitkräften verwendet, um die lokale Radioübertragung in besetzten Gebieten wie den Niederlanden zu verhindern [ver17]. Heutzutage wird diese Technik vorwiegend von Militär und Sicherheitskräften verwendet, um die Funkkommunikation zu unterbinden [Esh12].

Der folgende Abschnitt befasst sich mit einem Überblick über aktuelle Bahnanlagen. Auf dessen Basis können dann in den folgenden Kapiteln abgewandelte Architekturen erstellt werden, die dann auf ihre Eignung für eine digitalisierte Bahnanlage untersucht werden können.

4 Aktuelle Bahnanlagen

Aktuelle Bahnanlagen werden als zentralisiertes System rund um das Stellwerk betrieben. Signale und Weichen können aus diesem Punkt gesteuert werden. Jedes Stellwerk ist dabei für einen bestimmten Bereich zuständig, der je nach Komplexität der zu verwaltenden Streckenabschnitte unterschiedlich groß sein kann [Arn87]. Weichen und Signale verfügen nur über geringe Komplexität und werden lediglich zum Senden und Empfangen von Nachrichten, die überwiegend elektrisch in Schleifen übertragen werden, sowie zum Stellen der Weichen, Setzen von Signalen, Melden von Fehlerzuständen oder der Positionserkennung von Zügen verwendet. Die Logik für das Setzen der Weichen oder Signale befindet sich im Stellwerk. Hier laufen alle Informationen über den jeweiligen Bereich zusammen. Im Stellwerk können dann Weichen und Signale anhand der Routeninformationen und Positionen der einzelnen Züge gestellt werden.

Die Abbildung 4.1 zeigt die Systemarchitektur eines elektronisches Stellwerkssystems. Ein solches System wird in drei Ebenen unterteilt. In der ersten Ebene, dem Segment für externe Geräte, befindet sich der Leitstand. An diesem Punkt kann ein Fahrdienstleiter an einem Bedienplatz (siehe 2.1) den aktuellen Zustand des Streckenbereiches beobachten und gegebenenfalls Änderungen vornehmen. Die Bedienplätze kommunizieren über ein Bediensystem mit der Anlage. Das Bediensystem sorgt unter anderem dafür, dass alle Bedienplätze, die gleiche Sicht auf den Gleisabschnitt haben. Im Notfall kann durch diese Ebene der komplette Streckenabschnitt manuell gesteuert werden. Ist die Komplexität eines Stellwerks besonders gering, dann kann auch auf diese Ebene verzichtet werden [FNT03].

Die zweite Ebene ist die Sicherungs- / Bedienverarbeitungsebene. Hierbei handelt es sich um einen oder mehrere zentrale Sicherheitsbausteine, die die komplette Logik des Stellwerks darstellen. Die in dieser Ebene verbauten Komponenten sind in der Regel herstellerspezifisch und werden kommerziell vertrieben. Um große Stellwerke steuern zu können müssen gegebenenfalls mehrere dieser Bausteine verwendet werden. Die Sicherungskomponenten verfügen über redundante Datenleitungen, um eine Ausfallsicherheit zu ermöglichen. Des Weiteren

werden die Datenleitungen als Ringleitungen ausgelegt, die jeweils an dem Sicherungsbaustein starten und enden. Sollte eine Datenleitung an beliebiger Stelle beschädigt werden, kann das Signal durch die entgegengesetzte Richtung dennoch zum Ziel gelangen.

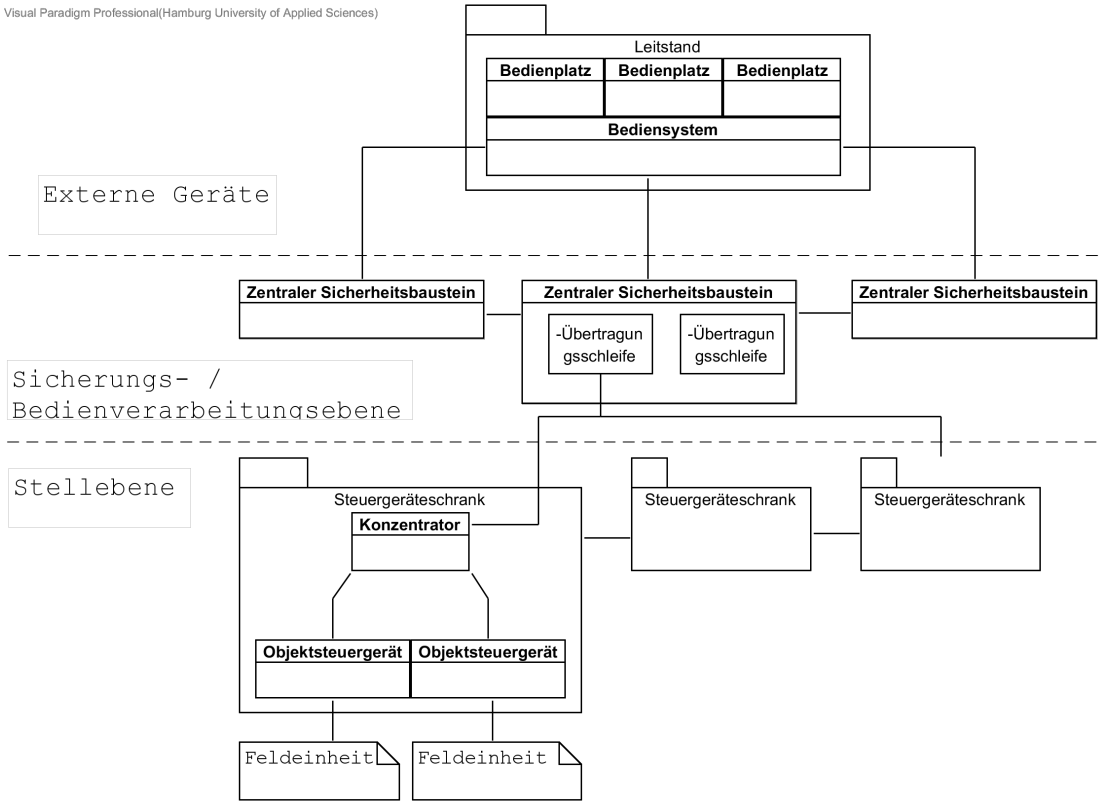

Abbildung 4.1: Systemarchitektur eines elektronischen Stellwerks [HB95]

Die Datenleitungen werden in der Regel mit einen Steuergeräteschrank verbunden der sich auf der dritten Ebene, der Stellebene, befindet. In diesen Schrank befinden sich Konzentratoren und Objektsteuergeräte. Die Aufgabe der Konzentratoren besteht darin die Steuersignale aus der Ringleitung zu ermitteln und dienen somit als Schnittstelle zwischen der Sicherungs- und der Stellebene. Die zweite Komponente innerhalb eines Steuergeräteschranks ist das Objektsteuergerät. Jedes dieser Geräte ist einer Feldeinheit zugeordnet und somit für die Steuerung einer Weiche oder eines Signals verantwortlich. Um ausreichend komplexe Streckenabschnitte zu ermöglichen können ca. 300 Objektsteuergeräte über einen zentralen Sicherheitsbaustein gesteuert werden. Um Informationen beispielsweise über die Position eines Zuges zu bekommen, können auch Achszähler (Balisen) mit einem Objektsteuergerät verbunden werden. Auf

diese Weise können so auch Informationen zurück an den Sicherheitsbaustein und damit auch an den Bedienplatz zurück gespielt werden. Um die Ausfallsicherheit des Systems zu erhöhen können die zentralen Sicherheitsbausteine redundant ausgelegt werden. Alle Daten werden an alle redundanten Bausteine gesendet. Auf diese Weise befindet sich das Reservesystem in dem gleichen Zustand wie das aktuell operierende System. Fällt ein System aus kann das Rückfallsystem ohne weiteren Zeitverlust die Arbeit übernehmen.

Möchte ein Fahrdienstleiter beispielsweise eine Weiche ändern, so modifiziert er an seinem Bedienplatz das entsprechende Element im Gleisschaltbild. Das darunterliegende Bediensystem wertet diese Änderung aus und gibt die Änderung an den zuständigen Sicherheitsbaustein weiter. Hier wird geprüft, ob diese Änderung durchgeführt werden kann. Der Sicherheitsbaustein prüft dabei unter anderem, ob es durch diese Änderung zu einer Gefährdung im Betrieb kommen kann. Wird die Änderung von System akzeptiert, so wird über die Übertragungsschleife der zugehörige Steuergeräteschrank angewählt und das passende Objektsteuergerät führt den Schaltvorgang durch. Wird die Änderung abgelehnt wird der Fahrdienstleiter informiert. Jedoch ist es möglich diese Änderung auch zu überschreiben und sich somit über die Sicherungsmaßnahmen des Systems zu stellen. Letzteres führte auch zum Zugunglück in Bad Aiblingen [Zei16]. Wird eine Änderung akzeptiert wird diese an den passenden Steuergeräteschrank weiter geleitet, dazu wird die Stellanweisung kodiert und auf einer Ringleitung verschickt. Im Steuergeräteschrank extrahiert der Konzentrator die Stellanweisung und schaltet die notwendigen Objektsteuergeräte. Diese sind dann mit den tatsächlichen Geräten (Signal, Weiche, Schranke,...) am Gleis verbunden. Auffällig hierbei ist, dass die Objektsteuergeräte nicht zusätzlich gegen Ausfälle gesichert sind. Fällt also eines dieser Geräte aus, so muss der komplette Abschnitt und alle davon abhängigen Bereiche gesperrt werden, bis der Ausfall behoben ist.

In aktuellen Anlagen ist es möglich, dass Stellwerke Informationen austauschen können. Hierzu ist es notwendig, dass diese Kommunikation gesichert abläuft und ein Empfangen der Nachrichten sichergestellt werden kann. Der folgende Abschnitt befasst sich mit den Kommunikationsmöglichkeiten innerhalb aktueller Bahnanlagen.

4.1 Kommunikation in Bahnanlagen

In aktuell eingesetzten Systemen ist es möglich auch komplexe Stellvorgänge durchzuführen. Dafür ist es in der Regel notwendig, dass mehrere Stellwerke miteinander kommunizieren. Die einzelnen Stellwerke sind dabei durch ein IP-Netzwerk verbunden und können auf diese Weise

Informationen und Steuerkommandos austauschen. Feldelemente, wie Weichen oder Signale, können nur durch die Objektsteuergeräte des jeweiligen Stellwerks verändert werden. Hierbei werden Technologien wie CAN-Bus verwendet.

Die Anforderungen an diesen Bereich einer Bahnanwendung werden in der Industrienorm EN 50159 [Eur10] definiert. In diesem Standard wird auf das ISO/OSI Schichtenmodell aufgesetzt und erweitert die einzelnen Schichten um gesonderte Anforderungen. Die folgende Abbildung 4.2 zeigt das Referenzmodell nach ISO/IEC 7498 [ISO94a], zudem wird das Modell auf die Kommunikation im Internet angewendet. Die Abbildung zeigt die unterschiedlichen Schichten, in denen der Transport von Daten realisiert wird. Wichtig hierbei ist, dass alle Schichten mit aufsteigender Nummer ineinander eingebettet werden. Dies bedeutet eine höhere Schicht erweitert immer die Funktionalität der unter darunterliegenden Schichten und verändert die Funktion der unteren Schichten nicht.

Physikalische Ebene Die physikalische Ebene oder auch Bitübertragungsschicht genannt bezeichnet die niedrigste Abstraktionsschicht. In dieser Ebene werden die Daten Bitweise durch das Medium übertragen.

Data Link Diese Schicht wird auch als Sicherungsschicht bezeichnet. Die Aufgabe dieser Schicht liegt darin, den Bitstrom in Blöcke aufzuteilen und eine weitgehend Fehlerfreie Übertragung zu ermöglichen hierzu werden den Blöcken Prüfsummen hinzugefügt. So können fehlerhafte Blöcke vom Empfänger erkannt werden und somit verworfen oder sogar korrigiert werden. Auf dieser Ebene können Daten in lokalen Netzen durch Switche an ihr Ziel weiter geleitet werden. Ziele außerhalb einer direkten Verbindung können durch diese Schicht nicht erreicht werden. [PR88]

Netzwerk Sollen Ziele erreicht werden, die sich außerhalb des lokalen Netzes befinden muss eine Vermittlungsschicht eingesetzt werden. Diese ist in der Lage (am Beispiel der Internetkommunikation) mit Hilfe von Routern einen Weg (Route) zu einem Ziel außerhalb des lokalen Netzes zu finden. Router legen zu diesem Zweck Routingtabellen an in diesen mögliche Ziele eingetragen werden. [Pos81]

Transport Die Transportschicht stellt Kontrollmechanismen für den Datenfluss zur Verfügung. Diese Schicht hat die Aufgabe den Datenfluss zu steuern, sodass Datenstaus vermieden werden. Außerdem stellt diese Schicht den darüberlegenden Schichten eine einheitliche Schnittstelle, sodass sich Applikationen nicht mit der Routenfindung einzelner Pakete

befassen müssen. Des Weiteren bietet diese Schicht die Möglichkeit beschädigte oder verlorene Pakete erneut anzufordern. [McK84]

Session Die Sitzungsschicht sorgt dafür, dass abgebrochene Verbindungen wieder aufgenommen werden können. Bricht eine Verbindung während beispielsweise eines Datentransfers ab, so muss die Übertragung nicht von Neuem begonnen werden. In dieser Schicht werden so genannte Check Points erstellt, ab denen bei einem Abbruch der Verbindung die Übertragung wieder aufgenommen werden kann. Des Weiteren sind Protokolle wie RPC (Remote Procedure Call) in dieser Schicht angesiedelt. [ISO96]

Präsentation Die Aufgabe dieser Schicht ist es für eine einheitliche Datendarstellung zu sorgen und diese für die Applikation darzustellen. Hierzu gehören Datenkompression oder Verschlüsselung. Die Präsentationsschicht kapselt diese Operationen und stellt sicher, dass die transformation der Daten korrekt durchgeführt wird. Die Anwendung möchte beispielsweise eine Datei versenden. Bevor dies geschieht wird diese Datei durch die Präsentationsschicht komprimiert und verschlüsselt. Auf der Empfängerseite stellt die Schicht sicher, dass die Datei wieder entschlüsselt und dekomprimiert wird, bevor die Daten an die Applikation weiter gegeben werden.[ISO94b]

Applikation Die Applikationsschicht stellt die Verbindung zu den unteren Schichten zur Verfügung. Anwendungen nutzten diese Schicht um Zugang zu den unteren Schichten zu erhalten.

In dem Beispiel „Kommunikation im Internet“ werden die Schichten Präsentation und Session nicht verwendet, in der Praxis ist es üblich die Funktionen dieser Schichten in der Applikation zu implementieren. Dies bietet den Entwicklern der Applikation volle Kontrolle über kritische Funktionen, wie Verschlüsselung. Wird eine solche Funktion durch die zugehörige Schicht erledigt, muss der Anwendungsentwickler sich auf die korrekte Implementierung der Verschlüsselung verlassen. Ein Beispiel für eine solche Umsetzung ist das HTTPS Protokoll [Res00]. Hierbei werden die Aufgaben der Präsentationsschicht, das ver- und entschlüsseln von Daten mit in die Anwendung gezogen.

Bezogen auf Bahnanwendungen wird die Applikationsschicht um zwei weitere Unterschichten erweitert. Die Abbildung 4.3 zeigt das Referenzmodell im Vergleich zu dem Schichtenmodell für eine Bahnanwendung. Diese wird durch den Standard EN 50159 definiert [Eur10]. Auffällig in der Abbildung ist, dass die unteren Schichten analog zur Abbildung 4.2 - Kommunikation im Internet - aufgebaut sind. Jedoch wird die Applikationsschicht in drei Unterschichten aufgeteilt.

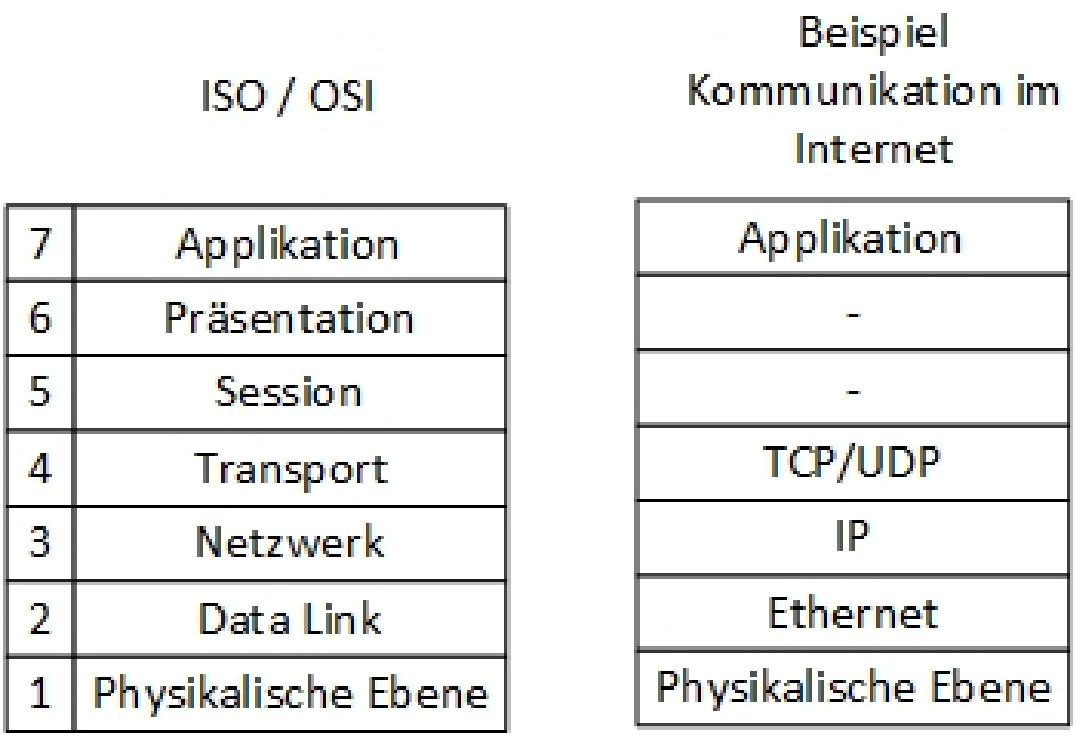

Abbildung 4.2: ISO/OSI Referenzmodell (links) - ISO/OSI angewendet auf Kommunikation im Internet (rechts)

Diese Schichten müssen den im Standard geforderten Safety-Anforderungen genügen. Vereinfacht bedeutet dies, dass für alle Anwendungen, die in diesen Schichten eingesetzt werden, ein Fehlerzustand vorhanden sein muss, in dem das System keinen weiteren Schaden verursachen kann, der sogenannte „Failsafe-State“. Anders als in der Internetkommunikation ist diese Schicht nicht allein für die Anbindung der Applikation an die unterliegenden Schichten verantwortlich. Zunächst wird eine Treiberschicht ergänzt. Diese erfüllt überwiegend die Aufgaben der Präsentationsschicht, ist aber individuell für einzelne Applikationen und somit nicht in der Präsentationsschicht anzuordnen. Auf dieser Schicht befindet sich die sogenannte „Rail Safe Transport Application“ (RaSTA), dieses Protokoll ist eine Sicherungsschicht, die eine hohe Verfügbarkeit des Systems gewährleisten soll. Wichtig ist hierbei, dass die Anforderungen an diese Schicht gleich bleiben unabhängig von der darunter liegenden Infrastruktur. Erst aufbauend auf dieser Schicht befindet sich die Anbindung an die tatsächliche Bahnapplikation.

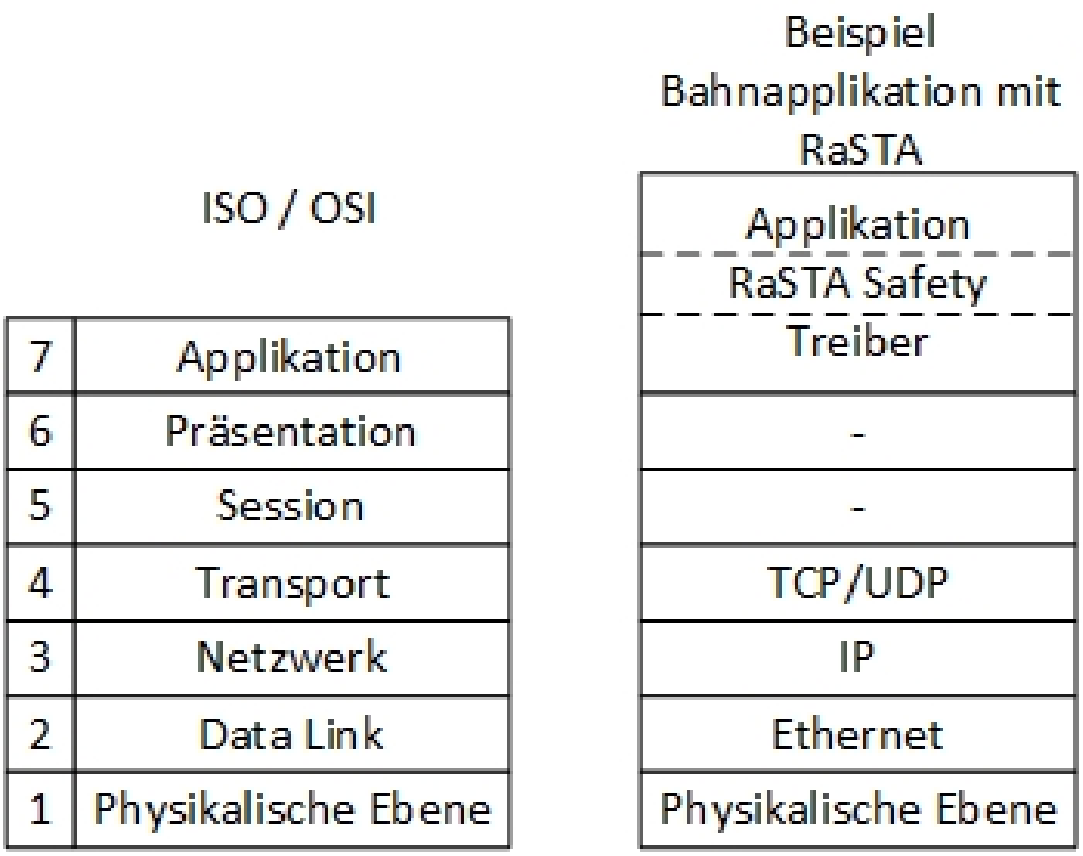

Abbildung 4.3: ISO/OSI Referenzmodell (links) - Beispielapplikation für den Bahnbereich mit RaSTA (rechts)

In besonderen Situationen kann es notwendig sein, dass der Fahrdienstleiter persönlich mit dem Zugpersonal in Kontakt tritt. Für diese Fälle ist ein separates Funknetzwerk vorgesehen, das sogenannte „Global System for Mobile Communications - Rail(way)“ (GSM-R) [Deu08]. Hierbei handelt es sich um ein separates Mobilfunknetz, welches speziell für Bahnsysteme aufgestellt wurde. Der Aufbau einer Kommunikationsverbindung vom Fahrdienstleiter zum Triebfahrzeugführer erfolgt durch Eingabe einer „funktionalen Rufnummer“. Diese Nummer enthält neben der Verbindungsart auch die Zugnummer und einen Funktionscode. Letzterer unterscheidet, ob der Triebfahrzeugführer oder der Zugführer angerufen wird. Bei einer Verbindung wird zwischen verschiedenen Arten unterschieden. Dies können Einzelverbindungen, bei denen nur zwei Teilnehmer involviert sind bis hin zu Gruppenverbindungen, bei denen komplette Funktionsgruppe, wie beispielsweise alle Rangierzüge, angerufen werden können. Zusätzlich existiert noch eine gesonderte Verbindungsart, die nicht für den Normalbetrieb

genutzt werden kann. Hierbei handelt es sich um Notrufverbindungen. Hierbei handelt es sich um eine Gruppenverbindung mit höchster Priorität. Kommt es zu einer Gefahrensituation werden also direkt ganze Gruppen über den Notruf informiert. Zusätzlicher Zeitverlust durch mehrere Anrufe wird so verhindert.

Dieser Abschnitt hat gezeigt, dass ein Stellwerkssystem bereits im Ist-Zustand hoch technische Systeme sind, die auch auf einer Security-Ebene untersucht werden müssen. Der folgende Abschnitt untersucht mögliche Angriffsszenarien auf der aktuell verwendeten Systemen.

4.2 Angriffe auf aktuellen Bahnanlagen

Bei der Betrachtung des Ist-Zustands einer solchen Bahnanlage wird deutlich, dass die zentrale Komponente das Stellwerk ist, hier werden alle Steuerentscheidungen und Routenplanungen durchgeführt. Gelingt es einem Angreifer also dieses System zu übernehmen oder zumindest zu behindern, dann ist eine Störung des Betriebsablaufs nicht mehr abzuwenden. Hierbei sind nun verschiedene Situationen denkbar. Eine Möglichkeit den Bahnbetrieb zu stören zeigt der am 12. Mai 2017 global durchgeführte Angriff auf kritische Infrastruktur mit der Ransomware „Wanna Cry“ [Mit17b]. Hierbei wurden weltweit Krankenhäuser, Energieversorger und Logistikunternehmen, wie beispielsweise die Deutsche Bahn attackiert. Medienberichten zufolge wurden durch den Angriff mindestens 450 Computer der Deutschen Bahn infiziert [Spi17]. Die angegriffenen Systeme wurden durch den Virus verschlüsselt und ein „Lösegeld“ wurde gefordert. Durch diesen Angriff fielen sämtliche Anzeigetafeln und Ticketautomaten der Bahnhöfe aus. Auch wenn der eigentliche Zugverkehr nicht betroffen war kam es zu erheblichen Verzögerungen im Betriebsablauf. Ein solcher Angriff war nur möglich, da die betroffenen Komponenten mit dem Internet verbunden sind.

Um einen Angriff auf den Zugbetrieb durchzuführen muss der Angreifer in die Lage gebracht werden Zugriff auf das in sich geschlossene Stellwerkssystem zu bekommen. Hierbei genügt es jedoch schon die Kommunikationskanäle des Systems zu stören. Um eine solche „Denial of Service“-Attacke durchzuführen würde es bereits genügen, wenn der Angreifer am IP-Netzwerk der Stellwerke teilnehmen könnte. Ein solcher Zugriff kann über einen Verteilerkasten oder ähnliche Infrastruktur erfolgen. Die Kommunikation zwischen den einzelnen Stellwerken ist jedoch verschlüsselt, daher kann ein Angreifer nicht direkt in die Kommunikation eingreifen und Nachrichten manipulieren. Dies ist jedoch nicht zwingend notwendig, wenn der Betrieb gestört werden soll. Wird die Netzwerkschnittstelle eines Stellwerks mit Anfragen überlastet bricht diese unter der Last zusammen und es können keine weiteren Anfragen bearbeitet

werden. Das angegriffene Stellwerk ist somit isoliert und kann keine Stellanfragen von anderen Stellwerken mehr verarbeiten. Kritisch ist ein solcher Angriff auf kleine Stellwerke, die rein durch eine Fernsteuerung betrieben werden (vgl. Abschnitt 4). Ist das Stellwerk nicht erreichbar kann kein Stellbefehl mehr durchgeführt werden und der Betrieb in dem betroffenen Bereich muss eingestellt werden.

Ein noch höheres Risiko entsteht, wenn es einem Angreifer gelingt einen Bedienplatz eines Stellwerks zu übernehmen. Ab diesem Moment können beliebige Signale und Weichen gestellt werden und die Zugführung wahllos geändert werden. Somit kann ein Zug in eine falsche Richtung geleitet werden oder zum Anhalten bewegt werden. Auch wenn die Sicherheitsbausteine fatale Änderungen am System verhindern sollen, können die Änderungen forciert werden und damit den Sicherheitsbaustein überschreiben. Auf diese Weise wären sogar Kollisionen von Zügen möglich.

Auch die drahtlose Kommunikation kann angegriffen werden. Hierzu können die GSM-R Sendemasten gestört werden. Somit wäre die direkte Kommunikation zwischen Zug und Stellwerk gestört. Wird das komplette Frequenzband des GSM-R Masten blockiert oder der Sendemast beschädigt, so kann auch der Notruf nicht genutzt werden. Sollte es zu Problemen am Zug kommen, kann das Zugpersonal das Stellwerk nicht erreichen. Das Stellwerk kann weiterhin mit Hilfe der Signale mit dem Zug kommunizieren. Ein solcher Angriff ist jedoch wenig erfolgversprechend solange es dem Zug möglich ist in die Reichweite des nächsten Sendemasten zu fahren. Dann kann die Kommunikation wieder normal durchgeführt werden. Effektiver wäre ein Angriff innerhalb des Zuges. Wird ein Störsender innerhalb des Zuges platziert verliert dieser dauerhaft seine drahtlose Kommunikationsfähigkeit. Die Gegenrichtung bleibt aber auch in diesem Fall aktiv, da das Stellwerk auch weiterhin durch Signale den Zug steuern bzw. stoppen kann.

Um ein solches System zu digitalisieren ist es sinnvoll die Funktionsweise des bisherigen Systems zu hinterfragen und die Problemstellung mit moderner Technologie zu überdenken. Der folgende Abschnitt betrachtet daher eine Möglichkeit mit der ein Stellwerksystem überdacht werden könnte und zeigt Vor- und Nachteile einer solchen Änderung auf.

5 Digitalisierung der Bahnanlagen

Für die Digitalisierung einer Stellwerksanlage ist es notwendig eine geeignete Architektur zu wählen, die den Besonderheiten der Bahnanwendungen genügt und gleichzeitig den Problemen von vielen kleinen Geräten an verteilten Orten gerecht wird. Dabei wäre es möglich ganz auf Stellwerke zu verzichten. Sollte dies jedoch ein zu drastischer Schritt sein, wären auch Mischformen denkbar. Der folgende Abschnitt untersucht diese Möglichkeiten und bewertet diese.

5.1 Bahnanlagen ohne Stellwerke

Wird der bisher verwendete Aufbau komplett in Frage gestellt, so gelangt man zu einer Architektur, die völlig ohne Stellwerke auskommt. Eine solche Architektur beinhaltet nur Züge und Feldeinheiten. Ein Streckenabschnitt wird von einer Feldeinheit verwaltet. Züge können Feldeinheiten auf der Route anfragen und einen Streckenabschnitt für sich reservieren. Die Feldeinheit kontrolliert dafür alle dazugehörigen Weichen, gegebenenfalls Bahnübergängen und Signale. Zusätzlich werden die Sensoren im Streckenabschnitt durch die Feldeinheit ausgewertet. Auf diese Weise kann die Feldeinheit ermitteln, wann der Zug den Abschnitt passiert hat und das Segment wieder freigegeben werden kann. Die Feldeinheiten in kritischen Abschnitten, beispielsweise an Weichen oder eingleisigen Streckenabschnitten, müssen miteinander verbunden werden. Möchte ein Zug nun eine eingleisige Blockstrecke reservieren, sendet der Zug eine Anfrage an die erste Feldeinheit. Die Feldeinheit prüft, ob der Bereich unter eigener Zuständigkeit belegbar ist. Ist dies der Fall müssen die zum kritischen Abschnitt gehörigen Feldeinheiten die gleiche Prüfung durchführen. Darf ein Bereich nicht reserviert werden, muss die angefragte Feldeinheit die Reservierungsanfrage ablehnen und die weiterfahrt des Zuges stoppen solange bis der kritische Abschnitt wieder frei ist. Ein solches System wäre denkbar für ein überschaubares Streckennetz mit wenigen Abzweigungen. Das System verfügt über keinen globalen Zustand, da jeder Zug nur den eigenen Zustand und den der Blockstrecken um ihn herum kennt. Jede Feldeinheit kennt nur den eigenen Zustand, außer Feldeinheiten in kritischen Bereichen. Diese kennen auch den Zustand der Feldeinheiten im kritischen Bereich. Dies bedeutet, dass Züge nur eine lokale Sicht auf das System haben und somit nur ihren

eigene Route planen können. Es jedoch gegebenenfalls sinnvoll Routen mehrerer Züge zu verschachteln, um eine höheren Durchsatz in den Blockstrecken zu erreichen. Des Weiteren können Probleme entstehen, die nur durch einen globalen Zustand erkannt werden können. Ein prägnantes Beispiel hierfür ist die Verklemmung (Deadlock). Die Abbildung 5.1 zeigt wie der Betrieb verklemmen kann [Pac11]. Hierzu ist sind eingleisigen Streckenblöcke notwendig. Der Zug A befindet sich auf dem weg auf die rechte Seite, während die Züge B und C auf die linke Seite fahren möchten.

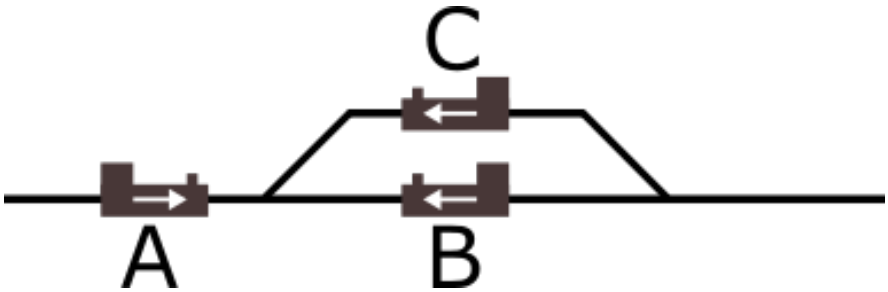

Abbildung 5.1: Beispiel für eine Verklemmung in einem Streckenabschnitt [Pac11]

Der Zug A reserviert seinen Streckenabschnitt und fährt ein. Im folgenden Versucht Zug A entweder die Ausweichstelle oder die Hauptstrecke zu reservieren. Beide sind durch einen anderen Zug belegt. Es kommt zur Verklemmung. Eine Lösung eines solchen Problems könnte sein, dass der gesamte abgebildete Bereich als kritischer Bereich reserviert werden muss. Dies würde einen Deadlock verhindert reduziert jedoch den Durchsatz den dieser Streckenabschnitt fassen kann. Des Weiteren würde die Ausweichstelle überflüssig werden, da ohnehin nur ein Zug zur Zeit in den Abschnitt einfahren darf.

Aus der Sicht der Cyber-Angriffe entstehen bei einer solchen Architektur signifikante Risiken. Dadurch dass es keinen globalen Zustand gibt und jeder Zug nur seine eigene Position im System kennt können Verletzungen bei der Reservierung von Streckenabschnitten erst spät erkannt werden. Fährt beispielsweise ein Zug in einen Streckenblock ein ohne diesen zuvor zu reservieren, so wird dieses Verhalten erst erkannt, wenn der Zug über einen Achszähler im Abschnitt fährt. Wenn nun gleichzeitig aus entgegenkommender Richtung ein Zug legitim in den Abschnitt einfährt kann es zur Kollision kommen. Eine solche Situation kann zustande kommen, wenn es einem Zug nicht möglich ist zu kommunizieren. Hierzu kann das in Abschnitt 3 vorgestellte Verfahren „Jamming“ verwendet werden. Des Weiteren können auch die Feldeinheiten gestört oder übernommen werden und zu massiven Störungen im Betriebsablauf führen. Wird eine Feldeinheit übernommen so könnte beispielsweise zwei Zügen, die

gleichzeitig den Streckenabschnitt reservieren wollen, die Einfahrt in den Abschnitt erlaubt werden. Auch hierbei ist eine Kollision denkbar.
Auf der anderen Seite bietet eine solche Architektur auch Vorteile gegenüber der herkömmlichen Architektur. Durch das Fehlen einer zentralen Einheit ist der Schaden durch einen Angriff lokal begrenzt. Sollte es einem Angreifer gelingen eine Feldeinheit zu übernehmen so kann dieser nur Kontrolle auf einen Streckenabschnitt oder einen kritischen Abschnitt ausüben. Die Übernahme eines Stellwerks würde die ganze Region lahm legen.

Zusammenfassend eignet sich eine solche Architektur nicht für den realen Einsatz. Das Fehlen eines globalen Zustands macht das Erkennen von Deadlocks sehr schwierig und die lokale Sicht der einzelnen Komponenten lässt ein Fehlverhalten im System erst spät aufdecken. Eine solche Architektur hat dennoch Vorteile gegenüber des aktuellen Aufbaus. Eine bessere Architektur wäre also eine Kombination der Architekturen. Der folgende Abschnitt skizziert eine solche Architektur.

5.2 Kombination von der Architekturen

Als Basis für diese Architektur wurden die Arbeiten von Kozlov et al. [LBX16] und Guth et al. [GBF16] zu Grunde gelegt. Diese Arbeiten befassen sich mit Architekturen im IOT Umfeld. Die Arbeit von Kozlov et al. legt dabei besonderen Wert auf eine sichere Verbindung zwischen den einzelnen Endgeräten untereinander und einem Server, der auch Steuerbefehle an die Endgeräte senden kann. Die Arbeit von Guth et al. liefert einen Überblick über verschiedene IOT Architekturen und deren Einsatzmöglichkeiten.

Ziel ist es eine Architektur mit besonderen Funktionalitäten bereitzustellen, wie zum Beispiel den Download von neuer Steuersoftware auf die im Feld installierten Komponenten. Solche Funktionen sind in aktuell im Einsatz befindlichen Stellwerkssystemen nicht installiert. Auch weitere Funktionen sind denkbar wie zum Beispiel zusätzliche Intelligenz innerhalb der im Feld befindlichen Komponenten, beispielsweise das Erkennen von Störungen und die direkte Reaktion auf diese. Auf diese Weise würden die passiven Feldgeräte, die nur auf Anweisung des Stellwerks handeln, zu aktiven Komponenten werden, die selbstständig Entscheidungen innerhalb ihres Wirkungsspektrums treffen können. Anders als in einer Architektur ohne Stellwerke würde jedoch der globale Zustand des Systems berücksichtigt, da ein Stellwerk, dass diesen Zustand kennt vorhanden ist. Im Folgenden werden zwei Architekturvarianten

vorgestellt, die für die Digitalisierung von Bahnanlagen genutzt werden können. Grundsätzlich werden dabei folgende drei Komponenten verwendet:

Stellwerksystem Diese Komponente dient der Planung und Steuerung der Zugfahrten durch das Gleissystem. Im Stellwerk befindet sich ein „User Interface“ welches durch den Fahrdienstleiter genutzt wird, um Fahrten zu Planen und auf besondere Umstände zu reagieren. Außerdem wird hier der globale Zustand des Systems überwacht. Ein Simulationssystem ermöglicht es Änderungen am System zu überprüfen bevor diese direkt ans System weiter geleitet werden. Das Steuersystem evaluiert die Änderungen und gibt die jeweiligen Steueranweisungen über die Netzwerkschnittstelle weiter an Feldeinheiten, die diese Befehle umsetzten. Außerdem werden an dieser Stelle Daten, die von den Feldeinheiten oder anderen Stellwerkssystemen empfangen werden verarbeitet. Die Netzwerkschnittstelle bildet ein kabelgebundenes Gateway zu den weiteren Komponenten, sowie zum Internet.

Feldeinheit Die Feldeinheit wird zum Stellen der Signale, sowie zum Betreiben der Weichen oder Bahnübergänge verwendet. Außerdem können in einer Feldeinheit auch Sensoren, wie Achszähler oder Kameras, angebracht werden, die dem Stellwerk Informationen über den Zustand des Systems liefern können. Eine Feldeinheit besteht aus zwei Kommunikationsmodulen, ein kabelgebundenes für die Kommunikation mit dem Stellwerk oder mit anderen Feldeinheiten und ein kabelloses, um mit vorbeifahrenden Zügen zu kommunizieren. Ein Steuermodul verarbeitet die Daten, die über die Kommunikationskanäle empfangen werden und steuert die Aktoren, wie Schranken, Weichen oder Signale. Des Weiteren liest dieses Modul die Sensoren aus und gibt die gesammelten Daten weiter an ein Stellwerk, andere Feldeinheiten oder einen Zug.

Zug Ein Zug kann mit Feldeinheiten entlang der Strecke kommunizieren. Da sich der Zug bewegt ist ein kabelgebundenes System hierbei nicht möglich. Funktechnologien machen eine Verständigung zwischen diesen jedoch Komponenten möglich. Ein Zug kann somit seine Position im System mitteilen und somit eine weitere Sicherung zusätzlich zu den Achszählern bieten. Außerdem kann der Zug auftretende Notfälle an die Feldeinheit melden. Die Feldeinheit könnte dann losgelöst von einer Entscheidung, die durch das Stellwerk, bzw. den Fahrdienstleiter im Stellwerk getroffen werden muss, bereits Sicherungsmaßnahmen einleiten, wie beispielsweise das Anhalten anderer Züge auf der Strecke.

Ein gravierender Unterschied zu beispielsweise Relaisstellwerken ist, dass das Verarbeiten von Steuersignalen in die Feldeinheiten ausgelagert wird. Dieser Ansatz entkoppelt somit die

feste Zuordnung einzelner Feldeinheiten vom Stellwerk, somit ist es unerheblich welches Stellwerk ein Steuerereignis an eine Feldeinheit sendet, solange der Sender über die notwendigen Berechtigungen verfügt.
Ein weiterer Aspekt, der in diesem Zusammenhand betrachtet werden muss ist die zusätzliche Positionserkennung im Zug. In aktuellen Bahnsystemen wird die Positionserkennung der Züge durch Achszähler in den Gleisen durchgeführt. Eine Zusätzliche Erkennung erhöht dabei den Zuverlässigkeit.

Ein weiter Punkt ist die Verwendung von GSM-R. Hierbei handelt es sich um ein bewehrtes System zur zusätzlichen Kommunikation zwischen beteiligten Personen. Da die Infrastruktur für dieses System bereits vorhanden ist gibt es keinen Grund diesen zusätzlichen Kommunikationskanal nicht als zusätzliche Sicherung zu verwenden.

Die folgenden Abbildungen 5.2 und 5.3 zeigen eine mögliche Umsetzung dieser Rahmenbedingungen. Die Besonderheit der in Abbildung 5.2 Architektur (A) ist dabei, dass alle Komponenten außer dem Zug direkt mit dem Internet verbunden sind. Dies hat den Vorteil, dass vorhandene Infrastruktur verwendet werden kann. Bietet jedoch den Nachteil, dass auch die kritischen Komponenten, wie die Feldeinheiten von überall durch das Internet erreicht werden können. Es müssen also zusätzliche Schutzmaßnahmen in die Feldeinheiten installiert werden. Besonders für Cyber-Angriffe ist die Erreichbarkeit der einzelnen Komponenten ein wichtiger Punkt.

Eine Variante dieser Architektur wird in Abbildung 5.3 dargestellt. Hierbei wird das Stellwerk als ein Gateway vor das Internet gestellt, sodass keine direkte Kommunikation von Außen mit den Feldeinheiten möglich ist. Dies trägt signifikant zur Abwehr von Cyber-Angriffen bei, da ein Angreifer zunächst über das Stellwerk ins System gelangen muss. Nachteilig ist jedoch, dass die Feldeinheiten und Stellwerke separat mit einander verbunden werden müssen, hierzu müssen zusätzliche Kabel, möglicherweise auch über weite Strecken, verlegt werden.

Durch die vorgestellten Architekturen sind nun Erweiterungen im Funktionsumfang des Systems möglich. Der folgende Abschnitt befasst sich mit möglichen zusätzlichen Features, die die aktuellen Funktionen eines Stellwerkssystems erweitern und ergänzen können.

5.3 Neuerungen durch die digitale Softwarearchitektur

Das Ziel einer weiteren Digitalisierung von Stellwerken ist es insbesondere, dass die Feldeinheiten Softwareupdates durch eine entfernte Verbindung erhalten können. Dies kann auf verschiedenen Arten durchgeführt werden. Zum Einen kann die Feldeinheit selbst mit dem Internet verbunden sein. Dieses Szenario wird durch die Architektur A in Abbildung 5.2 dargestellt. Dies hätte den Vorteil, dass keine weiteren Mechanismen mehr notwendig sind, um die

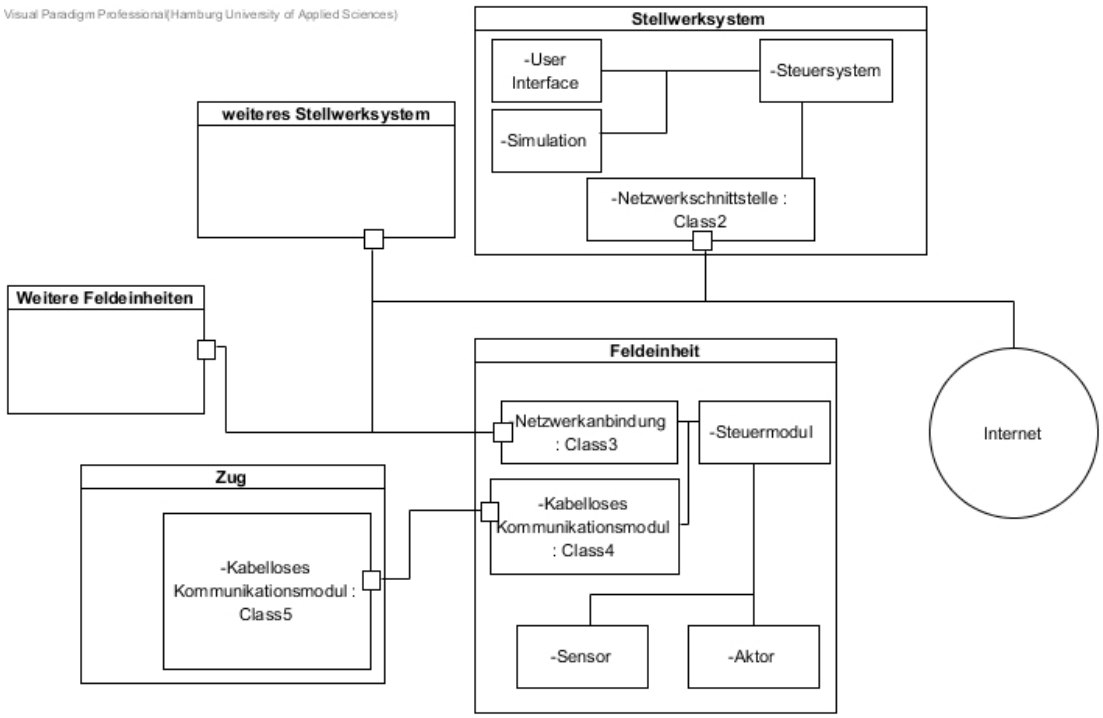

Abbildung 5.2: Referenzarchitektur A für ein digitalisiertes Bahnstellwerk

Software auf die Feldeinheiten zu spielen. Ein Nachteil dieser Variante ist, dass jede Feldeinheit direkt mit dem Internet verbunden ist und gesondert gesichert werden muss. Jede Feldeinheit ist somit potentiellen Angriffen ausgesetzt. Die Entscheidung, ob die Feldeinheiten direkt mit dem Internet verbunden sind, hat erheblichen Einfluss auf zusätzliche Maßnahmen, die zur Sicherung des Systems aufgewendet werden müssen. Zwar sind die Verbindungen durch ein verschlüsseltes Protokoll gesichert. Jedoch können Angriffe, wie „Denial of Service “, auch trotz einer solchen Sicherung durchgeführt werden. Die Variante (Architektur B) aus Abbildung 5.3 zeigt, dass nur das Stellwerk mit dem Internet verbunden wird. Somit besteht keine Möglichkeit direkt aus dem Internet auf die Feldeinheiten zuzugreifen oder diese durch hohe Last zu sabotieren. Die Komponenten sind durch ein internes Netz miteinander verbunden. Bei einer DOS-Attacke kann die Schnittstelle nach außen abgeschaltet werden und das System bleibt funktionsfähig. Nachteilig hierbei ist aber, dass im Stellwerk ein Mechanismus geschaffen werden muss, der den Download des Updates auf die Feldeinheiten ermöglicht. Des Weiteren soll mit diesen Architekturen möglich sein, dass ein vorbeifahrender Zug Informationen mit der Feldeinheit und über diese auch Informationen mit dem Stellwerk austauschen kann. In aktuellen Stellwerkssystemen ist es nur möglich, dass der Fahrdienstleiter im Stellwerk über

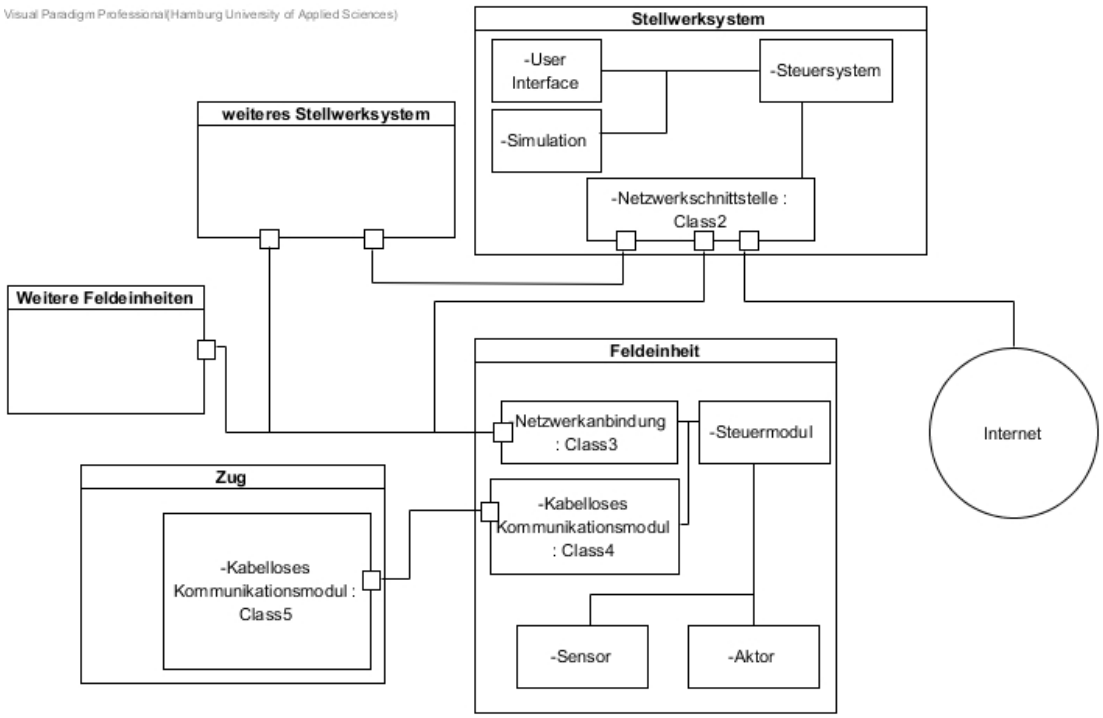

Abbildung 5.3: Referenzarchitektur B für ein digitalisiertes Bahnstellwerk

Signale mit dem Triebwagenführer kommuniziert. Diese Kommunikation ist jedoch auf die durch Signale beschreibbaren Situationen begrenzt. Hierbei handelt es sich um Anweisungen, wie: das Einhalten einer bestimmten Geschwindigkeit im nächsten Streckenabschnitt oder das Halten an einer bestimmten Position. Dem Triebwagenführer ist es nur im Notfall erlaubt selbst Kontakt mit dem Stellwerk aufzunehmen. Durch eine bidirektionale Kommunikation könnte beispielsweise der Status des Zugs ständig mit dem Stellwerk ausgetauscht werden und auf außerplanmäßige Situation schneller reagiert werden. Denkbar sind hierbei in erster Linie Situationen, die die Weiterfahrt des Zuges nicht gefährden. Beispielsweise der Ausfall der Klimaanlagen oder die Fehlfunktion einer Tür. Wird ein solcher Zustand frühzeitig an das Stellwerk weitergeleitet, so können im nächsten Bahnhof bereits Getränke für die Fahrgäste bereit gestellt werden oder ein Techniker in Bereitschaft versetzt werden, sofern das Problem während eines kurzen Aufenthalts behoben werden kann.

Eine Unterstützung für den Betrieb durch die vorgestellten Architekturen lässt sich im Stellwerkssystem identifizieren. Die Simulationskomponente soll dem Fahrdienstleiter ermöglichen Änderungen am System im Vorfeld zu simulieren und auf mögliche Fehler zu

überprüfen. Des Weiteren können so Varianten durchgespielt werden, die möglicherweise zu einer effektivere Nutzung des Streckennetzes führen könnten. Dabei ist ein mögliches Szenario, dass der Fahrdienstleiter eine Änderung am System vornimmt. Diese wird dann durch die Simulationskomponente auf einem virtuellem Gleisnetz ausgeführt. Falls nötig kann dies auch in Kombination mit anderen Stellwerken passieren. Erst dann wenn die Simulation keine Fehler in den Änderungen erkennen kann wird eine Änderung für das tatsächliche Schalten der Gleisanlage freigegeben. Diese Art „sanity check“ hätte den den Vorteil, dass grobe Fahrlässigkeiten, wie in Bad Aiblingen durch die Simulation frühzeitig erkannt werden können, bzw. solche Fahrbefehle gar nicht erst erteilt werden können. Ein Nachteil hierbei ist jedoch, dass sichergestellt werden muss, dass die Simulationskomponente in der Lage ist alle Randbedingungen zu erfassen. Dies erfordert einen hohen Entwicklungsaufwand und kann höchstens unterstützend für den Fahrdienstleiter eingesetzt werden.

Um die vorgestellten Architekturen auf Security-Aspekte untersuchen zu können ist es notwendig einige technische Details genauer zu spezifizieren. Der folgende Abschnitt beschreibt daher am Beispiel einiger kritischer Teilsysteme mit welchen Techniken und Technologien diese umgesetzt werden könnten.

5.4 Details zur Umsetzung

Für die Identifikation von möglichen Angriffen auf die Architekturen ist es notwendig über technische Details einer möglichen Implementierung zu verfügen. Dabei sind die Punkte Verschlüsselung und Netzwerkkommunikation besonders zu betrachten, da auf diesen Wegen Angriffe auf das System vorgenommen werden können. Dabei ist zu erwähnen, dass Angriffe durch physikalische Gewalt, wie beispielsweise Wandalismus, auf das System nicht in der Implementierung betrachtet wird. Der folgende Abschnitt behandelt technische Vorgaben, die an die Verschlüsselung des Systems gestellt werden.

5.4.1 Verschlüsselung

Für die Kommunikation zwischen Komponenten bei sicherheitskritischen Bahnanwendungen ist es notwendig, Verschlüsselungsverfahren zu verwenden, gemäß dem internationalem Standard IEC 62443-3-3 [IEC13]. Der Standard gibt dabei die Verwendung einer „Public Key Infrastucture “ (PKI) vor. PKI wird durch den Request For Comment 3647 definiert [CFS+03]. Hierbei handelt es sich um eine asymmetrische Verschlüsselungsmethode, bei der für jeden Kommunikationsteilnehmer einen privaten (geheimen) und einen öffentlichen Schlüssel er-

zeugt. Eine Datei oder Nachricht, die mit dem öffentlichen Schlüssel verschlüsselt wurde, kann nur mit dem Privaten wieder entschlüsselt werden. Des Weiteren ist es möglich eine Datei oder Nachricht mit dem privaten Schlüssel zu signieren. Mit Hilfe des öffentlichen Schlüssels kann geprüft werden, ob die Signatur der Inahlt unverändert ist. Für die Implementierung innerhalb der aufgezeigten Architekturen bedeutet dies, dass jede Stelle, die für Kommunikation genutzt werden soll ein solcher Mechanismus installiert werden muss. Eine Feldeinheit muss daher über ausreichend Rechenleistung verfügen, um kryptographische Operationen durchzuführen. Je nach Schlüssellänge steigt der Aufwand, der für diese Operationen benötigt wird. Gemäß der technischen Richtlinie für kryptographische Verfahren des Bundesamt für Sicherheit in der Informationstechnik [Bun17b] wird eine Schlüssellänge von mindestens 2000 Bit vorgegeben. Bei einem Einsatzzeitraum über das Jahr 2022 hinaus sollte bereits eine Schlüssellänge von 3000 Bit genutzt werden, dies gilt sowohl für aktuelle als auch für die in dieser Arbeit diskutierten Anlagen. Bahnanwendungen werden für mehrere Dekaden Einsatzzeit geplant, daher ist in diesem Punkt eine Verschlüsselung von mehr als 3000 Bit zu verwenden. Dadurch steigt jedoch die Rechenleistung, die für eine Feldeinheit benötigt wird. Eine solche Verschlüsselung ist notwendig unabhängig davon, ob die Feldeinheit mit dem Internet verbunden sind (Architektur A Abb. 5.2) oder nicht. In beiden Architekturen befinden sich alle notwendigen Komponenten unter der Kontrolle des Systems. Dies hat den Vorteil, dass alle Schlüssel im Vorfeld und Offline auf andere Komponenten übertragen werden können, ein sogenanntes „pre-shared-secret“. Auf diese Weise kann sichergestellt werden, dass alle Kommunikationsteilnehmer im Vorfeld bekannt sind und gegenseitig ihre Identität verifizieren können. Durch ein solches Verfahren ist es fremden Geräten nicht möglich mit den Geräten aus dem Bahnsystem zu kommunizieren. Versucht ein Gerät eine Verbindung aufzubauen, dessen Identität nicht verifiziert werden kann, wird die Verbindung durch das Bahnsystem beendet. Ein solches Ansatz stellt eine Neuerung gegenüber dem aktuellen Stellwerksystemen dar.

5.4.2 Netzwerkkommunikation

Die Art der Netzwerkkommunikation ist entscheidend für die Analyse späterer Angriffsszenarien. Des Weiteren muss die Netzwerkkommunikation für Steuerbefehle den Safety-Eigenschaften für Bahnanwendungen genügen (siehe 4.1). Da das RaSTA-Protokoll bereits im Einsatz und erprobt ist, ist es sinnvoll dies weiterhin als Sicherungsschicht für die Steuerkommunikation zu verwenden.

In den Architekturdarstellungen werden zwei verschiedene Netzwerkarten verwendet. Kabelgebundene Kommunikation und Funkübertragungen. Beide Netzwerkarten müssen den Safety-Standards genügen.

Kabelgebundene Kommunikation

Die Kommunikation zwischen den einzelnen Feldeinheiten, sowie zu den Stellwerkssystemen sollte über eine kabelgebundene Verbindung realisiert werden. Die Kommunikation der Stellwerke untereinander ist bereits durch kabelgebundene Verbindungen realisiert. Im Detail sollte hierbei der Ethernet Standard 802.3 [IEE15] verwendet werden. Dieser Standard ist im Bahnbereich weit verbreitet und zertifiziert. Da es sich hierbei um sicherheitskritische Infrastruktur (SIL 4 nach CENELEC [CEN17]) handelt müssen die Safety-Eigenschaften berücksichtigt werden. Dafür sorgt das RaSTA-Protokoll. In Architektur A (Abb. 5.2) sind die Feldeinheiten direkt mit dem Internet verbunden. Daher ist hier die Sicherung durch Safety-Eigenschaften nicht genug. Zusätzlich muss die Kommunikation gegen Cyber-Angriffe geschützt werden. Dazu sollte eine Verschlüsselung verwendet werden, wie sie bereits in Abschnitt 5.4.1 erläutert wurde.

Drahtlose Kommunikation

Bei der Kommunikation von Zug und Feldeinheit muss zwangsläufig auf kabellose Kommunikation zurück gegriffen werden. Ein Zug soll dabei in der Lage seine aktuelle Statusinformationen, wie zum Beispiel den aktuellen Zustand des Zuges, zu kommunizieren. In aktuellen Bahnsystemen ist es nicht möglich eine solche Verbindung Feldeinheit und Zug einzugehen. Es könnte jedoch von Vorteil sein, dass beispielsweise Störungen am Zug direkt an das Stellwerk propagiert werden können. Hierbei ist jedoch zu beachten, dass sich ein Zug in der Regel nicht sehr lange in der Reichweite für eine solche Kommunikation aufhält.

Ein Intercity Express (ICE) fährt mit einer Höchstgeschwindigkeit von 330 Km/h.
Daraus folgt:

$$330\frac{Km}{h} \Rightarrow 91,6667\frac{m}{s}$$

Eine übliche Sendereichweite für lokale Funknetzwerke sind 100 Meter.
Ein ICE benötigt also für eine solche Strecke bei voller Fahrt:

$$\frac{100m}{91,6667\frac{m}{s}} \Rightarrow 1,09s$$

Es bleibt also etwa eine Sekunde, um eine Verbindung aufzubauen, Daten auszutauschen und die Verbindung wieder abzubauen.

Eine der weit verbreitetsten Standards zur drahtlosen Kommunikation zwischen Geräten ist der Standard IEEE 802.15.1 Bluetooth [IEE02]. Hierbei handelt es sich um einen Funkstandard, wie er beispielsweise in Smartphones verwendet wird, um über kurze Strecken Daten zu versenden. Die höchstmögliche Sendereichweite von etwa 100 Metern dieses Standards ist mit einem Kasse 1 Bluetooth Netzwerk zu erreichen. Wie zuvor bestimmt bleibt etwa eine Sekunde, um eine Verbindung aufzubauen und die Informationen zu übertragen. Die Kontaktaufnahme zweier Teilnehmer erfolgt via Bluetooth durch ein Scan-Verfahren. Dieses Verfahren benötigt im schlechtesten Fall 2,56 Sekunden. In Konsequenz ist Bluetooth für diese Anwendung nicht geeignet, da bereits in der Zeit in der ein potentieller Kommunikationsteilnehmer identifiziert wird bereits die Sendereichweite des Netzes überschritten wird. Ein weiterer Argument gegen Bluetooth ist, dass der durchschnittliche Verbindungsaufbau etwa nach einem halben Scan-Intervall abgeschlossen wird, also etwa 1,28 Sekunden. Selbst wenn also ein Zug und eine Feldeinheit ohne Scan-Verfahren in Kontakt treten könnten, würde die Zeit für einen durchschnittlichen Verbindungsaufbau nicht ausreichen. Eine Machbarkeitsstudie von Murphy et al. [MWF02] zeigt, dass es möglich ist bei fahrenden Fahrzeugen die Verbindungszeit auf durchschnittlich 0.79 Sekunden zu verringern. Die dann verbleibende Zeit reicht nicht aus um Daten zu versenden. Technologien wie IEEE 802.11 (WLan) [IEE12b] benötigen mehr Zeit, um eine Verbindung aufzubauen und in der Lage zu sein Daten zu versenden. Daher können diese Technologien aus den bereits geschilderten Gründen nicht verwendet werden.

Eine Möglichkeit eine Zug-Feldeinheit Kommunikation zu ermöglichen ist ein sogenanntes „Wide Area Network“ (WAN). Diese haben größere Sendereichweiten und ermöglichen so, dass sich ein Zug eine ausreichend lange Zeit in Reichweite befinden kann um einen Datenaustausch vorzunehmen. WANs werden durch den IEEE Standard 1703-2012 definiert [IEE12a]. Übliche Reichweiten für solche Netzwerke liegen zwischen 2-15 Kilometern. Betrachtet man eine Minimalreichweite von 2 Kilometern und einem ICE mit Höchstgeschwindigkeit, so folgt daraus für die Zeit die ein Zug in Reichweite verbleibt:

$$\frac{2000m}{91{,}6667\frac{m}{s}} \Rightarrow 21{,}8181s$$

Ausprägungen dieser Technologie, wie beispielsweise das sogenannte „LoRaWAN“ [LEKO15], können eine Übertragungsgeschwindigkeit von bis zu 50 Kilobit/s erreichen. Bei einer durchschnittlichen Dauer für einen Verbindungsaufbau von 2 Sekunden können also etwa 1 Megabit an Daten übertragen werden. Eine solche Datenmenge könnte ausreichend sein, um den Status eines Zuges an eine Feldeinheit zu übertragen. Diese Annahme muss jedoch geprüft werden.

Unter der Annahme, dass es möglich ist eine ausreichend zuverlässige Kommunikation zwischen Zug und Feldeinheit herzustellen muss die Art der Kommunikation definiert werden. Hierbei ist denkbar, dass Statusdaten des Zuges mit der Feldeinheit ausgetauscht werden. Diese müssen so verarbeitet, dass diese in einem Megabit übertragen werden können. Hierbei sind Kompressionsverfahren sinnvoll, um größere Datenmengen zu transportieren. Dies ist notwendig, da es sich bei dieser Art von Kommunikation um eine verschlüsselte Verbindung handeln muss. Durch die Verschlüsselung wird ein zusätzlicher Overhead den Daten hinzugefügt und die Menge der tatsächlich übertragenen Nutzdaten sinkt. Durch eine Kompression der Daten kann dies ausgeglichen werden. Die Feldeinheit muss jedoch in der Lage sein diese Daten wieder herzustellen. Es handelt sich hierbei jedoch um maximal 1 Megabit Daten, somit ist der zusätzliche Rechenaufwand begrenzt. Des Weiteren müssen Ausfälle und Verbindungsabbrüche oder beschädigte Daten berücksichtigt werden. Hierbei ist denkbar, dass Regeln aufgestellt werden, wie in solchen Fällen verfahren wird.

Die zu übertragenen Zuginformationen sind zeitabhängige Daten. Somit verlieren sie ihren Informationsgehalt, wenn diese nicht korrekt übertragen werden. Schafft es ein Zug nicht in der verfügbaren Zeit seine Daten zu übertragen, kann ein erneuter Versuch erst in der Sendereichweite der nächsten Feldeinheit durchgeführt werden. Beim erreichen der nächsten Einheit beschreiben die Daten möglicherweise einen alten Zustand des Zuges und sind damit ungültig. Ein Zug sollte also immer nur den aktuellen Zustand übertragen.

Für die Kommunikation zwischen Zug und Feldeinheit ist ein solcher Angriff kritisch. Hierbei würde die Kommunikation zwischen den Teilnehmern nicht mehr möglich sein. In beiden Architekturen kann auf einen solchen Angriff nur schwer reagiert werden. Der Angriff erfordert jedoch eine physikalische Nähe des Angreifers und über eine ausreichend starke Sendeanlage verfügen. Somit ist eine solche Art Angriff unwahrscheinlich, darf jedoch nicht völlig ignoriert werden. Es können jedoch Gegenmaßnahmen getroffen werden. Wenn der Angreifer nicht das komplette Frequenzspektrum blockiert, kann durch ein sogenanntes „Frequenzhopping“ die Blockade umgangen werden. Hierbei wechseln Sender und Empfänger fortgehend ihre Frequenz. Kann der Angreifer nicht vorhersagen welche Frequenz als nächstes genutzt wird, kann er die Kommunikation auch nicht unterbinden.

5.4.3 Feldupates

Ein Feldupdate stellt eine besondere Herausforderung dar; es muss sicher gestellt werden, dass die Feldeinheit während des kompletten Update-Vorgangs ihre Funktionalität beibehält.

Eine Möglichkeit für ein solches Update könnte eine redundante Auslegung der Hardware bedeuten. Auf diese Weise kann ein System den Normalbetrieb gewährleisten, die redundante Komponente kann ein Update durchführen und dessen ordnungsgemäße Funktion überprüfen, bevor ein Wechsel auf die neue Version der Komponente durchgeführt wird. Eine technische Herausforderung dabei ist jedoch, dass beide Systeme zu jeder Zeit über die gleichen Informationen über das System verfügen müssen. Dies gilt insbesondere auch für den Update-Vorgang. Wichtig ist hierbei, dass unabhängig von der betrachteten Architektur, sichergestellt werden muss, dass ein Feldupdate nicht verändert wurde. Hierzu kann das Signieren der Update-Datei genutzt werden. Der Update-Server kann dazu das Update mit Hilfe seines privaten Schlüssels signieren und an die Feldeinheit übertragen. Die Feldeinheit kennt den öffentlichen Schlüssel des Update-Servers und kann mit dessen Hilfe prüfen, ob die Update-Datei während der Übertragung verändert wurde.

Durch die Festlegung auf bestimmte Technologien und Erläuterungen der zusätzlichen Features ist es möglich die vorgestellten Architekturen auf eventuelle Angriffsszenarien zu untersuchen. Hierbei ist es wichtig, dass ein Angriff nicht nur das Ausspähen von Daten oder die Kontrollübernahme des Systems bedeuten kann, es kann auch schon ausreichend sein die Kommunikation zwischen einzelnen Komponenten und so den Betriebsablauf zu stören. Das folgende Kapitel befasst sich mit der Analyse solcher Angriffsszenarien. Dabei wird versucht kritische Stellen innerhalb der in Abschnitt 5 vorgestellten Architekturen zu identifizieren. Außerdem wird versucht mögliche Gegenmaßnahmen aufzuzeigen. Vorweggenommen sei schon einmal angemerkt, dass nicht alle Angriffe, die auf aktuelle Bahnanlagen durchgeführt werden können, durch die vorgestellten Architekturen ausgeschlossen werden können.

6 Analyse möglicher Angriffsszenarien

Eine digitalisierte Bahnanwendung muss nicht nur Safety-Eigenschaften genügen. Wird eine solche Anwendung nicht mehr als abgeschlossenes System, sondern als global erreichbar betrieben, müssen zusätzlich noch die Security-Eigenschaften geprüft werden, da eine Verwundbarkeit im Security-Bereich zu schwerwiegenden Konsequenzen für Safety-Eigenschaften führen können. Dieser Abschnitt untersucht die in Abschnitt 5 vorgestellten Architekturen und zeigt Angriffsszenarien (Abschnitt 3) auf, die auf ein solches System einwirken könnten. Des Weiteren werden Gegenmaßnahmen vorgestellt, die den Angriffsszenarien entgegen wirken sollen.

Grundsätzlich lassen sich mögliche Angriffsszenarien in vier unterschiedliche Gruppen einordnen. Zunächst „Angriffe auf die Infrastruktur“; hierbei werden gezielt Angriffe auf Netzwerkinfrastruktur diskutiert. Des Weiteren muss die Angreifbarkeit eines Zuges betrachtet werden. Ist ein Zug in der Lage mit dem Rest des Systems direkt zu kommunizieren muss sichergestellt werden, dass dieser das System nicht mit Falschinformationen versorgen und somit einen Ausfall des Systems provozieren kann. Dabei ist zu prüfen, inwieweit ein Zug in der Lage ist, seine Kommunikationspartner zu beeinflussen und falls ja, in welchem Umfang kann dies geschehen. Wichtig sind hierbei auch die Wechselwirkungen der verschiedenen Komponenten. Ist beispielsweise ein Zug in der Lage Weiche zu stellen, oder im Bezug auf das Gesamtsystem, ist der Zug in der Lage falsche Informationen in das System zu streuen. Ein weiterer, besonders kritischer Punkt in den vorgestellten Architekturen sind die Feldeinheiten, diese sind in der Lage systemweit zu kommunizieren und beeinflussen die Entscheidungen aus dem Stellwerk. Die letzte Gruppe bilden Angriffe auf ein Stellwerk. Das Stellwerk ist die übergeordnete Entscheidungsinstitution ein erfolgreicher Angriff auf dieses Teilsystem kann zu erheblichen Safety-Risiken führen. Hierbei ist bemerkenswert, dass durch die Digitalisierung neue Risiken entstehen, die in aktuellen Bahnanlagen nicht auftreten.

6.1 Angriffe auf die Infrastruktur

In beiden vorgestellten Architekturen ist eine Kommunikation des Stellwerks mit dem Internet vorgesehen. In Architektur A sogar eine Verbindung jeder statischen Komponente (Feldeinheit, Stellwerk) mit dem Internet. Die Systeme haben somit eine global erreichbare Schnittstelle und unterliegen somit den gleichen Security-Risiken, wie jeder Server, der mit dem Internet verbunden ist. Angriffe auf die Infrastruktur sind alltäglich im Internet, daher muss auf dieses Risiko besonderes Augenmerk gelegt werden. Der folgende Abschnitt befasst sich mit einer Auswahl an Angriffen, die auf die Infrastruktur durchgeführt werden kann.

Lauschangriff

Ein Angriff, der zunächst die Funktionalität der Verbindung und somit des Systems nicht beeinflusst ist der Lauschangriff. Der Angreifer ist dabei passiv und horcht die ausgetauschten Daten mit. Hierbei können wichtige Informationen über das System abgefangen werden, außerdem können Erkenntnisse über interne Strukturen aufgedeckt werden. Ein Angreifer könnte beispielsweise alle Pakete, die zwischen einem Stellwerk und der Zentrale ausgetauscht werden umleiten und die auslesen, bevor sie an die Zentrale weiter geleitet werden oder umgekehrt. Der Angreifer kann so unbemerkt die Kommunikation nachvollziehen. Dies kann nur durch eine ausreichende Verschlüsselung verhindert werden. Wie jedoch in Abschnitt 5.4.1 erläutert wird bereits eine Verschlüsselung der Kommunikation gefordert. Diese Maßnahme kann präventiv ergriffen werden, somit wird das Risiko für einen Lauschangriff verringert, ist aber nicht auszuschließen. Eine Erkennung ist jedoch nur schwer möglich.

Datenmanipulation

Bei Datenmanipulation werden die gesendeten Daten durch einen Angreifer modifiziert oder entfernen. Ist das Kommunikationsprotokoll zwischen den Teilnehmern ausreichend bekannt, kann ein Angreifer die Nachrichten modifizieren und somit Befehle oder Informationen ändern. Sollte der Angreifer dadurch in der Lage sein Steuerbefehle an die Feldeinheiten zu senden kann dies verheerende Folgen nach sich ziehen (siehe 2.2). Die Architektur B (Abb. 5.3) erschwert eine solche Art Angriff drastisch, da das Stellwerk als Gateway fungiert. Alle Nachrichten von Außen müssen erst das Stellwerk passieren, bevor diese ins System kommen können. Dies hat zur Folge, dass zwischen dem Teilnehmer von Außen und dem Stellwerk eine stärke Verschlüsselung verwendet werden könnte, da das Stellwerk über mehr Rechenleistung verfügt als die Feldeinheiten. Im Stellwerk kann zusätzlich durch Sicherungsmaßnahmen geprüft werden, dass keine modifizierten Pakete interne Netz betreten haben. Gelingt es einem Angreifer

jedoch zwischen Feldeinheit und Stellwerk die Daten zu manipulieren und die verwendete Verschlüsselung zu umgehen bleibt das Risiko bestehen. Die Architektur A ist jedoch noch anfälliger gegen solche Angriffe. Da alle Kommunikationsteilnehmer direkt mit dem Internet verbunden sind kann hier keine zusätzliche Prüfung der Pakete vorgenommen werden. Komplexere Verfahren können auch auf Grund der geringeren Rechenleistung der Feldeinheiten nicht verwendet werden. Dennoch ist es möglich modifizierte Daten zu erkennen. Dafür kann eine Signatur verwendet werden. Im Speziellen liefert die Verwendung des PKI-Verfahrens in beiden Architekturen diese Funktionalität mit. Der Sender signiert kann das Datenpaket mit seinem privaten Schlüssel signieren. Der Empfänger kann diese Signatur mit Hilfe des öffentlichen Schlüssels überprüfen. Falls das Datenpaket während des Transports verändert wurde kann dies erkannt werden und das Paket verworfen werden. In beiden Fällen ist die Verwendung des PKI-Verfahrens zu empfehlen. Kann eine Manipulation mittels der Signatur festgestellt werden, so sollte der Absender als nicht vertrauenswürdig eingestuft werden und die Kommunikation mit dem Teilnehmer gestoppt werden.

Denial Of Service

Ein System kann nicht nur durch das Abhören oder Manipulieren von Daten angegriffen werden. Bei sicherheitskritischen Komponenten kann es auch ausreichen, dass diese nicht mehr reagieren können. Für den Kontext dieser Arbeit kann es ausreichen, wenn eine Feldeinheit nicht mehr auf Anweisungen des Stellwerks reagieren kann. Ein konkretes Beispiel: An einem Bahnübergang wird die Kommunikationsfähigkeit der zugehörigen Feldeinheit blockiert, so kann es dazu kommen, dass der Befehl für das Herunterlassen der Schranken nicht verarbeitet wird. Dies könnte einer Kollision führen, wie in Abschnitt 2.4 erörtert. Ein DOS Angriff belegt eine Schnittstelle solange mit Anfragen bis diese nicht mehr in der Lage ist alle Pakete zu bearbeiten. Es bildet sich ein Rückstau, solange bis das System oder zumindest die Schnittstelle unter der Last zusammenbricht. An diesem Punkt unterscheiden sich die zu untersuchenden Architekturen. Architektur B bietet nur eine Schnittstelle über das Stellwerk nach Außen. Somit kann auch nur diese Stelle angegriffen werden. Wird die Internetschnittstelle durch einen solchen Angriff lahm gelegt, verliert das Stellwerk zwar den Kommunikationskanal nach Außen, es bleibt aber betriebsfähig. Alle notwendigen Informationen werden innerhalb des Systems zusammengetragen und die Kommunikation innerhalb des Systems wird nicht belastet. Somit kann das System auch ohne Verbindung zum Internet alle notwendigen Entscheidungen treffen. Sollte sogar das komplette Stellwerk unter der Last zusammenbrechen kann dies auch kompensiert werden, da die Feldeinheiten nicht an ein bestimmtes Stellwerk gebunden sind. Fällt ein Stellwerk aus, so ist es möglich, dass ein anderes die Verwaltung

der Feldeinheiten übernimmt. Die Architektur A zeigt gegen diese Art Angriffe erhebliche Schwächen. Dadurch, dass alle nicht beweglichen Komponenten (alle außer Züge) direkt über das Internet kommunizieren, können auch einzelne Komponenten gezielt attackiert werden. Anhand des zuvor genannten Beispiels kann so eine Feldeinheit angegriffen werden, die für die Steuerung eines Bahnübergangs verantwortlich ist. Bricht diese unter der Last zusammen kann keine gesicherte Fahrt durch den Bahnübergang garantiert werden. Auch wenn es nicht zu einer Kollision kommt, darf diese Strecke nicht befahren werden und es würde zu erheblichen Behinderungen im Betriebsablauf kommen. Gegenmaßnahmen sind in dieser Architektur nur schwer zu implementieren. Eine übliche Gegenmaßnahme ist die Last auf verschiedene Systeme zu verteilen und so dass es nicht zu einer Überlast an einem Punkt kommen kann. Dies ist jedoch bei den Feldeinheiten nicht möglich. Es können noch weitere Gegenmaßnahmen getroffen werden, wie in der Arbeit von Vadehra et al. [VSC16] beschrieben wird. Hierbei werden die Verbindungsdaten mit dem System analysiert und entsprechende Verbindungen ausgeschlossen. Diese Gegenmaßnahmen benötigen jedoch einen leistungsstarken Analyseapparat, der nicht in jeder Feldeinheit untergebracht werden kann. Präventiv lassen sich DOS Angriffe nur schwer vereiteln.

6.1.1 Kabellose Kommunikation

Für kabellose Kommunikation können speziell auf solche Kommunikation zugeschnittene Angriffe durchgeführt werden. Das „Jamming“-Verfahren wurde in Abschnitt 3.8 erläutert. Hierbei ist erforderlich, dass sich der Angreifer in der Nähe der Funkanlage befindet. Diese kann dann mit einem Störsender außer Betrieb genommen werden. Eine Erkennung eines blockierten Frequenzbandes ist möglich, als Gegenmaßnahme kann die Frequenz geändert werden und durch ständiges Wechseln der Frequenz mit Absprache des Kommunikationspartners verhindert werden. Ist ein Angreifer jedoch in der Lage das komplette Frequenzband zu blockieren ist auch dies nicht mehr möglich.

6.2 Angriffe auf einen Zug

Auch ein Zug kann Ziel eines Cyberangriffes werden. Hierbei kann beispielsweise die Kontrolle über die Meldeeinheit übernommen werden. Der Angreifer kann die Statusinformationen, die der Zug and die Feldeinheiten übermittelt, manipulieren. Zugriff könnte durch einen Wartungsstecker oder ähnliche Schnittstellen erhalten werden. Das es sich bei einer solchen Situation, um eine realistische Gefährdung handelt zeigt ein Vorfall in den USA aus dem Jahr 2015. Ein Cybersecurity Consult melden dem FBI, dass er die Kontrolle über 20 mal die Kontrolle über ein

Flugzeug übernehmen konnte und sogar die Steuerung der Triebwerke übernehmen konnte [Per15]. Zugang zu dem System bekam der Security-Experte über eine Ethernet Steckdose für Wartungszwecke, die sich unter dem Sitz befand. Aus Sicherheitsgründen wurde nicht bestätigt, ob ein solcher Angriff tatsächlich erfolgreich war. Dennoch zeigt dieses Szenario, dass der physikalische Zugriff gesondert gesichert werden muss. Sollte also ein Angreifer über eine solche Verbindung Kontrolle über die Kommunikationsschnittstelle des Zuge erhalten, ist er in der Lage falsche Informationen an die Feldeinheiten weiterzuleiten. Dies könnte dazu führen, dass das Stellwerk den Streckenabschnitt sperrt und somit können erhebliche Verspätungen zur Folge haben. Um einen solchen Angriff zu verhindern muss der physikalische Zugriff auf Wartungsstecker eingeschränkt werden. Des Weiteren sollten Interfaces, die zur Nutzung dieser Wartungsschnittstellen genutzt werden zusätzlich durch einen Login gesichert werden. Hierbei muss darauf geachtet werden, dass der Login nicht durch Angriffe, wie in Abschnitt 3 beschrieben, angreifbar ist.

Gelingt es einem Angreifer trotz Gegenmaßnahmen die Kontrolle über den Zug übernehmen wäre er in der Lage falsche Statusinformationen an die Feldeinheit zu übermitteln. Dies könnte massive Störungen für den Betrieb bedeuten. Meldet der Zug beispielsweise eine Störung an die Feldeinheit, dann ist diese in der Lage direkt ohne Rückkopplung mit dem Stellwerk zu reagieren und den Streckenabschnitt zu sperren. Passiert dies auf einer viel befahrenen Strecke, so wird der Verkehr angehalten bis die Situation aufgeklärt wurde. Verspätungen auf allen betroffenen Verbindungen sind die Folge. Selbst wenn die Feldeinheit nicht entscheidet die Strecke zu sperren und die Informationen nur an das Stellwerk weiterleitet, so würde der Fahrdienstleiter vermutlich die gleiche Konsequenz daraus ziehen und den Streckenabschnitt vorläufig sperren.

6.3 Angriffe auf eine Feldeinheit

Die Feldeinheit ist eine kritische Komponente innerhalb des Systems. Sie steuert die Aktoren, wie Weichen oder Signale oder auch Schranken an Bahnübergängen innerhalb eines Streckenabschnittes. Des Weiteren liefert diese Einheit Sensordaten, die für die Bestimmung der Position der Züge innerhalb des Abschnittes genutzt werden. Daher liegt auf dieser Komponente besonderes Augenmerk für die Prüfung der Security-Eigenschaften. Wie auch im vorherigen Abschnitt ist es notwendig den physikalischen Zugriff auf Wartungsschnittstellen gesichert werden. Auch hier könnten Manipulationen oder Störungen an der Feldeinheit durch einen Angreifer durchgeführt werden und es kann zu Störungen im Betriebsablauf kommen.

Ein weiteres Angriffsszenario entsteht, wenn die Update-Funktionalität der Feldeinheit betrachtet wird. Ein Angreifer könnte hierbei den Update-Vorgang dazu nutzen, um schadhafte Software auf die Feldeinheit zu spielen. Auf diese Weise können alle getroffenen Sicherheitsmaßnahmen umgangen werden und der Angreifer erhält vollständige Kontrolle über die Feldeinheit und somit die Kontrolle über die Aktoren der Feldeinheit. Des Weiteren können die Sensordaten der Feldeinheit manipuliert werden, sodass ein Zug nicht erkannt wird. Dies könnte eine Kollision zur Folge haben.
Eine Gegenmaßnahme für einen solchen Angriff ist das Verifizieren des Updates. Wie in Abschnitt 5 beschrieben, sollte ein Update zunächst auf einer redundanten Komponente durchgeführt und geprüft werden. Die redundante Steuereinheit könnte durch eine Testschnittstelle geprüft werden. Somit hätte ein Angreife keine Möglichkeit zusätzlich zum Update noch das Testverfahren zu manipulieren.

Angriffe auf die Feldeinheit können auch auf niedrigem Level durchgeführt werden. Wird beispielsweise bei der Anfrage eines Stellwerks an die Feldeinheit ein Buffer aufgebaut, so kann durch geschickte anfragen an die Feldeinheit dieser Buffer zum Überlaufen gebracht werden. Auf diese Weise ist das Verhalten des Softwaresystems nicht mehr vorhersagbar. Ein Absturz des Systems ist wahrscheinlich. Um solche provozierten Abstürze zu verhindern ist es notwendig, dass alle Zugriffe auf Buffer gesondert geprüft werden. Da es sich hierbei um potentiell Safety-kritische Eigenschaften handelt, müssen diese gemäß des „Industrial communication networks“ Standards [IEC13] geprüft werden. Dieser sieht eine Prüfung von Buffer Over- und Underflows vor, verweist dafür aber auf den Review Guide der OWASP [Kon17]. Eine weitere Möglichkeit um einen solchen Angriff zu verhindern ist eine Instrumentierung der Applikation zur Laufzeit. Hierbei werden zusätzliche Informationen über Speichernutzung und Zugriffe gesammelt und mit einem Regelwerk verglichen. Sollten sich Speicheroperationen sich außerhalb des Regelwerks befinden, so kann dieser Zugriff verhindert werden.

Gelingt es dem Angreifer dennoch die Kontrolle über eine Feldeinheit zu übernehmen stellt dies ein hohes Sicherheitsrisiko da. Die Feldeinheiten kontrollieren Weichen, Bahnübergänge und Signale. Diese Geräte könnten somit von einem Angreifer gesteuert werden. Im harmlosesten Fall stoppt der Angreifer nur alle Züge, die in den Abschnitt fahren wollen. Eine Eskalationsstufe davon wäre die Weichen so zu ändern, dass passierende Züge in andere als die gewünschte Richtung umgelenkt werden. Die höchste Eskalationsstufe wäre die Kollision von Zügen. Hierzu könnten die Weichen so geändert werden, dass zwei Zügen aufeinander

zu fahren. Des Weiteren könnten die Signale so geändert werden, dass zwei Züge in beiden Richtungen eine Fahrerlaubnis bekommen. In Wechselwirkung mit dem Stellwerk könnte der Status der Achszähler nicht an das Stellwerk übertragen werden. Ein Zug würde somit aus dem System verschwinden.

6.4 Angriffe auf ein Stellwerk

Das Stellwerk ist die einzige Komponente, die im direktem Austausch mit Menschen steht. Der Fahrdienstleiter muss in der Lage sein Änderungen am System vorzunehmen, Weichen oder Signale zu ändern. Dadurch können weitere Angriffe vorgenommen werden. Hierbei ist es möglich den Fahrdienstleiter als indirekten Angreifer zu nutzen. Steckt beispielsweise der Fahrdienstleiter einen korrumpierten Datenträger an seinen Arbeitsplatzcomputer, so kann allein durch das Ansteuern des Datenträgers Schadsoftware auf das Zielsystem übertragen werden. Üblich für solche Art Angriff ist das verwenden von USB-Geräten [Tea17]. Diese werden so modifiziert, dass diese beispielsweise als Tastatur erkannt werden und führen automatisch und unsichtbar Tastendrucke aus, die schadhafte Software auf dem Zielsystem installieren. Eine weiter Alternative dieses Angriffes ist das Manipulieren des Loaders, der sich auf dem USB-Gerät befindet. Dieser wird beim einstecken des USB-Gerätes automatisch durch den Host ausgelesen. Auf diese Weise kann sogar eine durch Software deaktivierte USB-Schnittstelle umgangen werden. Statt des Loaders wird die Schadsoftware ausgeführt. In beiden Fällen kann die vollständige Kontrolle über das System übernommen werden. Gegenmaßnahmen für solche Angriffe ist das Sperren der USB Schnittstellen, dies sollte physikalisch geschehen, indem die Schnittstellen durch Blenden abgedeckt werden oder die Stromzufuhr der Schnittstellen unterbrochen wird. Auf diese Weise ist sichergestellt, dass ein Anwender physikalisch daran gehindert wird versehentlich ein USB-Gerät an kritische Komponenten zu stecken.

Ein weiteres Szenario ist das Manipulieren eines Updates. Ähnlich wie im vorherigen Abschnitt kann durch das modifizieren eines Updates schadhafte Software in das System gespielt werden. Der Angreifer ist auf diesem Weg in der Lage jegliche Änderungen oder Kontrollmechanismen in das System zu bringen. Auch im Stellwerk kann ein Update durch redundante Auslegung des Systems geprüft werden. Da es sich aber beim Stellwerk um die komplexeste Komponente im System handelt, ist es sinnvoll zusätzlich die Integrität des Updates zu prüfen.

Gelingt es einem Angreifer ein Stellwerk zu übernehmen so können wahllos Weichen und Signale verändert werden. Ähnlich wie bei der Übernahme einer Feldeinheit können Züge umgeleitet oder zur Kollision gebracht werden.

Um solche Angriffe verhindern zu können ist es Sinnvoll im Vorfeld so viele Ursachen für Angriffe wie möglich zu erkennen. Daher beschreibt der folgende Abschnitt Testansätze und Analyseverfahren mit denen, die in diesem Kapitel aufgezeigten Angriffsmöglichkeiten erkannt werden können.

7 Testen auf Verwundbarkeit

Um weiteres Vertrauen in die Software einer Bahnanlage zu gewinnen ist es üblich, dass die Applikation durch Tests geprüft wird. Für aktuell eingesetzte Systeme können bereits eine Reihe von Untersuchungen vorgenommen werden. Beispielsweise werden die einzelnen Komponenten auf verschiedenen Ebenen überprüft, dies reicht von der Prüfung auf einzelner Methodenebene bis hin zum Gesamtsystem. Das Testen von Security-Eigenschaften wird jedoch nur oberflächlich berücksichtigt, da sich die Bahnanwendungen in einem nicht frei zugänglichen Netz befinden. Die in dieser Arbeit aufgezeigten zusätzlichen Risiken, die durch die Digitalisierung des Systems entstehen können müssen auf unterschiedlichen Ebenen geprüft werden. Grundsätzlich ist es üblich, dass ein System während der Entwicklung auf Verwundbarkeiten geprüft wird, um das Risiko eines Angriffs im späteren Betriebs zu verringern. Jedoch gibt es Angriffe, wie „Denial Of Service"-Angriffe, die zwar erkannt jedoch nicht vollkommen verhindert werden können. Der folgende Abschnitt befasst sich daher mit Testansätzen, die verwendet werden können um Verwundbarkeiten aufzudecken. Zunächst werden Verfahren betrachtet, die während des Entwicklungsprozesses eingesetzt werden können. In einem weiteren Abschnitt dann Verfahren, die im Betrieb genutzt werden können. Um eine solche Untersuchung durchführen zu können, müssen jedoch einige Annahmen getroffen werden. Zunächst ist es üblich, dass die Software für hardware-nahe Systeme in C++ oder sogar in Teilen von Assembler umgesetzt wird. Einer der Hauptgründe ist hierfür die Standardisierung der Sprache. C++ ist durch die ISO/IEC 14882:2014 [Int14]. Des Weiteren ermöglicht C++ das Arbeiten auf unterschiedlichen Abstraktionsleveln, wie Objekt Orientierter Programmierung. Da C++ direkt in Maschinencode übertragen wird, kann auch direkt auf die darunter liegende Maschine Einfluss genommen werden. Daher wird in dieser Betrachtung angenommen, dass die Umsetzung der Software in C++ erfolgt. Für die in den Architekturen verwendeten Komponenten müssen Annahmen über die Softwarearchitektur gemacht werden. Für das Stellwerk bietet sich an bzw. ist es für die Feldeinheiten sogar notwendig, dass Stellanweisungen in klar definierbarer Zeit umgesetzt werden. Daher ist es in diesen Komponenten sinnvoll ein echtzeitfähiges Betriebssystem zu verwenden. Diese arbeiten in der Regel auf Basis von C++ und sind daher gut mit der Wahl der Programmiersprache zu verbinden. Wichtig ist jedoch

dabei, dass das Betriebssystem den Anforderungen aus der CENELEC [CEN17] genügen muss. Auf Basis dieser gewählten Randbedingungen können nun im folgenden Abschnitt Tests und Analysen untersucht werden, die zur Vermeidung oder Erkennung der vorgestellten Angriffe genutzt werden könnten. Dabei werden die Verfahren in aktuellen Systemen nicht verwendet, mit Ausnahme von Penetrationstests.

7.1 Over- / Underflow-Angriffe

In Abschnitt 6.3 werden Angriffe auf die Feldeinheiten beschrieben. Ein Szenario dabei ist es die Feldeinheit mittels Überlaufen oder Unterlaufen eines Buffers zu manipulieren oder gar zum Absturz zu bewegen. Für die Erkennung solcher Probleme kann während der Entwicklung der Komponente beispielsweise der von Haller et al. [HSNB13b] vorgestellte Ansatz verwendet werden. Hierbei wird ein „guided Fuzzer“, der statische und dynamische Analyse mit instrumentiertem Code verbindet. Zunächst werden in diesem Verfahren „Kandidaten“ ermittelt. Dies können beispielsweise Array-Zugriffe sein. Bei einer solchen Art Zugriff kann mit hoher Wahrscheinlichkeit ein Buffer-Overflow oder -Underflow auftreten. Entwickelt wurde dieser Ansatz um komplexe Overflow Probleme in weitverbreiteten Linux-Programmen, wie dem Webserver ngix oder dem Videoplayer ffmpeg zu erkennen. Mit Hilfe einer sogenannten „Taint Analyse“ [Sch10] werden kritische Variablen identifiziert. Die Taint Analyse markiert dafür von außen setzbare Variablen und verfolgt deren Verwendung durch den Quellcode. Wird eine markierte Variable verwendet, um eine andere Variable zu verändern, wird auch die veränderte Variable markiert. Taucht eine markierte Variable innerhalb eines Array-Zugriffs auf, ist ein Kandidat identifiziert. Diese Kandidaten beschreiben die Menge der Variablen, die potenziell zu Over-/Underflows führen können. Die ermittelten Variablen werden dann mit einem Fuzzer verändert und die Reaktion des Systems wird anhand des instrumentierten Quellcodes nachvollzogen. Eine von Haller et al. erstellte Engine wertet diese Informationen aus und ermittelt einen Pfad, der mit hoher Wahrscheinlichkeit zu einem Overflow führen kann. Auf diese Weise kann der Fuzzer gezielt Werte bestimmen, die zu einem Fehler führen können. Dieses Verfahren ist, wie alle Testverfahren nicht in der Lage alle möglichen Fehler dieser Art in allen Ausprägungen zu erkennen, dennoch ist dieser Ansatz in der Lage in kürzester Zeit (15 Minuten) ca. 80% der Overflow-Probleme in einem Projekt mit mehr als 300 Tausend Zeilen Quellcode zu erkennen [HSNB13a].
Für die Erkennung der Over-/Underflow-Problematik im Bahnkontext ist ein solcher Ansatz sehr gut geeignet. Die Arbeit von Haller et al. hat gezeigt, dass mit dem Ansatz auch bisher unerkannte Probleme aufgezeigt werden können. Zusätzlich spricht für eine solche Analyse, dass

diese rein statisch durchgeführt wird, somit kann eine solche Analyse gut parallel durchgeführt werden und korreliert nicht mit der Laufzeit des zu prüfenden Systems. Des Weiteren kann ein solcher Ansatz aufgrund seiner geringen Laufzeit gut in den Entwicklungsprozess eingebunden werden. Somit kann das Vertrauen in ein System bereits während der Entwicklung gestärkt werden.

Eine weitere Möglichkeit ein Softwaresystem zu Fehlverhalten zu bewegen ist der Zugriff auf uninitialisierten Speicher. Hierbei verarbeitet die Software einen zufälligen Wert, der üblicher Weise so nicht erwartet wird und das Programm wird zum Absturz gebracht [MIT17e]. Ein solches Problem kann nur in Programmiersprachen auftreten, die die direkte Verwaltung des Speichers zulassen. Die bekanntesten Vertreter solcher Sprachen sind C und C++. Gängige Tools für das Aufdecken eines solchen Problems, wie beispielsweise „Purify“ [IBM04] der Firma IBM, oder „Valgrind“ [Ent16] verwenden binäre Instrumentierung, um solche Stellen im Hauptspeicher zu erkennen. Dies hat den Nachteil, dass der Code ausgeführt werden muss. Somit ist die Laufzeit der zu untersuchenden Anwendung maßgebend für die Laufzeit der Analyse. Zusätzlich muss der Hauptspeicher mit weiteren Informationen versehen werden. Dabei ist jedoch nicht sichergestellt, dass alle Pfade der Anwendung durchlaufen werden und somit alle Möglichkeiten für den Zugriff auf uninitialisierten Speicher ausgeschlossen sind. Die Arbeitsweise dieser Tools sind nicht in der Lage selbstständig Tests zu entwickeln, die einen solchen unerlaubten Zugriff erzeugen. In der Regel wird ein solches Tool eher zu Debugging Zwecken verwendet, wenn bereits bekannt ist, dass ein Problem vorliegt. Einen anderen Ansatz wurde von Stephanov et al. [SS15] vorgestellt. Hierbei wird der Compiler mit einer Instrumentierung versehen. Es kann auf diese Weise eine Prüfung noch während des Übersetzens des Programms vollzogen werden. Dies stellt eine signifikante Verbesserung gegenüber den vorgestellten Tools dar, da die Anwendung nicht ausgeführt werden muss und auch über eine eigenständige Diagnose verfügt. Ähnlich wie bei dem Ansatz von Haller et al. kann eine solche Analyse direkt in den Entwicklungsprozess eingebunden werden. Des Weiteren können Analysen auf ausgeführten Code nur schwer aussagekräftige Fehlermeldungen liefern, da diesen nur die kompilierten Binärdaten zur Verfügung stehen. Bei einer Prüfung zur Compile-Zeit kann sich direkt auf den Quellcode bezogen werden. Und die Fehlermeldung kann direkt auf den zugehörige Stelle verweisen.

Für die Anwendung auf den Bahnbereich bedeutet dies, dass bei gleicher Erkennungsrate von Fehlern immer die statischen Analysen zu bevorzugen sind. Diese sind flexibler und können losgelöst von der kompilierten Anwendung oder erforderlichen Hardware durchgeführt werden.

Im Bezug auf die Architektur kann ein solcher Angriff durch Over-/Underflow in jedem der vorgestellten Komponenten durchgeführt werden, daher ist es sinnvoll die Prüfung auch für alle Komponenten durchzuführen. Zumal keine Spezialhardware vorhanden sein muss. Außerdem können solche Analysen auch für komplexe Programme in kurzer Zeit (Ansatz von Haller et al.) oder während des Übersetzungsvorgangs (Ansatz von Stephanov et al.) durchgeführt werden.

7.2 Modellbasiertes Testen

Das Testen auf Verwundbarkeiten muss nicht zwingend auf technisch niedrigen Ebenen durchgeführt werden. Es ist beispielsweise möglich einzelne Komponenten oder die Kommunikation der Komponenten als Modell darzustellen und dieses als Testgrundlage zu nehmen. Mit Hilfe eines solchen Modelles können Fehlerzustände ermittelt werden. Zum Einen können Fehler in der Architektur aufgedeckt werden, zum Anderen können aus Modellen Testfälle generiert werden. Modellbasierte Testansätze haben den Vorteil, dass sie üblicherweise anhand einer Spezifikation durchgeführt werden [KL16]. Das bedeutet, dass das Modell das Verhalten des Systems gemäß der Spezifikation beschreibt und unabhängig von der tatsächlichen Implementierung entwickelt wird. Aus dem Modell können dann Testfälle automatisch generiert werden, die die tatsächliche Implementierung gemäß der Spezifikation prüfen. Der Tester kann sich also mit wichtigeren Arbeiten befassen, als dem manuellen Erstellen von Testfällen. Ähnlich verhält es sich mit Änderungen an der Spezifikation. Hierbei müsste lediglich das Modell angepasst werden und die Testfälle neu generiert werden. Werden diese Modelle frühzeitig im Entwicklungsprozess entwickelt können sie auch in frühen Phasen der Softwareentwicklung für die Validierung und Verifikation des Systems genutzt werden. Fehler können so früher erkannt und behoben werden. Dabei zeigt eine Studie von Boberg [Bob08], wie modellbasiertes Testen zur signifikanten Steigerung von Fehlerfunden in frühen Entwicklungsstufen beitragen kann. Hierzu wurden modellbasierte Testverfahren in den Entwicklungsprozess integriert und mit den Ergebnissen aus manuellen Tests verglichen. Die Studie zeigt, dass in einer Applikation, die durch modellbasierte Tests geprüft wurde, signifikant mehr Fehler aufdecken werden konnte. Zusätzlich konnten diese Fehler in der Regel auch in früheren Entwicklungsstufen erkannt werden. Die Studie zeigt jedoch auch, dass der initiale Zeitaufwand, der für die Verwendung der Modelle aufgewendet werden muss größer ist, als in herkömmlichen Methoden.

Modelle können auch aus der Implementierung erzeugt werden. Diese können dann genutzt werden um die Implementierung auf einer höheren Abstraktionsebene zu betrachten. In der

anderen Richtung können Modelle auch verwendet werden, um eine Implementierung zu generieren. Wird ein solches Modell zusätzlich zum Generieren der Tests verwendet, muss das Modell besonders geprüft werden, da Fehler im Modell nicht von den daraus abgeleiteten Tests gefunden werden können.
Für das Testen der Sicherheitsrisiken im Bahnbereich können solche Methoden angewendet werden, da es klare Spezifikationen, in Form von Standards, gibt, die eingehalten müssen. Aus diesen Standards können Modelle entwickelt werden, die dann für die Prüfung der Anwendung genutzt werden können. Jedoch können dafür nur Anforderungen verwendet werden, die sich auch als Modell abbilden lassen. Dies sind beispielsweise Anforderungen, die sich als Zustandsmaschine darstellen lassen
Die folgenden Abschnitte zeigen verschiedene Verfahren, die für das Prüfen von Anforderungen verwendet werden können.

7.2.1 Modellieren von Bahnanwendungen mit Hilfe von Sequenzdiagrammen

Einen Ansatz, wie eine Bahnanwendung als Modell dargestellt werden kann und somit auch modellbasiert getestet werden kann bietet die Arbeit von Bohn et al. [BDW02]. Die Arbeit beschreibt wie die von der CENELEC geforderten Anforderungen zur Entwicklung von Bahnanwendungen mit Hilfe von modellbasierten Ansätzen nachgewiesen werden. Hierzu werden Erweiterung der „Statemate modeling tool“'s der Firma I-Logix Inc vorgenommen. Zum einen wird der sogenannte „Live Sequenz Chart“ verwendet. Hierbei handelt es sich um eine Variante des „Message Sequence Charts“ [ITU11] und dem UML Sequenz Diagramm [Uni15]. Diese Art der Modellierung wird verwendet um das Zusammenspiel der einzelnen Komponenten und Akteure zu verdeutlichen. Wichtig ist dabei, dass auf diese Weise auch die Kommunikation über sicherheitskritische Protokolle abgebildet werden kann. Als nächstes wurde „Model Checking“ integriert. Dies ist notwendig, um zu belegen, dass das Model bestimmte zustände nicht erreichen kann. Des Weiteren können so auch Protokolle verifiziert werden. Abschließend wird automatische Testfallgenerierung vorgestellt. Aus den zuvor beschriebenen Modellen können automatisch Testfälle erstellt werden, die dann genutzt werden können, um die tatsächliche Steuerhardware auf einem Testrigs in einem hardware-in-the-loop-Test zu prüfen. Bei der in der von Bohn et al. vorgestellten Arbeit werden nur safety-Risiken behandelt. Dennoch ist es denkbar, dass ein solches Verfahren für die Security-Prüfung von Bahnanwendungen verwendet werden kann.

Ein solches Verfahren kann beispielsweise verwendet werden, um die Kommunikation zwischen einzelnen Komponenten, wie dem Zug und der Feldeinheit oder einzelne Sequenzen innerhalb einer Komponenten, wie dem Ändern einer Weichenposition durch einen Fahrdienstleiter, verwendet werden. Diese Kommunikation läuft streng sequenziell ab und kann daher durch ein solches Diagramm gut dargestellt werden. Anders verhält es sich jedoch mit komplexeren Szenarien. Sind viele Kommunikationsteilnehmer involviert steigt der Zustandsraum erheblich. Außerdem lassen sich nicht alle notwendigen Sachverhalte als Sequenzdiagramm darstellen.

7.2.2 Modellierung von Angriffsszenarien durch „Attack Trees“

Das modellbasierte Ansätze für die Prüfung von Security-Aspekten genutzt werden können zeigt eine Arbeit von Morais et al. [MCM11]. Hierzu wird eine Vorgehensweise in sechs Schritten vorgestellt. Als erster Schritt werden Informationen zu möglichen Angriffen gesammelt. Dieser Schritt ist notwendig, um die Schwachstellen bzw. Angriffsszenarien eines Systems zu ermitteln. Als nächstes wird geprüft, wie Wahrscheinlich es ist, dass ein Angreifer die Ressourcen für einen Angriff aufzuwenden. An einem Beispiel bedeutet dies: Wie Wahrscheinlich ist es, dass ein Angreifer ausreichend Infrastruktur zur Verfügung hat, um eine Verschlüsselung zu knacken. Können Angriffsszenarien gefunden werden, die mit realistischem Ressourcenaufwand durchgeführt werden, folgt die Modellierung des Angriffs. Für die Modellierung der Angriffe werden sogenannte „Attacktrees “ [SDP08] verwendet, hierbei handelt es sich analog zu einem Fehlerbaum um eine Baumstruktur, an dessen Wurzel der erfolgreiche Angriff steht. Davon abgehend sind Knoten definiert. Diese beschreiben Ereignisse, zum erfolgreichen Angriff führen können. Das Auslösen dieser Ereignisse kann durch gleichzeitiges Auftreten (UND) oder durch einzelne Ursachen (ODER) verursacht werden. Diese Ereignisse können beliebig komplex sein, werden jedoch alle auf Basisereignisse runter gebrochen. Besonders interessant ist das resultierende „minimal cut set“, dass in boolscher Algebra angegeben wird. Diese Menge zeigt an, welche Ereignisse minimal notwendig sind, um den Angriff durchzuführen. Um dieses Vorgehen an einem Beispiel zu demonstrieren zeigt die Abbildung 7.1 einen Angriff auf „Wireless Transport Layer Security“-Protokoll (WTLS) durch einen „Attack Tree“.

In dieser Abbildung wird deutlich, dass einzelne Ereignisse ausreichen, um einen Angriff auf WTLS durchzuführen. Durch das „minimal cut set“ wird deutlich, dass fast alle Basisereignisse außer die unter Punkt 1.4 (UND-Verknüpfung) zusammen gefasst sind einen Angriff auf WTLS ermöglichen. Aus dieser Erkenntnis können dann Angriffsszenarien entwickelt werden. Hierzu

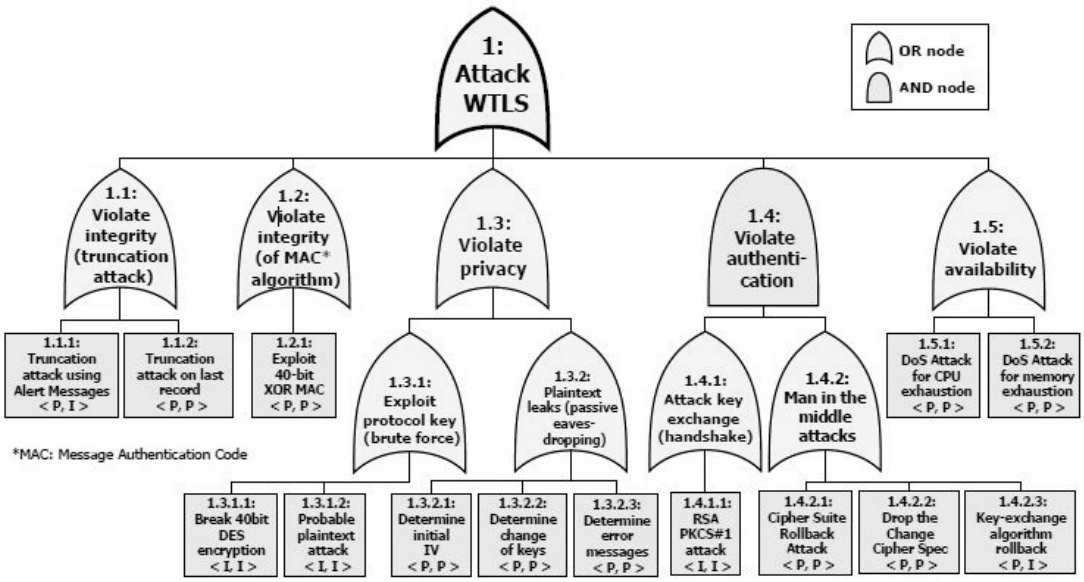

Abbildung 7.1: Grafische Repräsentation eines „WTLS Attack Tree“ [MCM11]

müssen nun der Ressourcenaufwand mit den „Attack Trees“ kombiniert werden. So entstehen dann Angriffsmöglichkeiten , die für den Angreifer auch durchführbar sind. Daraus lassen sich dann Angriffsscripte generieren, die dann im finalen Schritt zur Ausführung gebracht werden. Ein Testfall entsteht also aus den Angriffsscripten, die zur Ausführung gebracht werden und prüft dann die Reaktion des Systems auf diesen Angriff. Am Beispiel von WTLS könnte ein Testfall so aussehen, dass ein „brute force“ dazu genutzt werden könnte den Protokoll Schlüssel zu knacken und somit die Verschlüsselung außer Kraft zu setzten. Somit tritt das Ereignis 1.3.1.1 ein. Dieses Ereignis löst die übergeordneten Ereignisse aus (1.3.1 und 1.3) und resultiert schlussendlich im Aushebeln von WTLS. Der Test ist dann erfolgreich, wenn trotz dieses Angriffs auf die Verschlüsselung keine Informationen entschlüsselt werden können. Ist der Angriff erfolgreich, dann ist der Test fehlgeschlagen.

Bezogen auf das Testen der Security-Eigenschaften kann ein solcher genutzt werden, um Angriffe auf alle in dieser Arbeit vorgestellten Systeme zu modellieren, solange diese in ein Modell wandelbar sind. Es müssen jedoch die Möglichkeiten des Angreifers berücksichtigt werden. Der gravierende Nachteil, der sich dabei ergibt ist, dass in dem vorgestellten Verfahren immer der Angriff im Vordergrund steht. Das bedeutet, dass der Tester immer einen Angriff voraussetzten muss, der als Grundlage für die Modellierung verwendet wird. Dabei können möglicherweise Angriffsmöglichkeiten übersehen werden. Für die Verwendung im Bahnbereich spricht jedoch der Top-Down Ansatz, der bei der Modellierung der Attack-Trees genutzt wird. Dieser Ansatz

erzwingt eine gewisse Sorgfalt, da zunächst das Ergebnis betrachtet wird und dann immer detaillierter ermittelt wird, wie es dazu kommen kann. Außerdem ist ein ähnliches Verfahren (Fehlerbaumanalyse) für die Prüfung der Safety-Eigenschaften bereits üblich. Beispielsweise könnte ein solches Verfahren für die Analyse der Zug-Feldeinheit-Kommunikation genutzt werden. Als Wurzel wird der Ausfall der Kommunikation definiert. Davon ab werden dann Ereignisse definiert, die zu diesem Ausfall führen können. Zum einen kann die Kommunikation der Feldeinheit gestört werden, auf der anderen Seite die Kommunikation des Zuges. Wichtig hierbei ist, dass die Architektur oder sogar die Hardwarebesonderheiten der einzelnen Komponenten berücksichtigt werden muss. Spielen diese Faktoren alle mit ein so wird leicht ersichtlich, dass der Zustandsraum einer solchen Analyse schnell groß wird. Es muss also zuvor geprüft werden, ob der zu untersuchende Angriff überhaupt mit einem solchen Baum ausreichend detailliert dargestellt werden kann.

Einen weiteren Ansatz bietet Julliand et al. [JMT08]. Dabei werden funktionale Tests, die bei der formalen Analyse der Systeme entstehen, wiederverwendet und mit Security-Eigenschaften erweitert. Daraus wird ein neues Security-Modell des Systems entwickelt, dass die Basis für Generierung der Testfälle genutzt wird. An dieser Stelle wird jedoch ein Nachteil dieses Ansatzes deutlich. Für die Erstellung des Security-Modells ist das Know-How eines Security-Experten notwendig, der die neuen Modelle prüfen kann. Für die Modellierung wird in der Arbeit von Julliand et al. eine domänenspezifische Sprache vorgestellt, die auf regulären Ausdrücken basiert. Mit Hilfe dieser Sprache ist es möglich Regeln zu definieren, die durch das zu testende System eingehalten werden müssen. Aus dem erstellten Regelwerk können dann in einem weiteren Schritt Testfälle generiert werden. Ein besonderes Augenmerk legt die Arbeit von Julliand et al. auf Authentifizierungen an Systemen. Ein „normaler“ funktionaler Test würde für eine boolesche Variable, die den Zugriff auf ein System beschreibt die Werte true und false prüfen. Für eine Security-Analyse ist beispielsweise auch interessant, ob diese Variable ihren Zustand ändert, zum Beispiel ob die Variable erst auf true gesetzt ist und sich im Laufe der Zeit auf false ändert. Solch ein Verhalten würde auf Seiteneffekte hinweisen. Ein solches Verhalten kann mit Hilfe einer formalen Spezifikation modelliert werden.
Da ein solcher Ansatz kann auf verschiedenen Ebenen verwendet werden. Daher eignet er sich sowohl für die Modellierung der einzelnen Komponenten, als auch für die Modellierung der Zusammenarbeit der einzelnen Komponenten im Bahnbereich. Um aus diesen Modellen jedoch Testfälle ableiten zu können muss ein relativ niedriges Level verwendet werden, sodass die Systemeigenschaften in den Modellen berücksichtigt werden können. Des Weiteren gestaltet es sich als schwierig viele parallel voneinander ablaufende Komponenten zu modellieren. Der

Zustandsraum, der bei einer Prüfung der Modelle entsteht, explodiert dabei auch schon für wenige Komponenten. Für die Verwendung auf die in dieser vorgestellten Komponenten ist eine solche Analyse jedoch für isolierte Komponenten vorstellbar.

Zusammenfassend können modellbasierte Testansätze für die Analyse von Bahnanwendungen verwendet werden. Verschiedene Varianten werden bereits in der Safety-Analyse verwendet und sind dort gut erprobt. Jedoch ist die Modellierung von Security-Eigenschaften nicht immer klar ersichtlich. Viele Seiteneffekte und Abhängigkeiten lassen die benötigten Zustandsräume rasch wachsen und machen das Identifizieren von Testfällen schwierig. Dies gilt im Besonderen, wenn das Zusammenspiel von vielen Komponenten untersucht werden soll. Dies lässt vermuten, dass modellbasierte Ansätze zwar eher für die Prüfung einzelner Problemstellungen genutzt werden sollten.

7.3 Penetration Test

Ein gängiges Verfahren für das Testen auf Sicherheitslücken ist der „Penetrations Test“. Dieses Verfahren ist üblich in der Sicherung von Webservern oder dazu gehöriger Infrastruktur. Bei diesem Verfahren werden eine Reihe verschiedener Angriffsszenarien zusammen gestellt mit denen das Zielsystem angegriffen wird. Der folgende Abschnitt beschreibt verfahren, die sich auch für die Prüfung von Bahnanwendungen eignen.

Ziel des Penetrations Tests (Pentest) [Bun16a] ist es Schwachstellen in einem System aufzudecken; zu diesem Zweck werden eine Vielzahl verschiedener Angriffe zusammengestellt mit denen dann versucht wird in das System einzudringen [Bun16a]. Hierbei werden zunächst Angriffsmuster analysiert, über die das System erreichbar ist. Wichtig hierbei ist, dass die Angriffe in Testmodule zusammengefasst werden. Diese werden in I- und E-Module unterschieden. I-Module sind dabei Tests, die zur reinen Informationsbeschaffung verwendet werden. Informationen können in diesen Zusammenhang jegliche Art von Meta-Daten sein, die über das angegriffene System in Erfahrung gebracht werden können, beispielsweise die verwendete Software und deren Versionsnummer. Diese können Aufschluss über mögliche Schwachstellen liefern. E-Module werden für tatsächliche Eindringversuche genutzt. Das Eindringen beschreibt den aktiven Eingriff in die Funktion eines Systems. Dies kann beispielsweise das Ändern von Daten aber auch das Abschalten von bestimmten Komponenten sein. Ein detailliertes Vorgehen zu diesen Punkten kann dem „Durchführungskonzept für Penetrationstests“ des „Bundesamt für Sicherheit in der Informationstechnik“ [Bun03] entnommen werden. Diese Trennung legt

nahe, dass ein Angriff in mehreren Stufen durchgeführt werden muss. Zunächst werden durch I-Module Informationen gesammelt, die dann von E-Modulen verwendet werden um einen Eindringversuch in das System durchzuführen.

Eine Möglichkeit solche Tests durchzuführen wird in der Arbeit von Singh et al. [SLN04] vorgestellt. Bei herkömmlichen Pentests können nur wenige Pfade durch ein System geprüft werden. Dies ist damit zu begründen, das für die Erstellung von Security-Matrizen nur die Schnittstellen eines Systems zur Verfügung stehen. Welcher Pfad tatsächlich durch das System genommen wird ist dabei nicht ersichtlich. Eine andere Variante ist das System mittels Model Checking zu prüfen, hierbei entstehen sehr schnell sehr viele Zustände (state explosion), die für die meisten Tools nicht handhabbar sind. Aus diesem Grund werden in der Arbeit von Singh et al. Schätzungen und Heuristiken verwendet um gezielt Pfade durch das System zu ermitteln, die dann durch einen Pentest von Außen durchgeführt werden können.
Eine moderne Art des Penetration Testens wird in der Arbeit von Ceccato et al. [CS16] beschrieben. Hierbei werden gängige Maßnahmen des Penetration Test erweitert mit strukturbasierten Verfahren, wie Whitebox-Tests. Bei klassischen Penetration Tests kann das System nur als Blackbox betrachtet werden. Wird ein Fehlverhalten aufgedeckt hat der Entwickler nur schlechte bis keine Informationen wo sich der Fehler in der Anwendung befindet. Dies kann mit Hilfe von statischen Verfahren verbessert werden. In der Arbeit von Ceccato et al. [CS16] konnte so gezeigt werden, dass die Zeit, die benötigt wird einen solchen Fehler zu finden und zu beheben erheblich gesenkt werden.

Da es sich beim Penetrationstesten um ein gut erprobtes Verfahren für die Prüfung von Serveranlagen und Geschäftssystemen handelt, ist es sinnvoll ein solches Verfahren auch für die Prüfung von Bahnanlagen in Betracht gezogen werden sollte. Dazu muss jedoch noch geprüft werden, ob das Vertrauen in die Sicherheit, die durch einen Pen-Test gewonnen werden kann ausreichend ist, um den Anforderungen an Bahnanwendungen gerecht zu werden.

Zusammenfassend konnten in diesem Kapitel verschiedene Verfahren aufgezeigt werden, mit denen Bahnanwendungen auf Security-Eigenschaften untersucht werden können. Wichtig dabei ist, dass auf aktuelle Bahnanwendungen nur der Pentest angewendet wird. Dabei konnte auch aufgezeigt werden, dass verschiedene Tests auf unterschiedlichen Ebenen erforderlich sind. Dies ist durch die Beschaffenheit der verschiedenen Angriffsszenarien zu erklären. Ein Angriff kann auf technisch niedrigen Ebenen durchgeführt werden um beispielsweise einen Buffer zum Überlaufen zu bringen. Auf höheren Ebenen können auch Protokolle oder andere Schnittstellen angegriffen werden, bis hin zu Angriffen auf die Architektur des Systems. Daher

müssen für alle diese Ebenen passende Verfahren gefunden werden, um einen Angriff auf allen Ebenen vorzubeugen.

8 Fazit

Im Laufe dieser Arbeit wurden einige mögliche Ausprägungen von zukünftigen digitalen Zugsicherungssystemen betrachtet und deren Risiken untersucht. Hierzu wurden zunächst die Grundlagen für die Domäne der Bahnanwendung und der IT Sicherheitsrisiken in aktuellen Bahnanlagen betrachtet. In einem nächsten Schritt wurden dann zwei Architekturen für zukünftige digitale Systeme vorgestellt. Im Folgenden wurden dann die Risiken, die durch die Digitalisierung entstehen analysiert und in einem letzten Schritt Möglichkeiten aufgezeigt mit denen diese Risiken minimiert werden können.

Diese Arbeit wurde mit der Motivation zu diesem Thema begonnen. Es wurden die Vorteile eines digitalisierten Bahnbetriebs erläutert. Dieser kann durch neue Komponenten Störungen leichter auffangen und kann mit Hilfe neuer Technologien zuverlässiger Arbeiten. Zusätzlich dazu hat sich die Bundesrepublik Deutschland gemäß der EU-Richtlinie „UP KRITIS“ [Bun16b] zum Schutz und der Modernisierung kritischer Infrastruktur verpflichtet. Durch diesen Schritt entstehen Probleme, die für die Bahn vorher noch nicht dar gewesen sind.

Um einen Einblick darüber zu erhalten welchen Risiken der Bahnbetrieb in der heutigen Zeit ausgesetzt ist wurde im Kapitel 2 ein Überblick über die Domäne der Bahnanlagen gegeben. Hierzu wurden Sicherungsmaßnahmen, wie das Stellwerk, sowie kritische Punkte innerhalb des Streckennetzes erläutert. Hierzu zählen neben „Abzweigstellen“ (Weichen) auch Bahnhöfe oder Bahnübergänge. An diesen Orten kann es zu Gefährdungen im Betriebsablauf kommen. Hierbei kann es zu schwerwiegenden Unfällen kommen, wenn die vorhandenen Sicherungsmaßnahmen ausfallen oder Missachtet werden. Um einen Ausfall dieser Systeme zu verhindern müssen alle elektrischen Systeme, die für die Zugsicherung zuständig sind, gemäß der CENELEC [CEN17] umgesetzt werden.

Der Einführung in die Bahndomäne mit ihren Risiken für den Betriebsablauf folgenden in Kapitel 3 eine Übersicht über Cyberangriffe, die möglicherweise auf ein digitales Bahnsystem angewendet werden können. Hierbei wurden die häufigsten Angriffsszenarien vorgestellt, die

durch die OWASP [Kon17] ermittelt wurden. Diese reichen von Ausspähen von Nutzerdaten bis hin zur vollkommenen Übernahme des Zielsystems. Solche Angriffe müssen in Bahnanwendungen verhindert werden, da diese direkten Einfluss auf den Betrieb haben können. Sollte ein Angreifer in der Lage sein ein Steuersystem zu übernehmen, kann dieser Manipulationen mit nicht abschätzbaren Folgen verursachen. Diese reichen von Störungen im Betriebsablauf bis hin zur Kollision eines oder mehrerer Züge.

Das 4 Kapitel befasste sich mit dem Aufbau aktueller Bahnanlagen. Hierbei wurde detailliert auf den Aufbau der Stellwerksanalgen eingegangen. Sowie den Stellprozess, der durchgeführt werden muss, wenn ein Fahrdienstleiter eine Weiche oder ein Signal ändern möchte. Des Weiteren wurde die Funkkommunikation mitteln GSM-R erläutert. Über dieses separate Mobilfunknetz kann das Stellwerk in Kontakt mit den Zügen auf der Strecke treten und sogar durch Gruppengespräche mehrere Teilnehmer zur gleichen Zeit adressieren. Zusätzlich dazu gibt es einen Notfallkanal, der genutzt werden kann, um gefährdende Situation auf der Strecke zu melden. Des Weiteren wurden in diesem Kapitel aktuelle Bahnanlagen auf die Angreifbarkeit durch Cyberangriffe untersucht. Dabei zeigte sich, dass das Stellwerk dabei einen Flaschenhals bildet. Gelingt es einem Angreifer das Stellwerk zu übernehmen, dann kann ein gesicherter Betrieb nicht mehr garantiert werden.

Im folgenden Kapitel 5 wurde zunächst das gesamte aktuelle Konzept für Bahnanlagen in Frage gestellt und eine Alternative ohne Stellwerke vorgestellt. In dieser Variante gibt es nur Züge und Feldeinheiten. Züge, die eine Blockstrecke befahren möchten, müssen sich die Einfahrerlaubnis von einer zugehörigen Feldeinheit einholen und dürfen erst dann den Bereich befahren. Dieses Konzept ist jedoch sehr Störungsanfällig, da es nicht über einen globalen Zustand des Systems verfügt. Im Folgenden wurden dann zwei mögliche Architekturen erarbeitet, die sich in ihrem Grad mit dem sie mit der Außenwelt verbunden sind unterscheiden. Es handelt sich dabei um eine abgeschwächte Variante, die wieder über Stellwerke verfügt. Diese geben jedoch Funktionalität an die Feldeinheiten ab. Die Architekturen bieten neue Funktionen, die von aktuellen Systemen nicht unterstützt werden. Beispielsweise können Systemupdates der Sensoreinheiten (Feldeinheiten), die sich entlang der Strecke befinden über ein Fernupdate mit neuer Software versorgt werden. Eine weitere Neuerung ist die direkte Kommunikation des Zuges mit den Feldeinheiten. Auf diese Weise kann der Zug direkt kritische Informationen an die umliegenden Feldeinheiten weiter geben. Im Falle einer Störung können die Feldeinheiten direkt anliegende Streckenabschnitte sperren, um Zwischenfälle zu verhindern. Züge und Feldeinheiten müssen daher über funkbasierte Technologien kommunizieren können. Die erste

vorgestellte Architektur verbindet dafür direkt alle stationären Komponenten mit dem Internet. Dies bietet den Vorteil, dass alle Komponenten direkt angesprochen und mit Informationen versorgt, bzw. Informationen abgerufen werden können. Dieser Punkt ist zugleich ein großer Nachteil. Dadurch, dass alle Komponenten von überall ansprechbar sind können Angreifer direkt, die leistungsschwächeren Feldeinheiten angreifen.

Die zweite vorgestellte Architektur kapselt die Kommunikation mit der Außenwelt über das Stellwerkssystem. Das Stellwerk fungiert so als Gateway, dass die Kommunikation mit den Feldeinheiten sichern kann. Ein Nachteil dieser Architektur ist, dass die Datenlast an dem Stellwerk hoch ist. Somit ist das Stellwerk einfaches Ziel für „Denial of Service“-Angriffe.

Neben den bereits genannten Angriffsszenarien wurden im Kapitel 6 weitere Angriffe analysiert, die auf die vorgestellten Architekturen durchgeführt werden können. Hierbei wurden nicht nur Angriffe auf die Infrastruktur, wie „Denial of Service“ oder Angriffe auf Kommunikationsprotokolle berücksichtigt. Ferner wurden auch Angriffe direkt auf einzelne Komponenten in Betracht gezogen. Zusätzlich wurden Angriffsmöglichkeiten auf die Funkverbindung zwischen Zug und Feldeinheit aufgezeigt. Des Weiteren konnten für alle vorgestellten Angriffe passende Gegenmaßnahmen vorgeschlagen werden.

Im Kapitel 7 wurden die betrachteten Angriffe als Basis verwendet um geeignete Testansätze für diese Verwundbarkeiten zu identifizieren. Hierzu wurden bewährte Verfahren, wie das „Penetrations Testen“ vorgestellt, aber auch moderne Verfahren, wie statische Analyse. Ein besonderes Augenmerk wurde auf modellbasiertes Testen gelegt. Dieser Ansatz bietet die Möglichkeit bereits während der Designphase innerhalb der Entwicklung passende Modelle zu entwickeln, die das Sollverhalten des Systems abbilden können. Aus diesen Modellen können dann automatisch Testfälle generiert werden. Diese können dann nicht nur Safety-Eigenschaften prüfen, wie sie im CENELEC [CEN17] gefordert werden, sondern auch, wenn die Modelle erweitert werden auch Security-Eigenschaften prüfen.

Nach dieser Arbeit ergeben sich weitere offene Fragestellungen. Es könnte ein weiterer Blick auf modellbasierte Sicherheitsanalysen geworfen werden. Hierzu könnte untersucht werden, inwieweit Security Modelle aus den Anforderungen abgeleitet werden können und welche als Grundlage für weitere Security-Tests und Analysen genutzt werden können.

Des Weiteren könnte die Wechselwirkung von Safety- und Security-Eigenschaften genauer betrachtet werden. Hierzu wäre es sinnvoll detailliertere Analysen auf Basis von realen Bahnanwendungen durchzuführen. Dabei sollte unter anderem auch der Nutzen von Digitalisierung

gegen die neu entstehenden Risiken abgewogen werden. Ein solcher Schritt wäre jedoch nur in enger Zusammenarbeit mit Entwicklern von Bahnanwendungen möglich und sinnvoll.

Eine weitere Richtung ist der Transfer in eine andere Anwendungsdomäne. Die Fragestellung, die hierbei entsteht wäre, inwieweit sich Probleme und Erkenntnisse aus der Sicherheitsbetrachtung von Bahnanwendungen auf andere Bereiche wie die Kommunikation zwischen Fahrzeugen im Straßenverkehr, Luftfahrt oder in der Schifffahrt übertragen lassen.

Diese Arbeit konnte einen Einblick in die Digitalisierung von Zugsicherungssystemen geben. Dabei konnte aufgezeigt werden, dass es möglich ist auch weitgehende Veränderungen an den aktuell eingesetzten Systemen vorzunehmen. Jedoch muss bei jeder Änderung sorgfältig geprüft werden, welche neue Risiken entstehen und wie diese reduziert werden können.

Literaturverzeichnis

[Arn87] Dr.-Ing. Hans-Jürgen Arnold. *Eisenbahn-Sicherungstechnik*. transpress VEB Verlag für Verkehrswesen, 1987.

[Asp12] Aspect Security, Inc. *The Unfortunate Reality of Insecure Libraries*, 2012.

[Bah17] Deutsche Bahn. Db ergreift chancen der digitalisierung in allen dimensionen, March 2017. http://www.deutschebahn.com/de/Digitalisierung/DB_Digital/chancen.html.

[BDW02] Jürgen Bohn, Werner Damm, and Hartmut Wittke. Modeling and validating train system applications using statemate and live sequence charts. In *Integrated Design and Process Technology*, 2002.

[BM10] M.A. Beddoe and T.A. Maufer. Meta-instrumentation for security analysis, August 10 2010. US Patent 7,774,637.

[Bob08] Jonas Boberg. Early fault detection with model-based testing. In *Proceedings of the 7th ACM SIGPLAN Workshop on ERLANG*, ERLANG '08, pages 9–20, New York, NY, USA, 2008. ACM.

[Bun67] Bundesministeriums der Justiz. Eisenbahn-Bau- und Betriebsordnung (EBO). Technical report, Bundesministeriums der Justiz und für Verbraucherschutz, 1967.

[Bun03] Bundesamt für Sicherheit in der Informationstechnik. Durchführungskonzept für penetrationstests. Technical report, Bundesamt für Sicherheit in der Informationstechnik, 2003.

[Bun16a] Bundesamt für Sicherheit in der Informationstechnik. Ein Praxis-Leitfaden für IS-Penetrationstests. Technical report, Bundesamt für Sicherheit in der Informationstechnik, 2016.

[Bun16b] Bundesamt für Sicherheit in der Informationstechnik. Schutz kritischer infrastrukturen. Technical report, Bundesamt für Sicherheit in der Informationstechnik, 2016.

[Bun17a] Statistisches Bundesamt. Fachserie 8 Reihe 1.1 Verkehr, February 2017. https://www.destatis.de/DE/Publikationen/Thematisch/TransportVerkehr/Querschnitt/VerkehrAktuellPDF_2080110.pdf.

[Bun17b] Bundesamt für Sicherheit in der Informationstechnik. Bsi - technische richtlinie - kryptographische verfahren: Empfehlungen und schlüssellängen. Technical report, Bundesamt für Sicherheit in der Informationstechnik, 2017.

[Car15] Christopher Carr. Investigation report on the accident at santiago de cornpostela on 13 july 2013. Technical report, European Railway Aagency, 2015.

[CEN07] CENELEC. Standard: Cenelec - en 61025. Technical report, European Committee for Electrotechnical Standardization, 2007.

[CEN17] CENELEC. European committee for electrotechnical standardization, May 2017. https://www.cenelec.eu/.

[CFS+03] S. Chokhani, W. Ford, R. Sabett, C. Merrill, and S. Wu. Internet x.509 public key infrastructure certificate policy and certification practices framework. Technical report, IETF, 2003.

[CS16] Mariano Ceccato and Riccardo Scandariato. Static analysis and penetration testing from the perspective of maintenance teams. In *Proceedings of the 10th ACM/IEEE International Symposium on Empirical Software Engineering and Measurement*, ESEM '16, pages 25:1–25:6, New York, NY, USA, 2016. ACM.

[Deu08] Deutsche Bahn AG. Richtlinie 481 - telekommunikationsanlagen bedienen, modul 0201. Technical report, Deutsche Bahn AG, 2008.

[DIN03] DIN Deutsches Institut für Normung. DIN EN 50129 VDE 0831-129:2003-12 Bahnanwendungen - Telekommunikationstechnik, Signaltechnik und Datenverarbeitungssysteme - Sicherheitsrelevante elektronische Systeme für Signaltechnik. Technical report, Deutsche Industrie Norm, 2003.

[DIN12] DIN Deutsches Institut für Normung. Bahnanwendungen - telekommunikationstechnik, signaltechnik und datenverarbeitungssysteme - software für eisenbahnsteuerungs- und ueberwachungssysteme. Technical report, Deutsche Industrie Norm, 2012.

[Eic17] Ursula Eickhoff. Stellwerke und Sicherungstechnik. Pressemitteilung, May 2017. http://www.deutschebahn.com/presse/leipzig/de/hintergrund/themendienste/10779858/Stellwerke_Sicherungstechnik.html.

[End03] Dirk H. Enders. Bahn Praxis - Zeitschrift zur Förderung der Betriebssicherheit und der Arbeitssicherheit bei der DB AG. Print, June 2003. [Stand 17.03.2017] https://www.uv-bund-bahn.de/fileadmin//Dokumente/Publikationen/BahnPraxis_B/BahnPraxisB-2003_06.pdf#page=6.

[Ent16] Valgrind Entwickler. Valgrind, 2016. http://valgrind.org.

[Esh12] Col. David Eshel. Hezbollah's intelligence war, May 2012.

[Eur10] European Committee for Electrotechnical Standardization. Cenelec - en 50159 railway applications - communication, signalling and processing systems - safety-related communication in transmission systems. Technical report, European Committee for Electrotechnical Standardization, 2010.

[e.V17] StellwerkSim Betriebs-Verein e.V. Hamburg - schleswig-holstein: Hamburg eidelstedt, April 2017. http://www.stellwerksim.de/shot/see_796.jpeg.

[Fen07] Professor Dr.-Ing. Lothar Fendrich. *Handbuch Eisenbahninfrastruktur*. Springer-Verlag Berlin Heidelberg, 2007.

[FNT03] Wolfgang Fenner, Peter Naumann, and Jochen Trinckauf. Bahnsicherungstechnik - steuern, sichern und Überwachen von fahrwegen und fahrgeschwindigkeiten im schienenverkehr. Technical report, Siemens, 2003.

[Gar17] Ross Gardler. Apache software foundation, June 2017. http://apache.org/.

[GBF16] Jasmin Guth, Uwe Breitenbücher, and Michael Falkenthal, editors. *Comparison of IoT platform architectures: A field study based on a reference architecture*. IEEE, Cloudification of the Internet of Things (CIoT), November 2016.

[GLY14] Kanika Grover, Alvin Lim, and Qing Yang. Jamming and anti–jamming techniques in wireless networks: a survey. *International Journal of Ad Hoc and Ubiquitous Computing*, 17(4):197–215, 2014.

[HB95] H. Heller and W. Bachmann. Verfahren zum synchronisierten betrieb eines aus mehreren rechnern bestehenden verteilten datenverarbeitungssystems und einrichtung zur anwendung des verfahrens, August 31 1995. WO Patent App. PCT/-DE1995/000,174.

[HSNB13a] Istvan Haller, Asia Slowinska, Matthias Neugschwandtner, and Herbert Bos. Dowser: A guided fuzzer for finding buffer overf low vulnerabilities. In *;login:*, December 2013.

[HSNB13b] Istvan Haller, Asia Slowinska, Matthias Neugschwandtner, and Herbert Bos, editors. *Dowsing for Overflows: A Guided Fuzzer to Find Buffer Boundary Violations*, 22. USENIX, USENIX Association, Berkeley, California, U.S. A, August 2013.

[HVO06] William G Halfond, Jeremy Viegas, and Alessandro Orso. A classification of SQL-injection attacks and countermeasures. In *Proceedings of the IEEE International Symposium on Secure Software Engineering*, volume 1. IEEE, 2006.

[IBM04] IBM. Rational purifyplus, 2004. http://www-306.ibm.com/software/awdtools/purifyplus.

[IEC13] IEC. IEC 62443-3-3 Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels. Technical report, International Electrotechnical Commission (IEC), 2013.

[IEE02] IEEE STANDARD. 802.15.1-2002 - ieee standard for telecommunications and information exchange between systems - lan/man - specific requirements - part 15: Wireless medium access control (mac) and physical layer (phy) specifications for wireless personal area networks (wpans). Technical report, IEEE, 2002.

[IEE12a] IEEE STANDARD. 1703-2012 - ieee standard for local area network/wide area network (lan/wan) node communication protocol to complement the utility industry end device data tables. Technical report, IEEE, 2012.

[IEE12b] IEEE STANDARD. Ieee 802.11 wireless local area networks. Technical report, IEEE, 2012.

[IEE15] IEEE STANDARD. 802.3-2015 - ieee standard for ethernet. Technical report, IEEE Computer Society, 2015.

[Int14] International Organization for Standardization. ISO/IEC 14882:2014 Information technology – Programming languages – C++. Technical report, ISO, 2014.

[ISO94a] ISO/IEC JTC 1 Information technology. Iso/iec 7498-1:1994. Technical report, International Organization for Standardization, 1994.

[ISO94b] ISO/IEC JTC 1 Information technology. Iso/iec 8822:1994 information technology – open systems interconnection – presentation service definition. Technical report, International Organization for Standardization, 1994.

[ISO96] ISO/IEC JTC 1 Information technology. So/iec 8326:1996 information technology – open systems interconnection – session service definition. Technical report, International Organization for Standardization, 1996.

[ITU11] ITU-T. Itu-t z.120 (02/2011). Technical report, TU-T Study Group 17, 2011.

[JMT08] Jacques Julliand, Pierre-Alain Masson, and Regis Tissot. Generating security tests in addition to functional tests. In *Proceedings of the 3rd International Workshop on Automation of Software Test*, AST '08, pages 41–44, New York, NY, USA, 2008. ACM.

[jT17] jQuery Team. Jquery, June 2017. https://jquery.com/.

[Kal00] B. Kaliski. Password-based cryptography specification. Technical report, IETF, 2000. http://www.ietf.org/rfc/rfc2898.txt.

[KL16] Anne Kramer and Bruno Legeard. *Model-Based Testing Essentials - Guide to the ISTQB Certified Model-Based Tester - Foundation Level.* John Wiley & Sons, 2016.

[Kon17] Matt Konda. The open web application security project, May 2017. https://www.owasp.org/.

[Kus84] Wolfgang Kusche. *Gleisbildstellwerke (Reihe Stellwerks- und Blockanlagen).* transpress VEB Verlag für Verkehrswesen, 1984.

[Lap14] Jean-Claude Laprie. *Dependability: Basic Concepts and Terminology.* Springer-Verlag KG, 2014.

[LBX16] Yuhong Li, Fredrik Björck, and Haoyue Xue, editors. *IoT Architecture Enabling Dynamic Security Policies*, volume 4. nternational Conference on Information and Network Security, ACM, 2016.

[LEKO15] N. Sorninand M. Luis, T. Eirich, T. Kramp, and O.Hersent. Lorawan specification. Technical report, LoRa Alliance, 2015.

[M.A12] M.Aigner. Stelltisch drs, hütteldorf, October 2012. http://www.hmmueller.de/VonAnderen_x560/PA090022.JPG.

[Mas15] Ulrich Maschek. *Sicherung des Schienenverkehrs - Grundlagen und Planung der Leit- und Sicherungstechnik*. Vieweg+Teubner Verlag, 2015.

[Mat17] John Matherly. Heartbleed report (2017-01). Technical report, Shodan, 2017.

[McK84] Alex McKenzie. Iso transport protocol specification. Technical report, IETF, 1984.

[MCM11] Anderson Morais, Ana Cavalli, and Eliane Martins. A model-based attack injection approach for security validation. In *Proceedings of the 4th International Conference on Security of Information and Networks*, SIN '11, pages 103–110, New York, NY, USA, 2011. ACM.

[Mew09] Kirsten Mewes. *Domain-specific Modelling of Railway Control Systems with Integrated Verification and Validation*. PhD thesis, Universität Bremen, 2009.

[Mie17] Uwe Miethe. Betriebszentrale münchen. Bereitgestellt von der DB Pressestelle, June 2017.

[Mit17a] Mitre. Cve-2014-0160, June 2017. https://cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2014-0160.

[Mit17b] Mitre. Cve-2017-0144 (wanna cry), 2017. https://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0144.

[Mit17c] Mitre. Cwe-287: Improper authentication, March 2017. http://cwe.mitre.org/data/definitions/287.html.

[Mit17d] Mitre. Cwe-384: Session fixation, March 2017. http://cwe.mitre.org/data/definitions/384.html.

[MIT17e] MITRE. CWE-665: Improper Initialization, June 2017. https://cwe.mitre.org/data/definitions/665.html.

[Moc87a] P. Mockapetris. Rfc 1034 domain names - concepts and facilities. Technical report, IETF, 1987.

[Moc87b] P. Mockapetris. Rfc 1035 domain names - implementation and specification. Technical report, IETF, 1987.

[MWF02] P. Murphy, E. Welsh, and J.P. Frantz. Using bluetooth for short-term ad hoc connections between moving vehicles: a feasibility study. In *Vehicular Technology Conference, 2002. VTC Spring 2002. IEEE 55th*, 2002.

[MyS17] MySQL. Mysql 5.7 reference manual, June 2017. https://dev.mysql.com/doc/refman/5.7/en/resetting-permissions.html.

[Pac11] Jörn Pachl. Deadlock avoidance in railroad operations simulations. In *90th Annual Meeting des Transportation Research Board in Washington DC*, 2011.

[Pac13] Prof. Dr.-Ing. Jörn Pachl. *Systemtechnik des Schienenverkehrs*. Springer Vieweg, 2013.

[Per15] Evan Perez. Fbi: Hacker claimed to have taken over flight's engine controls, May 2015. [Stand 01.06.17] http://edition.cnn.com/2015/05/17/us/fbi-hacker-flight-computer-systems/index.html.

[Pos81] Jon Postel. Internet protocol. Technical report, IETF, 1981.

[PR88] J. Postel and J. Reynolds. A standard for the transmission of ip datagrams over ieee 802 networks. Technical report, Internet Engineering Task Force (IETF), 1988.

[Res00] E. Rescorla. RFC 2818 - HTTP Over TLS. Technical report, IETF, 2000.

[Sch10] Edward J. Schwartz. All you ever wanted to know about dynamic taint analysis and forward symbolic execution (but might have been afraid to ask). In , June 2010.

[SDP08] Vineet Saini, Qiang Duan, and Vamsi Paruchuri. Threat modeling using attack trees. *J. Comput. Sci. Coll.*, 23(4):124–131, April 2008.

[sIg17] solid IT gmbh. Db-engines ranking, June 2017. https://db-engines.com/de/ranking.

[SJT08] Karen Scarfone, Wayne Jansen, and Miles Tracy. Special publication 800-123 guide to general server security. Technical report, National Institute of Standards and Technology, 2008.

[SLN04] Sankalp Singh, James Lyons, and David M. Nicol. Fast model-based penetration testing. In *Proceedings of the 36th Conference on Winter Simulation*, WSC '04, pages 309–317. Winter Simulation Conference, 2004.

[Spi17] Spiegel Online. Erpressersoftware: 450 computer der bahn von "wannacryvirus betroffen. *Spiegel*, 2017. Stand 08.08.2017http://www.spiegel.de/netzwelt/web/wannacry-450-bahn-computer-von-cyber-attacke-betroffen-a-1147922.html.

[SS15] Evgeniy Stepanov and Konstantin Serebryany. Memorysanitizer: fast detector of uninitialized memory use in c++. In *Proceedings of the 2015 IEEE/ACM International Symposium on Code Generation and Optimization (CGO)*, pages 46–55, San Francisco, CA, USA, 2015.

[STA90] BRITISH STANDARD. Iec 1025 - reliability of systems, equipment and components - guide to fault tree analysis. Technical report, IEC, 1990.

[Sto96] Neil Storey. *Safety-critical Computer Systems*. Addison Wesley Longman, 1996.

[TDM08] Ari Takanen, Jared DeMott, and Charlie Miller. *Fuzzing for Software Security Testing and Quality Assurance*. Artech House, 2008.

[Tea17] CAPEC Content Team. Capec-457: Usb memory attacks, May 2017.

[ulz13] ulz/AFP/AP. Zugunglück in Spanien. *Spiegel Online*, July 2013. [Stand 17.03.2017] http://www.spiegel.de/panorama/justiz/zugunglueck-in-spanien-lokfuehrer-telefonierte-beim-crash-a-913.html.

[Uni15] Unified Modeling Language . Omg unified modeling language tm (omg uml). Technical report, OMG, 2015.

[ver17] verzetsmuseum. Cooperate?, June 2017. https://www.verzetsmuseum.org/museum/en/tweede-wereldoorlog/kingdomofthenetherlands/thenetherlands/thenetherlands-may_1940_-_february_1941/cooperate.

[VG81] W.E. Vesely and F.F. Goldberg. Fault tree handbook (nureg-0492). Technical report, U.S. Nuclear Regulatory Commission, January 1981.

[VSC16] Raghav Vadehra, Manjit Singh, and Nitika Chowdhary. Analysis of countermeasures for ddos attacks and evaluation of entropy based detection mechanism using ns2. , 2016.

[W3T17] W3Techs. Usage of web servers broken down by ranking, June 2017. https://w3techs.com/technologies/overview/web_server/all.

[Zei16] Zeit. Bad Aibling: Was wir über das Zugunglück wissen, February 2016. http://www.zeit.de/gesellschaft/zeitgeschehen/2016-02/bad-aibling-zugunglueck-hintergruende.

[Zho17] Weilin Zhong. Development guide: Configuration, June 2017. https://www.owasp.org/index.php/Configuration.

Hiermit versichere ich, dass ich die vorliegende Arbeit ohne fremde Hilfe selbständig verfasst und nur die angegebenen Hilfsmittel benutzt habe.

Hamburg, 29. August 2017 Torge Hinrichs