Safety und Security – zwei Sicherheitsaspekte im Widerspruch?

Safety and Security – two aspects in contradiction?

Barbara Streimelweger
Stragere Management Consulting e.U., A-3071 Böheimkirchen, Austria, b.streimelweger@stragere.at

Wolfgang Sturzeis
A-1160 Wien, Austria, wolfgang.sturzeis@hotmail.com

Kurzfassung

Wir leben in einem Zeitalter, das hochtechnologisch fortgeschritten ist. Daher ist es nur selbstverständlich, dass wir Menschen nach „Sicherheit“ streben, sei es im Alltag wenn wir mit der Bahn oder dem Auto unterwegs sind, Maschinen bedienen oder uns im Internet bewegen. Aber auch Begrifflichkeiten wie Sicherheit und Risiko unterliegen dem Wandel der Zeit. Über einen Ausflug zu den historischen Anfängen der Betrachtung sicherheitskritischer Aspekte übergeleitet zu den heute bekannten Methoden des Sicherheitsmanagements sowie der Divergenzen in der Begrifflichkeit Sicherheit – Safety –Security wird der technologische Fortschritt und Wandel aufgezeigt.

Abstract

Today we live in a highly advanced technologized era. Therefore it is only common that people strive for safety be it during everyday life while driving with a car or taking the train, using a machine or while surfing the net. However, even terms such as safety and risk are subject to the changing times. Taking a trip back to the historical beginnings of the assessment of safety critical aspects forth to the introduction of today´s known methods of safety management as well as the development of the terminologies Safety and Security, the technological progress and change will be demonstrated.

Publiziert in:
eb - Elektrische Bahnen
Ausgabe 11/2015
www.eb-info.org

1. Einleitung

In hochsicherheitstechnischen sowie hochsicherheitskritischen Bereichen wie Energie, Bahn, Flugsicherung, Seefahrt oder Gesundheitswesen befassen wir uns mit unterschiedlichsten Sicherheitsaspekten.

Im Bereich Bahn beziehungsweise für Bahnsysteme wie es gemäß der Norm EN 50126 [1] heißt, ist von einer gemeinsamen Sicherheitsmethode (Common Safety Method, CSM) zu Folge der Richtlinie für Eisenbahnsicherheit 2004/49/EG [2] die Rede, welche vor allem darauf abzielt, eine vergleichbare Ebene zur Bewertung der auftretenden Risiken/Gefahren im Bereich der Bahnsysteme zu erreichen. Im Bereich des Gesundheitswesens ist eines dieser Hauptziele zur Vergleichbarkeit die Patientensicherheit. Die Frage, die sich in diesem Zusammenhang stellt, ist, von welcher Sicherheit ist hier die Rede? Im Englischen unterscheidet man beim Begriff Sicherheit zwischen Safety und Security, welche gemäß ihrer Bedeutung gravierende Unterschiede aufweisen, und hier genauer herausgearbeitet werden.

Wir sind heutzutage von sozio-technischen Systemen umgeben, wobei je nach Branche der soziale oder technische Systemanteil überwiegt. Trendentwicklungen wie Industrie 4.0 oder M2M (Machine-to-Machine) zeigen, wie viele unserer Prozesse und Arbeitsschritte automatisiert werden und wie in diesem Zusammenhang der Softwareanteil an Produkten steigt und weiterhin steigen wird. Eine Frage die dadurch verstärkt in den Vordergrund tritt: Ist es heute noch ausreichend, Safety und Security für sich zu betrachten? Oder wäre es an der Zeit, Safety als auch Security aus einer Gesamtperspektive heraus zu betrachten und gegebenenfalls so weit zu gehen, diese zu harmonisieren?

Im Folgenden wird der Aspekt Sicherheit einst und jetzt sowie die Sichtweise auf Risiken erörtert. Die Begriffe Safety und Security werden abgegrenzt und deren rechtliche Rahmenbedingungen kurz dargestellt. Anhand von Fallbeispielen wird aufgezeigt, wie nahe Safety und Security beieinander liegen können. Des Weiteren werden bekannte Methoden angeführt, wie sie auch im Rahmen von CSM Anwendung finden, und wie diese bei der Entscheidungsfindung helfen können, ob „vorwiegend“ ein Safety oder Security Problem vorliegt und wie damit umzugehen ist. Die abschließende Diskussion soll dazu anregen, sich mit der Fragestellung auseinanderzusetzen, ob es in der heutigen Zeit unter Anbetracht der oben angeführten Punkte ausreicht, ein System ausschließlich hinsichtlich des Safety oder Security Aspektes zu betrachten oder ob eine erweiterte Betrachtung, welche sich auf beide Systeme bezieht sowie einen "Vergleich" dieser möglich macht, für die Zukunft angebrachter wäre. Dies bezieht sich vor allem darauf, dass wir derzeit auf Vorgaben und Methoden zurückgreifen, welche sich vorwiegend mit einem dieser Bereiche beschäftigen beziehungsweise welche zu Folge der Systemabgrenzung nur den Safety beziehungsweise Security Bereich betrachten müssen. In Folge dessen müsste allerdings auch die Folgewirkung etwaiger Fehler sowie Auswirkungen der Fehler auf ein Safety beziehungsweise Security System, welches dahinterliegt, betrachtet werden, oder nicht?

2. Sicherheit einst und jetzt

Sicherheit ist für uns Menschen eines der grundlegendsten Bedürfnisse, dies erkannte auch der amerikanische Psychologe Abraham Maslow, der in seiner Bedürfnispyramide Sicherheit bereits auf die 2. Stufe nach den Grundbedürfnissen stellte. Einerseits streben wir nach persönlicher und materieller Sicherheit, andererseits fordern wir permanent Sicherheit ein, beispielsweise wenn wir in einen Zug oder in ein Flugzeug steigen oder wenn wir einfach eine Maschine bedienen. Dass wir keinen Schaden an uns erfahren wollen, ist einerseits durch die stetige Entwicklung unserer gesellschaftlichen sowie technischen Strukturen beeinflusst, andererseits orientieren wir uns am sogenannten "Stand der Technik".

Doch von welcher Sicherheit ist hier die Rede? Sicherheit im Sinne von Safety oder Sicherheit im Sinne von Security? Im deutschsprachigen Raum wird selten bis kaum eine Unterscheidung zwischen Safety und Security getroffen, wir sprechen im Allgemeinen von Sicherheit. Der angloamerikanische Sprachraum hingegen differenziert strikt zwischen Safety und Security. Daher fällt es in unserem Sprachraum oftmals sehr schwer, eine klare Trennung beider Sicherheitsaspekte zu treffen, das in Folge zu Missverständnissen und abweichenden Ansichten hinsichtlich zu erfüllender Anforderungskriterien führen kann. Im Deutschen könnte man Safety mit *Betriebssicherheit* und Security mit *Angriffssicherheit* übersetzen und so eine Differenzierung schaffen.

Von der Industriellen Revolution 2.0 zum Zeitalter der Digitalisierung und IoT (Internet of Things)

Mit dem Beginn der Industrialisierung im 19. Jahrhundert, bekannt als die Industrielle Revolution 2.0, kam es erstmalig zu einem Umdenken hinsichtlich der Begriffe Risiko und Sicherheit im Sinne von Safety. Die Signifikanz von Risiken hat sich über die letzten Jahrzehnte hindurch drastisch geändert, “Until the first decades of the 19th century, risks were accepted as more or less natural in the sense that they were directly associated with human

activity rather than with failures of systems or equipment" [3]. Heute sprechen wir von System Safety und wissen, wie wichtig es ist, Risiken beziehungsweise Hazards rechtzeitig zu erkennen und Maßnahmen zur Minimierung einzuleiten um ein höchst mögliches Maß an Sicherheit gewährleisten zu können.

Mit der Industrialisierung änderte sich auch die Sichtweise auf Unfälle, und "… accidents became associated with the technological systems that people designed, built, and used as part of work, in the name of progress and civilisation" [1]. Jeder größere Unfall in der Geschichte, wie beispielsweise Nine-Eleven (2001), Three Mile Island Nuklear Reaktor Unfall (28. März 1979), Challenger Space Shuttle Explosion (Jänner 1986), King's Cross Underground Fire (18 November 1987), Piper Alpha Explosion, Clapham Bahnunglück, Exxon Valdez Ölverschmutzung (23. März 1989), Kegworth Flugzeugabsturz (8 January 1989), TMI (1979), Chernobyl (1986), usw. führte zu einem Umdenken hinsichtlich Risiko Management und Safety [4], [3]. Dies resultierte unter anderem in neuen und verbesserten Risiko Assessment Methoden, in neuen Standards, in nationalen und internationalen Vorgaben sowie in der Gründung spezifischer Aufsichtsorgane und Aufsichtsbehörden.

Heute stecken wir mitten in der Industrie 4.0, die unter anderem gekennzeichnet ist durch ihre Digitalisierung oder dem Trend M2M (Machine-to-Machine). Mit dem Zeitalter der Digitalisierung kam jedoch ein neuer Sicherheitsaspekt hinzu, besser bekannt als Security. Das ICS-CERT[1] (Department of Homeland Security, US) beispielsweise berichtet 2013 von 256 Zwischenfällen, sogenannten Incidents. Die Mehrheit dieser Zwischenfälle wurde in Netzwerken kritischer Infrastrukturen von Organisationen entdeckt, so zum Beispiel im Energie Sektor (59%), im Bereich kritischer Produktionen (20%), Transport (5%) oder in der Logistik [5]. Hinzu kommt, dass Security heute als "...a serious concern to safety-critical applications" [5] gesehen wird.

Paradigmenwechsel der Begrifflichkeiten Risiko und Sicherheit

Um diesen Paradigmenwechsel, den das Umdenken der Begrifflichkeiten Risiko und Sicherheit mit sich brachte, besser verstehen zu können, ist eine Betrachtung der geschichtlichen Entwicklung im Rahmen der Industrialisierung sowie der ersten automatischen Abläufe durchaus sinnvoll.

Einer der ersten automatischen Abläufe, welcher unter die Begrifflichkeit Automatisierung fällt und auch als ein solcher bezeichnet werden kann, war die Funktion einer Windmühle. Hierbei wird im Wesentlichen die Kraft des Windes dahingehend verwendet entsprechende Massen, in diesem Fall Mahlsteine, zu bewegen und damit Getreide zu mahlen. Eine Weiterentwicklung im Rahmen der Komplexität war der erste Webstuhl, welcher im Rahmen der Industrialisierung sowie der damit verbundenen Massenproduktion auftrat. Grundsätzlich sind diese zwei Errungenschaften für den Menschen von enormer Bedeutung. Im Rahmen der Thematik Safety versus Security ist allerdings schnell klar, dass es sich hierbei nur um Safety bezogene Systeme handeln kann, da die Abläufe dieser zwei Maschinen ausschließlich über mechanische Funktionen gewährleistet wurden und nicht eigenständig durch ein Programm gesteuert werden konnten.

Dies änderte sich jedoch mit der Einführung des ersten industriell funktionstüchtigen Computers. Eines der besten Beispiele hierfür ist die Luftfahrt. Die grundsätzliche Steuerung der ersten Flugzeuge basierte auf einem mechanischen System, wo über Hebel und Drähte die entsprechenden Höhen- und Seitenruder, sowie die weiteren Funktionen des Flugzeuges gesteuert wurden. Im Rahmen der ersten Mondlandung wurden erstmals die Steuerbefehle einer "Flugmaschine", in diesem Fall der Landekapsel Apollo, durch einen Computer übertragen. Dies führte zur Entwicklung der Steuerung der heutigen Flugzeuge, bekannt als Fly-by-Wire.

Bei Fly-by-Wire erfolgt die Flugzeugsteuerung im Grunde genommen so, dass die Eingabe zur Steuerung des Flugzeuges über den Steuerknüppel erfolgt und diese Eingaben werden dann von einem Computer interpretiert und entsprechend umgesetzt.

Anhand dieser technischen Entwicklung ist klar zu erkennen, dass sicherheitstechnische Kriterien, welche damals bezogen auf mechanische Abläufe betrachtet wurden, heute immer mehr in Richtung computergestützte bzw. sogar Computer gesteuerte Abläufe übergehen und damit den Security Aspekt in ein System miteinbringen.

Sicherheitsdenken heute

Sicherheitsdenken und Sicherheitsbedenken gibt es überall. Heute treffen wir auf Probleme wie mangelnde Kompetenz in einzelnen Fachbereichen. Es gibt eine Vielzahl an Regulatorien wie nationale und internationale Richtlinien, Standards und Frameworks, die helfen sollen, Sicherheit zu gewährleisten. Jedoch führen uneinheitlich geltende Regeln unter anderem zu Konflikten zwischen Safety und Security, was wiederum zu gemäß Vorgaben umgesetzten und damit verbundenen bekannten Verletzungen von Richtlinien führt [5].

[1] ICS-CERT - Department of Homeland Security http://www.dhs.gov; ICS - Industrial Control System, CERT - Computer Emergency Response Team

Personen, die für die Umsetzung von Risk Management sowie von Safety und Security und in Folge von Sicherheits-Management-Systemen verantwortlich sind, werden oftmals mit Aussagen konfrontiert, dass hier lediglich Kosten versursacht werden oder der den Kosten gegenüberstehende Nutzen einfach zu gering sei. Die Norm ISO 31000 sieht „Risk Management als Garant für Wertezuwachs“ [6], so ist „Risikomanagement schafft und schützt Werte“ einer der Grundsätze der ISO 31000 [7]. Dieser Wertezuwachs kann beispielsweise durch Safety und Security, Compliance (Einhaltung von gesetzlichen und regulatorischen Vorschriften), Umweltschutz, menschliche Gesundheit, Qualitätssicherung, Projektmanagement, aber auch durch gute Führung (Governance) und Reputation [7], [6] erreicht werden.

3. Gemeinsame Sicherheitsmethode für Eisenbahnsicherheit

Im Bereich Bahn und Bahnsysteme wird eine gemeinsame Sicherheitsmethode (CSM) gemäß der Richtlinie für Eisenbahnsicherheit 2004/49/EG [2] gefordert. Die Anforderungen an diese Common Safety Method (CSM) sind in der CSM-Verordnung gemäß der Verordnung (EG) Nr. 352/2009 [8] bzw. in der nachfolgenden Durchführungsverordnung (EU) Nr. 402/2013 [9] beschrieben. Verwenden wir den englischen Begriff, wird sehr schnell klar, dass es sich um eine gemeinsame Sicherheitsmethode im Sinne von Safety handelt. Dies lässt jedoch folgende Fragestellungen aufkommen:

- Inwieweit finden bei CSM Security Aspekte Berücksichtigung?
- Werden hier bereits Maßnahmen hinsichtlich Cyber Safety und Cyber Security, zwei neue beobachtbare Entwicklungen, gesetzt?

Bevor wir uns im Folgenden dieser Fragestellung widmen, eine Abgrenzung der Begriffe Safety und Security und den dahinter liegenden bekannten Regulatorien.

3.1. Safety versus Security

Eine klare Abgrenzung zwischen Safety und Security ergibt sich unter anderem bereits aus dem Anwendungsgebiet (Abbildung 1). Im Sinne von *Safety* beziehungsweise Safety Management versucht man die Gefährdung, welche durch einen oder mehrere Fehler beziehungsweise Hazards, sowie möglicher zusammenhängender Abläufe hervorgerufen wird und das damit verbundene entstehende Risiko sowie dessen Ausmaß, auf ein vertretbares Maß zu reduzieren. Risiken können lediglich reduziert und nie zu 100 % vermieden werden, dessen muss man sich bewusst sein. Betrachtet man allerdings *Security* geht es hierbei vor allem darum, das Innere eines Systems gegen Angriffe von außen aber auch von innen zu schützen, so dass die daraus entstehenden Fehler beziehungsweise Hazards keinen Einfluss auf das System selbst haben können.

Safety beispielsweise bezieht sich vor allem darauf, ein System an sich am Laufen zu halten und mögliche Fehler beziehungsweise auftretende Hazards soweit abzuschwächen, sodass ein gravierender Ausfall des Systems unwahrscheinlich scheint. Der Security Teil dient hierbei vor allem dazu, das System vor möglichen Angriffen von außen und damit vor zusätzlich auftretenden Fehler beziehungsweise Hazards zu schützen.

Wie erwähnt steigt durch Industrie 4.0 aber auch durch M2M der Software-Anteil in unseren Systemen. Hier können Security-kritische Aspekte durchaus zu Auswirkungen auf die Systemsicherheit im Sinne von Safety führen, so auch im Eisenbahnwesen beispielsweise beim Einsatz von ETCS (European Train Control System) oder im Bereich Signaltechnik oder Leit- und Sicherungstechnik (siehe dazu Absatz 5.3).

Nach ISO/IEC 25010 bedeutet *Security* der *Schutz der Informationen vor unbefugten Zugriff*: “The capability of the software product to protect information and data so that unauthorised persons or systems cannot read or modify them and authorised persons or systems are not denied access to them” [10]. *Safety* steht für den S*chutz der Umwelt vor den Ergebnissen der Software*: “The capability of the software product to achieve acceptable levels of risk of harm to people, business, software, property or the environment in a specified context of use” [10].

Der Zusammenhang von System Safety und System Security hinsichtlich Verfügbarkeit (availability) einzelner Funktionen für befugte Beteiligte ist in Abbildung 1 skizziert.

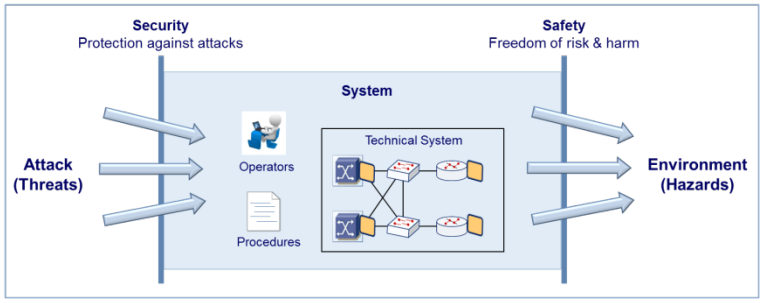

Abbildung 1: System Safety & System Security [5]

3.2. Safety – Begriffserklärung und Rahmenbedingungen

Die International Civil Aviation Organization[2] (ICAO) beschreibt Safety als “the state in which the possibility of harm to persons or of property damage is reduced to, and maintained at or below, an acceptable level through a continuing process of hazard identification and safety risk management.”

Im Eisenbahnwesen ist Sicherheit im Sinne von Safety nach EN 50126 definiert als “das Nichtvorhandensein eines unzulässigen Schadensrisikos“ [1] beziehungsweise als „freedom from unacceptable risk of harm“ [11], wobei Risiko definiert ist als „die Wahrscheinlichkeit des Auftretens einer Gefahr, die einen Schaden verursacht, sowie der Schweregrad eines Schadens“ [1] beziehungsweise „the probable rate of occurrence of a hazard causing harm and the degree of severity of the harm” [11]. Unter Gefahr versteht man “eine physikalische Situation, die potentiell einen Schaden für den Menschen beinhaltet“ [1] beziehungsweise unter Hazard „a physical situation with a potential for human injury“ [11].

Beziehen wir uns im Konkreten auf die Eisenbahnsicherheit, so ist, wie erwähnt, in der Richtlinie über die Eisenbahnsicherheit 2004/49/EG Artikel 6 von Anforderungen an gemeinsame Sicherheitsmethoden [2] zu lesen. Hierzu gibt es die CSM Durchführungsverordnung(EU) Nr. 402/2013 [9], welche mit Mai 2015 die CSM Verordnung(EG) Nr. 352/2009 [8] abgelöst hat. Diese Verordnung soll unter anderem den Zugang zum Markt für Schienenverkehrsdienste durch eine Harmonisierung der Risikomanagementverfahren erleichtern, die zur Bewertung der Auswirkungen von Änderungen auf das Sicherheitsniveau und die Erfüllung der Sicherheitsanforderungen angewandt werden [8]. Es fällt auf, dass hier von Sicherheit im Sinne von Safety die Rede ist. Die Komplexität von Systemsicherheit (System Safety) wächst bekanntlich. Das Hauptanliegen hierbei ist das Managen von Risiken beziehungsweise Gefahren (Hazards), die mittels entsprechender Analysemethoden sowie Design und Management Verfahren identifiziert, evaluiert, vermieden beziehungsweise minimiert und kontrolliert werden können. Im Rahmen von CSM greift man auf gemeinsam definierte Common Safetey Indicators (CSI) zurück, die wiederum einen EU-weiten Vergleich von Unfällen gestatten.

Zusätzlich für Bahnanwendungen und ortsfeste Anlagen kann bei Fragen rund um Sicherheit die Technische Spezifikation CLC/TS 50562 herangezogen werden, welche Prozesse, Maßnahmen und eine Nachweisführung für die Sicherheit in der Bahnstromversorgung spezifiziert [12]. Zufolge dieser Technischen Spezifikation muss eine Gefährdungsermittlung durchgeführt werden, die zu einer Auflistung der Gefährdungen führt, welche im Zusammenhang mit dem elektrischen Bahnenergieversorgungssystem stehen. Hierzu wird eine Liste übergeordneter Hazards vorgegeben und es ist zu evaluieren und zu überprüfen, welche dieser Hazards zutreffend sind oder nicht.

Zur Bewältigung einzelner Safety Belange nutzt man den systematischen Ansatz von Safety Management Systemen (SMS), welche auch Aspekte wie erforderliche Organisationsstrukturen, Verantwortlichkeiten, Richtlinien und Verfahren berücksichtigen.

3.3. Security – Begriffserklärung und Rahmenbedingungen

Das Center for Research on Information Systems der University of Texas führte in den 2010er Jahren eine Studie zum Thema Informationssicherheit durch und kam zu dem Schluss: „50 Prozent aller Firmen, die wichtige Daten bei einer Katastrophe verloren haben, konnten sich nie davon erholen und 90 Prozent jener Firmen mussten in der Folge innerhalb von zwei Jahren ihre Geschäftstätigkeit aufgeben."

[2] ICAO - International Civil Aviation Organization: http://www.icao.int

Wenn es um das Management von Informationen geht, werden sehr hohe Anforderungen an Integrität (integrity, Richtigkeit und Vollständigkeit der Daten), Verfügbarkeit (availability, Daten für Befugte verfügbar, zugreifbar und brauchbar machen), Vertraulichkeit (confidentiality, Daten sind ausschließlich für Befugte verfügbar) sowie Datensicherheit (data security) gestellt. Hier sprechen wir von Sicherheit im Sinne von Security. Auch hier gibt es Regulatorien wie Richtlinien hinsichtlich Compliance und Standards wie beispielsweise Standards zur IT-Sicherheit (Normenreihe ISO 27000[3]) oder für das IT Service Management (ITSM, Normenreihe ISO 20000[4]) sowie Best Practice Modelle beziehungsweise Frameworks wie CoBIT[5] oder ITIL[6].

Informationssicherheit (Information Security, IS) bedeutet im Sinne der ISO 27001 die „Aufrechterhaltung der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen; andere Eigenschaften wie Authentizität, Zurechenbarkeit, Nichtabstreitbarkeit und Verlässlichkeit können ebenfalls berücksichtigt werden“ [13].

3.4. Safety versus Security – Gemeinsamkeiten und Unterschiede

Sowohl Safety als auch Security verfolgen einen prozess-orientierten Ansatz und folgen einem definierten Lebenszyklus (Absatz 4.2). Bereits in frühen Entwurfsphasen sollte berücksichtigt werden, welche Funktionen umgesetzt werden, welche sozusagen ein „must“ und welche lediglich „nice to have“ sind, da jegliche spätere Ergänzungen, sogenannte Add-ons, hinsichtlich der Erfüllung von Sicherheitsanforderungen gemäß Safety beziehungsweise Security kostspielig werden können. Zusätzliche technische und finanzielle Aufwendungen sollten nur dann getätigt werden, wenn sie auf lange Sicht einen entsprechenden Nutzen darstellen. Eine weitere Gemeinsamkeit von Safety und Security ist der Risk Assessment basierende Ansatz, wobei Risiken sowie Restrisiken evaluiert werden, eine entsprechende Kategorisierung vorgenommen wird (wie Risikokategorien und Risikolevel) sowie Maßnahmen zur Herabsetzung von Risiken erfolgt. Eine Einführung und einen Überblick hinsichtlich Risk Assessment und Methoden finden Sie in Absatz 4.3.

Ein wesentlicher Unterschied zwischen Safety und Security ist jedoch die Tatsache, dass es heute keinen gemeinsamen Standard gibt sondern, lediglich Standards und Richtlinien die ausschließlich Sicherheit aus Sicht Safety oder Security betrachten.

Dies kann beispielsweise dazu führen, dass Safety-Anforderungen Security-Anforderungen überstimmen – oder auch umgekehrt, was in weiterer Folge zu Konflikten führen kann. Zum Beispiel fordert Security ein komplexes und einmaliges Passwort für einen Login um sicherzustellen, dass keine unbefugten Personen Zugriff auf Systeme und deren sensible Daten bekommen. Safety wiederum fordert kurze und leicht merkbare Passwörter um in kritischen Situationen nicht Gefahr zu laufen, dass der Befugte ein System in einer Gefahrensituation nicht stoppen kann. In diesem Fall wird ganz klar die Anforderung an Security durch jene von Safety überstimmt, wobei es zu einer bewussten Verletzung der Security Anforderungen kommt.

4. Risk Management Modelle und Methoden zur Sicherstellung von Safety und Security

Um mögliche vorhandene Potentiale von Risiken sowie Gefährdungen in Safety und Security Bereichen bestmöglich managen zu können, greift man auf Methoden und Techniken des Risk Management zurück. Neben integrierten Risk-Management-Systemen kommen auch Sicherheits-Management-Systeme (SMS) zum Einsatz. Für die Identifizierung, Evaluierung, Analyse sowie Bewertung von Risiken aber auch Gefährdungen gibt es 31 bekannte Risk Assessment Methoden, die in Risk Management bezogenen Normen übersichtlich dargestellt sind und auszugsweise in ihrer Anwendung erklärt werden. Im Folgenden ein vertiefender Einblick in diese Themen.

Wir sprechen meistens von Risiken. jedoch sollte man sich dessen bewusst sein, dass Risiken auch neue Chancen bedeuten können. Letztendlich kommt es auf den richtigen Umgang an!

[3] ISO/IEC 27000 Normenreihe - beinhaltet eine Reihe von Standards der IT-Sicherheit (IT-Security). Sie deckt sich mit einer Reihe von anderen Themen, darunter ISO 9000 (Qualitätsmanagement) und ISO 14000 (Umweltmanagement);herausgegeben von ISO (International Organization for Standardization) und IEC (International Electrotechnical Commission); http://www.27000.org

[4] ISO/IEC 20000 - Norm zum IT Service Management (ITSM); herausgegeben von ISO (International Organization for Standardization) und IEC (International Electrotechnical Commission);

[5] CoBIT–Control Objectives for Information Technology; COBIT 5 ist das übergeordnete Rahmenwerk für die Governance und das Management der unternehmensweiten IT; herausgegeben von ISACA www.isaca.org

[6] ITIL - Information Technology Infrastructure Library; ITIL ist eine Sammlung von Best Practices in einer Reihe von Publikationen zur Umsetzung eines IT-Service-Managements (ITSM). Inzwischen gilt ITIL als internationaler De-facto-Standard im Bereich IT-Geschäftsprozesse; http://www.itil.org/en

4.1. Risk Management

Gemäß der Normenfamilie ONR 49000, welche als österreichische Technische Norm ein Leitfaden zur Umsetzung der ISO 31000, Risk Management - principles and guidelines, ist, „erstreckt sich die Anwendung des Risikomanagements auf Organisationen und Systeme“ [14].

Um die zunehmende Komplexität von Systemen bewältigen zu können, zeigt sich integriertes Risk Management als kraftvolles Führungsinstrument von Organisationen. Dabei werden der Top-down Ansatz und der Bottom-up Ansatz verbunden und koordiniert (Abbildung 2) und entsprechend zur Risikobeurteilung und Risikobewältigung herangezogen.

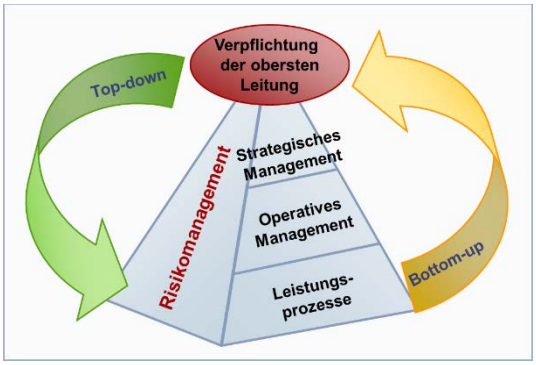

Abbildung 2: Risikomanagement - Top-down- und Bottom-up Ansatz; Quelle: [14], Bild 3

Risikobeurteilung und Risikobewältigung mit dem Bottom-up Ansatz

„In den vergangenen Jahren kam das Risikomanagement vor allem im Zusammenhang mit Arbeitssicherheit, Umweltsicherheit, Produktsicherheit und Produkthaftung (bzw. deren Versicherung) zur Anwendung“ [14]. Dabei steht die Sicherheit der Menschen sowie der Umwelt, der technischen Systeme und Prozesse im Vordergrund des Interesses. Allerdings beschränken sich hier einzelne Risk Management Anwendungen auf Teilgebiete innerhalb einer Organisation, die meist weder in einen Gesamtrahmen integriert noch untereinander abgestimmt sind [14].

Eine weitverbreitete und etablierte Risk Assessment Methode die dem Bootom-up-Ansatz folgt, ist beispielsweise die Failure Mode and Effects Analysis (FMEA).

Risikobeurteilung und Risikobewältigung mit dem Top-down Ansatz

Mit Corporate Governance kam dem Risk Mangement eine weitere Bedeutung hinzu, die „Verpflichtung der obersten Leitung und der Führungskräfte im Rahmen der Grundsätze der Führung der Organisation“ [14]. Dabei ist die Zielerreichung der Organisation, wie beispielsweise strategische, operationelle, finanzielle Ziele genauso wie Ziele im Bereich der Sicherheit von Menschen und der Umwelt, primäre Aufgabe.

Eine weitverbreitete und etablierte Risk Assessment Methode die dem Top-down Ansatz folgt, ist beispielsweise die Fault Tree Analysis (FTA).

Berechnung des Risikos

Es ist immer wieder die Rede von Risiko. Doch wie berechnet sich das Risiko?

Mathematisch gesehen ist Risiko (R) definiert als Produkt der Wahrscheinlichkeit (P) eines Ereignisses, welches zu einem Fehler führt, und der Schwere (S) des Fehlers, wenn dieses Ereignis eintritt [16] .

$$Risk = (probability\ of\ event\ occurring)\ x\ (severity\ of\ event\ occurring) \quad (1)$$

$$R = P\ x\ S \quad (2)$$

Selbige Nomenklatur wird in der EN 60812 FMEA [18] verwendet, mit

- S … dimensionslose Größe, die für Schwere steht, d. h., ein Schätzwert dafür, wie stark die Auswirkungen eines Ausfalls das System oder den Anwender beeinflussen können
- P … dimensionslose Größe, die die Eintrittswahrscheinlichkeit bezeichnet

4.2. Systemischer Ansatz

Die Ausrichtung auf Ziele und Strategien der Organisation sowie der Auftrag und die Verpflichtung des obersten Managements, den Risk-Management-Prozess im Alltag anzuwenden, sind für ein wirksames Risk Management unabdingbar und somit Voraussetzung. Dies kann als allgemein notwendig und gültig angesehen werden und ist demzufolge sowohl auf Safety- als auch auf Security-Bereiche übertragbar.

Der Risk-Management-Prozess umfasst „Tätigkeiten, die darauf ausgerichtet sind, eine Organisation bezüglich Risiken zu steuern und zu überwachen“ [14]. Im Mittelpunkt stehen dabei die Definition der Rahmenbedingungen, die Risikoidentifikation, die Risikoanalyse, die Risikobewertung und die Risikobewältigung, begleitet von Risikokommunikation und Risikoüberwachung. Abbildung 3 zeigt den Prozess gemäß ISO 31000.

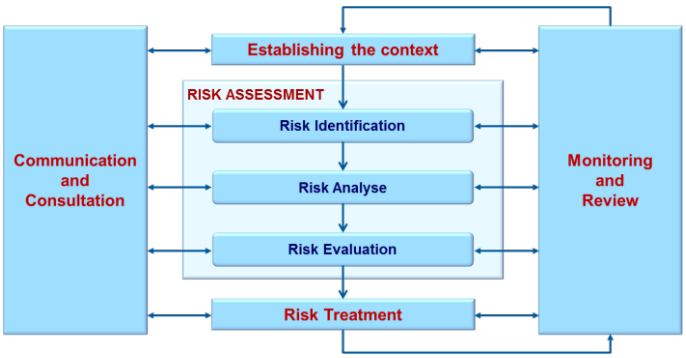

Abbildung 3: Risk-Management-Prozess gemäß ISO 31000, Darstellung in Anlehnung an [7], Bild 3

Der Risk-Management-Prozess ist Teil des Risk-Management-Systems, welches alle Elemente des Management-Systems einer Organisation umfasst, deren Aufgabe die Risikobewältigung ist. Das Risk-Management-System beschreibt die Führungsaufgaben in einer Organisation und umfasst die Planung, die Umsetzung, die Leistungsbewertung und die laufende Verbesserung [14]. Dies kann als PDCA Zyklus, „Plan-Do-Check-Act“, beschrieben werden. Hierbei entspricht der Risk-Management-Prozess dem „DO“. In ONR 49000 ist dies veranschaulicht dargestellt (Abbildung 4).

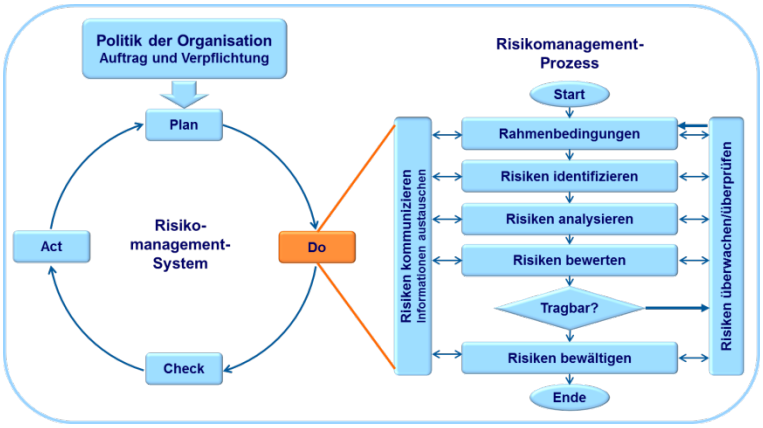

Abbildung 4: Risk-Management-System, Quelle: [14], Bild 4

Im folgenden Abschnitt werden einige ausgewählte Risk Assessment Methoden erläutert, die im Rahmen der Umsetzung von CSM Anwendung finden und auch bei Risikoanalysen im Bereich Security verwendet werden können.

4.3. Risk Assessment und Risk Assessment Methoden

Wie in Abschnitt 3.4 erwähnt, verwenden sowohl Safety als auch Security den Risk Assessment basierenden Ansatz. Das Ziel hierbei liegt darin, Risiken sowie Restrisiken zu evaluieren und eine entsprechende Kategorisierung vorzunehmen (wie Risikokategorien, Risikolevel) sowie Maßnahmen zur Herabsetzung von Risiken zu definieren. Risiken lassen sich nicht zu hundert Prozent eliminieren, ein gewisses Restrisiko wird immer bestehen bleiben. Man spricht hier von Risikoakzeptanz, dem „Entscheid, ein Risiko zu tragen“ [14].

Wie erwähnt, gibt es 31 Risk Assessment Methoden. Eine Übersicht über alle 31 Methoden sowie eine Beschreibung des Zweckes, des Ziels sowie mögliche Anwendungsgebiete und eine kurze Erläuterung zu jeder einzelnen Methode kann dem Anhang der Norm EN 31010 [15] entnommen werden. Beispiele für einzelne Methoden im Bereich Bahn und Bahnsysteme sind unter anderem in der Norm EN 50126 [11] nachzuschlagen. Für einige Methoden liegen eigene Normen vor, wie FMEA und FTA). Eine ausführliche Beschreibung einzelner Methoden finden sich auch in Büchern für Qualitätsmanagement sowie Normen, die sich mit Risikoanalysen befassen (EN 31010, EN 50126, ISO 27005, …).

Abbildung 5 zeigt eine mögliche Kategorisierung von Methoden, die im Bereich Risk Assessment Anwendung finden sowie einige Methoden. In der Praxis kommt es oft zu einer Kombination einzelner Methoden. Insbesondere Kreativitätstechniken wie Brainstorming, Brainwriting, Checklisten oder Interviews und Fragebögen helfen beispielsweise bereits im Vorfeld, bestimmte Daten oder Informationen, die für weitere Analysen notwendig sind, zu erheben. Im Folgenden werden einige ausgewählte Methoden wie FMEA und FTA, die im Bereich Bahn und Bahnsysteme sowie im Bereich für Security Agenden Anwendung finden, näher erörtert. Zusätzlich wird eine kurze Einführung in RAMS (Absatz 4.4) und SIL (Absatz 4.5) gegeben, zwei Methoden, die für Bahnanwendungen unabdenkbar sind.

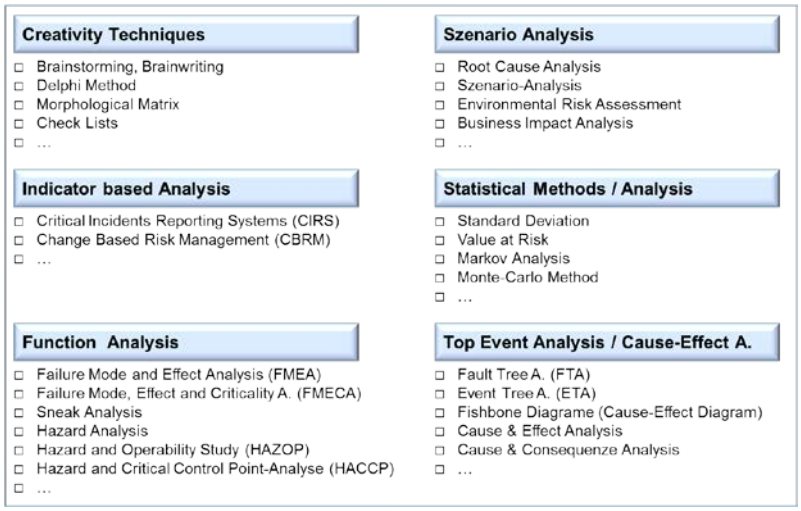

Abbildung 5: Risk Assessment Methoden – eine Übersicht,
Quelle: Stragere Management Consulting e.U., Seminar Risk Management

Failure Mode and Effects Analysis – FMEA

Die FMEA gehört zu den induktiven Verfahren und verfolgt damit den Bottom-up Ansatz. Bereits 1995 stellte Stamatis fest, “Failure mode and effects analysis (FMEA) is a widely used engineering technique for defining, identifying and eliminating potential failures” [17].

„FMEA ist eine Methode zum Bestimmen der Schwere möglicher Ausfallarten und zum Bereitstellen von Eingangsinformationen für Risikoverringerungsmaßnahmen. Darüber hinaus stellt die FMEA in manchen Anwendungen einen Schätzwert für die Eintrittswahrscheinlichkeit der Ausfallarten bereit“ [18].

Mit Hilfe der FMEA wird die sogenannte Risikoprioritätszahl RPN (Risk Priority Number) gebildet:

$$Risk\ Priority\ Number\ (RPN) = Severity\ (S)\ x\ Occurrence\ (O)\ x\ Detection\ (D) \quad (3)$$

Einige Anwendungen der FMEA oder FMECA unterscheiden zusätzlich den Grad der Fehlererkennung auf Systemebene. In diesen Anwendungen wird eine zusätzliche Kategorie für Fehlererkennung, D (ebenfalls eine dimensionslose Größe), benutzt, um eine Risikoprioritätszahl RPN wie folgt zu bilden:
Dabei ist gemäß EN 60812 FMEA [18]:

- S … Schadensausmaß (Severity) bzw. Schwere, d. h., ein Schätzwert dafür, wie stark die Auswirkungen eines Ausfalls das System oder den Anwender beeinflussen können
- O … Eintrittswahrscheinlichkeit (Occurrence) für eine Ausfallart für einen angenommenen oder festgelegten Zeitraum – selbst wenn sie als Rangzahl definiert ist, statt der tatsächlichen Eintrittswahrscheinlichkeit;
- D … Erkennung (Detection), d. h., ein Schätzwert für die Chance, den Ausfall zu erkennen und zu beheben, bevor das System oder der Kunde betroffen werden. Diese Kenngröße wird üblicherweise ihrer Größe nach geordnet, umgekehrt zu den Rangzahlen für Schwere oder Eintrittshäufigkeit: Je höher die Erkennungszahl ist, desto unwahrscheinlicher ist ihre Erkennung. Folglich führt die geringere Erkennungswahrscheinlichkeit zu einer höheren RPN, und einer höheren Priorität für die Behandlung der Ausfallart.

Üblicherweise werden S, O und D von 1…10 skaliert und die Risikokategorien entsprechend definiert. Demzufolge ist RPN_{max} = 10x10x10 =1000 möglich. Mit Hilfe der RPN lassen sich Risiken bewerten und entsprechend der Höhe Maßnahmen definieren. Es wird empfohlen ab einer RPN = 125 mit entsprechenden Maßnahmen zu starten, diese zu definieren und zu implementieren um einzelne Faktoren S, O oder D und somit RPN zu reduzieren.

Jede Methode hat ihre Vorteile aber auch Nachteile. FMEA erweist sich als effizient für die Analyse von Elementen, die den Ausfall des gesamten Systems oder einer Hauptfunktion des Systems verursachen. Bei komplexen Systemen mit Mehrfach-Funktionen, an denen unterschiedliche Systemkomponenten beteiligt sind, stößt die FMEA jedoch an ihre Grenzen und erweist sich als schwierig und mühsam. Der Grund hierfür liegt einerseits in der Menge der zu berücksichtigenden detaillierten Informationen über das System, andererseits können derartige Schwierigkeiten verstärkt werden, indem mehrere mögliche Betriebsarten vorliegen sowie durch die Berücksichtigung von Reparatur- und Instandhaltungsvorschriften [18].

Fault Tree Analysis (Fehlerbaumanalyse) – FTA

Die FTA gehört zu den deduktiven Verfahren und verfolgt damit den Top-down Ansatz. Bei der FTA handelt es sich um ein Verfahren zur Zuverlässigkeitsanalyse von technischen Anlagen und Systemen. Beispielsweise findet die FTA Anwendung bei Bahnsystemen, in der Luft- und Raumfahrttechnik oder als probabilistische Sicherheitsanalyse in der Kernkraftwerkstechnik.

Sie basiert auf der booleschen Algebra, um die Wahrscheinlichkeit eines Ausfalls einer Anlage oder des Gesamtsystems zu bestimmen. Im Rahmen der FTA werden logische Verknüpfungen von Teilsystemausfällen auf allen kritischen Pfaden ermittelt, welche zu einem Gesamtsystemausfall führen. Dabei wird das Gesamtsystem im Rahmen der Analyse in Minimalschnitte unterteilt, welche Ereigniskombinationen sind, die zu einem Gesamtausfall führen können. Da die Anzahl der Minimalschnitte je nach Anwendung bis zu einigen Millionen Ereigniskombinationen umfassen kann, werden zur Erstellung und Auswertung komplexer Fehlerbäume spezielle Softwarepakete herangezogen.

Die FTA ist unter anderem als internationaler Standard IEC 61025 (EN 61025)[7] unter dem Begriff Fehlerzustandsbaumanalyse bekannt und hier beschrieben. In Deutschland ist die FTA Inhalt der nationalen DIN 25424[8].

4.4. RAMS (Reliability, Availability, Maintainability, Safety)

Im Bereich Bahn beziehungsweise Bahnsysteme wird für Bahnanwendungen oftmals der Nachweis hinsichtlich Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit und Sicherheit (RAMS) gefordert. Die Spezifikation dazu sowie

[7] International Electrotechnical Commission (IEC) (Hrsg.): Fault Tree Analysis, IEC 61025. 2. Auflage. 2006, ISBN 2-8318-8918-9
[8] DIN 25424 Fehlerbaumanalyse, Ausgabe 1981-09, Beuth Verlag Berlin

Anforderungen zur Nachweiserbringung sind in der Norm EN 50126 beschrieben. Bei der Ermittlung einer RAMS spielt Safety ebenfalls eine wesentliche Rolle, die durch das „S“ in RAMS zum Ausdruck gebracht wird.

Im Rahmen der Umsetzung von CSM wird mitunter auch auf RAMS-Berechnungen zurückgegriffen, um Risiken und Gefahren zu identifizieren, zu evaluieren und zu bewerten sowie in Folge Maßnahmen zur Reduzierung definieren zu können. Bei der RAMS Ermittlung wird ebenfalls auf bekannte Risk Assessment Methoden zurückgegriffen (Absatz 4.3). Oftmals greift man im Rahmen der Risikobewertung auf die in der EN 50126 definierten vier Stufen hinsichtlich Risikominderung/-überwachung zurück [11]:

- intolerabel - muss ausgeschlossen werden
- unerwünscht - darf nur akzeptiert werden, wenn eine Risikominderung praktisch nicht durchführbar ist und eine Zustimmung des Bahnunternehmens vorliegt
- tolerabel - akzeptierbar bei geeigneter Überwachung und mit der Zustimmung des Bahnunternehmens
- vernachlässigbar - akzeptierbar ohne weitere Zustimmung des Bahnunternehmens

Demzufolge kann eine Risiko-Matrix (Risk Map) wie folgt definiert werden:

Häufigkeit-Konsequenz-Matrix				
Häufigkeit von Gefahrenfällen	Risikostufen			
häufig	unerwünscht	intolerabel	intolerabel	intolerabel
wahr-scheinlich	tolerabel	unerwünscht	unerwünscht	intolerabel
gelegentlich	tolerabel	unerwünscht	unerwünscht	intolerabel
selten	vernachlässigbar	tolerabel	tolerabel	unerwünscht
unwahr-scheinlich	vernachlässigbar	vernachlässigbar	tolerabel	tolerabel
unvorstellbar	vernachlässigbar	vernachlässigbar	vernachlässigbar	vernachlässigbar
	unbedeutend	marginal	kritisch	katastrophal
	Gefahrenstufen			

Abbildung 6: Häufigkeit-Konsequenz-Matrix zur Risikobewertung - Beispiel
(Quelle: EN 50126:1999, Kap. 4.6 Risiko, Tab. 6, [1])

Bei der Anwendung von RAMS ist es wichtig sich dessen bewusst zu sein, dass es sich hierbei um eine Methode handelt, welche darauf basiert die Zuverlässigkeit (R, Reliability), Verfügbarkeit A, Availability) sowie Instandhaltbarkeit (M, Maintainability) eines Systems an Hand von Daten aus LCC, Störungsstatistiken, Instandhaltungsmanagement, Technischer Randbedingungen etc. zu eruieren. Der letzte Teil bezieht sich auf die Betrachtung von Sicherheit (S, Safety). Setzt man sich mit den Fragen im Rahmen einer RAMS auseinander, so merkt man schnell, dass es sich hinsichtlich Safety eher um einen Fragenkatalog der vorhandenen Risiken in Bahnsystemen sowie der Maßnahmen (Normen, Gesetze, Arbeitsanweisung, etc.) handelt. Als oberste Prämisse gilt es zu belegen, dass man über entsprechende Vorschriften, Regelwerke, das entsprechend geschulte Personal, die entsprechende Umsetzung von Normen im Bereich der Planung und des Baues sowie der Instandhaltung und dergleichen verfügt, um damit etwaige auftretende Gefahren/Hazards zu reduzieren.

Der Security Aspekt wird im Rahmen der EN 50126 höchstens durch die beiden Normen EN 50128 und EN 50129 abgedeckt, welche allerdings speziell für Telekommunikationstechnik, Signaltechnik und Datenverarbeitungssysteme gelten. Aus dieser Sicht gibt es eine strikte Trennung zwischen Safety und Security bezogen auf RAMS. Darüber hinaus geht vor allem die EN 50129 eher den Weg, den Security Aspekt mittels SIL (Sicherheits-Integritäts-Level) abzudecken, mit anderen Worten, die Systeme grundsätzlich ausfallsicherer zu machen. Das entsprechende SIL wird hierbei über eine Risikobewertung ermittelt, siehe hierfür Absatz 4.5.

Das Ziel von Security sollte wie jenes von Safety sein: die Betrachtung eines Systems oder Teilsystems und die Ermittlung von Risiken beziehungsweise Gefahren/Hazards sowie deren Folgewirkung. In einem weiteren Schritt sind aus diesen Daten entsprechende Maßnahmen abzuleiten, um die Wahrscheinlichkeit des Auftretens eines Risikos beziehungsweise einer Gefahr/eines Hazards zu reduzieren.

Von daher stellt sich die Frage ob der derzeitige Ansatz gemäß „Stand der Technik“ zielführend ist und somit einen Mehrwert bringt beziehungsweise erwirtschaftet. Oder ob andererseits dem „Trial and Error“ Prinzip gefolgt wird und einfach nur zu Folge der Redundanz der Systeme kein Error auftritt.

4.5. Safety Integrity Level - SIL

Auf der Grundlage von Ergebnissen der Risikobewertung wird das Sicherheitsniveau für die Anwendung festgesetzt und die erforderliche Risikominderung eingeschätzt. Daraus werden die Anforderungen an die Safety Integrity abgeleitet. „Die Safety Integrity kann gesehen werden als eine Kombination von zahlenmäßig erfassbaren Elementen (grundsätzlich verknüpft mit Hardware, d. h. zufällige Ausfälle) und zahlenmäßig nicht erfassbaren Elementen (grundsätzlich verknüpft mit systematischen Ausfällen in Software, Lastenheft, Dokumenten, Vorgängen usw.)“ [1].

Um das vorgegebene Sicherheitsniveau einhalten zu können ist es notwendig, sowohl externe als auch systemeigene Einrichtungen zur Risikominderung zu implementieren, welche die Erreichung der geforderten Reduzierung des Risikos für das System sicherstellen.

„Safety Integrity bezieht sich auf die Ausfallwahrscheinlichkeit, die notwendig ist, um die geforderte sichere Funktionsfähigkeit zu erzielen“ [1]. Eine Korrelation zwischen Safety Integrity und der Ausfallwahrscheinlichkeit für Bahnsysteme ist in der EN/IEC 61508 - Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/ programmierbarer elektronischer Systeme - angegeben. Die Festlegung dieser Korrelation für Bahnanwendungen liegt in der Verantwortlichkeit der Bahnunternehmen.

Im Bereich Maschinensicherheit sind folgende drei Standards maßgeblich:

- IEC 61508 - Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/ programmierbarer elektronischer Systeme
  - ausgerichtet auf elektronische Systeme
  - Safety Integrity Level (SIL) von SIL1 bis SIL4
- EN 62061 - Sicherheit von Maschinen - Funktionale Sicherheit sicherheitsbezogener elektrischer, elektronischer und programmierbar elektronischer Steuerungssysteme
  - ausgerichtet auf elektronische Systeme
  - Safety Integrity Level (SIL) im Maschinenschutz von SIL1 bis SIL3
  - Sicherheits-Lebenszyklus, SIL-Risikomatrix, Strukturelle Einschränkungen, Strukturmodell
- EN ISO 13849 - Sicherheit von Maschinen – Sicherheitsbezogene Teile von Steuerungen
  - ausgerichtet auf elektronische Systeme und anwendbar für mechanische Systeme
  - Performance Level (PL) a-e
  - Iterativer Gestaltungsprozess, Risikograph, vorgesehene Architekturen (Kategorien), Säulendiagramm

Folgende Abbildung zeigt eine mögliche Bewertungsgrundlage für eine SIL Bewertung nach EN 62061:

Klassifikation der Häufigkeit und der Dauer der Exposition [F]	
Häufigkeit der Exposition	Dauer > 10 min
≥ 1 pro h	5
< 1 pro h bis ≥ 1 pro Tag	5
< 1 pro Tag bis ≥ 1 pro 2 Wochen	4
1 pro 2 Wochen bis ≥ 1 pro Jahr	3
< 1 pro Jahr	2

F

+

Klassifikation der Wahrscheinlichkeit [W]	
Wahrscheinlichkeit des Auftretens	Wahrscheinlichkeit [W]
sehr hoch	5
wahrscheinlich	4
möglich	3
selten	2
vernachlässigbar	1

W

+

Wahrscheinlichkeit der Vermeidung oder Begrenzung des Schadens [P]	
unmöglich	5
selten	3
wahrscheinlich	1

P

=

Klasse der Wahrscheinlichkeit des Schadens [K]				
4	5 - 7	8 - 10	11 - 13	14 - 15
SIL 2	SIL 2	SIL 2	SIL 3	SIL 3
	AM	SIL 1	SIL 2	SIL 3
		AM	SIL 1	SIL 2
			AM	SIL 1

K

Abbildung 7: SIL Bewertung nach EN 62061 (Grafik: Autoren)

Im Rahmen der Prozesssicherheit ist hinsichtlich Funktionaler Sicherheit der Standard EN 61511 - Funktionale Sicherheit – Sicherheitstechnische Systeme für die Prozessindustrie maßgebend.

5. Gemeinsame Sicherheitsmethode für Eisenbahnsicherheit- Änderung der Sichtweise

Durch die Digitalisierung und den erhöhten Einsatz von Software kommt es heute zu kriminellen Vorgängen, bekannt unter dem Schlagwort Cyber Crime. Passwörter werden gestohlen um sich Zugang zu sensiblen Daten zu verschaffen (z.B. Login Daten von Banken oder zu Firmenrechnern), Netzwerke werden gehackt um schädliche Malware und Viren einzuschleusen. Bekannte Beispiele hierfür sind die Stuxnet-Attacke [19] auf das SCADA System von Siemens 2010 [20], oder der Heartbleed-Bug in OpenSSL im April 2014, [21].

Erinnern wir uns an die eingangs erwähnten Ergebnisse der Studie der ICS-CERT hinsichtlich gemeldeter Zwischenfälle in Netzwerken kritischer Infrastrukturen von Organisationen, so zeigt dies, dass auch vor hochsicherheitskritischen Anwendungen nicht Halt gemacht sondern versucht wird, hier in Systeme einzugreifen um vorrangig bewusst einen Schaden anzurichten. Im Bereich Flugverkehr gibt es bekannte Vorfälle, wo von einer Malware (W32.Stuxnet) in ATM (Air Traffic Management) Systemen berichtet wurde. Hierbei handelt es sich eindeutig um ein Security-Problem, das weitreichende Auswirkungen in den Safety-Bereich hat, geht es doch darum, dass Flugzeuge nicht abstürzen.

Betrachten wir nun die CSM Verordnung hinsichtlich Eisenbahnsicherheit, so ist ersichtlich, dass hier kein einziges Mal von Security, System Security oder Informationssicherheit gesprochen wird. Dies bringt uns zu der Fragestellung zurück, inwieweit werden bei einer gemeinsamen Sicherheitsmethode neben den Safety-Aspekten und Anforderungen auch Security-Aspekte und Anforderungen berücksichtigt.

5.1. Safety – Signifikante Unfälle

Seit 2006 werden seitens den Nationalen Sicherheitsverantwortlichen (National Safety Authorities) Unfälle im Eisenbahnwesen in der ERAIL-Datenbank[9] gemäß den definierten CSIs (Common Safety Indicators) berichtet (Abbildung 8).

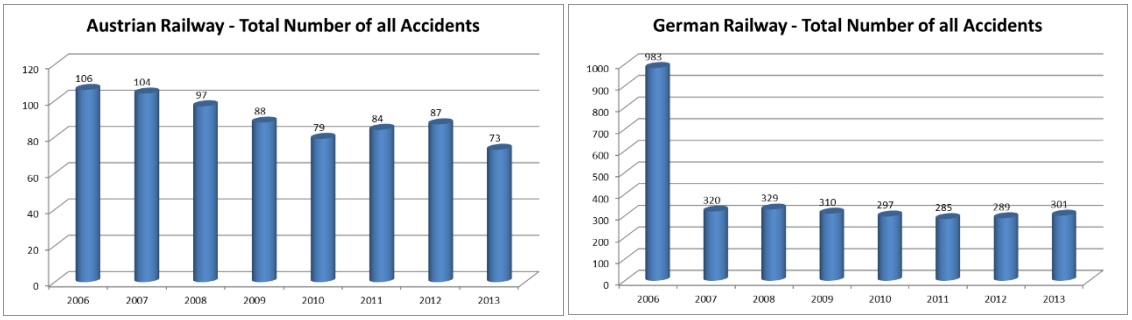

Abbildung 8: In der ERAIL Datenbank gemeldete Unfälle – Anzahl Unfälle gesamt AT, D
(Grafik: Autoren)

In 2013 sind bezogen auf das Jahr 2006 die Unfälle in Österreich um 31% gesunken, hingegen in Deutschland um beachtliche 69%. Eine mögliche Begründung hierfür wäre, dass in Deutschland in 2006 auch Unfälle registriert wurden, die nicht den definierten CSIs unterlagen.

Unter anderem wird differenziert zwischen Vorstufen von Unfällen zufolge falsch freigegebener Signale oder seitens Triebfahrzeugführer falsch beachteter Signale (total precursors of accidents with wrong - side signalling failures) sowie überfahrener Haltesignale (Total precursors of accidents with signals passed at danger). Abbildung 9 gibt eine Übersicht über die gemeldeten Unfälle zwischen 2006 und 2013 für Deutschland und Österreich.

[9] ERAIL Datenbank: http://erail.era.europa.eu; Datenbankabruf am 24.04.2015

Austria				
CSI		Total Number of all accidents	Total precursors of accidents with wrong-side signalling failures	Total precursors of accidents with signals passed at danger
YEAR	2006	106		15
	2007	104	7	12
	2008	97	3	16
	2009	88	0	20
	2010	79	4	11
	2011	84	4	5
	2012	87	2	10
	2013	73	3	12

Germany				
CSI		Total Number of all accidents	Total precursors of accidents with wrong-side signalling failures	Total precursors of accidents with signals passed at danger
YEAR	2006	983	0	
	2007	320	0	727
	2008	329	0	760
	2009	310	0	355
	2010	297	0	352
	2011	285	0	464
	2012	289	0	400
	2013	301	0	368

SOURCE: ERAIL database (http://erail.era.europa.eu)

Legend: (Classification of deviation in data)
Natural variation
Change of definition or reporting procedure

Abbildung 9: In der ERAIL Datenbank gemeldete Unfälle – Anzahl Unfälle gesamt im Vergleich Unfällen zufolge gefährlicher Ausfälle von Signaleinrichtungen beziehungsweise überfahrener Haltesignale (Grafik: Autoren)

5.2. Cyber Attacken – nur ein Security Problem?

Das Bewusstsein und die Sorge um sicherheitsrelevante Zwischenfälle und Bedrohungen im Internet und der Cloud erreichen inzwischen die Anwender beziehungsweise Verbraucher, so auch Unternehmen und Organisationen. PwC spricht bei Cyber Security inzwischen von einem beharrlichen Geschäftsrisiko und kam zu der Schlussfolgerung, Cyber Security "is no longer an issue that concerns only information technology and security professionals; the impact has extended to the C-suite and boardroom" [22]. Das Beratungsunternehmen *PricewaterhouseCoopers* (PwC) spricht in der von ihnen durchgeführten Umfrage *Managing cyber risks in an interconnected world*, über den drastischen Anstieg hinsichtlich Datendiebstahl, "…this year, aerospace and defense respondents reported a 97% increase in hard IP theft and a 66% jump in soft IP compromise - higher by far than any other sector" [22].

Neben Bereichen wie Energie, Luftverkehr und Verteidigungseinrichtungen sind auch Börsen zu alltäglichen Zielen für Cyber Attacken geworden. Eine seitens der International Organization of Securities Commissions (IOSCO) und der World Federation of Exchanges Office durchgeführten Umfrage an 46 globalen Wertpapierbörsen ergab, dass bereits 53%, also mehr als die Hälfte, einer Cyber Attacke ausgesetzt waren [23], [22].

Bennet berichtet in TheHill, "the number of detected cyberattacks skyrocketed in 2014 - up 48 percent from 2013 - and they are costing companies more money…; this year is expected to see 42.8 million cyberattacks, roughly 117.339 attacks each day" [24]. Dabei stützt er sich auf die von PwC veröffentlichte Studie [22]. Kaspersky Lab ein führender Anbieter von Security Software, schätzt, "an average data security incident costs a company $720.000" [25].

Es ist wichtig, dass Sicherheitspraktiken Schritt mit sich ständig weiterentwickelnden Bedrohungen und den daraus resultierenden Sicherheitsanforderungen halten. Nur so kann den Vorkommnissen von Cyber Attacken Einhalt geboten werden beziehungsweise ist zumindest eine Reduzierung der Vorfälle möglich. Ganz ausschließen wird man derartige Attacken wohl nie können.

5.3. Cyber Safety und Cyber Security im Eisenbahnwesen

Wir unterliegen einer ständigen technischen Weiterentwicklung und Automatisierung, so auch im Eisenbahnwesen. Neue Technologien wie ETCS (European Train Control System) sollen den Zugverkehr unter Erreichung kürzerer Intervalle und Blockabstände der Züge zueinander für den Reisenden noch schneller und sicherer machen. Im Bereich Signaltechnik aber auch in der Leittechnik sowie in Unterwerken selbst kommt es vermehrt zum Einsatz von Software-betriebenen Steuerungen. Würde sich jemand von außen hier Zugriff auf derartige Infrastruktursysteme verschaffen, könnte das ungeahnte und fatale Auswirkungen haben. Neben der Erfüllung der Safety-Anforderungen haben wir es hier auch mit Security-Anforderungen zu tun.

Ein Angriff könnte hier aber auch von innen erfolgen, indem beispielsweise in Steuerungen eingegriffen wird und schadhafte Malware eingeschleust wird, die folglich auf das System wirken und einen Schaden verursachen. Dies kann unter anderem durch eigene Mitarbeiter geschehen oder durch Unbefugte, die sich Zutritt zu bestimmten Räumlichkeiten verschaffen. Dass derartige Vorkommnisse möglich sind, bestätigt Stupples, Professor an der City University in London und Experte für vernetzte elektronische Anlagen und Funkanlagen, im Gespräch mit der BBC, "… the European Rail Traffic Management System, a new digital system aimed to make lines safer, could be exposed to malicious software, or malware, used to cause a "nasty accident" … It's the clever malware that actually

alters the way the train will respond. So, it will perhaps tell the system the train is slowing down, when it's speeding up." [26], [27]. Man ist sich durch aus des Risikos bewusst, Opfer einer Cyber Attacke zu werden, solange weiterhin Digitaltechnik über Netzwerke ausgerollt wird [26], [27]. Stupples ergänzte, "that part of the reason that transport systems had not already been hacked as frequently as financial institutions and media organisations was that much of the technology involved was currently too old to be vulnerable" [27]. Dies sollte zu denken geben, denn "…all of that will change in the coming years, as aircraft, cars and trains become progressively more computerised and connected" [27], so Stupples.

6. Safety und Security aus einer Gesamtperspektive betrachtet - Diskussion

6.1. Konkrete Anwendungsfälle

Betrachten wir den Bereich Bahn beziehungsweise Bahnsysteme, ergeben sich hierbei vor allem zwei mögliche Anwendungsfelder, wo sowohl Safety als auch Security zusammenspielen müssen um mögliche Risiken für den Endbenutzer, dies kann der Reisende (Passagier) oder aber auch der Betreiber selbst sein, zu vermeiden.

Anwendungsfall 1 – Betriebliche Signalisierung in der Leit- und Sicherungstechnik

Hier ist es bereits ohne größere softwaretechnische Einmischung zu Fehlern zu Folge von Fehlverhalten von Anlagen beziehungsweise menschlichem Versagen oder ähnlichem gekommen. Mit Einführung von ETCS erhofft man sich, einen interoperablen Eisenbahnverkehr zumindest im Bereich der Sicherungstechnik zu ermöglichen und hiermit die derzeit bekannten Systeme wie PZB (Punktförmige Zugbeeinflussung), LZB (Linienförmige Zugbeeinflussung, Deutschland), ATC (Automatic Train Control, Schweden), Crocodile (Belgien, Frankreich), TVM (Transmission Voie-Machine, Frankreich), ZUB (Zugsicherung Integra-Signum, Schweiz, Spanien) und dergleichen abzulösen. Des Weiteren können durch Einführung von ETCS die Blockabschnitte der Züge sowie die damit verbundenen Zugintervalle teilweise erheblich reduziert werden. Voraussetzung hierfür ist allerdings eine gemeinsame Kommunikationsplattform zwischen unterschiedlichen Systemen. Diese erweist sich durch die unterschiedlichen Systeme der Hersteller als komplex und herausfordernd. Hierbei muss sowohl eine Kommunikation der Systeme von Betreiberseite für die Signalisierung als auch vom Endnutzer, in diesem Fall dem Triebfahrzeug und dessen ETCS Antenne, ermöglicht werden. Zu Folge der Vielzahl an zu berücksichtigenden Schnittstellen sowie den unterschiedlichen Systemen, welche hierbei zum Einsatz kommen, und den damit verbundenen teilweise massiv unterschiedlichen Verschlüsselungssystemen, ist es nicht auszuschließen, dass teilweise ein Safety ein Security System beziehungsweise umgekehrt, überstimmt. Unter in Betrachtnahme der zu erzielenden Vorteile von ETCS, wie verringernde Zugfolgen und der damit verbundenen verringerten Zugabstände zueinander, könnte ein Fehler im Gesamtsystem fatale Folgen haben!

Anwendungsfall 2 – Softwaretechnisch gestützte Energieverteilung

Eine im Rahmen der immer weiter voranschreitenden Technologisierung ist die heutzutage größtenteils softwaretechnisch gestützte Energieverteilung, wobei hier im konkreten von Strom die Rede ist. Man stelle sich beispielsweise vor, dass jemand in der Lage wäre, softwareseitig in eine Zentrale Leitstelle einzudringen und hier die Verteilung des erzeugten oder gekauften Stromes des Eisenbahninfrastrukturbetreibers manipuliert. Abgesehen von der Möglichkeit ganze Streckenabschnitte und Landesteile vom Netz zu nehmen, besteht hierbei auch die Möglichkeit, den gesamten Stromhandel, soweit dieser betrieben wird, zu beeinflussen und damit beträchtliche finanzielle sowie imagemäßige Schäden zu verursachen. Im Falle eines derartigen "Security Breach" wäre der Schaden an Anlagenteilen, sowie Passagieren und dergleichen grundsätzlich minimal beziehungsweise vertretbar, zu Folge der daraus entstehenden Verspätungen, sowie nicht getätigter finanzieller Transaktionen, wie zum Beispiel dem Verkauf von Spitzenstrom, kann es allerdings zu massiven finanziellen Beeinträchtigungen kommen.

6.2. System zur Betrachtung des Lebenszyklusses

Ein interessanter Aspekt bezogen auf die zwei dargestellten Bespiele ist vor allem ein in den letzten Jahren bekannt gewordenes System zur Betrachtung des Lebenszyklusses von Systemen im Bereich von Bahn beziehungsweise Bahnsystemen. Betrachtet man heute beispielsweise den Lebenszyklus eines Systems in diesem Bereich, von der Konzept-, über die Betriebsphase bis hin zur Außerbetriebsetzung, so wird man unweigerlich mit dem Begriff RAMS (Reliability, Availability, Maintainability, Safety) konfrontiert. Wie bereits in der Erläuterung dieses Begriffes ersichtlich, ist Safety ein Teil der Betrachtung des System-Lebenszyklusses zu Folge von RAMS und wie im Absatz 3.2 dargestellt, bezieht sich Safety hierbei auf "das Nichtvorhandensein eines unzulässigen Schadensrisikos" [1]. Auf Grundlage dieser Erläuterung ist die Frage inwieweit Security als Teil dieses Systems-

Lebenszyklusses, bezogen auf RAMS, vor allem im Bereich von Bahn beziehungsweise Bahnsystemen Anwendung findet.

6.3. Herausforderung an Systemgrenzen

Ein weiterer Aspekt, welcher die derzeitige Vorgehensweise im Bereich der Betrachtung von Safety beziehungsweise Security im Bereich Risk und Safety Management unterstützt, ist die Möglichkeit entsprechende Systemgrenzen setzen zu können. Dadurch muss nur ein gewisser Teil betrachtet werden. Bezogen auf die oben angegebenen Beispiele (Absatz 6.1) zeigen sich jedoch folgende mögliche Problemstellungen:

Bezogen auf das Zugsicherungssystem ETCS sind die entsprechenden Systemgrenzen für die Betrachtung von Seiten Risk und Safety Management bereits teilweise über die Beteiligung beziehungsweise Aufgabenverteilung auf die unterschiedlichen Hersteller sowie den Betreiber gegeben.

In diesem Fall ist es zum Beispiel möglich, als Hersteller der Empfangsantenne des Zugsicherungssystems ETCS einzig das Fahrzeug sowie die Kommunikation zwischen Empfangsantenne (Fahrzeugseitig) und der ETCS Balise zu betrachten. Hier zeigt sich allerdings bereits ein Problem bezogen auf unterschiedliche Hersteller. Im Normalfall wird eine ETCS Empfangsantenne am Triebfahrzeug nachgerüstet. Dies bedeutet, ein entsprechendes Steuerungssystem ist Triebfahrzeug seitig bereits vorhanden, welches nun die Steuerung ETCS seitig adaptieren muss.

Im Bereich der Bahnanwendungen kommt hinsichtlich Telekommunikationstechnik, Signaltechnik und Datenverarbeitungssysteme die Norm EN 50128 zum Tragen, deren Anwendungsgebiet unter anderem „ausschließlich auf Software und die Wechselwirkung zwischen Software und dem System anwendbar ist, zu dem die Software gehört“ [28].

Dieser Ansatz an sich erscheint zwar logisch, allerdings stellt sich vor allem bei Systemen wie ETCS die Frage, inwieweit eine Wechselwirkung zwischen System und Software zu betrachten ist. Folgende Systeme mit ihrer zugehörigen Software sollen dies verdeutlichen:

- Die Antenne des Triebfahrzeuges ist ein System für sich mit eigener zugehöriger Software, genauso wie das Triebfahrzeug selbst ein System mit eigener Software ist; somit liegen hier bereits zwei unterschiedliche Systeme sowie zwei unterschiedliche Software Programme vor;
- Die Empfangsantenne der Balise ist ein eigenes System mit einer Software, welche sowohl mit der Software der Antenne des Triebfahrzeuges als auch mit der Fernwirktechnikanlage des Infrastrukturbetreibers kommunizieren muss; hier sind somit bereits drei Systeme mit drei unterschiedlichen Software Programmen zu berücksichtigen und zu betrachten;

Letztendlich ergibt sich daraus eine entsprechende Anzahl unterschiedlicher Systeme einschließlich der unterschiedlichen Systemanforderungen selbst sowie der zugehörigen unterschiedlichen Software-Programme. Ein weiterer Aspekt der zum Tragen kommt, ist das Alter einer Anlage und damit verbunden die Aktualität des Software-Programms. Letzteres zielt auf die Art der Programmierung sowie verwendeter Programmiersprache selbst ab. Beides hat durchaus Auswirkungen auf die Kapazität der Datenverarbeitung

Des Weiteren kann es durchaus vorkommen, dass die ETCS Empfangsantennen in Folge der Liberalisierung der Märkte von mehreren Herstellern mit unterschiedlichen Codierungssystemen geliefert werden. Dies macht eine Betrachtung mehrerer Systeme im Gesamtkontext erforderlich.

Dieselbe Thematik zeigt sich in der Kommunikation zwischen den ETCS Balisen (Infrastrukturseitig) sowie der ETCS Empfangsantenne (Fahrzeugseitig). Hierbei ist nun die Kommunikation der ETCS Balisen mit der ETCS Empfangsanatenne sowie darüber hinaus die Kommunikation der ETCS Balisen mit den entsprechenden fernwirktechnischen Einrichtungen des Infrastrukturbetreibers zu betrachten.

Von Seiten des Infrastrukturbetreibers ist darüber hinaus die Funktionsweise des Systems innerhalb der fernwirktechnischen Einrichtungen sowie der möglichen Zusammenarbeit mit bereits bestehenden Systemen des Infrastrukturbetreibers zu berücksichtigen.

Zu Folge der langen Lebensdauer der Infrastruktur von Bahn beziehungsweise Bahnsystemen sind heutzutage vor allem auch die Kommunikation der einzelnen Programme untereinander sowie die verfügbare und eingesetzte Hardware in diesem Zusammenspiel zu beachten.

Wie am Beispiel ETCS ersichtlich, gibt es verschiedene Möglichkeiten ein System übergreifend zu betrachten. Die Herausforderung liegt unter anderem in der Aufgliederung in Teilsysteme und im Festlegen von mehr oder weniger sinnvollen Systemgrenzen. Diese werden beispielsweise durch die Firmenstruktur (z.B. mehrere

Geschäftsbereiche), der Vielzahl an unterschiedlichen Komponenten und Herstellern sowie Infrastrukturseitiger software- und hardwaretechnischer Restriktionen mitbestimmt.

6.4. Auswirkungen auf künftige Betrachtungsweise von Safety und Security Systemen

Auf Grundlage der beiden hier aufgezeigten Möglichkeiten zur Beeinflussung von Bahn beziehungsweise Bahnsystemen sowie der damit verbundenen derzeit gültigen Vorgehensweisen in der Bewertung dieser Systeme stellt sich die Frage, wie diese Systeme in Zukunft betrachtet werden sollten. Sollte man wie bisher Safety- und Security-Systeme für sich selbst betrachten oder doch unter einer gemeinsamen Sichtweise und unter Verwendung von Methoden zur Risikobewertung und Minimierung heranziehen?

Wie man auf Grundlage obiger Erläuterungen feststellen kann, sind die Methodiken (FMEA, FMECA, FTA, SIL, …) zur Ermittlung von Risiken sowie Gefährdungen/Hazards, deren Bedeutung, Auftretenswahrscheinlichkeit und Ersichtlichkeit sowie die Ermittlung von Maßnahmen zur Risikoverminderung beziehungsweise zur Verringerung der Wahrscheinlichkeit und Erhöhung der Ersichtlichkeit durchaus gleichwertig wenn nicht sogar teilweise dieselben.

Allerdings ist eine entsprechende gemeinsame Lösung für die Betrachtung von Safety und Security noch nicht wirklich absehbar. Ein Grund dafür ist, dass sich jeder Bereich eher mit seinen Eigenheiten beschäftigt, was wiederum dazu führen kann, dass einer der beiden Aspekte Safety oder Security im Rahmen einer Betrachtung vernachlässigt werden könnte.

Es stellt sich natürlich auch die Frage ob es überhaupt sinnvoll ist oder wäre, beide Bereiche zu betrachten, da es sich hierbei meistens um firmeninterne unterschiedliche Bereiche mit unterschiedlichen Zielen, Ausrichtungen und auch Ansichten handelt.

Darüber hinaus ist es überlegenswert, ob letztendlich eine gesamtheitliche Betrachtung von Systemen sowie gesamtheitliche Sicht auf Systeme für alle Beteiligten nicht die bessere Lösung wäre, anstelle der Betrachtung der einzelnen Systeme durch einzelne Bereiche selbst. Dies gilt insbesondere bei komplexen Anwendungsgebieten wie zum Beispiel ETCS, wo ein Gesamtsystem aus sehr vielen unterschiedlichen Systemen beziehungsweise Teilsystemen und Software-Programmen unterschiedlicher Hersteller besteht und wo auch unterschiedliche Betreiber, Nutzer und Anwender, die nicht unbedingt zur selben Firma gehören müssen, auf dieses Gesamtsystem zugreifen beziehungsweise in dieses Gesamtsystem eingreifen.

7. Conclusio

Die Anforderungen an Safety und Security sind unterschiedlich und situationsbedingt kann es vorkommen, dass Safety-Anforderungen über jenen von Security gestellt werden beziehungsweise werden müssen oder umgekehrt.

Eine Harmonisierung vorhandener Standards oder die Entwicklung eines eigenen gemeinsamen Standards für Safety und Security ist aus praktischer Sicht aufwendig und würde wohl mehrere Jahre in Anspruch nehmen. Es bleibt die Frage im Raum, wäre ein eigener gemeinsamer Standard oder eine Harmonisierung zielführend und Nutzen bringend? Außerdem bleibt die Frage offen, ob es möglich wäre, klare und eindeutige Richtlinien auszusprechen, wann Safety oder Security zum Tragen kommt und wie damit in unterschiedlichsten Situationen umzugehen wäre, sollte es zwischen den beiden Aspekten zu einem Konflikt kommen.

Dennoch wäre es zu Folge dem Aspekt der Sicherheit empfehlenswert, Safety und Security als Gesamtheit zu betrachten und zwar für all jene Fälle, wo Software oder Software gesteuerte Komponenten in einem System enthalten sind, das wiederum strengen Safety Anforderungen unterliegt. Hierzu könnten folgende Ansätze als einheitliche Methoden als Empfehlung ausgesprochen werden:

Inhärenter Entwicklungsansatz

Bereits in der Design- und Entwicklungsphase sollten Security beziehungsweise Safety Anforderungen berücksichtigt und entsprechende Maßnahmen implementiert werden anstatt über ein fertiges System oder Produkt Anforderungen als eine Art Schirm darüber zu spannen.

Risikobewertung/-analyse (Risk Assessment) Methoden

Methoden zur Risikobewertung und Risikoanalyse wie sie heute bereits in CSM Verwendung finden, können auch im Bereich Security ihre Anwendung finden. Dies ermöglicht es, sowohl Security als auch Safety relevante

potentielle Risiken aufzuzeigen und jedes für sich zu bewerten. Das Ergebnis der Bewertung liefert eine klare Aussage darüber, welches Risiko als „gefährlicher“ gesehen wird und demzufolge können entsprechende Maßnahmen zur Minimierung dieses Safety- beziehungsweise Security-Risikos gesetzt werden. Dies hat zur Folge, dass Safety- beziehungsweise Security-Anforderungen, vorgegebenen durch Richtlinien und Vorgaben beziehungsweise Normen, korrekt umgesetzt werden.

Die Betrachtung der beiden Sicherheitsaspekte Safety und Security in ihrer Gesamtheit wird durch die Digitalisierung und in Software dominierenden Bereichen unumgänglich werden. Die beiden oben genannten Ansätze können hier gegebenenfalls helfen.

8. Referenzen

[1] ÖVE/ÖNORM EN 50126:1999; Ausgabe: 2000-05-01, Bahnanwendungen Spezifikation und Nachweis der Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit und Sicherheit (RAMS); Österreichischer Verband für Elektrotechnik (ÖVE) und Österreichisches Normungsinstitut (ON)

[2] "Richtlinie über die Eisenbahnsicherheit": RICHTLINIE 2004/49/EG DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 29. April 2004 über Eisenbahnsicherheit in der Gemeinschaft und zur Änderung der Richtlinie 95/18/EG des Rates über die Erteilung von Genehmigungen an Eisenbahnunternehmen und der Richtlinie 2001/14/EG über die Zuweisung von Fahrwegkapazität der Eisenbahn, die Erhebung von Entgelten für die Nutzung von Eisenbahninfrastruktur und die Sicherheitsbescheinigung

[3] Hollnagel, E., de Paris, E. d., & Antipolis, S. (2008); *The Changing Nature Of Risks*; Ergonomics Australia Journal 22, 1-2 (2008), pp. 33-46.

[4] Reason, J. (1995); *Understanding adverse events: human factors*; Quality in Health Care 1995; 4: 80-89.

[5] Schedl Gabriele; *We know all about Safety – but what is Cyber Safety?*; Vortrag im Rahmen der Safety Day Konferenz; FH Campus Wien, University of Applied Sciences, Vienna Institute for Safety & Systems Engineering; 15.04.2015;

[6] Klipper S. (2015); *Information Security Risk Management – Risikomanagement mit ISO/IEC 27001, 27005 und 31010*; Springer Verlag

[7] ISO 31000:2009; Risk management — Principles and guidelines, Austrian Standards Institute/Österreichisches Normungsinstitut (ON)

[8] „CSM Verordnung“ VERORDNUNG (EG) Nr. 352/2009 DER KOMMISSION vom 24. April 2009 über die Festlegung einer gemeinsamen Sicherheitsmethode für die Evaluierung und Bewertung von Risiken gemäß Artikel 6 Absatz 3 Buchstabe a der Richtlinie 2004/49/EG des Europäischen Parlaments und des Rates

[9] „CSM Durchführungsverordnung“ - DURCHFÜHRUNGSVERORDNUNG (EU) Nr. 402/2013 DER KOMMISSION vom 30. April 2013 über die gemeinsame Sicherheitsmethode für die Evaluierung und Bewertung von Risiken und zur Aufhebung der Verordnung (EG) Nr. 352/2009

[10] ISO/IEC 25010:2011 Systems and software engineering - Systems and software Quality Requirements and Evaluation (SQuaRE) -- System and software quality models; ISO, IEC

[11] EN 50126:1999, Railway applications - The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS); CENELEC

[12] Technische Spezifikation CLC/TS 50562; Bahnanwendungen - Ortsfeste Anlagen - Prozess, Maßnahmen und Nachweisführung für die Sicherheit in der Bahnstromversorgung; Ausgabe 20012

[13] ÖNORM ISO/IEC 27001:2008, Informationstechnologie - Sicherheitstechnik Informationssicherheits-Managementsysteme – Anforderungen

[14] ONR 49000:2010-01-01; Risikomanagement für Organisationen und Systeme - Begriffe und Grundlagen - Umsetzung von ISO 31000 in die Praxis; Austrian Standards Institute - Österreichisches Normungsinstitut (ON)

[15] ÖVE/ÖNORM EN 31010 (IEC/ISO 31010:2009); Risk management – Risk assessment techniques; Ausgabe 2010-12-01; ÖVE Österreichischer Verband für Elektrotechnik, Austrian Standards Institut

[16] Geiger, W. (1994); Qualitätslehre, Einführung, Systematik, Terminologie; Vieweg Verlag, 2. Auflage

[17] Stamatis, D. (1995), Failure Mode and Effect Analysis: FMEA from Theory to Execution. ASQC Quality Press, Milwaukee, WI: ASQC Quality Pres

[18] ÖVE/ÖNORM EN 60812: 2006-12-01; Analysetechniken für die Funktionsfähigkeit von Systemen – Verfahren für die Fehlzustandsart und -auswirkungsanalyse (FMEA) (IEC 60812:2006); (Analysis techniques for system reliability – Procedure for failure mode and effects); Österreichisches Normungsinstitut (ON)

[19] Stuxnet ist ein Computerwurm, der im Juni 2010 entdeckt wurde. Das Schadprogramm wurde speziell für ein System zur Überwachung und Steuerung (SCADA-System) der Firma Siemens – die Simatic S7 – entwickelt; http://de.wikipedia.org/wiki/Stuxnet; abgerufen: 2015-04-26

[20] Danielle Veluz, *STUXNET Malware Targets SCADA Systems*, TrendMicro, http://www.trendmicro.com/vinfo/us/threat-encyclopedia/web-attack/54/stuxnet-malware-targets-scada-systems, accessed 2015-04-26

[21] Der Heartbleed-Bug ist ein schwerwiegender Programmfehler in älteren Versionen der Open-Source-Bibliothek OpenSSL, durch den über verschlüsselte TLS-Verbindungen private Daten von Clients und Servern ausgelesen werden können; http://de.wikipedia.org/wiki/Heartbleed; abgerufen: 2015-04-26

[22] PricewaterhouseCoopers (PwC); *Managing cyber risks in an interconnected world - Key findings from The Global State of Information Security® Survey 2015*; 30 September 2014; http://www.pwc.com/gsiss2015

[23] IOSCO (International Organization of Securities Commissions) and the World Federation of Exchanges Office, *Cyber-crime, securities, markets and systemic risk*; July 2013; http://www.iosco.org/research/pdf/swp/Cyber-Crime-Securities-Markets-and-Systemic-Risk.pdf

[24] Cory Bennett, *Study: Cyberattacks up 48 percent in 2014*, http://thehill.com/policy/cybersecurity/221936-study-cyber-attacks-up-48-percent-in-2014; published on 10/27/14 11:30 AM EDT;

[25] Kaspersky Lab; *IT Security Risks Survey 2014 – A Business Approach to Managing Data Security Threats*; http://media.kaspersky.com/en/IT_Security_Risks_Survey_2014_Global_report.pdf

[26] Thomas Tamblyn; *Hackers Could 'Crash Trains' Using A Cyber Attack;* The Huffington Post UK, posted: 24/04/2015 11:05 BST, http://www.huffingtonpost.co.uk/2015/04/24/hackers-could-crash-trains-using-a-cyber-attack_n_7134068.html

[27] Richard Westcott, BBC Transport Correspondent; *Rail signal upgrade 'could be hacked to cause crashes'*; posted 2015-04-24; http://www.bbc.com/news/technology-32402481

[28] ÖVE/ÖNORM EN 50128:2002-01-01; *Bahnanwendungen – Telekommunikationstechnik, Signaltechnik und Datenverarbeitungssysteme, Software für Eisenbahnsteuerungs- und Überwachungssysteme*; Österreichischer Verband für Elektrotechnik (ÖVE), Österreichisches Normungsinstitut (ON)

9. VITA

DI Barbara Streimelweger, MBA, CMC (44),
1995 Studium der Elektrotechnik /Industrielle Elektronik und Regelungstechnik mit Schwerpunkt Biomedizinische Technik an der Technischen Universität (TU) Wien; 1999 Post-graduale-Studium der Betriebs-, Rechts- & Wirtschaftswissenschaften (TU Wien) sowie 2002 das MBA-Studium in General Management (Donau-Universität Krems und TU Wien); 2010 Ausbildung zum Certified Management Consultant (CMC) sowie umfassende Zusatzausbildungen. Publikationen im Bereich Healthcare, Risk Management und Patient Safety; von 1997 bis 2008 im Bereich der Telekommunikation und ICT in internationalen Unternehmen tätig; 2008 Firmengründung von Stragere Management Consulting e.U.; seither Beraterin und Fachexpertin im Bereich Risiko Management, Safety, Innovationsmanagement; seit 2009 Dozentin am Bildungsinstitut tecteam/DE.

Adresse: Stragere Management Consulting e.U.,
Am Kirchenweg 8, 3071 Böheimkirchen, Österreich;
Fon: +43 664 5324685;
E-Mail: b.streimelweger@stragere.at

Ing. Wolfgang Sturzeis (26),
2008 Studium an der Höheren Technischen Lehranstalt (HTL) für Maschinenbauingenieurswesen – Maschinen- und Anlagentechnik in Wien/AT; 2009 Ausbildung zur Elektrotechnikfachkraft für 15-kV-Oberleitungsanlagen und zum Schaltantragsteller und Örtlichen Aufsichtsführenden gem. DV EL 52; unter anderem Betriebsleiterbeauftragter; diverse Zusatzqualifikationen; 2008 bei ÖBB Infrastruktur Bau AG als Junior Systemtechniker; 2009 Weiterentwicklung zum Systemtechniker bei ÖBB Infrastruktur AG; 2012 Wechsel zu ÖBB Technische Services, als Komponententechniker verantwortlich für Türsteuerungen/-systeme sowie Drehgestelle; 2013 Ingenieur im Bereich Bahnsysteme Schwerpunkt Energietechnik/Oberleitungsanlagen und Bahnstromversorgung sowie Funktion als Fachgruppenleiter Engineering bei Signon Österreich GmbH; im Juni 2015 Rückkehr zur ÖBB Infrastruktur AG, GB SAE als Systemspezialist Oberleitungsanlagen.

Adresse: 1160 Wien, Österreich
E-Mail: wolfgang.sturzeis@hotmail.com

