Berliner Gesamtkonferenz der Sicherheitsinstitutionen

- Sicherheitslandkarte für Deutschland
- Smart Energy Grid der Zukunft – Securityprobleme und Lösungsansätze
- Der Transrapidunfall von Lathen als Beispiel für die Anwendung der Publikation „Technical Safety – An Attribute of Quality“
- Stärkung digitaler Infrastrukturen in Deutschland
- Herausforderungen einer domänenübergreifenden Risikoanalyse
- Weltkongress der Sicherheit

FORUM TECHNOLOGIE & GESELLSCHAFT

Eine Initiative des FORUM46 – Interdisziplinäres Forum für Europa e. V.

Die Veranstaltung wurde ermöglicht durch die freundliche Unterstützung des Fördervereins Ada Deutschland e.V., der DEKRA und der Bundesanstalt für Materialforschung- und prüfung (BAM als Gastgeber).

INHALT

PROJEKT „LANDKARTE DER SICHERHEITSINSTITUTIONEN IN DEUTSCHLAND“

Dr.-Ing. Bernd Schulz-Forberg

Einleitung

Sicherheit ist ein Querschnittsthema und damit praktisch in vielen (fast allen) Bereichen der Wirtschaft von Bedeutung. Die Sicherheitsinstitutionen innerhalb der Bereiche verantworten sicherheitsrelevante Teile bei Planung, Realisierung und Betrieb von Produkten, Systemen und Anlagen, und sorgen für ausreichenden Schutz durch geeignete Maßnahmen in allen Phasen der Produkt- / System- / Anlagenlebensdauer. Das Thema Sicherheit i.w.S. umfasst „Safety“ und / oder „Security“ einschließlich Vorsorge, Risikobetrachtung, Folgenabschätzung, Notfall- und Wiederanlaufplanung in allen Phasen.

Hauptkriterien als Sicherheitsinstitution

1. Ständige Aufgabe, ständiger Auftrag, gewählte Mission

2. Sicherheit ist ein Schwerpunkt in der Institution

(Der Schwerpunkt kann in Form von Ressourcen, Wirkung oder konkrete Aufgabe definiert werden.)

Unterkriterien

Den Sicherheitsdisziplinen werden die Akteure zugeordnet

Die Unterkriterien können in einer Matrix oder Liste angegeben werden, aus der sich die Zuordnung der Bereiche zu den handelnden Institutionen ablesen lässt. Dabei müssen die in den Wirtschaftsbetrieben agierenden Einheiten zu Sicherheitsaspekten wie Sicherheitsinstitutionen geführt werden.

Disziplinen

Angaben auf der Basis des Workshops des Fachausschusses 512 „Safety & Security“ der Gesellschaft für Produkt- und Prozessgestaltung im VDI

1. Arbeitssicherheit
2. Bauwerksicherheit
3. Automobile Sicherheit
4. Verkehrswesen
5. Mobilität
6. Öffentliche Sicherheit
7. Industrie 4.0
8. Lebensmittel-Sicherheit
9. Industrieanlagen / Produktionsanlagen
10. Produktsicherheit
11. Kritische Infrastruktur
12. Medizintechnik
13. Railway

Diese Disziplinen sind ein erster Entwurf der Fachgebiete und werden zur Zeit noch diskutiert.

SMART ENERGY GRID DER ZUKUNFT – SECURITYPROBLEME UND LÖSUNGSANSÄTZE

Dr. Hubert B. Keller

Schriftliche Fassung des Vortrags auf der Berliner *Gesamtkonferenz* der Sicherheitsinstitutionen

Einleitung

Der Vortrag behandelt die Sicherheit im Sinne IT-Security, die nachfolgend immer auch Auswirkungen auf Safety im Energiesystem der Zukunft hat. Es wird die typische Struktur des Energiesystems der Zukunft, mögliche Angriffsszenarien und Angriffsklassen vorgestellt. Eine typische Struktur des Smart Grid der Zukunft zeigt Bild 1. Aus der Struktur abgeleitet wird skizziert, wie mit diesen Angriffsszenarien umgegangen werden kann, welche klassischen und auch neueren Ansätze es hierzu für syntaktische und semantische Prüfungsmöglichkeiten und welche entsprechende Werkzeuge es gibt.

Bestimmte Manipulationen wie „False Data Injection" (FDI) sind allerdings mit klassischen Werkzeugen bzw. Ansätzen direkt nicht erkennbar. Ein typisches Beispiel hierfür ist Stuxnet, ein Wurm, der im Juni 2010 im Iran entdeckt wurde (/25/). Die Schadsoftware ist von Experten entwickelt worden, um industrielle Produktionsprozesse zu sabotieren und umfasste etwa 15 kLOC (Zeilen Programmtext). Stuxnet versuchte mit speicherprogrammierbaren Steuerungen (SPS) in Kontakt zu treten und wurde erst aktiv, wenn außer dem Betriebssystem Windows auch die Prozesssteuerungssoftware Siemens Step7 implementiert war. Die Schadsoftware manipulierte die gemessene Drehzahl der Geräte so, dass sie sich durch Überdrehzahl selbst zerstörten. Stuxnet kann sich über einen USB-Stick installieren, benötigt zur Infektion also keinen Internetzugang. Zur Absicherung gegen FDI wird kurz die modellbasierte Plausibilitätsprüfung vorgestellt. Eine kurze Darstellung von Normen rundet den Beitrag ab.

Bild 1: Zukünftige Struktur des Smart Energy Grid. Aus /1/

Das Institut für Automation und angewandte Informatik (IAI, https://www.iai.kit.edu/) hat eine methodische Ausrichtung mit zusätzlich Real-Laboren wie das Energy Lab 2.0. Die Anbindung ist sowohl an der Fakultät Informatik als auch an der Fakultät Maschinenbau. Das Institut ist in den Helmholtz Forschungsprogrammen Energie, im Energy Lab 2.0, im Projekt Kopernikus ENSURE, dem Projekt Energie System 2050 sowie im Rahmen des Projekts KASTEL (Kompetenzzentrum für angewandte Sicherheitstechnologie, https://www.kastel.kit.edu/) im Bereich der Sicherheit für Energiesysteme hoch interdisziplinär aktiv.

Das Smart Grid der Zukunft

Im Smart Grid der Zukunft wird Software die zentrale Basis für diese hoch vernetzte Infrastruktur. Die Automatisierung basiert dabei auf softwaretechnischen Funktionen unter Echtzeitbedingungen. Dazu charakterisiert der Münchner Kreis (siehe /2/) das Smart Grid wie folgt:

- intelligente, dezentrale Steuerung auf der Basis von Informations- und Kommunikationstechnologien (IKT)
- dezentral gestaltetes IKT-Steuerungssystem ... wird ... bezüglich seiner Komplexität über alle bisher bekannten IKT Systeme hinausgehen
- Die IT-Infrastruktur muss Sicherheit und Zuverlässigkeit gewährleisten
- besonders relevant: ..... die Gestaltung von System-Software-Architekturen ..., ... Entwicklung von gesamtsystemischer Resilienz... die Entwicklung von Evolutions- und Migrationsstrategien für Legacyinfrastrukturen und -systeme ...
- neue Verschlüsselungsmethodiken für ressourcenbeschränkte Sensoren benötigt.

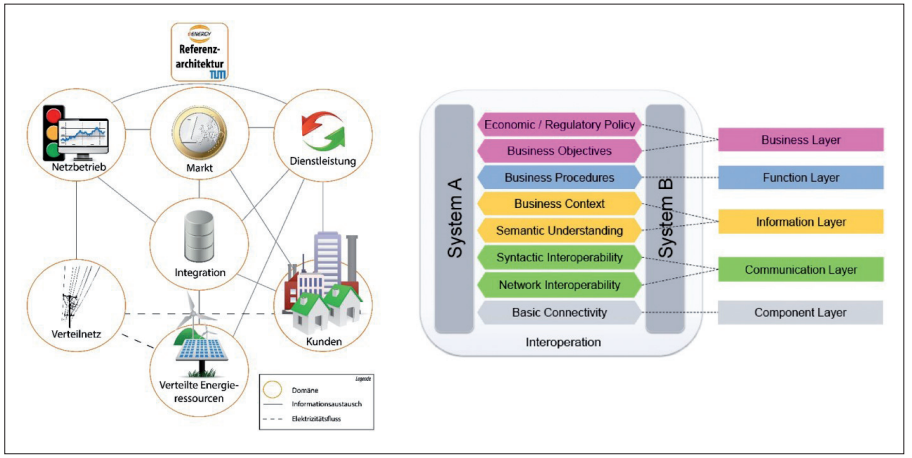


Bild 2: Wechselwirkungsprozesse und Geschäftsebenen im Smart Energy Grid. Aus /3/

Die Veränderungen bestehen im Ersatz großer, zentraler Kraftwerke durch viele kleine und verteilte Kraftwerke mit Steuerung aus der Ferne (Remote). Statt einer kontinuierlichen Verfügbarkeit in einem statischen Stromnetz macht eine schwankende Verfügbarkeit, flexible Netzstrukturen und vielen steuerbaren Elementen erforderlich. Die bisherige Sicherheit über physische Beschränkungen im direkten Zugriff kann bei unsicheren Netzwerken wie dem Internet und zahlreichen Zugangspunkten nicht mehr garantiert werden. Hierzu bedarf es eines erheblichen IT-Sicherheitsschutzes.

Die strukturelle Komplexität beinhaltet alle Ebenen des Smart Grid, von der physikalischen Stromschnittstelle über Netzwerkdienste bis hin zu Geschäftsmodellen im Stromhandel. Das Bild 2 (siehe /3/) verdeutlicht diese Ebenen und deren Wechselbeziehungen.

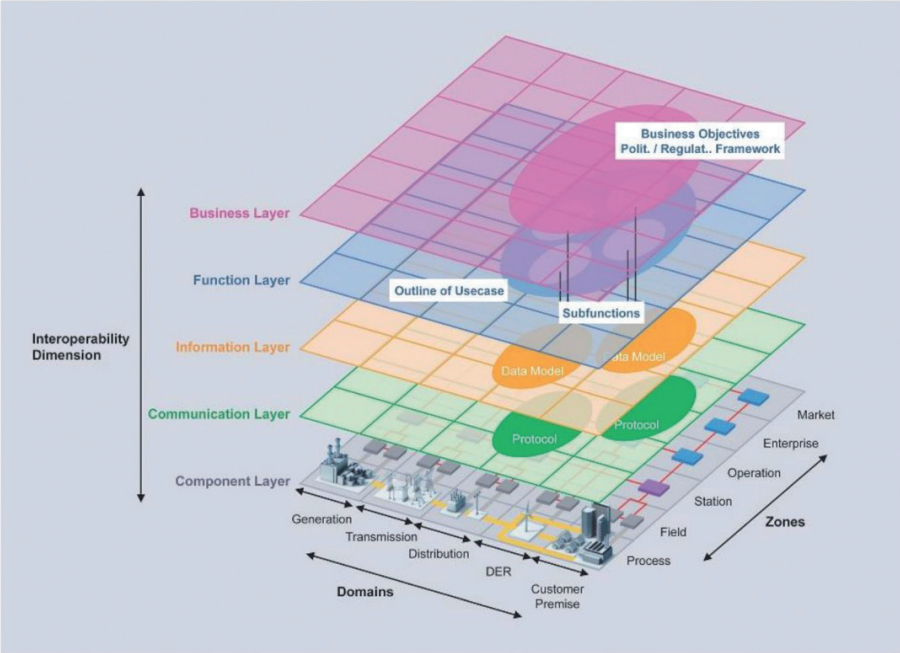


Bild 3: Dreidimensionale Bezüge im Betrieb des Smart Energy Grid (Smart Grid Achitecture Model – SGAM). Aus /3/.

Die Dimensionen des Smart Grid sind dabei sowohl in den Bereichen der Erzeugung und des Verbrauchs, der Ebenen der Geschäftsvorgänge vom Erzeugungsprozess bis zum Handel und der verschiedenen Interaktionsebenen zu sehen (vgl. Bild 3).

Der einzelne Kunde wird dabei auch als Privatperson lokal ebenfalls ein komplexes System zu verwalten haben, das im Rahmen der möglichen Geschäftsvorgänge zu konfigurieren und zu steuern ist (vgl. Bild 4).

Der aktuelle Status in den verschiedenen Funktionen des Smart Grid und die zukünftig zu erwartenden komplexen Funktionen sind im Bild 5 dargestellt.

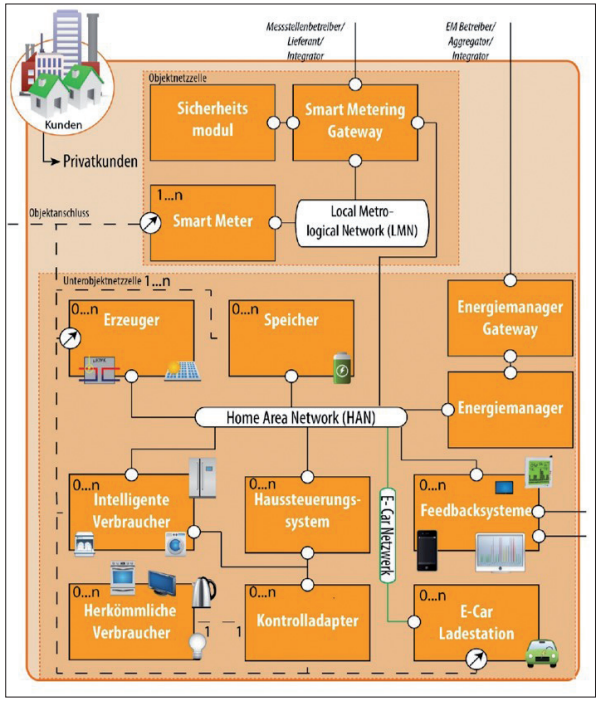


Bild 4: Komplexität der Steuerung im Privathaus. Aus /3/.

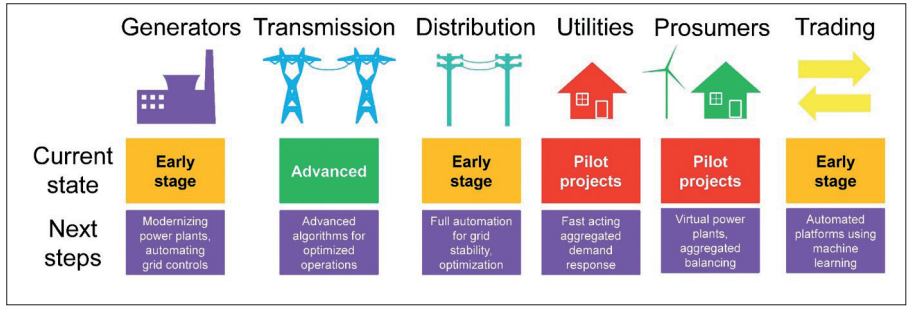


Bild 5: Aktueller Status und zukünftige Perspektive im Smart Grid. Aus /4/.

Anforderungen an das Smart Grid

An das Smart Grid als verteilte und in Echtzeit zu reagierende kritische Infrastruktur ergeben sich umfangreiche Anforderungen.

1. Verfügbarkeit in Echtzeit:

Dies bezieht sich auf den Zugriff auf Daten oder Dienste für autorisierte Beteiligte bei Bedarf. Die Ver-

fügbarkeit garantiert eine unterbrechungsfreie Funktion der Anlagen ohne unerwartete Ausfallszeiten. Kommunikationsbeziehungen beinhalten aber auch Totzeiten, welche sich auf das Gesamtverhalten auswirken.

2. Integrität:
Dies bezieht sich auf die Konsistenz, die Verlässlichkeit und die Authentizität der Informationen durch Verhinderung von nicht autorisierten Veränderungen. Das Vertrauen in die erzeugten, übertragenen, gespeicherten und visualisierten Daten in syntaktischer und semantischer Hinsicht sowie die Legitimation von Sender und Empfänger muss gesichert sein.

3. Vertraulichkeit:
Dies bezieht sich auf den Schutz der Daten vor Einsicht gegenüber nichtautorisierten Beteiligten. Der Bruch der Vertraulichkeit bewirkt noch keine Fehlfunktion.

4. Zuverlässigkeit:
Dies ist die Fähigkeit eines Systems über einen definierten Zeitraum seine Funktionalität unabhängig vom Bedarf zu realisieren. Durch Redundanz wird die Zuverlässigkeit erhöht.

5. Resilienz oder Widerstandsfähigkeit:
Resilienz stellt die Widerstandsfähigkeit bei Störungen, Angriffen oder auch Naturkatastrophen bei Aufrechterhaltung oder der schnellen Wiederherstellung von Diensten dar. Resilienz-Verfahren erhöhen auch die Zuverlässigkeit.

6. Skalierbarkeit:
Dies betrifft die Frage der prinzipiellen Eignung für beliebig große Smart Grid Architekturen. Smart Grids bestehen aus einer hohen Anzahl unterschiedlicher Komponenten. Dieses Netzwerk im Sinne Resilienz in seiner Architektur zu modellieren, ist eine große Herausforderung.

7. Privatheit:
Der Schutz privater Daten bei der Übertragung über unterschiedliche Komponenten wie von modernen Smart Meter betrifft die Vertraulichkeit der Nutzung und deren Art privater Geräte und die Nichtzurückverfolgbarkeit aggregierter Informationen.

8. Funktionale Sicherheit:
Dies beinhaltet alle Maßnahmen und Vorschriften im Betrieb von Smart Grids, um Anlagen und Menschen vor unverhältnismäßigen Risiken wie Unfälle etc. zu schützen.

Eigenschaften von Smart Grids

Im Unterschied von klassischer IT ist bei Smart Grids kein permanentes Updaten von Software der Automatisierungssysteme möglich. Gleichzeitig sind Security Mechanismen auch in klassischen IT-Systemen nicht langzeitstabil und ausgetestet. In klassischen IT-Systemen bezieht sich ein Angriff meist auf lokale Daten, bei Smart Grids entstehen durch die physikalische Vernetzung im Stromnetz massive Kollateralschäden.

Normalerweise haben auch industrielle Automatisierungssysteme eine eher hierarchische Struktur. Dies gilt allerdings nicht mehr für das Smart Grid. Hinzu kommt, dass neben der klassischen Ethernet-Kommunikation eine Vielzahl weiterer Protokolle für die Verbindung von Geräten und die übergeordnete Kommunikation wie Distributed Network Protocol (DNP) 3, IEC61850, Inter-Control Center Protocol (ICCP), usw. benutzt werden. Security-Lösungen sind daher nicht auf Basis eines allgemeinen Netzwerk Protokolls möglich.

Smart Grids entwickeln sich also von einer hierarchischen zu einer flachen und vielfältig vernetzten Struktur. Es werden eine Vielzahl small-scale-Erzeuger in das Netz integriert. Die schwankende Energieverfügbarkeit erfordert eine hohe Flexibilität beim Verbraucher hin zu einem sogenannten demand-site Management. Die notwendigen Informationen werden durch Smart Devices erfasst und als Basis für eine massive flexible Automatisierung und Beobachtung weitergegeben. Letztlich muss für die Auslegung und den Betrieb sowohl das Stromnetz als auch das Kommunikationsnetz modelliert und entsprechend ausgelegt werden. Hinzu kommt, dass weiterhin klassische IT-Systeme im Verbund mitwirken.

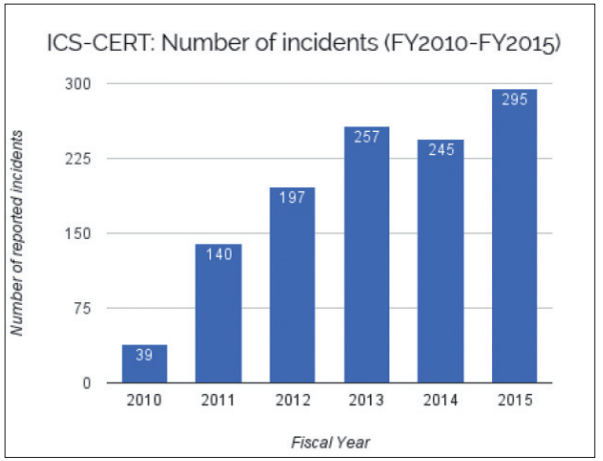


Bild 6: Entwicklung der Angriffe, die an ICS-CERT gemeldet wurden. Siehe /5/.

Angriffsszenarien

Cyber-Angriffe nehmen zu (siehe Bild 6), ebenso aber auch die immer wieder festgestellten Schwachstellen in der Software von Automatisierungssystemen aber auch in Security-Geräten, die die Sicherheit eigentlich verbessern sollen.

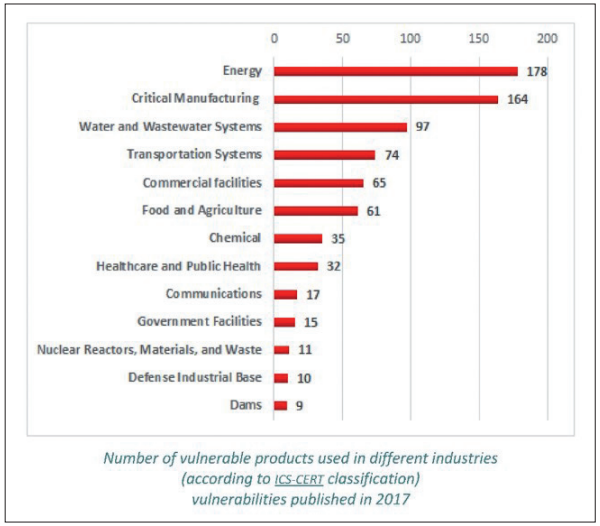


Bild 7: Angriffsziele von durch ICS-CERT registrierte Cyber-Attacken im Jahr 2017. Aus /6/

Nach dem US CERT stiegen die Vorfälle in industriellen Automatisierungssystemen seit 2010 permanent an. Gleichzeitig ist der Energiesektor das Angriffsziel Nummer 1. Das Bild 7 zeigt die aktuellen Fallzahlen aus dem Jahre 2017.

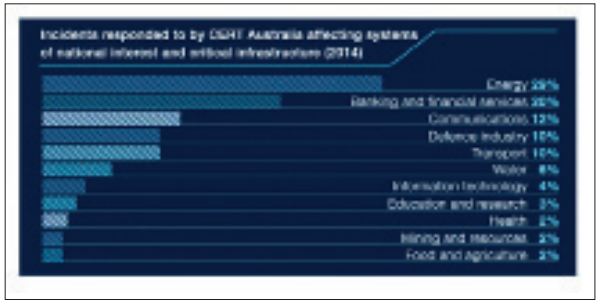


Bild 8: Angriffsziele von durch CERT Australia registrierten Cyber Attacken in Australien im Jahr 2014. Aus /7/.

Damit übereinstimmend zeigen die Zahlen z.B. aus 2015 des Australischen Cyber Security Center, dass der Energiesektor unter den betrachteten Systemen dem höchsten Angriffsdruck ausgesetzt ist (Bild 8).

Die möglichen Angriffszenarien sind

- Denial of Service (kurz DoS, englisch für Dienstverweigerung),
- die Umgehung bestimmter Sicherheitsmechanismen, wie zum Beispiel die Angriffsvariante Man in the Middle,
- die absichtliche Fehlbedienung durch zulässige Aktionen, wie zum Beispiel Passwort-Diebstahl,
- die Fehlbedienung durch nicht oder falsch konfigurierte Zugriffsrechte,
- das Ausspionieren von Daten, wie zum Beispiel Rezepturen und Geschäftsgeheimnisse bzw. Betriebspläne für Anlagen und deren Sicherheitsmechanismen,
- die Manipulation von Daten, wie zum Beispiel Bagatellisieren der Bedeutung von Alarmen, das Löschen von Daten, wie zum Beispiel Log-Dateien, um Attacken zu vertuschen sowie
- die besonders kritische Bad Data Injection oder False Data Injection (Sensormanipulation)

Der zuletzt genannte Angriff ist der gefährlichste, da die manipulierten Werte innerhalb der zulässigen Wertebereiche liegen, mittels normalem Kommunikationsverkehr (Traffic) übermittelt werden, aber die physikalische Anlage in nicht zulässige Grenzbereiche bringen und damit zur Zerstörung führen. Der Stuxnet-Virus war ein solcher Angriff, bei dem der Sensor für die Drehzahlerfassung manipuliert wurde, permanent zu niedrige Drehzahlen gemeldet wurden und der Regler die Zentrifuge bis zur Zerstörung hoch geregelt hatte. Ähnliches kann auch bei einer Windkraftanlage geschehen, wenn z.B. der Sensor für die Windgeschwindigkeit oder des Pitch-Winkels manipuliert wird (vgl. Bild 9). Außerdem können erlaube Werte in Wechselwirkung mit anderen Werten eine Anlage in einen kritischen Gesamtzustand bringen und in Kombination Schäden verursachen. Das erstere geht von der Manipulation eines zentralen Wertes aus, das zweite von einer kritischen Kombination von Werten.

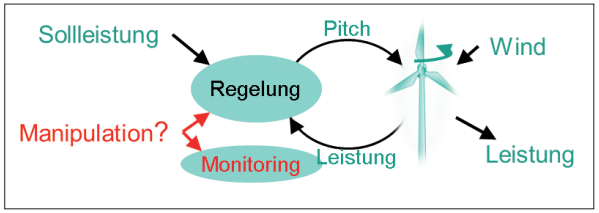


Bild 9: Prüfung auf Manipulation der Regelkreise bzw. Sensoren bei Windkraftsystemen. Aus /8/.

Angriffspunkte physikalischer Natur werden nachfolgend beschrieben:

- Trägheits-Angriffe erzeugen eine Veränderung der Geschwindigkeiten von schweren Komponenten, was zu massiven Schäden an der Anlage führt.
- Resonanzangriffe bewirken durch geringfügige Veränderungen das mehrfache Durchlaufen von nicht zulässigen Resonanzfrequenzen und führen ebenfalls zur Zerstörung.
- Verschleißangriffe erfolgen über böswillige Kommandos und reduzieren die Lebensdauer der Anlagen.
- Impulsartige Angriffe überschreiten die Grenzen der zulässigen Prozesszustände und führen zum Not-Aus der Anlage.
- Angriffe zum Ausnutzen verborgener Eigenschaften führen ebenfalls zum Abschalten oder zur Zerstörung der Anlagen. In vielen Software-Systemen sind verborgene Funktionen enthalten, welche

aktiviert werden können.

- die Manipulation von Daten, wie zum Beispiel Bagatellisieren der Bedeutung von Alarmen, das Löschen von Daten, wie zum Beispiel Log-Dateien, um Attacken zu vertuschen sowie
- die besonders kritische Bad Data Injection oder False Data Injection (Sensormanipulation).
- False Data Injection liefert eine falsche Zustandsinformation. Die Daten für die Analyse, Regelung und Optimierung müssen in Echtzeit erfasst und bereitgestellt werden. FDI liefert manipulierte bzw. falsche Zustandswerte durch Veränderung der Messungen oder übertragenen Daten. Es gibt zwar Verfahren zur Erkennung fehlerhafter Werte (Bad Data Detection Tool), dies ist aber im Wesentlichen auf rein syntaktischer Ebene oder semantisch bzgl. grundsätzlicher Wertebereiche angesiedelt. Damit kann die Korrektheit der Struktur der Daten geprüft werden. Ein korrekt generierter Datenwert innerhalb des zulässigen Wertebereichs des Messgeräts löst keinen Alarm aus und kann dennoch das System in einen kritischen Zustand führen.
- Nur eine partiell auf das Messgerät ausgerichtete oder eine volle Kenntnis des Systemzustands bzw. eine modellbasierte Plausibilitätsprüfung kann solche Manipulationen erkennen. Sowohl die Kenntnis des Systemzustands als auch die Existenz eines Modells des Systems sind zur Überprüfung notwendig. Diese Prüfung muss permanent parallel zum Betrieb erfolgen.
- Hinzu kommen die klassischen Angriffsvektoren wie „Buffer Overflow", was nach wie vor in hoher Zahl auftritt. Hier wird ein Datum bestimmter Größe mit Daten von deutlich umfangreicherer Größe überschrieben und damit weitere Daten- oder Adressbereiche (Rücksprungadressen etc.) überschrieben. Strategien wie zufällige Speicherbelegungen stellen eine Abhilfe dar, besitzen aber selbst wieder neue Schwachstellen.
- Schwachstellen in der Auswertung von Zeichenketten wie z. B. Dateibezeichnungen besitzen Eigenschaften, die es durch bösartige Zeichenkompositionen ermöglichen, in Speicheradressen zu schreiben oder die Zugriffsroutine selbst zu manipulieren.
- Weitere klassische Angriffe erfolgen durch Viren, Würmer, Trojaner und Bots sowie Man in the Middle und Reply-Angriffe.

Eine Übersicht über die Angriffe zeigt Bild 10.

Schwachstellen

Angriffe richten sich immer gegen existierende Schwachstellen in der Software eines Systems. Diese können in nicht aktualisierter Software bei erkannten Schwachstellen liegen, in der Mensch-Maschine-Schnittstelle über das Internet, in fehlerhaften Protokollen zur Remote-Darstellung von Prozesszuständen, fehlerhaften Festlegungen der Zugriffsrechte bzw. deren Auswertung, fehlerhafte Feststellung der berechtigten Person, Buffer Overflow, Kommando - und Parameterwert-Manipulationen und nachfolgend die fehlerhafte Auswertung mit Übergang in einen unzulässigen Zustand des Systems, Datenbankmanipulation durch SQL-Anweisungen, die Verwendung von Protokollen mit Klartext sowie der ungeschützten Übertragung von Zugangsdaten (siehe hierzu Bild 10 und den Literaturverweis /10/).

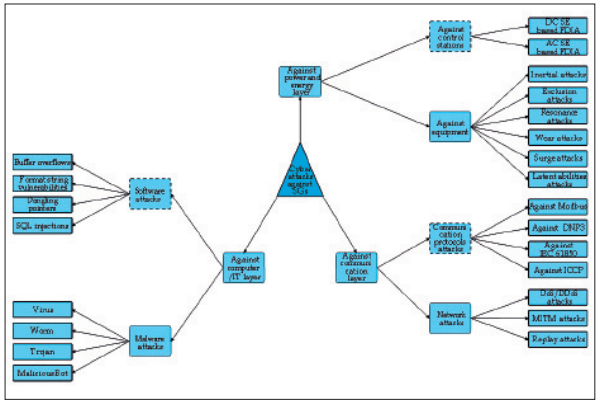


Bild 10: Klassifikation von Cyber Angriffen. Aus /9/.

Die Bewertung der Kritikalität einer Schwachstell erfolgt anhand des "Common Vulnerability Scoring System" – CVSS.
Bewertet wird

- wie sich die Schwachstelle nach außen äußert,
- die Angriffskomplexität,
- die Zahl der Anmeldevorgänge zur Identitätsfeststellung,
- das Maß des Vertrauensbruchs, der Integritätsverletzung sowie
- der Verfügbarkeit.

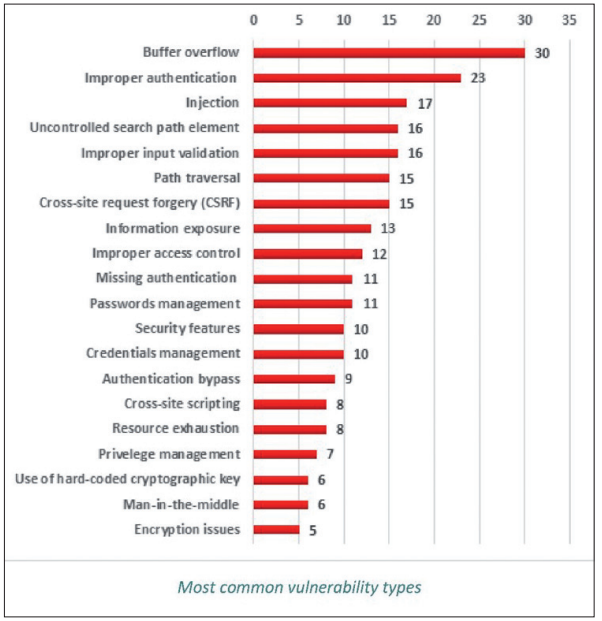


Bild 11: Verteilung der entdeckten Schwachstellen bei ICS Systemen im Jahr 2017 (Summe = 322). Zusammenstellung durch Kaspersky Lab auf Basis der Meldungen des ICS-CERT. Aus /6/.

Nach wie vor ist der Buffer

Overflow die häufigste Schwachstelle (vgl. Bild 11 und 12). Damit zeigt sich, dass die grundlegende Zuverlässigkeit in der Software nicht gewährleistet ist. Denn die Prüfung von Eingangsdaten auf syntaktische und semantische Korrektheit sollte ein zentraler Vorgang sein. Werte der Indexbereichsverletzungen führen immer zu fehlerhaftem Verhalten von Software. Sprachen, welche dies nicht automatisch über die Typbeschreibungen und -prüfungen leisten, sollten für Software von kritischen Infrastrukturen etc. nicht eingesetzt werden.

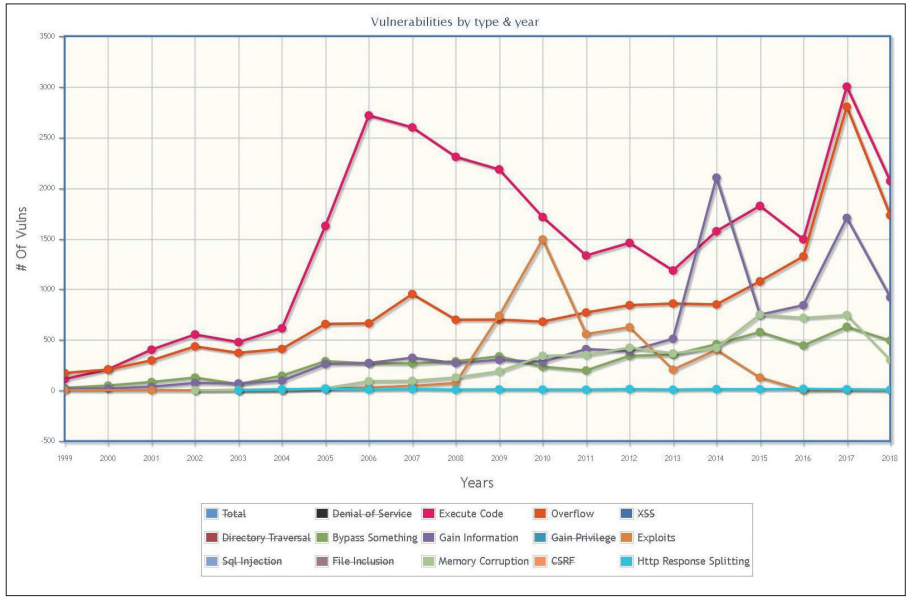


Bild 12: Entwicklung ausgewählter, entdeckter Schwachstellen bei ICS Systemen. Zusammengestellt durch Kaspersky Lab auf Basis der ICS-CERT Meldungen. Aus /6/.

Die überwiegende Anzahl der Security-Schwachstellen (z.B. Buffer Overflow) können damit auf Implementierungsschwachstellen zurückgeführt werden. Die genannten Schwachstellen betreffen auch Betriebssysteme und gerade auch Security-Infrastruktursysteme wie Security-Router, virtuelle Maschinen etc. Deutlich mehr als die Hälfte (194 von 322) waren kritische bzw. höchstkritische Schwachstellen mit einem Risikofaktor über 7 bei einem Maximalrisikowert von 10. Der Risikowert beschreibt dabei die Einfachheit eines dadurch möglichen Angriffs.

Für Automatisierungssysteme (SCA – Supervisory Control and Data Akquisition sowie ICS – Industrial Control Systems) wurde in den USA eine sogenannte ISA-SCADA-Architektur für Securityanforderungen

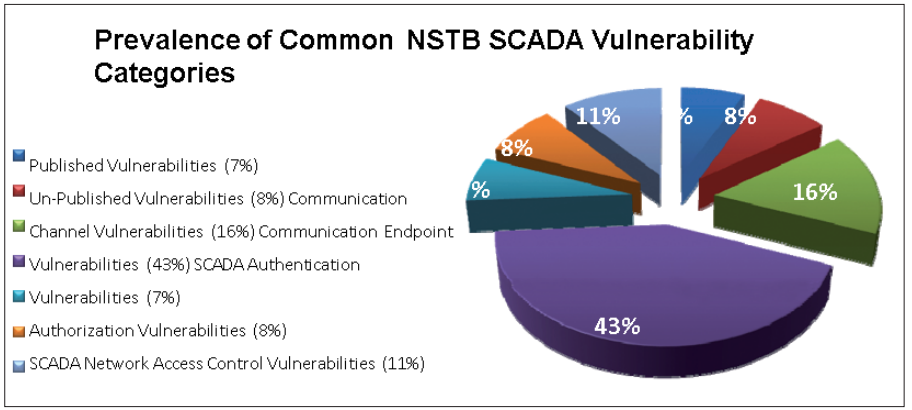
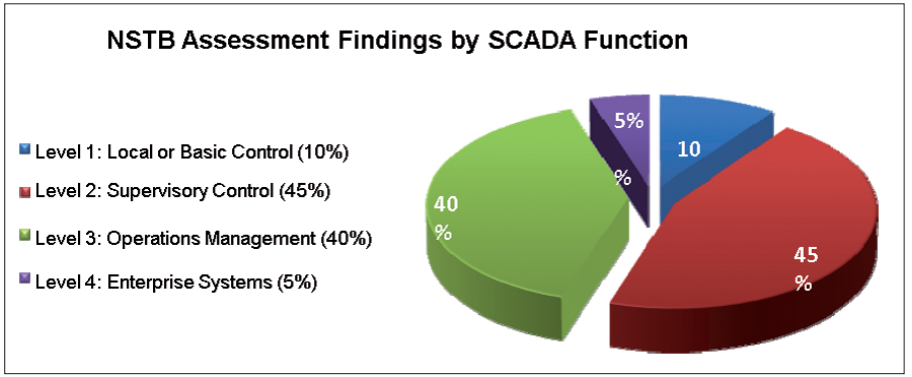


Bild 13: Schwachstellen in SCADA-Systemen. Aus /11/.



definiert (ISA99 - Industrial Automation and Control Systems Security, International Society of Automation), diese ist aber anhängig von sicheren Kommunikationsroutern etc. für die Verbindung der getrennten Ebenen usw. Da diese Systeme selbst die genannten Schwachstellen besitzen, werden damit eher noch zusätzliche Angriffsvektoren eingeführt.
Im Bericht „NSTB Assessments Summary Report: Common Industrial Control System Cyber Security Weaknesses" (/11/) wurden 45% der Schwachstellen auf der SCADA-Ebene eingeordnet (vgl. Bild 13). 43% der festgestellten Schwachstellen waren Authentifizierungsfehler.

Hersteller von Automatisierungssystemen wie Siemens propagieren Sicherheitsgeräte analog der ISA SCADA-Architekturstruktur. Das Bild 14 zeigt diese Konzepte.
Allerdings haben diese Systeme nachweislich den Meldungen des US bzw. ICS CERT immer wieder festzustellende Schwachstellen, wobei dies für alle Hersteller synonym gilt:

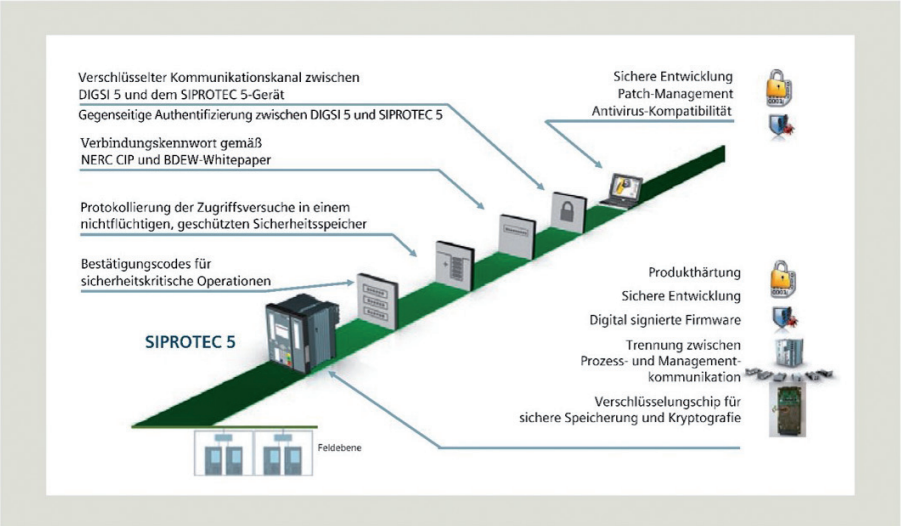


Bild 14: Sicherheitsarchitektur in ICs und SCADA-Systemen. Aus /12/.

Advisory (ICSA-18-067-01) Siemens SIPROTEC 4, SIPROTEC Compact, DIGSI 4, and EN100 Ethernet Module (Update B) Original release date: March 08, 2018 | Last revised: May 17, 2018

CVSS v3 7.5 – ATTENTION: Exploitable remotely/low skill level to exploit – Vendor: Siemens – Equipment: SIPROTEC 4, SIPROTEC Compact, DIGSI 4, and EN100 Ethernet module – Vulnerabilities: Missing Authentication for Critical Function, Inadequate Encryption Strength

Successful exploitation of these vulnerabilities could allow an attacker to upload a modified device configuration that could overwrite access authorization passwords, or allow an attacker to capture certain network traffic that could contain authorization passwords.

Auch CISCO als Hersteller von Security Komponenten für die Kommunikation hat hier erhebliche Defizite:

- Cisco Releases Security Updates,
- Original release date: May 16, 2018
- Cisco has released updates to address vulnerabilities affecting multiple products.
- A remote attacker could exploit some of these vulnerabilities to take control of an affected system.
- NCCIC encourages users and administrators to review the following Cisco Security Advisories and apply the necessary updates:
  - Digital Network Architecture Center Static Credentials Vulnerability cisco-sa-20180516-dnac
  - Digital Network Architecture Center Authentication Bypass Vulnerability cisco-sa-20180516-dna2
  - Digital Network Architecture Center Unauthorized Access Vulnerability cisco-sa-20180516-dna
  - Enterprise NFV Infrastructure Software Linux Shell Access Vulnerability cisco-sa-20180516-nfvis
  - Meeting Server Media Services Denial-of-Service Vulnerability cisco-sa-20180516-msms
  - Identity Services Engine EAP TLS Certificate Denial-of-Service Vulnerability cisco-sa-20180516-iseeap
  - IoT Field Network Director Cross-Site Request Forgery Vulnerability cisco-sa-20180516-fnd

Methoden für IT-Security

Die Grundlagen für Safe & Secure-Systeme sind die konstruktive Sicherstellung der Zuverlässigkeit durch den Einsatz sicherer Programmiersprachen wie Ada oder Rust, die Erkennung von Manipulationen in der Kommunikation, die Absicherung der Regelkreise durch Plausibilitätsprüfungen, die Identifikation kritischer Komponenten und deren Expositionskritikalität mit nachfolgender Absicherung und die Verwendung redundanter Messsysteme. Diese Aspekte zeigt das Bild 15.

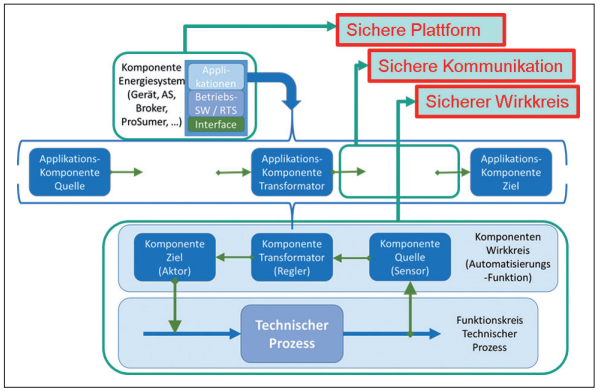


Bild 15: Zentrale Sicherheitsanforderungen im Smart Energy Grid. Vgl. hierzu /9/.

Eine sichere Plattform als Basis für Applikationen erfordert ein verlässliches und transparentes Betriebssystem. Leider hat hierzu die Entwicklung in Deutschland komplett ausgesetzt. Das von der GMD bzw. Fraunhofer First entwickelte Betriebssystem L4 Mikro-Kernel ist leider nie Grundlage für eine deutsche Entwicklung geworden. Dafür wurde es aber in den USA als Basis für die Entwicklung sicherer Betriebssysteme von General Electric verwendet.

Bei der Absicherung von Systemen gegen Cyber Angriffe existieren grundsätzliche Vorgehensweisen:

- die sogenannte Härtung,
- der Einsatz von Honey Pots zur Ablenkung und Analyse des Angriffsverhaltens,
- Intrusion Detection und Prevention Systeme sowie
- die modellbasierte Plausibilitätsprüfung gegen FDI.

Eine absolute Sicherheit gibt es nicht, diese kann aber über Resilienzeigenschaften, als die Fähigkeit

eines Systems, seine Funktionsfähigkeit unter Belastungen aufrechtzuerhalten, beziehungsweise kurzfristig wiederherzustellen, deutlich erhöht werden. Redundante Sensoren, diversitäre Software, konfigurierbare Kommunikationswege etc. sind Methoden, um die Resilienz eines Systems zu erhöhen. Basis ist aber immer die konstruktive Zuverlässigkeit der Softwarerealisierung.

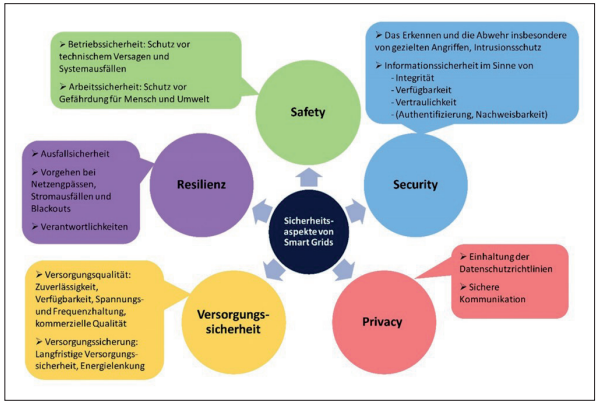


Bild 16: Sicherheitsaspekte in Smart Grids. Aus /13/.

Das Bild 16 verdeutlicht diese gesamte Eigenschaftsstruktur für das zukünftige Smart Grid.

Wesentliche Vorgaben sind:

- Absicherung der Angriffsoberflächen (Angriffsvektoren)
- Entwurf und Implementierung von sicherem Programmcode
- Potentiell unsichere Funktionen durch sichere Alternativen ersetzen
- Eingaben bzw. Kommunikationsdaten immer validieren (syntaktisch und semantisch)
- Maßnahmen gegen Buffer Overflow einsetzen (Eingabewerte, Längen und Wertebereiche prüfen)
- Bei Datenbankabfragen SQL-Anweisungen prüfen
- Weboberflächen bzw. Zugänge gegen Angriffe über Scripts prüfen
- Dateinamen und Verzeichnisnamen prüfen

Weitere Maßnahmen sind

- Bei bekannten Schwachstellen
  - Ports und Dienste nur in minimalem Umfang anbieten (unbedingt notwendig)
  - Anwendungen und Dienste auf das absolut notwendigste zu beschränken
  - Ein effektives Update und Patch Management installieren
- Allgemeine Protokolle in SCADA-Systemen
  - Zugangsberechtigungen bei Übertragungen schützen
  - Sichere Fernzugriffe implementieren

- SCADA-Daten, und Kommando-Übertragungsprotokolle
  - Schutz der Zugangsberechtigungen bei der Kommunikation
  - Implementierung sicherer Zugriffskontrollen und Prüfung der Datenintegrität
  - Verschlüsselung von Daten einsetzen
- Schutz vor Man-in-the-Middle-Angriffen (Signaturen)
- Datenbanken und Webanwendungen umfassend schützen
- Eindeutige Feststellung der Identitäten und Berechtigungen mit einem sicheren Verwaltungssystem

Inwieweit die Absicherung, Segmentierung und Überwachung eines Netzwerks, die Protokollierung der Ereignisse und die Verbesserung erkannter Schwachstellen hilft, bleibt aufgrund prinzipieller Schwachstellen fraglich. Die Purdue Enterprise Reference Architecture (Bild 17) definiert dazu eine erste Schicht der Verteidigung, einen Sicherheitsbereich (Zaun) zwischen Geschäfts- und Steuerungsbereich, weitere Unterteilungen mit Absicherung im Steuerungsbereich sowie Segmentierungen mit zusätzlichen Zugangskontrollen. Allerdings bedeutet der Einsatz von z.B. Security-Routern auch die Einfüh-

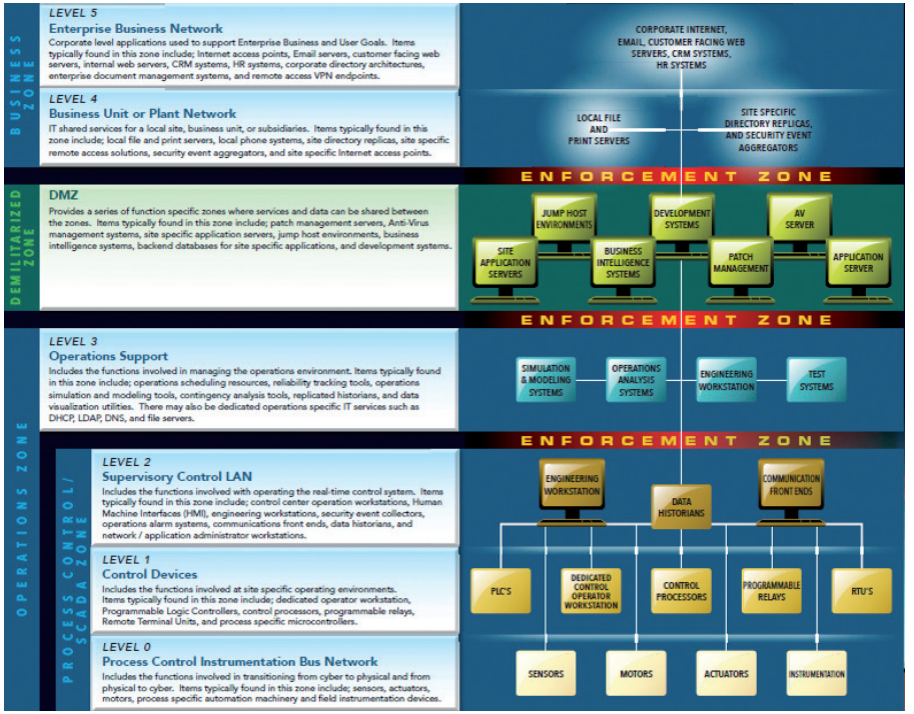


Bild 17: Segmentierung in SCADA-Systemen zur Sicherheit. Aus /14/.

rung neuer Schwachstellen. Sogenannte Datendioden sollen sicherstellen, dass Informationen nur in eine Richtung fließen können. Firewalls sind meistens nicht dafür ausgelegt, tiefe semantische Analysen der übermittelten Daten durchzuführen.

Die Konkretisierung der Verfahren setzt eine Kultur voraus, welche Security massiv adressiert, Entwickler in der Programmierung sicherer Software trainiert und hierzu erzieht, Schwachstellen schnell kommuniziert, eine strenge Feststellung der Identität und der Rechte beim Zugang durchführt und erheblichen Fokus auf Safety und Security legt.
Letztlich bedeutet dies beim Betrieb die Minimierung aller Funktionalitäten auf das absolut notwendige. Das Motto lautet also:

- Schalte alles ab, was nicht gebraucht wird
- Vermeide jeden nicht absolut notwendigen Zugriff
- Prüfe jedes Datum, das von außen kommt
- Programmiere sicheren Code
- Setze eine sichere Programmiersprache und ein sicheres Betriebssystem ein

Diese sukzessive Vorgehensweise ist im nachfolgenden Bild 18 dargestellt.

Weitere Methoden sind der Einsatz von Honey Pots, Intrusion Detection bzw. Intrusion Prevention Systeme. Diese verhindern Angriffe aber nicht und können auch nicht alle Angriffsarten erkennen. Modellbasierte Ansätze erlauben auch tiefe semantische Analysen und die Erkennung von False Data Injection (FDI). Nachfolgend werden diese Verfahren kurz skizziert.

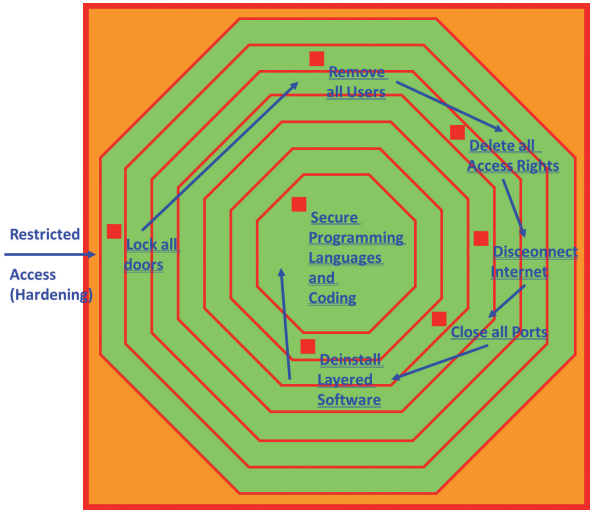


Bild 18: Sukzessive Härtungsspirale

Honey Pots (Honigtöpfe)

Das Ziel von Honey Pots ist die Erfassung und Identifikation unbekannter Gefährdungen durch die Beobachtung von Angriffen auf vorgeschaltete Pseudo-Anlagen. Damit lassen sich Informationen gewinnen über die Vorgehensweise der Angreifer und gleichzeitig die realen Anlagen abschotten. Allerdings ist der Aufwand nicht zu unterschätzen, da reale Anlagen sehr detailliert nachgebildet werden müssen, um den Angreifer wirkungsvoll zu täuschen. Honey Pots sind immer zusätzliche Maßnahmen zu den anderen Security-Maßnahmen.

Intrusion Detection Systems (IDS)

IDS gehen von der Annahme eines normalen Profils an Kommunikationsverkehr aus und suchen Aktivitäten, welche hiervon abweichen. Dazu wird der Datenverkehr intensiv überwacht und analysiert. Abweichungen vom normalen Kommunikationsmuster dienen zur Erkennung von Angriffen. IDS untersuchen nicht den Angriff selbst und ergreifen auch keine Gegenmaßnahmen. In der Kommunikation unter Echtzeitbedingungen sind IDS nur schlecht einsetzbar, da sie die Übertragungszeiten negativ verändern. Signaturen erlauben dem IDS auch zu prüfen, ob Firewall-Regeln korrekt umgesetzt worden sind. FDI können durch IDS nicht erkannt werden.

Intrusion Prevention Systems (IPS)

IPS sind gleichzeitig auch IDS und untersuchen den Datenverkehr analog. Darüber hinaus sind sie in der Lage ihr Security-Profil zu ändern, falls neue Bedrohungen erkannt werden. Dies beinhaltet eine tiefere Analyse der Daten, die Veränderung von Konfigurationen, die Blockade des Weges der Übertragung manipulierter Daten, die Rekonfiguration von Geräten und die Erweiterung von Regeln bis hin zum Streichen bzw. zum Ersatz der manipulierten Daten. IPS arbeiten mit einer Signatur basierten Erkennung (Muster) in den übertragenen Daten, mit einem Vergleich der festgestellten Aktivitäten gegen eine Normalaktivität sowie bis zu einer Zustandsanalyse des Netzwerk-, Transport- und Anwendungsprotokoll. Allerdings kann der Zustand des technischen Systems, das abgesichert werden soll, nicht überwacht und geprüft werden. FDI Angriffe können also auch nicht erkannt werden. Details zu IDS und IPS finden sich in /15/.

Modellbasierte Plausibilitätsprüfung

Ohne tiefe Kenntnis des zu schützenden technischen Prozesses können FDI nicht erkannt werden. Aus einer Voranalyse wird die Exposition und Kritikalität bestimmter Zustandsgrößen und Komponenten

wie Sensoren abgeleitet. Zusätzlich wird untersucht, wie eine Zustandsgröße gemessen wird und ob es Redundanzen direkt oder über Modellansätze gibt. Ein Angreifermodell ist bei diesem Ansatz nicht erforderlich.

Es wird eine Systembeschreibung in Form von Gleichungen (Modell) erstellt und es erfolgt ein Vergleich der Messwerte mit dem Modell. Eine Methode hierzu ist das „Data Reconciliation" in Form der Minimierung der Differenz zwischen optimiertem und gemessenem Wert mit dem Modell als Nebenbedingung. Entweder die Modellgleichung wird erfüllt oder es ergeben sich größere Differenzen. Die Fehlerdetektion bzw. Fehlerlokalisierung erfolgt über statistische Methoden und Zusatzwissen aus Voranalysen. Bei erkannten Manipulation wären gezielte Gegenmaßnahmen z.B. eine Unterbrechung von Kommunikationskanälen, die Verwendung eins BackUp Konzepts oder letztlich die Notabschaltung. Eine zurzeit untersuchte Anwendung ist die Windkraftanlage zur Stromerzeugung (siehe Bild 19).

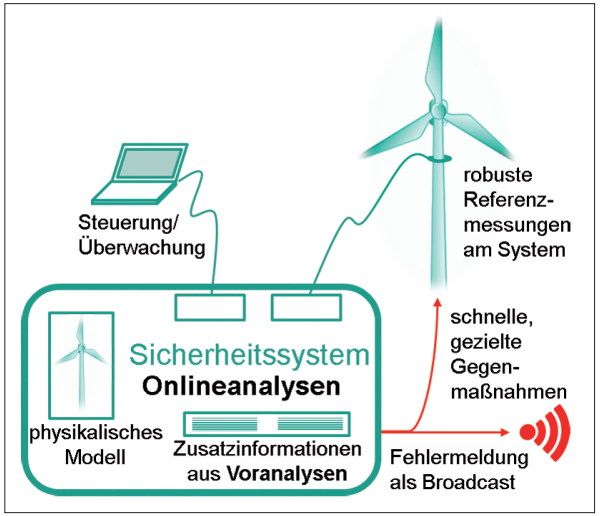


Bild 19: Modellbasierte Plausibilitätsprüfung. Aus /8/.

Konstruktive Security

Eine konstruktive Security erfordert die Einbeziehung der Security-Anforderungen im Requirements Engineering. Es ist eine sichere Software-Architektur zu entwerfen und jede Funktion ist bzgl. ihres Sicherheitslevels zu betrachten. Nachfolgend muss die Implementierung mit einer sicheren Programmiersprache auf einem sicheren Betriebssystem oder Laufzeitsystem erfolgen.

Bild 20: Status im Einsatz von Programmiersprachen. Aus 16/.

Die Tabelle in Bild 20 zeigt den Status im Software Engineering hinsichtlich des Einsatzes konstruktiv zuverlässiger Methoden und Werkzeugen. Es erstaunt, dass im Web Design auf zuverlässige Programmiersprachen (Rust) und definierte Prozesse (Compilierungssystem mit inkrementeller Erweiterung) gesetzt wird und im Automatisierungsbereich nach wie vor Sprachen wie C und C++ mit massiven

Jahr	Web	Industrie	Automotive	Energie
ca 1989	**Öffnung von Systemen**			
2000-2010	Hacks, Botnetze, Kreditkartenbetrug, Verletzung von Privatsphäre	**Öffnung von Systemen**	Multimedia Software mit Benutzerinput	
2010-2015	Abschaffung von C/C++, PHP, rohem SQL	Hacks, Ransomware, Wirtschaftsspionage	**Öffnung von Systemen**	
2015-jetzt	Statische Analysen, sichere Sprachen	Industrie 4.0, Statische Analysen	Hacks, Diebstahl, Manipulation	Smart Meter, Windkraftanlagen am Internet, ...
Zukunft	Formale Security Beweise	Eliminieren von Legacy Systemen, Formale Beweise, sichere Sprachen		**Öffnung von Systemen**

Bild 20: Status im Einsatz von Programmiersprachen. Aus 16/.

Schwachstellen eingesetzt werden.

Der Forscher Robert Seacord vom Software Engineering Institute der Carnegie Mellon University hat für C bzw. C+++ folgende „Secure Coding Prcatices" definiert (vgl. /17/):

- Validate input.
  Validiere Daten von jeder nicht vertrauensvollen Quelle. Die Validierung von Eingabedaten kann die die überwiegende Zahl an Software-Schwachstellen beheben!
- Heed compiler warnings. Übersetze Programme mit den höchsten Überprüfungseinstellungen des Compilers. Setze statische und dynamische Analysewerkzeuge zur Erkennung und Beseitigung von Sicherheitsschwachstellen ein.
- Architect and design for security policies.
  Erzeuge eine Architektur und ein Design, das die Sicherheitsrichtlinien erfüllt.
- Keep it simple.
  Reduziere die Komplexität und halte alles so einfach wie möglich. Komplexität erhöht die Wahrscheinlichkeit von Fehlern in der Implementierung, der Konfiguration und in der Benutzung.
- Default deny.
  Grundsätzlich ist erst einmal der Zugriff verboten. Basis ist dann immer die explizite Erlaubnis.
- Adhere to the principle of least privilege.

Jeder Vorgang sollte nur die minimal notwendigen Berechtigungen haben.

- Sanitize data sent to other systems.
  Desinfiziere alle Daten und Kommandos bevor eine Funktion aufgerufen wird.

Die Problematik bestimmter Schwachstellen in einzelnen Programmiersprachen wird umfassend im Bericht ISO/IEC TR 24772 (/23/) untersucht. Dabei ist Vulnerability definiert als, Schwachstelle in Programmen, die es einem Angreifer erlauben, durch spezielle Bitmuster die Ausführung von nicht vorgesehenem Code initiieren. Ursache ist die nicht typstrenge Prüfung von Kommandos und Daten und nachfolgend Programmmanipulation.

Das National Institute of Standards and Technology stellt in einem Report (/18/) fest:

- "... many software security weaknesses are introduced at the implementation phase ..."
- "...identify code weaknesses that significantly affect the security of software applications ..."
- "... C, C++ and Java, because they are the languages in which most of today's vulnerabilities have been identified ..."
- "There are languages that are, by design, more suitable for secure programming. ... Such languages entirely preclude many common weaknesses .... Choosing such languages mitigates many security risks." (Ada, Rust, Spark)

Weshalb weiterhin unsichere Programmiersprachen eingesetzt werden, ist unverständlich. Dies insbesondere, da die Schwachstellen massiv und grundsätzlich sind, wie die Mitteilung des US CERT vom Juli

Primary Vendor -- Product	Description	Published	CVSS Score
cisco -- unified_computing_system_ performance_manager	The web framework in Cisco Unified Computing System (UCS) Performance Manager 2.0.0 and earlier allows remote authenticated users to **execute arbitrary commands via *crafted parameters*** in a GET request, aka Bug ID CSCuy07827.	2016-07-27	9.0
rockwellautomation -- factorytalk_energymetrix	SQL injection vulnerability in Rockwell Automation FactoryTalk EnergyMetrix before 2.20.00 allows remote attackers to **execute arbitrary SQL commands via *unspecified vectors***.	2016-07-27	7.5
siemens -- simatic_batch	Siemens SIMATIC WinCC before 7.3 Update 10 and 7.4 before Update 1, SIMATIC BATCH before 8.1 SP1 Update 9 as distributed in SIMATIC PCS 7 through 8.1 SP1, SIMATIC OpenPCS 7 before 8.1 Update 3 as distributed in SIMATIC PCS 7 through 8.1 SP1, SIMATIC OpenPCS 7 before 8.2 Update 1 as distributed in SIMATIC PCS 7 8.2, and SIMATIC WinCC Runtime Professional before 13 SP1 Update 9 allow remote attackers to **execute arbitrary code via *crafted packets***.	2016-07-22	10.0

Bild 21: Beispiele von „hand crafted" Attacken beschrieben durch ICS-CERT. Siehe /19/.

2016 zeigt. Durch „hand crafted" Kommandos und Werte, also bestimmter Bitmuster, werden beliebige Systeme korrumpiert und die Angreifer erhalten Administratorrechte oder können beliebigen Code ausführen (siehe Tabelle in Bild 21).

Neben den Programmiersprachen sind aber auch die Werkzeugketten zu umständlich, um ohne größeren Aufwand Schwachstellen zu analysieren und dann in der Programmierung zu beheben. In diesem Themenfeld sind inkrementell erweiterbare Compilierungssysteme ohne spätere nachgelagerte Phasen sinnvoller.

Im Gegensatz zu klassischer Ansätzen in der Softwareentwicklung mit einer Werkzeugkette besteht die Innovation aus einem inkrementell erweiterbare Compilierungssystem ohne spätere Phasen. Der Compiler erlaubt Add-Ons, die Erkenntnisse aus fehlerhaften Entwicklungen / Implementierungen zu integrieren. Dazu erzwingen Regeln bestimmte Arten der Implementierung. Die Basis dazu ist der „abstrakte Syntaxbaum" (AST) für statische Analysen und Prüfung der Vorgaben sowie auch Komplexitätsanalysen. Es können damit die Einhaltung der Prüfung auf Validierung von Eingabedaten, auf Prüfung auf Indexgrenzen etc. überwacht werden. Diese Entwicklung ist auch ein Projekt der Mozilla Foundation für Rust (vgl. /16/).

Standard	Titel	Bereich	Kurzbeschreibung
IEEE 1547	Standard for Interconnecting Distributed Resources with Electric Power Systems	Dezentrale Energieerzeugung	Zusammenschaltung dezentraler Energieressourcen mit Elektrizitätssystemen
IEEE 2030	IEEE Guide for Smart Grid Interoperability of Energy Technology and Information Technology Operation with the Electric Power System (EPS), End-Use Applications, and Loads	Interoperabilität; Referenzarchitektur	Interoperabilität in den Bereichen Elektro- energietechnik, Kommunikations- und Informationstechnologie; Smart Grid Referenzmodell
IEC 61508/ DIN EN 61508	Funktionale Sicherheit sicherheitsbezogener elektrischer/ elektronischer/programmierbarer elektronischer Systeme	Funktionale Sicherheit elektronischer Systeme	Sicherheitsanforderungen an industrielle Systeme werden hier definiert; Software Qualitätssicherung
IEC 61850/ DIN EN 61850	Kommunikationsnetze und -systeme in Stationen	Schaltanlagen-Automatisierung	Definiert ein Netzwerkprotokoll für die Leittechnik in elektrischen Schaltanlagen der Mittel- und Hochspannungstechnik
IEC 61968/ DIN EN 61968	Integration von Anwendungen in Anlagen der Elektrizitätsversorgung - Systemschnittstellen für Netzführung	Datenaustausch	Informationsaustausch zwischen Verteilnetzen; Schnittstellendefinition für dieIntegration von IT-Systemen im Verteilnetzmanagement-Umfeld; Common Information Modell Erweiterungen für das Verteilnetzmanagement
IEC 61970/ DIN EN 61970	Schnittstelle für Anwendungsprogramme für Netzführungssysteme (EMS-API)	Datenaustausch	Im Standard wird eine Programmierschnittstelle für Energiemanagementsysteme beschrieben; Common Information Model (Definition von Objekten und Datenaustauschformaten)
IEC 62351	Power systems management and associated information exchange - Data and communications security	IT-Sicherheit	IT-Sicherheit von Netzleitsystemen
IEC TR 62357	Power system control and associated communications - Reference architecture for object models, services and protocols	Referenzarchitektur – elektrischen Energieversorgung	Setzt verschiedene Standards in Kontext zu- einander; Seamless Integration Reference Ar- chitecture
DIN EN 13757	Kommunikationssysteme für Zähler und deren Fernablesung	LMN; Smart Meter	Fernablesung von Messgeräten mit Hilfe von Kommunikationssystemen (M-Bus, Wireless M-Bus)
DIN EN 50438/ VDE 0435-901: 2008-08	Anforderungen für den Anschluss von Klein-Generatoren an das öffentliche Niederspannungsnetz	Dezentrale Energieerzeugung, Niederspannungs- Verteilnetz	Anschluss von Kleinerzeugern an das öffentliche Niederspannungsnetz

Bild 22: Normübersicht. Aus /20/.

Normen

Normen sind in aller Regel deskriptiver Natur und machen keine konstruktiven Vorgaben. Damit hat der Entwickler großen Freiraum für die Realisierung seiner Lösung. Eine Richtlinie, welche deutliche Vorgaben macht, ist die NE 153 – Automation Security 2020 – Design, Implementierung und Betrieb industrieller Automatisierungssysteme (/24/).

Im Kern lassen sich die Anforderungen der NE153 darauf zusammenfassen, dass IT-Security-Konzepte und Funktionen ein integraler Bestandteil der Anforderungsprofile sind und damit auch zum integralen Funktionsumfang automationstechnischer Komponenten und Lösungen gehören. Die NE153 definiert folgende Bereiche:

- Secure by Default
- Secure by Design
- Secure by Implementation
- Secure in Deployment

Normen sind deskriptiv und nicht konstruktiv (vgl. den Orientierungsleitfaden für Hersteller zur IEC 62443, ZVEI). Security-Normen nehmen Wahrscheinlichkeiten für die Kompetenz der Angreifer an, die so nicht existieren bzw. nicht dem „worst case" Szenario aus dem Echtzeitdatenverarbeitungsbereich entsprechen. Damit lassen sich Bedrohungsrisiken immer klein rechnen. Außerdem sind Faktoren wie Kompetenz der Angreifer unsinnig, wenn laut Europool im Darknet leistungsfähige Tools für Angreifer schon für 150,00$ gehandelt werden.

Neben den direkten Security-Normen wie z.B. IEC 62443 (ISA99), ISO 27001 etc. existieren noch die Richtlinien von BSI, NIST, EU Direktiven etc. Weitere Normen zeigt die Tabelle in Bild 22.

Zusammenfassung

Das Smart Energy Grid der Zukunft ist ein komplexes, auf Software Funktionen basierendes hochgradig verteiltes und massiv vernetztes System. Damit hält die Problematik von Cyber-Angriffen und Software-Schwachstellen massiv Einzug in eine kritische Infrastruktur. Dabei ist der Stand in der Entwicklung und Zuverlässigkeit von Software nach wie vor nicht befriedigend (vgl. hierzu /21/).

In allen Bereichen bewirken Security-Probleme auch nachfolgend Probleme im Safety Bereich. Ob dies autonome Fahrzeuge, die Wasserversorgung, Verkehrsinfrastrukturen oder das Smart Energy Grid ist, überall können Angriffe zu Ausfällen und Abschaltungen führen. Damit sind die Zuverlässigkeit der Energieversorgung und die davon möglicherweise abhängende funktionale Sicherheit (siehe hierzu /22/) nicht mehr garantiert. Die bisherige stabile und sichere Versorgung im Energiebereich könnte merklich gefährdet werden.

In diesem Kontext gilt es wesentliche Fragestellungen zu klären, um den weiteren Ausbau der Digitalisierung sicher zu stellen. Hierzu gibt es folgende empfehlungen:

- Abklärung des Sicherheitslevels in der Automatisierung hinsichtlich IT-Security.
- Analyse und Bewertung der Sicherheit von klassischen Methoden wie Security Router, Firewalls, virtuelle Maschinen, VPNs usw.
- Kontinuierliche Feststellung der Entwicklung der Anzahl der festgestellten Schwachstellen in der allgemeinen Software und in der Automatisierungssoftware.
- Kontinuierliche Überwachung und Darstellung der Entwicklung der Zahl der Angriffe auf vernetzte Systeme allgemein und besonders auf kritische Infrastrukturen entwickelt.
- Untersuchung und eindeutige Bewertung der Sicherheit der überwiegend eingesetzten Betriebssysteme und deren Nachvollziehbarkeit hinsichtlich der Transparenz der internen Funktionalität.
- Feststellung und Bewertung der Konzepte um Angriffe auf Komponenten kritischer Infrastrukturen wie Smart Meter im Energienetz der Zukunft bei neu entdeckten Schwachstellen im Sinne Massenmanipulationen in der Energieversorgung zu begegnen.
- Analyse und Einordnung sowie Entwicklungsvorgaben für Ansätze und Konzepte um Sicherheitsschwachstellen zu beherrschen als Entscheidungsgrundlage für das BMBF, das BMI sowie das BMWi.
- Vergleich der Situation in der Entwicklung sicherer Software gegenüber den USA (Stichwort Secure Coding Guidelines sowie NIST Richtlinien).
- Darstellung, welche Forschungsförderungen es im Bereich Entwicklung sicherer Software und sicherer Gerätebetriebssysteme bzw. gibt, was folgt daraus und welche Förderungen sind angedacht.
- Analyse und Bewertung der Entwicklung von SDNs (Software Defined Networks) und deren Eignung für redundante und überwachte Kommunikationswege.
- Auflistung der Normen mit konstruktiver Auslegung, die von den Ministerien als zielführend gesehen werden.
- Feststellung der Umsetzung der Namur Empfehlung NE 153 über die Ministerien.
- Strategie seitens des BMWi, damit Deutschland und Europa den Vorsprung der USA mit den schon existierenden Standards, z. B. SEI CMU, NIST etc., aufholen können.
- Feststellung der Ansätze seitens des BMWi um die Aspekte Safety und IT-Security in ihren Anforderungen zu integrieren bzw. um entsprechende Forschungsanstrengungen auf den Weg zu bringen.

Es sind insbesondere ökonomisch vertretbare und technisch notwendige Maßnahmen kurz- und mittelfristig durchzuführen. Zuerst sind alle Komponenten mit jeweils eigenen komplexen Benutzernamen und Passwörtern zu initialisieren, damit keine Standardzugänge mehr existieren. Alle weiteren Zugänge wie Ports etc. haben per se geschlossen zu sein und müssen explizit eingerichtet werden. Software Funktionen, welche nicht zur Zielfunktionalität gehören, müssen ebenfalls per se deaktiviert sein und ihre Aktivierung muss erschwert werden. Basiskonfigurationen haben dem Least-Privilige-Prinzip zu entsprechen und sind bei Auslieferung auf maximale Sicherheit einzustellen. Bedienungsanleitungen dürfen keine 800 Seiten umfassen, sondern sind kompakt und klar zu formulieren. Hierzu sind politische Vorgaben und rechtliche Regelungen kurzfristig festzulegen. Schwachstellen in Securitykomponenten sind umfassend zu kommunizieren und über gesetzliche Regelungen als kritische Produktfehler einzuordnen, welche entsprechend dem Risiko mit einer hohen Haftung verbunden und zwingend schnellstens behoben sein müssen. Der Gesetzgeber hat hier umgehend zu reagieren und auch das BSI muss sehr klare und eindeutige Vorgaben festlegen.

Die Automatisierungshersteller müssen jetzt beginnen, ihre Software unter Security Gesichtspunkten neu zu entwerfen und mit sicheren Programmiersprachen zu implementieren. Technische Zuverlässigkeit und Sicherheit geht vor kaufmännischen Einsparpotentialen. Gleichzeitig muss in der Ausbildung von Programmieren, Informatikern und Ingenieuren der Fokus in der Softwareentwicklung auf konstruktive Zuverlässigkeit und Sicherheit (Safety und Security) gelegt und der Einsatz sicherer Programmiersprachen propagiert werden. Kein Softwareentwickler wird sich die Mühe machen Kommando- oder Dateneingaben vollständig auf syntaktische und semantische Korrektheit zu prüfen, wobei Sprachen wie C oder C++ schon von ihrer Sprachdefinition nicht eindeutig sind und im Sprachstandard von undefinded behaviour gesprochen wird. Damit die Drittmittelabhängigkeit der Universitäten und Hochschulen von der Industrie nicht zu anderen Zielvorgaben führen kann, muss die finanzielle Ausstattung hier deutlich verbessert werden. Nur durch umfassende Maßnahmen auf den Gebieten der Politik, Gesetzgebung, rechtliche Vorgaben, Bildung und Ausbildung, in der Herstellung von Automatisierungssoftware und –systemen sowie im Verständnis für Zuverlässigkeit und Sicherheit kommen wir zu verlässlichen Lösungen.

Literatur

/1/ https://www.siemens.com/global/de/home/unternehmen/innovationen/pictures-of-the-future/zukunft-der-energie.html, 27.08.2018

/2/ 50 Empfehlungen für eine erfolgreiche Energiewende. MÜNCHNER KREIS, Übernationale Vereinigung für Kommunikationsforschung e.V., Tal 16, 80331 München. www.muenchner-kreis.de, Stand Juli 2015

/3/ DIE EENERGY REFERENZARCHITEKTUR. EINE VISION FÜR EIN SMART ENERGY SYSTEM MADE IN GERMANY. MAXIMILIAN IRLBECK, VASILEIOS KOUTSOUMPAS. TECHNISCHE UNIVERSITÄT MÜNCHEN. EENERGY BEGLEITFORSCHUNG, BEREICH INFORMATIONS- UND KOMMUNIKATIONSTECHNOLOGIE. Stand: 15. Juni 2015

/4/ Digitalization of Energy Systems. A white paper. November 6, 2017. Bloomberg New Energy Finance

/5/ https://ics-cert.us-cert.gov/, 27.08.2018

/6/ Threat Landscape for Industrial Automation Systems in H2 2017 Kaspersky Lab ICS CERT

/7/ The Australian Cyber Security Centre Threat Report 2015

/8/ Kathrin Reibelt, Ghada Elbez, Oliver Schneider, Jörg Matthes und Hubert Keller. IT-Sicherheit für die vernetzten cyber-physikalischen Komponenten zukünftiger Energiesysteme. 82. Jahrestagung der DPG, Arbeitskreis Energie, Erlangen, März 2018.

/9/ Ghada Elbez, Hubert B. Keller, and Veit Hagenmeyer. A New Classication of Attacks against Cyber-Physical Security of Smart Grids. The 13th International Conference on Availability, Reliability and Security (ARES 2018), Hamburg, Germany, August 27-30 2018.

/10/ Ten common vulnerabilities identified in NSTB assessments (Table 1), National Supervisory Control and Data Acquisition (SCADA) Test Bed (NSTB), Vulnerability Analysis of Energy Delivery Control Systems, September 2011, Idaho National Laboratory, Idaho Falls, Idaho 83415, http://www.inl.gov.

/11/ NSTB Assessments Summary Report: Common Industrial Control System Cyber Security Weaknesses, May 2010, Idaho National Laboratory, Idaho Falls, Idaho 83415, http://www.inl.gov

/12/ Cyber Security im Energiemanagement. Auszug aus dem Power Engineering Guide, Ausgabe 8.0, Siemens AG

/13/ Sicherheitsaspekte von Smart Grids, DRAFT (Version Juni 2016), Michael Hübner, bmvit; Erika Ganglberger, ÖGUT. Mit Beiträgen von Thomas Bleier, Lucie Langer, Austrian Institute of Technology GmbH; Christoph Kohler, Albrecht Reuter, Fichtner IT Consulting AG; Dominik Engel, Josef Ressel Center for User-Centric Smart Grid Privacy, Security and Control; Angela Berger, Technologieplattform Smart Grids Austria

/14/ Purdue Enterprise Reference Architecture (PERA), reference model for enterprise architecture, by Theodore J. Williams / Industry-Purdue University Consortium for Computer Integrated Manufacturing

/15/ Guide to Intrusion Detection and Prevention Systems (IDPS). Recommendations of the National Institute of Standards and Technology. Karen Scarfone, Peter Mell. Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, Gaithersburg, MD 20899-8930, February 2007 (National Institute of Standards and Technology Special Publication 800-94)

/16/ Oliver Schneider: Programmiersprachen und Konzepte zur Entwicklung zuverlässiger und sicherer Automative Software. Automotive Security Workshop (VDI), Best presentation Award, September 27-28 2017.

/17/ Robert Seacord, https://www.securecoding.cert.org/confluence/display/seccode/Top+10+Secure+Coding+Practices

/18/ NIST – National Institute of Standards and Technology 2011, Source Code Security Analysis Tool, Functional Specification Version 1.1. Siehe auch: Seacord. R. C. et al.: A Structured Approach to Classifying Security Vulnerabilities. TECHNICAL NOTE, CMU/SEI-2005-TN-003, January 2005.

/19/ US CERT Vulnerability Summary for the Week of July 25, 2016,High Vulnerabilities, 27.08.2018

/20/ Sicherheit und Datenschutz im Smart Grid. Bachelor-Thesis. Kristian Antic. 8. März 2012. Hochschule der Medien Stuttgart. Prüfer: Prof. Dr. Joachim Charzinski, Christoph Lindenmüller

/21/ Hubert B Keller, Oliver Schneider, Joerg Matthes, and Veit Hagenmeyer. 2016. Reliable, safe and secure software of connected future control systems challenges and solutions. AT-AUTOMATISIERUNGSTECHNIK 64, 12, 930–947.

/22/ Hubert B. Keller, Wolf-Dieter Pilz, Bernd Schulz-Forberg, Christian Langenbach: „Technical Safety – An Attribute of Quality. An Interdisciplinary Approach and Guideline". © Springer International Publishing AG 2018. ISBN 978-3-319-68624-0

/23/ ISO/IEC TR 24772, Guidance to Avoiding Vulnerabilities in Programming Languages through Language Selection and Use.

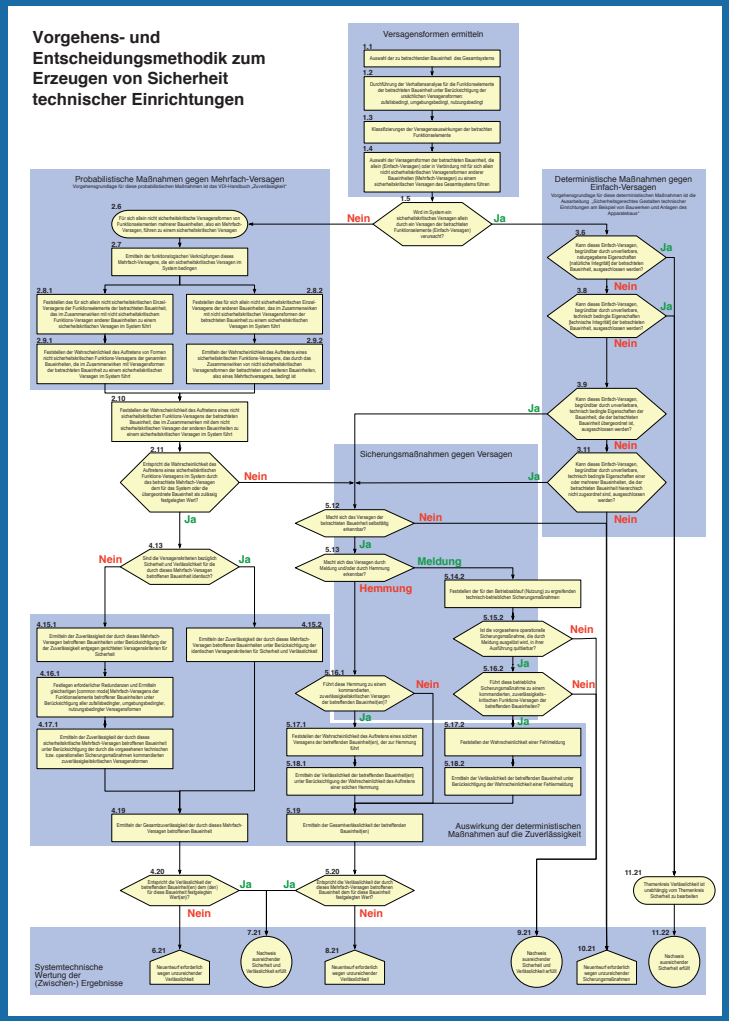
/24/ NE 153 – Automation Security 2020 – Design, Implementierung und Betrieb industrieller Automatisierungssysteme, Ausgabe 2015-06-11 der Namur (Empfehlung des Normenausschusses der Mess- und Regelungstechnik in Deutschland)

/25/ Sharon Weinberger: Stuxnet - Erstschlag im Cyberkrieg? Link: http://www.spektrum.de/magazin/stuxnet-erstschlag-im-cyberkrieg/1121043, 5.9.2018

/26/ Yao Liu, Peng Ning, Michael K Reiter: False data injection attacks against state estimation in electric power grids. ACM Transactions on Information and System Security (TISSEC) 14, 1, 13. 2011.

TECHNISCHE SICHERHEIT
DAS VERDECKTE GEMEINSAMEINE SUCHEN – FINDEN– NUTZEN

Dipl.-Ing. Wolf-Dieter Pilz



Systematik hilft Fehleinschätzungen zu vermeiden

Am Beispiel der Magnetbahn TRANSRAPID wird gezeigt, wie schnell mangelnde Systematik und Nachlässigkeiten bei der Erzeugung „Technischer Sicherheit" zum tödlichen Ende führen können. Der spätere Strafprozess verdeutlicht zudem sehr anschaulich, mit welchen technischen Verständnisschwierigkeiten sowohl die ermittelnden Strafverfolgungsbehörden als auch das befasste Gericht zu kämpfen hatten, ohne dennoch die tatsächlichen Ursachen für dieses tödliche Ende zu ermitteln. In Folge derartiger Schwierigkeiten ist stets damit zu rechnen, dass es im Hinblick auf die handelnden Personen gelegentlich zu technischen und damit rechtlichen Fehleinschätzungen kommen kann.

Das Technologievorhaben „Magnetbahn TRANSRAPID"

Im Jahr 1979 beauftragte die Regierung der Bundesrepublik Deutschland das Konsortium „Magnetbahn TRANSRAPID" mit der Entwicklung und dem Bau der „TRANSRAPID Versuchsanlage Emsland (TVE)" zur Erprobung einer anwendungsgerechten Magnetbahn-Technologie. „Anwendungsgerecht" in diesem Sinne heißt aber auch, *Technische Sicherheit* hinein zu entwickeln und hinein zu bauen, damit bei der Zulassung für den öffentlichen Personentransport nachgewiesen werden kann, dass von diesem Magnetbahn-System auch im Störungsfall keine Gefahr für Leib und Leben ausgeht und geschützte Rechtsgüter Dritter nicht verletzt werden. Unsere Rechtsordnung verweist in diesem Zusammenhang auf **unbestimmte Rechtsbegriffe** wie „*Allgemein anerkannter Stand der Technik*", „*Stand der Technik*" und „*Stand von Wissenschaft und Technik*". Hinter diesen unbestimmten Rechtsbegriffen verbergen sich technische Regelwerke wie z.B. DIN-Normen und VDI-Richtlinien. Bei deren Anwendung wird davon ausgegangen, dass das betreffende technische Erzeugnis bzw. System sicher und damit – nach entsprechender Nachweisführung – rechtlich zulassungsfähig ist.

Noch immer sind die Regelwerke für Technische Sicherheit nach Anwendungsgebieten verschiedener Technikfelder strukturiert. So gibt es Regelwerke für das Bauwesen, die Schifffahrt, den Strassenverkehr, das Eisenbahnwesen, die Luftfahrt, die Raumfahrt, die Kernenergie, den Umgang mit Niederspannungen usw. Für die neuartige Magnetbahn-Technologie suchte man jedoch vergebens nach technischen Regelwerken, die in Sachen „Technischer Sicherheit" angewendet werden könnten. Bislang gab es ja auch keine Magnetbahn-Technologie, für die bereits technische Regelwerke hätten erarbeitet sein können. Es stellte sich damals also die Frage, wie hier bei der Entwicklung der Magnetbahn-Technologie vorzugehen sei. Es wurde einzig das Versuchsanlagengesetz geschaffen, das Abweichungen vom klassischen Rad-Schiene-System zuließ („*Gesetz über den Bau und den Betrieb*

von Versuchsanlagen zur Erprobung von Techniken für den spurgeführten Verkehr" vom 29. Januar 1976) – allerdings ohne den erforderlichen technischen Unterbau. Zu diesem Zeitpunkt stellte das konzipierte Magnetbahn-System die am umfangreichsten digitalisierte technische Einrichtung der Welt dar. Wie wir heute wissen, war die TVE das bisher letzte große Technologievorhaben, das zu 100% von der Bundesrepublik Deutschland gefördert und finanziert wurde. Zudem delegierte sie sicherheitstechnisch anerkannte Fachleute als projektbegleitende Berater.

Beim Kick-off-Meeting zur Technischen Sicherheit wurde deshalb umfassend diskutiert, mit welchem der bereits existierenden Technikfelder die Magnetbahn-Technologie wohl am ehesten vergleichbar wäre, um auf dieser Grundlage ein neues für die Magnetbahn-Technologie geeignetes technisches Sicherheitskonzept zu entwickeln: Eisenbahn, Einschienenbahn, Schwebebahn, Seilbahn, Flugzeug, Luftschiff, Rolltreppe, Aufzug usw. In diesem Zusammenhang äußerte sich der anwesende Sicherheitsexperte aus dem Eisenbahnbereich dahingehend, dass **Digitaltechnik nicht „sicherheitsfähig"** sei und deshalb die damit umfassend ausgestattete Magnetbahn-Technologie niemals die sicherheitstechnische Zulassungsfähigkeit als öffentliches Bahnsystem erreichen könnte. Diese überraschende Behauptung wurde zwar bis zum heutigen Tag nicht begründet und muss vor dem Hintergrund heutiger Planungen zur Verwendung von IT-basierten Systemen aller Art dringend eingefordert und soweit möglich berichtigt werden. Letztendlich einigten sich die Teilnehmer an diesem Kick-off-Meeting auf ein Nutzungsprofil, das mit **„Fliegen in Höhe Null"** wohl am zutreffendsten beschrieben werden kann.

Mit diesem Thema musste sich nun erst einmal die zentrale Projektleitung des „Konsortiums Magnetbahn TRANSRAPID" beschäftigen. Zu diesem Zweck wurde zunächst innerhalb dieses Konsortiums eine Arbeitsgruppe einberufen, die mit den Sicherheitsfachleuten aus den beteiligten Unternehmen besetzt wurde und die Aufgabe erhielt herauszuarbeiten, wie in den vertretenen Technikfeldern Technische Sicherheit generiert wird. Im Jahr 1982 übernahm dann der Verein Deutscher Ingenieure (VDI) die interdisziplinäre Fortführung dieser Aufgabe, indem nach einstimmigem Votum eines hochrangig besetzten ad hoc-Ausschusses

- der Kurator des VDI, *Herrn Dr. rer. nat. Gustav Wagner*, Stuttgart (Mitglied des Aufsichtsrats der Robert Bosch GmbH) zusammen mit
- dem Direktor des VDI, *Herrn Dr.-Ing. Reinhard Menger*, Düsseldorf,

den VDI-Ausschuss „Technische Sicherheit" initiierte. Der VDI betrachtete dies als zukunftsweisende und Erfolg versprechende interdisziplinäre Aufgabe.
Im Jahr 2016 erschien dann beim Beuth-Verlag unter dem Titel „Das Qualitätsmerkmal ‚Technische Sicherheit' – Denkansatz und Leitfaden" [ISBN 978-3-410-26196-4] zunächst die deutsche Ausgabe und Anfang 2018 bei Springer International Publishing AG die englische Ausgabe unter dem Titel „‚Technical Safety', An Attribute of Quality – An Interdisciplinary Approach and Guideline" [ISBN 978-3-319-68624-0].
Die in beiden Publikationen enthaltene Vorgehens und Entscheidungsmethodik (Handlungsschema) ist umfassend und enthält sämtliche nötigen Handlungs- und Entscheidungsschritte sowie die Beurteilungen der technischen Auslegung hinsichtlich sicherheitsgerechter Gestaltung.

Der Transrapidunfall von Lathen als Beispiel für die Anwendung der Publikation „Das Qualitätsmerkmal ‚Technische Sicherheit' – Denkansatz und Leitfaden"

Am 22. September 2006 ereignete sich auf der TVE gegen 09:54 Uhr ein Unfall mit 23 Todesopfern und 10 Verletzten. Wie konnte es dazu kommen?

Mitte 1979 hatte das „Konsortium Magnetbahn TRANSRAPID" (AEG-Telefunken, BBC, Dyckerhoff & Widmann, Krauss-Maffei, Siemens, Thyssen-Henschel und Messerschmitt-Bölkow-Blohm, die auch die zentrale Projektleitung stellte) mit den Planungs- und Bauarbeiten für die „TRANSRAPID Versuchsanlage Emsland" begonnen. Obwohl zum Jahreswechsel 1984/85 weder der Bau der TVE vollendet, noch die Erprobung begonnen hatte, verlangte das Bundesministerium für Forschung und Technologie als Geldgeber bereits zu diesem Zeitpunkt die Übertragung der TVE an die „Versuchs- und Planungsgesellschaft für Magnetbahnsysteme" (MVP), einer Tochter der damaligen Deutschen Bundesbahn und der Lufthansa. Diese beauftragte ihrerseits die damals noch staatliche Industrieanlagen-BETRIEBSGESELLSCHAFT (IABG) mit der Betriebsdurchführung auf der TVE. Die Vertragsverhandlungen hierzu fanden kurz vor Weihnachten des Jahres 1984 statt. Sie waren durch die Forderung der MVP gekennzeichnet, dass das „Konsortium Magnetbahn TRANSRAPID" schriftlich erklären solle, dass die nicht vollendete TVE, deren Erprobung noch nicht einmal in Angriff genommen werden konnte, „*100% sicher*" sei. Das „Konsortium Magnetbahn TRANSRAPID" entgegneten darauf, dass das Vorgehen zur Technischen Sicherheit der TVE in den im Rahmen des Konfigurationsmanagements erstellten und zur Anwendung freigegebenen Rahmen- und produktbezogenen Spezifikationen festgelegt sei. Der komplette Satz all dieser Spezifikationen war der MVP in 6-facher Ausfertigung – gegen Empfangsbestätigung – über-

geben worden. Allerdings erfolgte auf diese Entgegnung hin seitens der MVP keine weitere Reaktion. So gab es aus Sicht der ehemaligen Zuständigkeit für Technische Sicherheit innerhalb der zentralen Projektleitung des „Konsortiums Magnetbahn TRANSRAPID" Anlass, beim Bundesministerium für Forschung und Technologie (BMFT) um Klärung zu bitten, wie die beim „Konsortium Magnetbahn TRANSRAPID" in Angriff genommene und ordnungsgemäß (im Rahmen des Konfigurationsmanagements) verfolgte interdisziplinäre Vorgehensweise zur „Technischen Sicherheit" unter Verantwortung der MVP fortgeführt werden würde. Leider beschränkte sich der erbetene Rückruf darauf, die angesprochene Besorgnis um die zukünftige „Technische Sicherheit" der Magnetbahn-Technologie zu zerstreuen. Mit wohlgesetzten Worten erklärte der Mitarbeiter des BMFT, dass dem Thema „Sicherheit" weiterhin höchste Priorität zukäme. Über das tatsächliche Vorgehen hierzu vermied er jedoch jede Aussage.

Der Unfall vom 22.09.2006 auf der TVE beweist nicht nur, wie berechtigt die damalige Besorgnis gewesen war, sondern auch, wie wenig technisches Sachverständnis dieser Anrufer für die Besorgnis aufbrachte. Bei sachgerechter Fortführung des vom „Konsortium Magnetbahn TRANSRAPID" in Angriff genommenen Vorgehenskonzepts zur „Technischen Sicherheit" wäre dieser Unfall einfach nicht möglich geworden.

Sicherheitstechnisch zu berücksichtigenden Sachverhalte

Der Fahrweg der „TRANSRAPID Versuchsanlage Emsland" (TVE) ist einspurig. Auf ihm verkehren normalerweise das Magnetbahn-Fahrzeug mit hoher Geschwindigkeit, aber auch mehrere Hilfsfahrzeuge mit deutlich geringerer Geschwindigkeit. Gegenseitiges Ausweichen oder aneinander vorbei Fahren ist nicht möglich. Wegen seiner hohen Geschwindigkeit ist mit dem Magnetbahn-Fahrzeug ein Fahren nach Sicht nicht möglich; damit entfällt auch die Möglichkeit zur optischen Signalisierung (mit Form- bzw. Lichtsignalen). Die örtlich physikalisch zulässigen Höchstgeschwindigkeiten (z.B. in Kurven) sind digital in einem streckenabhängigen Geschwindigkeits-Grenzprofil hinterlegt. Bei – zufälliger bzw. beabsichtigter – Überschreitung des Grenzprofils bremst sich das Magnetbahn-Fahrzeug selbsttätig auf die physikalisch zulässige örtliche Höchstgeschwindigkeit ab. Bei offenem Weichenende gilt die Höchstgeschwindigkeit „Null" (Stillstand). Aufgrund des geschwindigkeitsbedingt besonders langen Bremswegs des Magnetbahn-Fahrzeugs muss die beabsichtigte Fahrstrecke auf dem Fahrweg frei von Hindernissen sein.

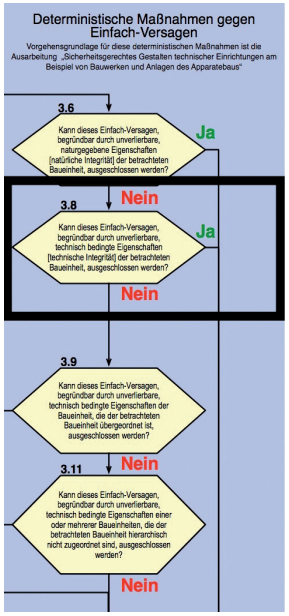
Im Gegensatz zu den kleineren Radfahrzeugen, die für Fahrten auf dem TVE-Fahrweg vorgesehen sind

und im Versuchszentrum der TVE über eigene Stellplätze verfügen, befindet sich der Abstellplatz für das massige Sonderfahrzeug, dessen Leistung danach bemessen wurde, dass es das teilschwebende Magnetbahn-Fahrzeug schleppen kann, aus pragmatischen Überlegungen in der Halle des Versuchszentrums in Ausfahrtrichtung vor dem Magnetbahn-Fahrzeug abgestellt. Dies bedingt, dass das Sonderfahrzeug vor Aufnahme des Fahr- und Versuchsbetriebs mit dem Magnetbahn-Fahrzeug die Halle verlassen und auf dem Fahrweg bis zur Stütze 120 des Fahrwegs vorrücken muss, damit das Magnetbahn-Fahrzeug über die Abzweig-Weiche des Versuchszentrums zum Fahrweg ausrücken kann. Nachdem bei diesem Rangierbetrieb zwei Fahrzeuge zur selben Zeit auf dem Fahrweg verkehren, erfordern deren Fahrten zur Kollisionsvermeidung geeignete Sicherungsmaßnahmen.

Sicherung des Sonderfahrzeugs

Das **Konsortium Magnetbahn TRANSRAPID** sicherte das Sonderfahrzeug gemäß dem in den betroffenen Spezifikationen unmissverständlich dargelegten *interdisziplinären Denkansatz und Leitfaden zur „Technischen Sicherheit"* unter **Anwendung des technisch begründeten Versagensausschlusses**. Folgende sicherheitstechnische Lösung wurde hier als geeignet befunden und spezifiziert:

Bei regulären Magnetbahn-Fahrten wird das Sonderfahrzeug nicht benötigt. Deshalb dürfen reguläre Magnetbahn-Fahrten erst dann aufgenommen werden, wenn sich das Sonderfahrzeug wieder an seinem Platz im Versuchszentrum befindet. Erst wenn es dort „angekettet" ist (Vorbild: Einkaufswagen im Supermarkt), können reguläre Magnetbahn-Fahrten aufgenommen werden (siehe **Handlungsschema** - Entscheidungsschritt 3.8). Rangierfahrten mit beiden Fahrzeugen vor Aufnahme der regulären Magnetbahn-Fahrten erfolgen mit Schrittgeschwindigkeit, auf Sicht und in Funkkontakt zu den beteiligten Fahrdienstleitern. Damit auch sichergestellt ist, dass der gesamte Fahrweg frei von sonstigen Fremdkörpern ist und sowohl Nord- als auch Südweiche in funktionsfähigem Zustand sind, wird anschließend noch mit dem Magnetbahn-Fahrzeug ein kompletter Fahrzyklus durchgeführt – allerdings nach Sicht bei bremsfähiger Geschwindigkeit – die sogenannte „Leerfahrt".



Dieses Sicherungskonzept ist logisch jederzeit nachvollziehbar und allgemein verständlich, also nicht nur für Ingenieure nachvollziehbar.

An dieses – schriftlich dokumentierte – Sicherungskonzept fühlte sich die **Versuchs- und Planungsgesellschaft für Magnetbahnsysteme** nicht gebunden. Nach etwa 20 Jahren unfallfreiem Fahrbetrieb mit Magnetbahn-Fahrzeugen kam vielmehr ein elektronischer „Marker" zum Einsatz, umgangssprachlich auch **„Fahrwegsperre"** genannt. Mittels Setzen der Fahrwegsperre wird die nicht nutzbare Strecke von der befahrbaren Strecke des Fahrwegs getrennt, wobei das Geschwindigkeits-Grenzprofil der noch befahrbaren Strecke des Fahrwegs den veränderten Gegebenheiten angepasst wird. Im Bedarfsfall, d.h. bei einem Hindernis (wie z.B. das Sonderfahrzeug) auf dem Fahrweg, muss die Fahrwegsperre gesetzt werden. Erst wenn sich dieses Hindernis nicht mehr auf dem Fahrweg befindet, darf die Fahrwegsperre gelöscht werden, was Vorbedingung für die Aufnahme des Magnetbahn-Fahrbetriebs ist. Sowohl das Setzen als auch das Löschen der Fahrwegsperre erfordert beim hiermit befassten Personal die Kenntnis, ob sich auf dem Fahrweg – noch – ein Hindernis befindet oder nicht – bzw. nicht mehr. Menschliche Irrtümer können hierbei allerdings immer wieder vorkommen und lassen sich auch durch Setzen der Fahrwegsperre nicht einfach ausschließen. Mit besagter Fahrwegsperre wird sicherungstechnisch in das Geschwindigkeits-Grenzprofil eingegriffen, damit das Magnetbahn-Fahrzeug nicht in einen Bereich des Fahrwegs einfährt, der nicht befahrbar ist. Diese Sicherungsfunktion erstreckt sich allerdings nicht auch auf die Ursache (z.B. das Sonderfahrzeug), deswegen dieser Bereich des Fahrwegs nicht befahrbar ist. So ist keine sicherungstechnische Maßnahme für das auf dem Fahrweg befindliche Sonderfahrzeug vorgesehen, deswegen die Fahrwegsperre gesetzt werden muss.

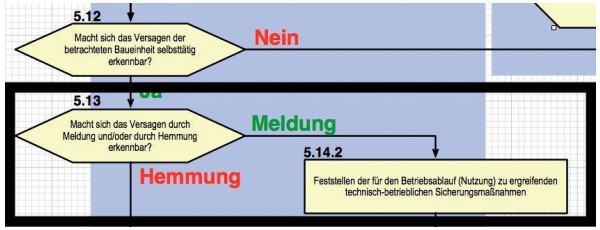
Diese sicherheitstechnische Unzulänglichkeit der „irrtumsanfälligen Fahrwegsperre", die nach 20 Jahren unfallfreiem Magnetbahn-Betrieb auf der TVE plötzlich eingeführt werden sollte, erkannte der längst in den Ruhestand verabschiedete – und am Unfalltag gar nicht anwesende –, ehemalige Betriebsleiter. In Wahrnehmung seiner Verantwortung für den Betrieb ließ er damals neben der Nutzung der neu eingeführten Fahrwegsperre die bereits zuvor eingeführten, zwei zusätzlichen Sicherungsmaßnahmen weiter bestehen:

- Vier-Augen-Prinzip auch im Leitstand (2. Fahrdienstleiter) und
- GPS-Überwachung des Sonderfahrzeugs mit entsprechender Bildschirmanzeige für den 2. Fahrdienstleiter.

Am Unfalltag wurden beide Sicherungsmaßnahmen, die sich in einem jahrelangen, unfallfreien Betrieb (*überwiegend ohne Fahrwegsperre*) bewährt hatten, durch das ablenkende „Streitgespräch" im Leitstand wirkungslos. Deshalb konnte es am 22. September 2006 auch zu dem tragischen Unfall kommen.
Aufgrund der an diesem Tag bedenkenlos geänderten Abläufe (wie Mitfahrt von Fahrgästen beim Rangieren des Magnetbahn-Fahrzeugs auf die eigentliche Fahrtrasse, Verzicht auf die sicherheitstechnisch gebotene Leerfahrt) zur morgendlichen Inbetriebnahme ist – ganz offensichtlich – *das bei Stütze 120 vorübergehend abgestellte Sonderfahrzeug schlichtweg vergessen* worden. Deshalb hat das Betriebspersonal der TVE nicht die Fahrwegsperre gesetzt, – und nicht, weil ihm dies nicht hinreichend bewusst gemacht worden sei.

Die nach dem Unfall angeordnete innerbetriebliche Untersuchung hatte ergeben, dass die Fahrwegsperre – von verschwindend wenigen Ausnahmen abgesehen – im Zuge des morgendlichen Rangierbetriebs stets gesetzt worden war. Allein dies beweist unmissverständlich, dass dem Betriebspersonal der TVE nicht nur die Bedeutung der Fahrwegsperre hinreichend bewusst war, sondern deren Setzen (und wieder Löschen) längst zum Bestandteil ihrer betrieblichen Routine gehörte. Selbst bei exakter Überlegung erscheint der Sachverhalt nicht nachvollziehbar, auf deren Grundlage die Große Strafkammer des Landgerichts Osnabrück gefolgert haben will, dass die Fahrwegsperre zu setzen am 22. September 2006 nur deshalb vergessen worden sei, weil deren Bedeutung dem TVE-Personal nicht hinreichend bewusst gemacht worden sei. Dafür seien strafrechtlich ausschließlich abwesende Personen verantwortlich, die infolge ihrer Abwesenheit nicht einmal in der Lage waren, wegen des vergessenen Sonderfahrzeugs korrigierend – d.h. unfallverhütend – einzugreifen.

Das Setzen und Löschen einer derartigen Fahrwegsperre erfordert vom Betriebspersonal Erkenntnisse und Handlungen, die dem menschlichen Irrtum unterworfen sind. Allein deshalb entbehrt die Fahrwegsperre jegliche Eignung als technische bzw. operationelle Sicherungsmaßnahme für den Fahr- oder Versuchsbetrieb.
Die „Vorgehens- und Entscheidungsmethodik zum Erzeugen von Sicherheit technischer Erzeugnisse" gibt auch hierzu unmissverständlich Aufschluss:



Mit Entscheidungsschritt 5.13 wird gefragt: *„Macht sich das Versagen [infolge des menschlichen Irrtums] durch **Meldung** und/oder **Hemmung** erkennbar?“*. Die Antwort lautet klar: NEIN! In Bezugnahme auf Hinweis 5.14.2 muss dann noch festgestellt werden, dass *„**es weder eine** [andere] **technische noch betriebliche Sicherungsmaßnahme gibt**“*.

Beim Abarbeiten der „Vorgehens- und Entscheidungsmethodik zum Erzeugen von Sicherheit technischer Erzeugnisse“ wäre es folglich *nicht nur für Ingenieure verständlich* geworden, **dass die Fahrwegsperre wegen ihrer Irrtumsanfälligkeit keinerlei Eignung als Sicherungseinrichtung auf der TVE aufweist.**

Anmerkungen zur juristischen Aufarbeitung

Anhand der zugänglichen Informationen über den Unfall vom 22. September 2006 auf der TVE wurde der Betriebsablauf dieses Morgens analysiert, um herauszufinden, wie dieser Unfall hat überhaupt zustande kommen können. Ganz offensichtlich haben 5 Mitarbeiter der Versuchsanlage an diesem Morgen insgesamt 10 Verstöße gegen bestehende Betriebs- und Sicherheitsvorschriften begangen. Wäre nur ein einziger dieser Verstöße nicht begangen worden, hätte es gar nicht zu diesem Unfall kommen können. Einige dieser Verstöße waren schon sehr augenfällig:

- Abweichend von bestehenden Sicherheits- und Betriebsvorschriften steigen die Fahrgäste im Versuchszentrum ein statt wie vorgesehen über den „Bahnsteig des Besucherzentrums“ an der Hauptstrecke nördlich des Versuchszentrum.

- Die Fahrgäste befinden sich im Magnetbahn-Fahrzeug, während dieses zusammen mit dem Sonderfahrzeug aus dem Versuchszentrum heraus auf die Hauptstrecke rangiert wird.

- Während dieser Rangierfahrten, die beim hiermit befassten Personal volle Konzentration erfordern, lenkt der für den Fahr- und Versuchsbetrieb dieses Tages stellvertretend Verantwortliche die beiden Fahrdienstleiter ab, indem er sie in ein Gespräch über weitere Fahrten auf der TVE verwickelt (in den Medien damals koordiniert als „Streitgespräch“ bezeichnet).

- Der zweite Fahrdienstleiter, auf dessen 2. Bildschirm das GPS-Signal des Sonderfahrzeugs klar erkennbar angezeigt wird, nimmt dieses gar nicht erst wahr. Gerade deshalb wird die „Fahrwegsperre“ nicht gesetzt.

- Die vor Aufnahme des Fahr- und Versuchsbetriebs sicherheitstechnisch vorgeschriebene „Leerfahrt“ mit niedriger Geschwindigkeit (nur mit den beiden Fahrern an Bord) wurde einfach unterlassen.

- Das Sonderfahrzeug auf der zu befahrenden Strecke des Fahrwegs wurde vergessen; das nach wie vor auf dem 2. Bildschirm angezeigte GPS-Signal des Sonderfahrzeugs nimmt der 2. Fahrdienstleiter auch im Verlauf des weiteren Betriebsgeschehens immer noch nicht wahr.

- Die Abzweigweiche, über die das Sonderfahrzeug gemäß Betriebsvorschrift hätte zurück ins Versuchszentrum geführt werden müssen, wird weder um- noch zurückgestellt.

- Als die Fahrgäste bereits im Versuchszentrum einstiegen, musste dem gesamten diensttuenden Betriebspersonal bereits klar geworden sein, dass infolge dieses Verstoßes die anschließende Routine, die sich sicherheitstechnisch mehr als 20 Jahre bewährt hat, an diesem Tag nicht mehr praktiziert werden kann. Der Ablauf zur morgendlichen Aufnahme des Fahr- und Versuchsbetriebs hätte zwingend an die so geänderten Umständen angepasst werden müssen.

- Als die beiden Fahrdienstleiter gerade dabei waren, gegen weitere wesentliche sicherheitstechnische Vorschriften zur morgendlichen Aufnahme des Fahr- und Versuchsbetriebs zu verstoßen befand sich auch der als Betriebsleiter stellvertretend Verantwortliche auf dem Leitstand:

  - Mitnahme von Fahrgästen während des kritischen – weil zeitgleichen – Rangierbetriebs von Magnetbahn- und Sonderfahrzeug;

  - Verzicht auf die sicherheitstechnisch anschließend gebotene Leerfahrt vor Aufnahme des regulären Fahr- und Versuchsbetriebs;

  - Vergessen des Sonderfahrzeugs auf der Fahrstrecke mit der folglich nicht gesetzten Fahrwegsperre.

- Es wäre die Pflicht des stellvertretend Verantwortlichen gewesen, hier umgehend ordnend in den Fahr- und Versuchsbetrieb einzugreifen. Ebenso wie das „*Vier Augen-Prinzip*" und das „*Handshake-Verfahren*" gehört auch die „*Sicherheits-Checkliste*" zu den klassischen Praktiken, die sich in der Sicherheitstechnik umfassend bewährt haben. Bei **Änderungen von sicherheitskritischen Abläufen** – wie z.B. wegen der Kollisionsgefahr bei der morgendlichen Aufnahme des Fahr- und Versuchsbetriebs (bei der sich Sonderfahrzeug und Magnetbahn-Fahrzeug gleichzeitig auf der Fahrstrecke befinden) ist es zwingend erforderlich, die bestehende Sicherheits-Checkliste den Änderungen entsprechend anzupassen und dem gesamten diensttuenden Betriebspersonal auszuhändigen (im Sinne: geänderter Fahrauftrag). Zuständig hierfür wäre der zu diesem Zeitpunkt als Betriebsleiter „stellvertretend Verantwortliche" gewesen. Stattdessen ließ dieser dem weiteren Geschehen seinen verhängnisvollen Lauf. Weder das Gerichtsurteil noch die diesbezüglichen Medienberichte enthalten einen Anhaltspunkt über die erforderlichenfalls „geänderte" Sicherheits-Checkliste.

- Der „vordere" Fahrer des Magnetbahn-Fahrzeugs, das – wohlgemerkt wie bei jeder ersten morgendlichen Fahrt – beim „Bahnsteig des Besucherzentrum" (vermeintlich „abfahrtbereit") wartete, meldete die Abfahrtbereitschaft zwar an den Leitstand, vergewisserte sich jedoch nicht, ob die vor ihm einsehbare Strecke des Fahrwegs frei von Hindernissen ist (das massige Sonderfahrzeug befand sich bei klarer Sicht nur etwa 1.200 m vor ihm).

- Obwohl sich das Magnetbahn-Fahrzeug mit zunehmender Geschwindigkeit diesem – eigentlich unübersehbaren Hindernis – näherte, betätigte der Fahrer bis zum tödlichen Aufprall nicht die Not-Taste, um damit die immer dringender gebotene Zwangsbremsung auszulösen.

Sowohl die Strafermittlungsbehörden als auch die 10. Große Strafkammer des Landgerichts Osnabrück zogen zwar einen Sachverständigen für Eisenbahnsicherungstechnik hinzu, der jedoch mit den Besonderheiten der Magnetbahn-Technologie und den Erfordernissen beim Umgang mit neuartigen Technologien nicht sonderlich vertraut gewesen schien. So wird der morgendliche Betriebsablauf zur Aufnahme des Fahr- und Versuchsbetriebs erst gar nicht untersucht. Auch die augenfälligen Verstöße des diensttuenden Betriebspersonals gegen bestehende Betriebsvorschriften werden zwar zur Kenntnis genommen, aber im erforderlichen Umfang nicht als Grundlage für die Strafverfolgung gewertet. Stattdessen wird der – sicherheitstechnisch keineswegs vollumfänglich tauglichen – „Fahrwegsperre" besondere Bedeutung für den Rangierbetrieb (mit Sonderfahrzeug und Magnetbahn-Fahrzeug) zugemessen. Obwohl das am Unfall beteiligte Betriebspersonal bei der Erstellung der Betriebsvorschriften selbst mitgewirkt hat, intensive und ständig wiederholte Schulungen durchlaufen hat, zum Zeitpunkt des Unfalls bereits über mehr als 20 Jahre Betriebserfahrung verfügte, lässt die Strafkammer bei den Beweiserhebungen deren Verstöße gegen die Betriebs- und Sicherheitsvorschriften weitgehend außer Acht.

Stattdessen konzentriert die Kammer ihre Beweiserhebung auf sprachliche Formulierungen in Betriebs- und Sicherheitsvorschriften und die Art der Verwendung von Querverweisen auf vertiefend weiterführende Vorschriften mit der – juristischen – Schlussfolgerung, dass hier die Ursache für die „nicht gesetzte" Fahrwegsperre und den angeblich dadurch zustande gekommenen Unfall zu suchen sei. Wieso die drastischen Änderungen des morgendlichen Rangierablaufs und der leichtfertige Verzicht auf die sicherheitstechnisch gebotene Leerfahrt vor Aufnahme des regulären Fahr- und Versuchsbetriebs nicht ursächlich gewesen sein sollten, darüber schweigt sich die Kammer aus.

Immerhin stand das Magnetbahn-Fahrzeug, als der „vordere" Fahrer die – vermeintliche – Abfahrtbereitschaft an den Leitstand meldete, genau an derselben Stelle des „Zugangsgebäudes für Ein- und Ausstieg", an dem es auch sonst bei Aufnahme des anstehenden Fahr- und Versuchsbetriebs steht. Aus diesem Grund darf hier ein „*Bestandsirrtum*" nicht einfach ausgeschlossen werden. Leider gibt das befasste Gericht keinen Aufschluss darüber, dass es ausgerechnet hier keinen Grund für einen Irrtum vermutet haben will. Hätten sich die strafrechtlichen Ermittlungen auch auf die morgendlichen Abläufe des Unfalltags erstreckt, dann wäre dieser Bestandsirrtum gewiss offenbar geworden. Populär ausgedrückt: Das diensttuende Personal hatte den jeweiligen „Bestand" der Abfolge der vorgeschriebenen Betriebs- und Sicherheitsvorschriften durcheinander gebracht. Es befand sich schlichtweg „im falschen Film"! Die Ursachen sind wohl unstrittig:

- Mitfahrt von Fahrgästen beim Rangieren des Magnetbahn-Fahrzeugs und

- Verzicht auf die sicherheitstechnisch gebotene Leerfahrt.

Gerichtsurteile dienen nicht nur dem Recht im Allgemeinen sondern auch dem Recht in Sachen Technik und technologischer Innovation. Es ist in diesem Zusammenhang gewiss nicht förderlich, wenn ein Gericht klassische Praktiken, die sich auch in der Sicherheitstechnik umfassend bewährt haben (wie das

Vier Augen-Prinzip und das Handshake-Verfahren) und in der „Verfahrensanweisung für den Betrieb mit dem Magnetbahnfahrzeug – VA-BT-FB-06" schriftlich vorgeschrieben sind, als „*zur Unfallvermeidung nicht geeignet*" bezeichnet und für diese eigenartig anmutende Auffassung nicht einmal eine Begründung liefert.

Selbstverständlich handelt es sich bei diesen Verfahrensanweisungen um technische Betriebs- und Sicherheitsvorschriften, die ausdrücklich der „*Unfallvermeidung*" dienen. Deren „*Eignung*" einfach in Abrede zu stellen, nur weil am Unfalltag gegen sie – umfassend – verstoßen worden ist, würde ja in Bezug auf analoge Rechtsvorschriften heißen, dass auch diese als „*nicht geeignet*" angesehen werden müssten, sobald bei deren bestimmungsgemäßen Anwendung gegen sie verstoßen würde. Führen Verstöße gegen Vorschriften zu Stör- oder Unfällen, sind diese (ggf. strafrechtlich) zu ahnden – und zwar unabhängig davon, ob es sich bei diesen Vorschriften um technische Betriebs- und Sicherheitsvorschriften oder um Rechtsvorschriften handelt. Voraussetzung ist allerdings, dass die in Frage kommenden Vorschriften sorgfältig erfasst, lückenlos zusammengestellt und fachkundig analysiert werden – und nicht a priori als „*zur Unfallvermeidung nicht geeignet*" ins strafrechtliche Abseits geschoben werden.

Im Zusammenhang mit dem TVE-Unfall vom 22. September 2006 liegt das Problem darin, dass sich aus der Sicht des Ingenieurs ein und derselbe technische bzw. betriebliche Ablauf zur morgendlichen Betriebsaufnahme völlig anders erschließt als dies die Laien aus den Bereichen Strafverfolgung und Rechtsfindung zu sehen glaubten. **Nicht die Fahrwegsperre ist am Unfalltag „vergessen" worden zu setzen sondern das Sonderfahrzeug** selbst –, das sich bei Fahrtantritt des Magnetbahn-Fahrzeugs immer noch auf der zu befahrenden Strecke befand und dort mittels Fahrwegsperre (gegen Kollision) zu sichern gewesen wäre. Für die Verstöße des diensttuenden Betriebspersonal gegen bestehende Betriebs- und Sicherheitsvorschriften, die das Sonderfahrzeug auf der Strecke wohl vergessen ließen, lassen sich nun einmal Personen, die am Tag dieses Unfalls gar nicht zugegen waren, einfach nicht verantwortlich machen.

In Abwesenheit des eigentlichen Betriebsleiters führte am Unfalltag ein „*stellvertretend Verantwortlicher*" die sicherheitstechnische Aufsicht über den Betrieb auf der TVE. Zudem befand er sich im Leitstand – zumindest anfänglich, als dort die verhängnisvollen Verstöße gegen sicherheitstechnische Vorschriften des Betriebsablaufs erfolgten, ohne dass er ordnend oder korrigierend eingriff. In Kenntnis dieses Sachverhalts erscheint es schon sehr merkwürdig, dass ausgerechnet dieser Stellvertreter, der am Unfalltag für den Fahr- und Versuchsbetrieb verantwortlich war, von Strafverfolgung und Verurteilung verschont blieb.

Hat dieser am Unfalltag für den Betrieb „stellvertretend Verantwortliche" die Irrtumsanfälligkeit der Fahrwegsperre etwa in Abrede gestellt und sich bei seiner Toleranz hinsichtlich der verhängnisvollen Verstöße gegen bestehende Betriebs- und Sicherheitsvorschriften möglicherweise auf die sicherungstechnische Wirksamkeit der Fahrwegsperre verlassen? Niemand außer ihm selbst vermag dies zu beantworten! Die Strafkammer akzeptierte damals ohne jede Rückfrage seine Aussageverweigerung als Zeuge, die er von einen Anwalt vortragen ließ.

Anregung

In den USA (*wie z.B. das National Transportation Safety Board – NTSB*) und in den Niederlanden (*wie z.B. das Dutch Transport Safety Board [Raad voor de Transportveiligheid – RvTV]*, heute das *Dutch Safety Board, [https://www.onderzoeksraad.nl/en]*) ist es längst Gepflogenheit, dass zunächst der technische Sachverstand einen Stör- oder Unfall untersucht und analysiert, ehe die juristische Würdigung erfolgt. Die Rechtsordnung der Bundesrepublik Deutschland ist allgemein gesprochen durchaus beispielhaft. Trotzdem kommt es immer wieder – wie die strafrechtliche Aufarbeitung des Magnetbahnunfalls auf der Versuchsanlage im Emsland 22. September 2006 verdeutlicht – zu Ungereimtheiten. Wie sollen die Vorgehensweisen von Ingenieurs- und Rechtswissenschaften in Einklang gebracht werden können, wenn die Rechtsanwendung gar so selbstherrlich gegenüber den Ingenieurwissenschaften auftritt – in der Meinung, dass hochqualifizierte Ingenieure mit Jahrzehnten an Erfahrung gar so einfältige Fehler machen könnten, wie sie ihnen die 10. Große Strafkammer des Landgerichts Osnabrück in ihrem Urteil 10 KLs 730 Js 40273/06 - 26/07 vom 23. Mai 2008 unterstellte.

Das ließe sich recht einfach vermeiden. In der Bundesrepublik Deutschland wäre nur ein „Technikrat für Technische Sicherheit" nach niederländischem Muster einzurichten, der zunächst die technischen Sachverhalte klärt, auf denen dann die rechtliche Entscheidung erfolgt (siehe „Das Qualitätsmerkmal ‚Technische Sicherheit' – Denkansatz und Leitfaden", Beuth-Verlag, Berlin 2016 [ISBN 978-3-410-26196-4]).

ALLIANZ ZUR STÄRKUNG DIGITALER INFRASTRUKTUREN IN DEUTSCHLAND – EINE INITIATIVE VON ECO E.V.

Dipl.-Komm.-Wirt Alexander Rabe

Über die Allianz zur Stärkung digitaler Infrastrukturen in Deutschland

Die Internetwirtschaft ist Schlüsselbranche und Wachstumsmotor unserer Zeit: Ihr Anteil an der Gesamtwirtschaft steigt seit Jahren kontinuierlich. Doch während Provider und große Anbieter sozialer Plattformen häufig im Fokus von Politik und Öffentlichkeit sind, bleiben die Unternehmen, die am Anfang der Wertschöpfungskette Internet stehen – nämlich Betreiber digitaler Infrastrukturen wie Rechenzentren oder Co-Location-Anbieter – bislang weitgehend unbekannt. Gleichwohl ist diese Branche von herausragender Bedeutung für eine gelingende digitale Transformation in Deutschland. Die Allianz zur Stärkung digitaler Infrastrukturen in Deutschland ist ein Zusammenschluss führender Unternehmen aus verschiedenen Branchen digitaler Infrastrukturen wie etwa Rechenzentrumsbetreiber, Co-Location-Anbieter, Internet Service Provider, Carrier, Cloudanbieter, Softwarehersteller und Vertreter aus der Anwendungsindustrie unter dem Dach von eco – Verband der Internetwirtschaft e.V.. Ihre Mitglieder wollen auf die Bedeutung ihrer Branche für den Digitalstandort Deutschland aufmerksam machen und in einen konstruktiven Dialog mit Politik und Öffentlichkeit treten.

Der Anfang der Wertschöpfungskette, nämlich die Betreiber digitaler Infrastrukturen, müssen in den Fokus der Politik gerückt werden.

Über eco

Mit über 1.100 Mitgliedsunternehmen ist eco der größte Verband der Internetwirtschaft in Europa. Seit 1995 gestaltet eco maßgeblich das Internet, fördert neue Technologien, schafft Rahmenbedingungen und vertritt die Interessen seiner Mitglieder gegenüber der Politik und in internationalen Gremien. Die Zuverlässigkeit und Stärkung der digitalen Infrastruktur, IT-Sicherheit und Vertrauen sowie eine ethisch orientierte Digitalisierung bilden Schwerpunkte

eco fasst über 1100 Mitgliedsunternehmen zusammen

der Verbandsarbeit. eco setzt sich für ein freies, technikneutrales und leistungsstarkes Internet ein.

Digitale Souveränität

Funktionierende und leistungsfähige digitale Infrastrukturen sind das Rückgrat einer gelingenden digitalen Transformation in Deutschland und gleichzeitig Wachstumsmotor, Innovationstreiber und Multiplikator für andere Industrien, insbesondere im Bereich Industrie 4.0. Dennoch wird dieser Wirtschaftsfaktor in Deutschland von Öffentlichkeit und Politik bisher wenig wahrgenommen

Die Wahrnehmung der digitalen Infrastruktur als Rückgrat der digitalen Transformation muss massiv gesteigert werden.

Facts & Figures

In Deutschland gibt es über **50.000** Rechenzentren, davon rund 3.000 mit über 100m² Fläche.

Energiebedarf von Server und Rechenzentren in DE 2016: 12,4 TWh/a. Das entspricht einem Anteil von **2,3%** des gesamten dt. **Strombedarfs**.

Im Jahr 2021 werden **93%** der Deutschen **online** sein.

In Rechenzentren sind ca. **130.000** Personen vollzeitbeschäftigt. Hinzu kommen über **80.000** abhängige Arbeitsplätze.

Mit 12,58 ct/kWh zahlen Rechenzentren in Deutschland weltweit mit den **höchsten Strompreis**.

Bis 2021 wird es voraussichtlich **760 Millionen** vernetzte Geräte geben.

Deutsche Rechenzentren gehören zu den **energieeffizientesten** weltweit.

In Deutschland wird sich der **mobile Datenverkehr** bis 2021 voraussichtlich **versechsfachen**.

Die **Investitionen** in Rechenzentrumsinfrastruktur stiegen 2016 um **10%** auf knapp eine Milliarde Euro.

und politisch praktisch gar nicht adressiert. Das ist überraschend, angesichts der anspruchsvollen Wachstumsziele, die die Bundesregierung zuletzt im neuen Koalitionsvertrag im Bereich Digitalisierung definiert hat. Fachkräftemangel, langwierige Genehmigungsverfahren und nicht zuletzt die hohen Stromkosten sind eindeutige Standortnachteile und eine Gefahr für den Digitalstandort Deutschland.

Rechenzentren, lokale, regionale und nationale, müssen gefördert werden.

Neue Studie belegt schlechte politische Rahmenbedingungen für Betreiber digitaler Infrastrukturen in Deutschland

Angesichts ihrer volkswirtschaftlichen Bedeutung für den Standort Deutschland erfahren Betreiber digitaler Infrastrukturen hierzulande aktuell keine angemessene politische Unterstützung und Förderung. Gerade im internationalen Vergleich sind die politischen Rahmenbedingungen für Betreiber digitaler Infrastrukturen suboptimal. Zu diesem Ergebnis kommt eine neue Studie über die sozioökonomischen Chancen und Herausforderungen von Rechenzentren und anderer Betreiber digitaler Infrastrukturen im internationalen Vergleich, die vom Borderstep Institut im Auftrag der **Allianz zur Stärkung digitaler Infrastrukturen in Deutschland** und eco – Verband der Internetwirtschaft e.V. erstellt und am 13. Juni 2018 in Berlin vorgestellt wurde.

Deutschland droht hier im internationalen Vergleich den Anschluss zu verlieren. Andere Länder haben bereits die Bedeutung der Branche erkannt und schaffen aktiv die notwendigen Rahmenbedingungen um auch zukünftig als Standort im Wettbewerb attraktiv zu sein.

10 Politische Forderungen der Allianz zur Stärkung digitaler Infrastrukturen in Deutschland

„Die Bundesregierung muss digitale Infrastrukturen in Deutschland endlich als Standortfaktor anerkennen und dringend eine Strate-

gie für die Sicherung und den Ausbau der digitalen Infrastruktur hierzulande entwickeln", fordern daher die Mitglieder der Allianz zur Stärkung digitaler Infrastrukturen in Deutschland. Was politisch nötig ist, um den Digitalstandort Deutschland langfristig international wettbewerbsfähig zu halten, hat die Allianz in insgesamt zehn Forderungen zusammenfasst:

1. **Digitale Infrastrukturen als wichtigen Faktor für Wirtschaftsstandort Deutschland anerkennen**
2. **Breitbandausbau vorantreiben**
3. **Deutschland als Rechenzentrumsstandort strategisch stärken und weiterentwickeln**
4. **Maßnahmen unter Berücksichtigung unterschiedlicher Geschäftsmodelle entwickeln**
5. **Forschung im Bereich Rechenzentren fördern**
6. **Bürokratie abbauen, Verwaltungsprozesse effizienter und schlanker gestalten**
7. **Aus- und Weiterbildung fördern**
8. **Ressortübergreifendes Vorgehen lernen**
9. **Strategien auf EU-Ebene implementieren**
10. **Stromkosten wettbewerbsfreundlicher gestalten**

Mitglieder und Unterstützer

Die Allianz zur Stärkung digitaler Infrastrukturen in Deutschland wird aktuell von folgenden Unternehmen und Organisationen unterstützt:

Breite Unterstützung der Allianz zur Stärkung digitaler Infrastrukturen

- DECIX
- e-shelter
- equinix
- Interxion Deutschland GmbH
- Telehouse
- noris network AG
- Siemens AG
- Telemaxx
- bitmi Bundesverband IT Mittelstand e.V.
- GasLine
- GI Gesellschaft für Informatik
- Net Cologne

Ausblick

Digitale Infrastrukturen wie Rechenzentren sind zwingende Voraussetzung für die digitale Transformation in die Volkswirtschaft.

Die Allianz ist offen für alle Betreiber digitaler Infrastrukturen sowie der Anwenderindustrie (bspw. aus dem Bereich Industrie 4.0). Sie wird mit jedem Mitglied einflussreicher, um mit dem gebotenen Nachdruck auf Politik und Wirtschaft zum Wohle der Volkswirtschaft zugehen zu können.

Weitere Informationen

Die Borderstep-Studie **„Bedeutung digitaler Infrastrukturen in Deutschland"** ist online verfügbar unter https://www.eco.de/wp-content/uploads/dlm_uploads/2018/06/DI_Studie.pdf.

Weitere Informationen zur **Allianz zur Stärkung digitaler Infrastrukturen in Deutschland** gibt es online unter: www.digitale-infrastrukturen.net.

HERAUSFORDERUNGEN EINER DOMÄNENÜBERGREIFENDEN RISIKOANALYSE

Univ.-Prof. Dr.-Ing. Kai-Dietrich Wolf

Safety und Security sollten zusammen betrachtet werden, insbesondere vor dem Hintergrund widersprüchlicher Anforderungen und der zunehmenden Durchdringung der Disziplinen mit IT-Elementen.

Zielsetzung

Der im April 2017 gegründete Fachausschuss „Synthese von Safety und Security" nimmt die oft widersprüchlichen Anforderungen und Wechselwirkungen der Domänen Safety und Security in den Blick, betrachtet Unsicherheiten und Gesamtrisiken in den unterschiedlichen Sicherheitsdisziplinen und hat es sich zum Ziel gesetzt, einen Überblick über Methoden in den Disziplinen zu geben und Ansätze zur übergreifenden Risikoanalyse aufzuzeigen. Die übergreifende Analyse erfordert im Wesentlichen eine Quantifizierung auf Basis einer einheitlichen Metrik, was zum gegenwärtigen Zeitpunkt ggf. nur in einzelnen Disziplinen realisierbar ist. Der Einfluss von Unsicherheiten sowie ethische Fragen sind zu adressieren.

Grundlegende Zielsetzung des Fachausschusses ist es, einen ersten Statusbericht zum Stand der Anwendungen und Entwicklung von Methoden zur übergreifenden Betrachtung von Safety und Security zu erstellen. Dieser soll u.a. die Frage beantworten, warum in welcher Disziplin welche Methoden, Verfahren und Beschreibungsarten zur Darstellung von Risikobeiträgen verwendet werden. Es gilt zu klären, wie und unter welchen Einschränkungen (z.B. Unsicherheit) technologisch-organisatorische, ausgewogene Maßnahmen zur Risikominderung quantitativ bewertet werden können.

Status quo – Security-Analyse von kritischen Infrastrukturen im Bereich der Energieversorgung

Kann eine Risikoquantifizierung bei Security-Fällen gelingen?

Bisher werden oft qualitative Konzepte zur Bewertung von Infrastrukturen wie z.B. des Stromnetzes eingesetzt; im Vordergrund steht hier meist die Erfüllung von rechtlichen Anforderungen an den Betreiber. Unternehmen aus dem Bereich der Betreiber kritischer Infrastrukturen befinden sich zunehmend in der Situation, eine Risikoquantifizierung zur Kosten- und Nutzenabschätzung der Investitionen in Sicherungsmaßnahmen vornehmen zu müssen.

Dies dient einerseits der Absicherung von Geschäftsführung oder Vorstand sowie auch einer adäquaten Rechtfertigung gegenüber Aktionären, Stakeholdern, Netznutzern sowie nicht zuletzt auch gegenüber der Öffentlichkeit.

Auf europäischer Ebene wird eine detaillierte Sicherheitsanalyse für Energieinfrastrukturen z.B. durch eine modular aufgebaute Handreichung der Europäischen Kommission (EC) beschrieben, deren Entwicklung das DG Energy im Rahmen des European Program for Critical Infrastructure Protection (ERCIP) extern an die Harnser Risk Group in Auftrag gegeben hat und welche Teil eines umfassenden Risikomodells für Sicherheit ist. Der sogenannte „Reference Security Management Plan for Energy Infrastructures“ (HARNSER) ist aus Operatorsicht verfasst und soll Betreibern von kritischen Infrastrukturen als Leitfaden für den sicheren Betrieb von Energieinfrastrukturen dienen.

Eine Handreichung der Europäischen Kommission kann für die Risikobetrachtung der Energieinfrastruktur herangezogen werden.

Dieser ist allerdings nicht rechtlich bindend und konzentriert sich auf mögliche Angriffe von außen, die sich gegen die Energieinfrastrukturen richten können. Er enthält eine komplette Prozessbeschreibung und bezieht auch andere Disziplinen wie strategische Planungen, Projektmanagement, technisches Design, Stakeholder-Analysen und Risiko-Reporting mit ein. Einige weitere Dokumente, die auf nationaler Ebene z.T. auch in jüngerer Zeit erscheinen sind, lassen leider viele Fragen bei der Durchführung von Security-Risikoanalysen für Energieinfrastrukturen oder Kritische Infrastrukturen offen.

Es gilt, das Risiko eines physischen Angriffs auf die Energieinfrastruktur als Rückrat unserer vernetzten Gesellschaft objektiv abschätzen zu können.

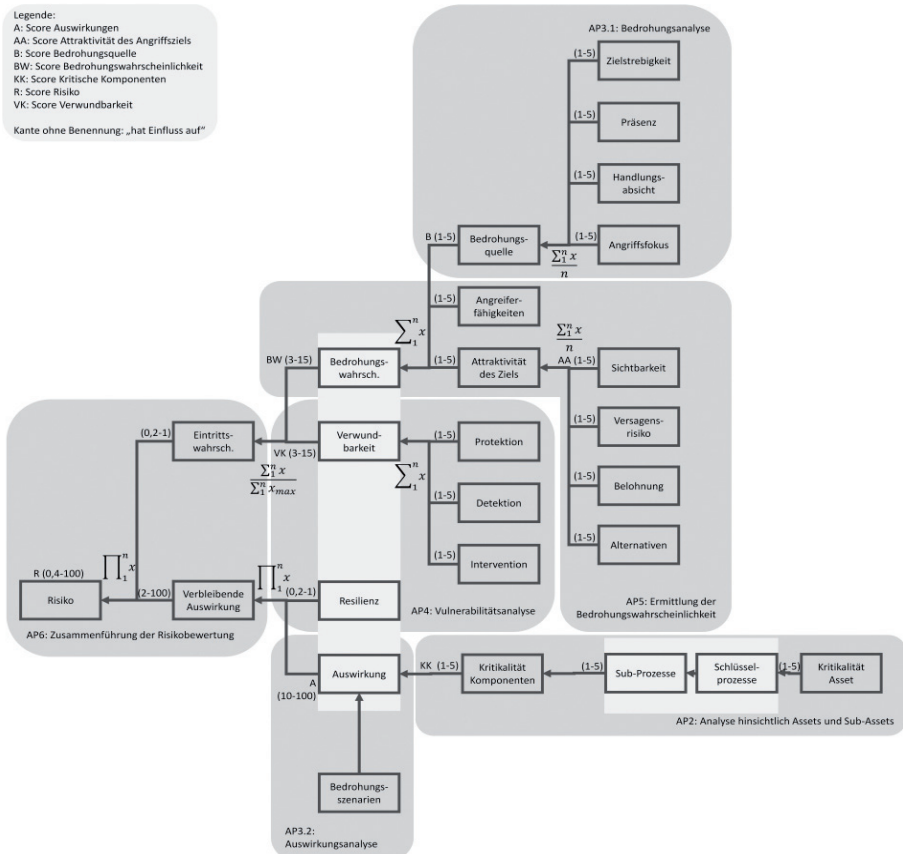


Abb.1: Du-Pont-Schema der Security-Bewertung nach HARNSER

Grundlage der EC-Handreichung ist das sogenannte Harnser Modell, welches als semi-quantitatives Modell Teil eines umfassenden Risikomodells für Sicherheit ist und somit ein Vorgehen zur Risikobewertung beschreibt. Das Modell weist eine entsprechende Bewertungsskala mit Kriterien von 1 – 5 auf; es findet ein qualitatives, Szenario-bezogenes Ranking der Risiken von entsprechenden Assets statt.

Basis der Evaluation ist die Auswahl der betrachteten wichtigsten Schlüsselprozesse der Infrastruktur. Es ergibt sich somit ein semi-

quantitativer Risiko-Score, der als Funktion der Eintrittswahrscheinlichkeit und Auswirkung beschrieben werden kann. Eine quantitative Kosten- und Nutzen-Abwägung ist über dieses Modell allerdings nicht möglich.

Die modellseitig zugrundeliegende Risikogleichung lässt sich wie folgt beschreiben:
Risiko = Bedrohungswahrscheinlichkeit X Verwundbarkeit X Auswirkung (X Minderung).

Für den Betrieb von Energieinfrastrukturen lässt sich so folgender Status Quo in Bezug auf eine entsprechende Security-Analyse festhalten: Der Betrieb / die Integrität der kritischen Energieinfrastruktur muss sichergestellt werden; dies sollte unter Beachtung der rechtlichen und technischen Rahmenbedingungen geschehen. Dabei findet ein Paradigmenwechsel im Hinblick auf die Analyse der Vulnerabilität statt; gefordert sind Performance-basierte Vulnerabilitätsanalysen (gemäß Reference Security Management Plan for Energy Infrastructures) sowie Konzepte zur Bewertung der Risikofaktoren (Bedrohungs-, Vulnerabilitäts- und Auswirkungsanalysen).

Die Verfügbarkeit von Energieinfrastrukturen muss höchste Priorität haben.

Letztlich erfordert die oben dargestellte Security-Analyse (semi-) quantifizierbare Antworten auf die Frage: Wie sicher sind unsere Energieinfrastrukturen in Abhängigkeit der Performance von Sicherungsmaßnahmen? Kosten-Nutzen-Analysen müssen jedoch die Frage beantworten: Wieviel Risikoreduktion erhalte ich für wieviel Invest in Security-Maßnahmen? Hier wird eine objektive, quantitative Grundlage für die Bewertung des Risikos im Sinne einer Vulnerabilitäts- bzw. Security-Metrik notwendig, die einen Vergleich unterschiedlicher Risiken (Kosten vs. Risikominderung) zulässt. Eine Minderung des Security-Risikos kann dabei z.B. durch Prävention,

Kosten-Nutzen-Analysen müssen Bestandteil einer umfassenden Sicherheitskonzeption sein und helfen, Ressourcen zur Sicherung optimal und zielgerichtet einzusetzen.

technische Sicherungsmaßnahmen oder auch Resilienz der kritischen Energieinfrastruktur erfolgen.

Wechselwirkungen von Safety und Security anhand konkreter Beispiele

Zielkonflikte zwischen Safety- und Security-Maßnahmen müssen sorgfältig ausgewogen werden.

Es muss allerdings konstatiert werden, dass es im Bereich der Sicherheitsmaßnahmen und Sicherheitsstrategien zwischen Safety und Security Wechselwirkungen bzw. sogenannte Tradeoffs gibt. Diese bestehenden Zielkonflikte können anschaulich anhand des Absturzes von Germanwings-Flug 9525 beschrieben werden. Als eine Folge der Anschläge von 09/11 ist die Tür zum Cockpit des Piloten durch schusssichere Auslegung und ein besonderes Schließsystem vor willkürlichen (z.B. terroristischen) Öffnungsversuchen durch Unbefugte oder Angreifer geschützt.

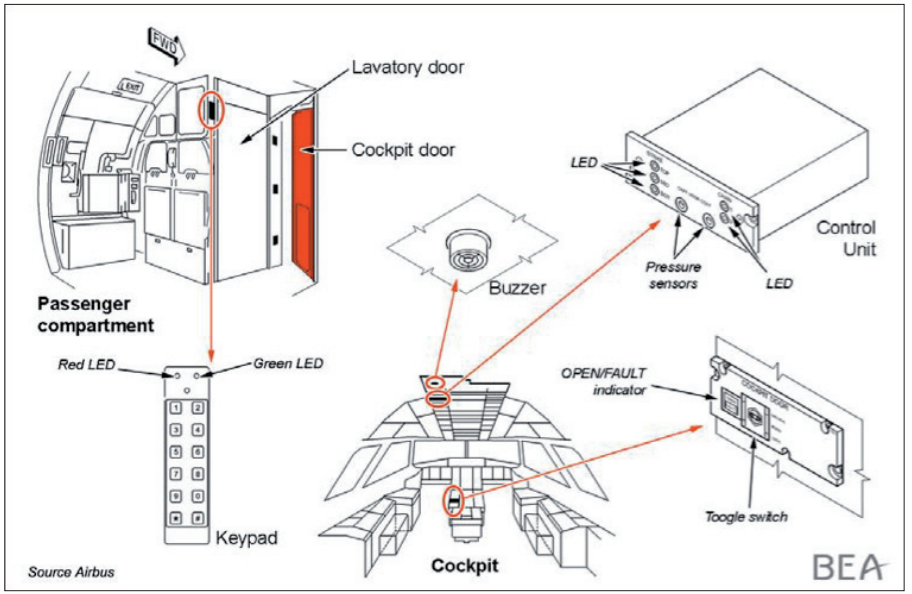


Abbildung 2: Sicherheitsrelevante Elemente in Cockpit und Kabinenbereich [BEA]5/.

Dieses Security-Szenario steht aber im Widerspruch zur Safety-Anforderung, die Passagiere bei einer eintretenden z.B. gesundheitlichen Beeinträchtigung der Piloten z.B. durch Druckabfall (Pilot Incapacitation), die dann das Flugzeug nicht mehr steuern oder landen und auch nicht mehr die Tür von innen öffnen können, durch Öffnen der Tür von außen zu schützen.

Diesen Widerspruch löst man durch einen Öffnungsvorgang der Tür, der durch Eingabe eines Sicherheitscodes durch die Kabinenbesatzung über ein Keypad (Abbildung 2) ausgelöst wird. Dies ist also eine Safety-Maßnahme, mit der sich eine Security-Maßnahme umgehen lässt. Aus Security-Gründen wiederum kann der eingeleitete Öffnungsvorgang, der dem Piloten über einen Summton angezeigt wird, durch den Piloten innerhalb von 15 Sekunden aktiv unterbunden werden. Im Ergebnis und auch als Folge der verketteten und widersprüchlichen Anforderungen an die Sicherheitssysteme in den Bereichen Safety und Security konnte es bei mutmaßlich vorliegender Suizidabsicht des Piloten so zum Absturz des Flugzeuges kommen.

Am Beispiel der Verriegelung einer Cockpit-Tür (Germanwings Flug 9525) werden klare Widersprüche zwischen Safety- und Security-Anforderungen deutlich.

Ein weiteres Beispiel für die Wechselwirkungen, die Safety- und Security-Anforderungen hervorrufen können, kann am Modell eines Wohnhauses aufgezeigt werden. Vor dem Hintergrund unterschiedlicher Safety- und Security-Szenarien und Betrachtungsweisen entstehen systemische Wechselwirkungen. Eine mögliche Risikobewertung bezieht sich auf Angriffs- und Fluchtwege: Ist z.B. die Haustür nur zugezogen oder gar abgeschlossen? Die denkbaren Szenarien wie Einbruch (Security) oder Hausbrand (Safety) führen zu unterschiedlichen Anforderungen. In beiden Fällen ist zu unterscheiden, ob das Ereignis tagsüber (Haustür unverriegelt) oder in der Nacht (Haustür verriegelt) stattfindet. Ein dreigliedriges Security-Risikomodell erweitert um Safety-Aspekte kann die systemischen Wechselwirkungen erfassen (Abbildung 3).

Am Beispiel eines Wohnhauses lässt sich zeigen, wie Safety- und Security-Widersprüche technologisch aufgelöst werden können.

Risikobetrachtung

Dreigliedriges Security-Risikomodell der Security erweitert auf Sicherheit (Safety + Security) (technologisch):

R = **B**edrohung mal **V**erwundbarkeit mal **A**uswirkung

durch:	**Technologische** Maßnahmen zur Verhinderung:	auf:
· Einbrecher · Feuer	· Sicherungssysteme · Brandschutz	· Eigentum · Leben, Gesundheit

Systemische Wechselwirkungen

Abbildung 3: Dreigliedriges Security-Risikomodell in Anlehnung an [HARNSER] erweitert auf Sicherheit (Safety + Security)

wirtschaftlichen Einsatz können unerwünschte Wechselwirkungen hier eliminiert werden.

Mit Hilfe konstruktiver Maßnahmen wie z.B. einem Panikschloss findet eine Entkoppelung der Szenarien statt.

Fazit und Ausblick

Es sind im Wesentlichen zwei globale Entwicklungen bei der Verknüpfung von Safety- und Security-Szenarien zu befördern:

Zum einen treten Security-Bedrohungen z.B. durch zunehmende Evidenz und Wahrnehmung terroristischer Aktivitäten in der Öffentlichkeit immer mehr in den Vordergrund. Der bisherige Fokus auf Safety-Strategien führt zu Widersprüchen mit neuen Security-Anforderungen, die nicht immer technologisch aufzulösen sind.

Zweitens gilt es zu berücksichtigen, dass die zunehmende Vernetzung (IoT) und Globalisierung einen erhöhten Bedarf an verschlüsselter Kommunikation sowie auch Authentifizierung mit sich bringt. IT-Security (wie auch Embedded Security) muss damit als Bestandteil aller sicherheitsrelevanten Systeme in eine Sicherheitsbewertung einbezogen werden. Diese Vernetzung führt zu einer

Verknüpfung von Safety- und Security-Anforderungen und Funktionen, aber auch völlig neue Bedrohungslagen; Vernetzung und moderne Technologien (z.B. Drohnen) bieten neue Angriffs- aber auch Abwehrmaßnahmen.

Fokus 1: Safety-Strategie

Gleichermaßen rücken kritische Versorgungs-, Kommunikations- und Verkehrsinfrastrukturen in den Fokus. Security rückt in den Vordergrund und erfordert ggf. erhebliche Investitionen in Sicherheitsmaßnahmen. Eine getrennte Betrachtung von Safety und Security werden wir uns in Zukunft immer weniger leisten können!

Fokus 2: Security-Strategie

Referenzen

- [HARNSER] Harnser Group: A Reference Security Management Plan for Energy Infrastructure
- https://ec.europa.eu/energy/sites/ener/files/documents/2010_rsmp.pdf
- [BEA] Abschlussbericht zum Absturz Germanwings 9525 in den französischen Alpen 2015, Bureau d'Enquêtes et d'Analyses pour la sécurité de l'aviation civile (BEA) – in deutscher Fassung https://www.bea.aero/uploads/tx_elyextendttnews/BEA2015-0125.de-LR_04.pdf

Es ist das Gebot unserer Zeit: Safety- und Security-Fragen müssen zusammen behandelt werden.

KONZEPT FÜR DEN 3. WELTKONGRESS FÜR SICHERHEITSWISSENSCHAFT

Dr.-Ing. Bernd Schulz-Forberg

Anlass:

1991 fand der 1. Weltkongress für Sicherheitswissenschaft in Köln unter der Federführung des TÜV Rheinland statt, u.a. auch mit Grußworten von dem damaligen BM für Umwelt, Naturschutz und Reaktorsicherheit, Herrn Dr.-Ing Klaus Töpfer. Die Proceedings sind unter ISBN 3-88585-864-9 veröffentlicht und weisen in zwei Bänden zusammen mehr als 1300 Seiten auf.

Zehn Jahre später setzten die TÜV`s das Projekt fort und veranstalteten 2001 in Saarbrücken federführend den „Weltkongress Sicherheit moderner technischer Systeme", veröffentlicht unter ISBN 3-8249-0659-7 mit insgesamt fast 740 Seiten.

Die Proceedings der beiden Sicherheitswissenschaftlichen Weltkongresse 1991 und 2001 weisen folgende Sektionen auf: 1991: Energie, Stoffe/Material, Verkehr, Transport und Produktion; 2001:Energie, Verkehr, Produktion, IT-Sicherheit und /Bio/Med./Gen-Technik. Jetzt müssen sicher z.B. der Arbeitsschutz, der Gesundheitsschutz und der Umweltschutz hinzugefügt werden.

Wie auch immer, es ist sicher an der Zeit, das Thema Sicherheit wieder intensiv aufzuarbeiten und damit eine Standortbestimmung vorzunehmen, denn Sicherheit ist ein bedeutender Wirtschaftsfaktor (Sicherheit macht Märkte)."

Jetzt kann aus der Berliner Gesamtkonferenz der Sicherheitsinstitutionen ein valider Anlauf angeregt werden.
Zeitraum: 2020 / 2021
Veranstalter: BGKdSi mit N.N.

Die vorlaufenden Weltkongresse 1991 und 2001 haben die volkswirtschaftliche Bedeutung gerade auch für die Bundesrepublik Deutschland deutlich aufgezeigt. Es gilt daran anzuknüpfen und die veränderten Bedingungen besonders hervorzuheben.

Inhalte:

- IT-Sicherheit (einschließlich Industrie 4.0, automated systems)
- Industrielle Sicherheit (einschließlich Anlagensicherheit, Energie, Civil Engineering)
- Verkehrssicherheit (einschließlich Gefahrgutsicherheit, Luftverkehrssicherheit, Raumfahrt)
- Arbeitsschutz (einschließlich Strahlenschutz)
- Gesundheitsschutz (einschließlich Verbraucherschutz, Medizinprodukte, Nahrungsmittel)
- Umweltschutz (einschließlich Katastrophenschutz)
- Organisatorische Voraussetzungen (Verantwortung, Managementsysteme, Faktor Mensch)

Wissenschaftliches Komitee / Unterstützer:

VDI, TÜV Süd AG, BAM, BSI, RKI, UBA, KIT, BAST, DLR, VDI, ACATECH, Geramanischer Lloyd, Dekra, Gesamtverband der deutschen Versicherer (GDV) , DAkkS, Deutsche Gesetzliche Unfallversicherung (DGUV, Berufsgenossenschaften), Bundesverband der Deutschen Industrie e.V. (BDI),Deutscher Gewerkschaftsbund (DGB), ...
Eine Internationalisierung wird gemeinsam anzustreben sein, z.B. KIVI aus den Niederlanden, EU OSHA (Bilbao), EU-VRi, EU Kommission, World Safety Organization (WSO), International Labor Organization (ILO), ... sowie die herausragenden Akteure aus der Wirtschaft und den beiden ersten Kongressen.

Organisationskommittee:

BGKdSi und N.N.
Organisation:
Federführende Organisation mit beauftragtem Dienstleister
Finanzierung: Wird mit den Stakeholdern zu klären sein.

DER FÖRDERVEREIN ADA DEUTSCHLAND E.V.

Dr. HUBERT B. KELLER

automotive safety & security

www.automotive-deutschland.de

Reliability – Safety – Security – Quality

Der Automotive Bereich erfährt einen grundlegenden Wandel durch die rasch fortschreitende Digitalisierung, alternative Antriebskonzepte, Vernetzung von Fahrzeugen und Infrastrukturen sowie autonomen Fahrfunktionen. Die Weiterentwicklung klassischer Methoden und Vorgehensweisen zur Sicherstellung der erforderlichen Software-Qualität sicherheitskritischer Anteile wird aktuellen automobilen Anforderungen nicht mehr gerecht. Mit der Öffnung der Systeme für weltweite Netze entstehen neue Anforderungen an die Absicherung gegen illegale Zugriffe und an die Geheimhaltung personenbezogener Daten..

safeware engineering
safe and secure software

www.saveware-engineering.org

Smarte Systeme und das Internet der Dinge (IoT) beginnen unsere ganze Lebenswelt zu durchdringen. Für die gesellschaftliche Akzeptanz dieser Anwendungen ist es essentiell, dass sie einfach und ohne Gefahr verwendet werden können.

Damit Software zur SafeWare wird, einer Software, die Menschen auch im weitesten Sinn keinen Schaden zufügt, muss sie ihre versprochene Funktion ohne zusätzliche Freiheitsgrade (Schwachstellen) auch bei widrigen Umständen wesentlich erfüllen. Sie muss gegen nicht-autorisierte Zugriffe gesichert sein und die Vertraulichkeit von Daten bewahren. Aspekte der Zuverlässigkeit, Verfügbarkeit, Fehlertoleranz, Sicherheit gegen Angriffe und der Schutz privater und geheimer Daten müssen zusammenwirken, um den Übergang zur SafeWare zu bewerkstelligen. Wir, die Träger hinter SafeWare Engineering, wollen mit unseren Workshops und Konferenzen hierzu beitragen.

Smart Systems and the Internet of Things (IoT) are beginning to permeate our entire life. For the social acceptance of these applications, it is essential that they can be used easily and without danger.

In order for software to become SafeWare, a software that does not harm people in the broadest sense, it must fulfill its promised function without any additional variances (vulnerabilities), even in adverse circumstances. It must be secured against unauthorized access and protect the confidentiality of data. Aspects of reliability, availability, fault tolerance, security against attacks, and the protection of private and secret data must work together to make the transition to SafeWare. We, the professional sponsors behind SafeWare Engineering, want to contribute with our workshops and conferences.

Fachgruppe Ada – Zuverlässige Software-Systeme

Unser Leben hängt zunehmend von der Sicherheit Software/ Computergesteuerter Systeme ab. Dazu zählen Verkehrssysteme zu Lande, zu Wasser und in der Luft, medizintechnische Systeme, Kernkraftwerke, aber auch Telekommunikationssysteme oder Netzleitsysteme der Stromversorgung.

In den Bereichen Verkehr, Gesundheit, Luft/Raumfahrt und Prozesssteuerung, wo Softwarezuverlässigkeit direkt die Sicherheit für Menschen garantiert, ist Ada zu einer bevorzugten Sprache geworden. In mehreren internationalen Sicherheitsstandards wird Ada explizit als geeignete Programmiersprache aufgeführt. Dazu zählen der IEC 61508, EN 50128 und DO-178B.

Die Luftfahrtindustrie z.B. hat mit dem DO-178B einen weltweiten Standard geschaffen, der diese Probleme behandelt und das Airlines Electronic Engineering Committee hat eine Liste von Ada Eigenschaften aufgestellt, die für die Verwendung in Avionik Software besonders geeignet sind.

Ada unterstützt in einzigartiger Weise moderne Analyse, Design und Programmiermethoden. Deshalb erachten wir Ada als die beste Programmiersprache zur Entwicklung großer zuverlässiger Anwendungen mit knappem Kostenrahmen.

www.fg-ada.gi.de/startseite.html

Als GI-Fachgruppe will Ada Deutschland technisch-wissenschaftliche Beiträge auf dem Gebiet der Ada-Technologie leisten. Darüber hinaus hat Ada Deutschland das Ziel, die Aufmerksamkeit der Öffentlichkeit und der Fachwelt auf die Programmiersprache Ada und deren Bedeutung für die Softwaretechnologie zu lenken und die Verbreitung der Ada-Technologie zu fördern.

Förderverein Ada Deutschland e. V.

www.ada-deutschland.de

Der Förderverein Ada Deutschland e.V. wurde am 15. Juli 1998 in Karlsruhe gegründet und verfolgt ausschließlich und unmittelbar gemeinnützige Zwecke und ist daher steuerbegünstigt. Er unterstützt die Ziele der Fachgruppe Ada der Gesellschaft für Informatik und arbeitet eng mit dieser zusammen, steht allen Organisationen und Personen offen, die sich mit den Zielen des Vereins identifizieren und finanziert sich bis auf weiteres nur durch Spenden und freiwillige Mitgliedsbeiträge.

Die Ziele des Vereins sind:

- die Programmiersprache Ada in Forschung und Lehre verbreiten,
- das Verständnis für die Sprache und deren Anwendungspotential in Ausbildung und Praxis fördern,
- Konzepte und Verfahren zur korrekten Erstellung von Software-Systemen entwickeln,
- das Grundlagenwissen der Entwicklung zuverlässiger Software mit der Programmiersprache Ada vertiefen,
- die Publikation von wissenschaftlichen Arbeiten im Zusammenhang mit Ada fördern,
- Treffen von Fachleuten und wissenschaftlich und technisch Interessierten ermöglichen,
- Finanzierungsbeihilfen für Forschungsvorhaben und Veranstaltungen sowie Reisen in diesem Zusammenhang zu vergeben,
- Forschung und Lehre sowie die Öffentlichkeitsarbeit unterstützen,

- Kolloquien und Workshops zu den oben genannten Themen veranstalten,
- nationale und internationale Tagungen organisieren,
- Beziehungen mit gemeinnützigen Institutionen mit gleichartiger Zielsetzung pflegen.

Darüber hinaus will der Verein die Öffentlichkeit über Potentiale, Risiken und Methoden zur Erstellung komplexer Software-Systeme informieren. Hierfür unterstützt er die SafeWare Engineering Veranstaltungen, die Automotive – Safety&Security Tagungen und auch die Berliner Gesamtkonferenz der Sicherheitsinstitutionen.

Förderverein Ada Deutschland e.V.
Dr. Hubert B. Keller (Vorsitzender)
Dr. Peter Dencker (Stellvtr.)
Erasmusstr. 3
D-76139 Karlsruhe
Tel. 0721 608 25756
Fax 0721 9 68 35 30

IMPRESSUM

Das FORUM Technologie & Gesellschaft ist eine Initiative getragen vom
FORUM46 – Interdisziplinäres Forum für Europa e. V.
Kontakt: Dr. Bernd Schulz-Forberg
bernd.schulz-forberg@forum46.eu
Grafik: HÖPPNERDESIGN
Foto Titelseite: © Elnur - Fotolia.com

Postfach 640237
D-10048 Berlin
www.forum46.eu

Berliner Gesamtkonferenz der Sicherheitsinstitutionen

In der Sicherheitslandschaft ist die Vorgehensweise über alle Disziplinen nicht gleichartig fundiert, es fehlen ausreichende gegenseitige Information, Kooperationen und Synergien. Dr.-Ing. Bernd Schulz-Forberg (Forum46) und Dipl.-Ing. Dirk Pinnow (Ltr. AKSi BV BB) haben 2015 diesen Gedanken von Prof. Dr. sc. Prof. e.h. Gerhard Banse, Berliner Zentrum Technik & Kultur, in Kooperation mit Dr.-Ing. Dennis Göge, Deutsches Zentrum für Luft- und Raumfahrt e.V., aufgegriffen und eine regelmäßig tagende Gesamtkonferenz der mit Sicherheit befassten Institutionen nach Berlin einberufen. Dabei wird auch der fachliche Austausch mit mitteleuropäischen Kooperationspartnern (Plattform für Europäische Vordenker) angestrebt.

Erklärtes Ziel der BGKdSi ist die Überwindung von individuellen als auch übergreifenden Verständnisgrenzen. Die gegenseitige Information und vor allen Dingen Kommunikation und Kooperation sind von herausragender Bedeutung. Eine allgemein etablierte Sicherheitskultur mit Konzepten zur Technischen Sicherheit, zur IT-Sicherheit sowie zu Sicherungsverfahren (Security) verstärkt die Möglichkeiten der Volkswirtschaften. Diese so verstandene Sicherheitskultur bildet die Kernaufgabe der Berliner Gesamtkonfernz der Sicherheitsinstitutionen (BGKdSi).

Erste Ergebnisse sind Abhandlungen zur Erstellung einer umfassenden Sicherheitslandkarte für Deutschland und – im Rahmen der political awareness – ein Vorschlag für eine IT Sicherheits-Kommission, wobei die Erfolgsaussichten der Digitalen Transformation nur bei gewahrtem Sicherheitsniveau erwartet werden können. Ferner sind die Themen Lernkultur, also das Lernen aus großen Schadensvorfällen wie auch aus den nicht-meldepflichtigen Störfällen oder Beinahe-Unfällen, und Verfahren zum Management zunehmender Komplexität (Human factor) heraus zu stellen.