Berliner Gesamtkonferenz der Sicherheitsinstitutionen

Zu Gast im Bundesministerium für Wirtschaft und Energie (BMWi)

- Grußworte
- Akkreditierung und Konformitätsbewertung in globalen Lieferketten
- Lessons learned – PISEA Ergebnis in Safety und IT-Security
- Nukleartechnologie als Vorreiter für Sicherheitskonzepte
- Sicherheit im STIHL-AKKU-System
- Arbeiten 4.0
- Fortsetzung von Themen der BGKdSI

FORUM Technologie & Gesellschaft

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

Die Veranstaltung wurde ermöglicht durch die freundliche Unterstützung der DEKRA , der Framatom GmbH, der Firma STIHL, Ada Deutschland e.V. und der Deutschen Akkreditierungsstelle DAkkS.

.

INHALT

GRUSSWORTE

Dipl.-Ing. Dirk Pinnow
Dr. Arne Höll
Prof. Dr. Thomas Schendler

Für die BGKdSI-Konferenzleitung begrüßte Dirk Pinnow die Anwesenden und dankte dem BMWi, vertreten durch **Herrn MR Dr. Arne Höll** für die durch Stellung des Sitzungssaales gewährte Unterstützung. Herr Höll seinerseits betonte in seinem Grußwort die thematische Breite der Sicherheit – Konflikte gelte es dabei angemessen zu adressieren und auch Effizienz sowie Effektivität im Auge zu behalten. Im BMWi widme sich die Abteilung VI der Digitalisierung und Innovation und stütze sich auf eine breit gefächerte Qualitätsinfrastruktur, so auch der Marktüberwachung und Normung. Das BMWi lege großen Wert auf Kooperation – beispielhaft benannte er die BAM, die DAkkS, das DIN und die PTB.

Der Erfolg der Qualitätsinfrastruktur basiert auf Sicherheit.

Herr Prof. Dr. Thomas Schendler überbrachte die Grüße des Präsidenten der Bundesanstalt für Materialforschung und -prüfung (BAM) (**Prof. Dr. rer. nat. habil. Ulrich Panne**). Er unterstrich das Interesse seitens der BAM an der BGKdSI und verwies auf das BAM-Motto **„Sicherheit in Technik und Chemie“**. Die BAM ist eine wissenschaftlich-technische Bundesoberbehörde im Geschäftsbereich des Bundesministeriums für Wirtschaft und Energie. Im nächsten Jahr feiert sie ihr 150-jähriges Bestehen. Unter Ihrem o.a. Motto und mit ihrem Slogan **„Sicherheit macht Märkte“** setzt und vertritt die BAM für Deutschland und seine globalen Märkte hohe Standards für Sicherheit in Technik und Chemie zur Weiterentwicklung der erfolgreichen deutschen Qualitätskultur **„Made in Germany“**.

Die BAM als Ressortforschungsanstalt hat Sicherheit im Fokus.

Der Begriff „Sicherheit“, der sich naturgemäß wie ein roter Faden durch die heutigen Beiträge dieser wie auch der vorangegangenen Gesamtkonferenzen zieht, ist, wie aus den eben gemachten Ausführungen ersichtlich, das Leitmotiv für die Arbeiten der BAM. In ihren Themenfeldern „Energie“, „Infrastruktur“, „Material“,

„Umwelt“ und „Analytical Science“ hat die BAM ihre jeweiligen Arbeitsschwerpunkte und Aufgaben unter ihrem Motto **„Sicherheit in Technik und Chemie“** gestellt und integriert Forschung, Bewertung und Beratung in Technik und Chemie unter einem Dach.

Wie es heute deutlicher als früher ist, bedarf der Begriff **„Sicherheit“** aber auch einer kontinuierlichen Neuinterpretation in einer beschleunigten globalisierten Welt, in welcher Risiken in komplexer Weise entstehen und beherrscht werden müssen. Diese notwendige ständige Anpassung wird auch deutlich ersichtlich, wenn man die Begriffe **„Safety“** und **„Security“** als Schlagworte nimmt und in den zurückliegenden Dekaden wissenschaftlicher Veröffentlichungen in Hinblick auf ihre unterschiedlichen Schwerpunkte analysiert.

Die fortschreitende Digitalisierung aller Lebensbereiche ist die Herausforderung für sicheres Handeln.

Während in den vergangenen Jahrzehnten der Fokus in der Sicherheitsforschung auf dem Thema **„Safety“** lag, nimmt heute das Thema **„Security“** immer mehr einen größeren Raum ein. Hierzu seien beispielhaft die Schlagworte **„Cyber Security“** oder **„zivile Sicherheitsforschung“** genannt. Sicherheit war und ist aber ein wesentlicher Faktor für den verantwortungsvollen technologischen Wandel und damit ein Garant für den Wohlstand unserer Gesellschaft. Neue Technologien sind die Basis für die erfolgreiche Weiterentwicklung des Wirtschaftsstandortes Deutschland und für eine Wertschöpfung in globalen Märkten.

Die nachhaltige Sicherheit neuer Technologien schafft das Vertrauen von Bürgern in den Wandel und sichert unsere Zukunft. Die Gewährleistung der Sicherheit von neuen Technologien und Produkten ist somit auch ein wichtiger vertrauensbildender Faktor für die gesellschaftliche Akzeptanz neuer Technologien. Dies ist besonders wichtig für die heutigen Herausforderungen wie zum Beispiel der **„Energiewende“**, hier sei z. B. auf die zu erwartende exponentiell

Vertrauen in das Wirken von Wissenschaft und Technik muss stets erarbeitet werden.

Worte können alles mögliche auslösen. „Verbrenner“ abschaffen ist so ein gefährlich falsches Wort!

Schwerpunktthemen werden politisch behandelt. Querschnittsthemen wie Sicherheit tun sich schwer.

ansteigende Bedeutung der Wasserstofftechnologie hingewiesen, der **„eMobilität“** und der Digitalisierung/Industrie 4.0. So wird der mögliche Umstieg von fossilen Brennstoffen auf Wasserstoff oder **„Power to x“**-Produkten nur gelingen, wenn die Gesellschaft Vertrauen in die damit verbundenen Technologien gewinnt. Dies ist auch eine wesentliche **Aufgabe der Sicherheitsinstitutionen**. *„Insoweit bin ich mir sicher, dass diese Gesamtkonferenz auch unter diesem Fokus erfolgreich verlaufen wird“*, so Professor Schendler.

Herr Dr.-Ing. Bernd Schulz-Forberg stellte für die Konferenzleitung die unter seiner Federführung vom „FORUM Technologie & Gesellschaft“ im FORUM46 e.V. erstellte Broschüre zur vorhergehenden Auflage vor (**6. BGKdSI vom 14. September 2018 zu Gast beim BDI**) und berichtete kurz über ein aktuelles Buchprojekt zum Thema „Anlagensicherheit“. Von den darin aufgeführten 18 Thesen hob er insbesondere die These 8 hervor: „Die Verbindlichkeit von untergesetzlichen Regeln kann gesteigert werden.“ Die Notwendigkeit zur Schaffung von Standards unterstrich er mit zwei kurzen Videos über einen Fall- und einen Kollisionsversuch mit Behältern für radioaktive Stoffe. Er betonte, dass in Analogie zur Deutschen Gesellschaft für Qualität (DGQ) eine „Deutsche Gesellschaft für Sicherheit“ etabliert werden müsste, um eben der Querschnittsaufgabe **„Sicherheit“** besser gerecht werden zu können.

AKKREDITIERUNG UND KONFORMITÄTSBEWERTUNG IN GLOBALEN LIEFERKETTEN

Ing. Dr. jur. Raoul Kirmes,
Leiter Stabsbereich II Grundsatzaufgaben der
Deutschen Akkreditierungsstelle GmbH (DAkkS)

1. Einleitung

Rechtliche Vorgaben werden durch technische Normen ergänzt.

Zur Einleitung in das Thema wird ausgeführt, dass im 19. Jahrhundert der preußische Staat nur über technische Beamte in der Bauverwaltung verfügte und deshalb personell nicht in der Lage war, die aufkommenden Probleme der Dampfkesselanlagen selbst zu lösen. Nach Vec, Miloš in „Recht und Normierung in der industriellen Revolution", kann der dazu erfolgende Paradigmenwechsel wie folgt beschrieben werden: *„Der Staat macht somit die gesellschaftliche Selbstnormierung zur Grundlage seiner eigenen Sicherheitsstandards. Dieses Mischmodell bei der Überwachung gefährlicher gewerblicher Anlagen wird zur Keimzelle des modernen Rechts der technischen Sicherheit"*. Man kann das auch als die Geburtsstunde von Organisationen wie TÜV und Dekra verstehen. Selbstverwaltung sowohl im Bereich der Erstellung technischer Vorschriften als auch für die technische Überwachung griff Platz mit dem Gesetz vom 3. Mai 1872.

2. Vom „New and Global Approach" zum „New Legislative Framework" (NLF)

Der Staat beschränkt sich in weiten Bereichen auf das Gewährleistungsprinzip.

Seit 1985 laufen die Bemühungen, die Regulierung im Binnenmarkt voranzubringen. Bekannt geworden ist zunächst der sog. New and Global Approach, der das o.a. Prinzip der gesellschaftlichen Selbstnormierung aufgegriffen hat. Man kann auch sagen, dass Prüf- und Sicherheitsleistungen für Konsumgüter vom Staat in die Wirtschaft verlagert wurden. Erste Erfahrungen konnten dann bei der Überarbeitung aufgegriffen werden und in das heute geltende Leitkonzept der Binnenmarktregulierung in der EU, dem New Legislative Framework einfließen.

Dabei geht es um die technische Harmonisierung von Anforderungen zum Abbau von Handelshemmnissen in der EU, die wesentliche Anforderungen für die Sicherheit von Produkten (hohes Schutzniveau Art 114 AEUV), die Nationalen Gesetze und

das EU-Sekundärrecht mit den grundlegenden Anforderungen, den Technischen Spezifikationen in Normen (auf die vom Gesetzgeber verwiesen wird), die Stärkung der Herstellerverantwortung (Produkthaftung) und der staatlichen Verantwortung durch die Marktüberwachung.

Der Staat zieht sich aus der Durchführungsverantwortung weitestgehend zurück und nimmt ganz wesentlich nur die Gewährleistungsverantwortung wahr. Ein Überblick über die Regelungen ergibt sich aus nachstehender Abbildung

Die Abwägung zwischen Durchführungs- und Gewährleistungsverantwortung muss risikobasiert erfolgen.

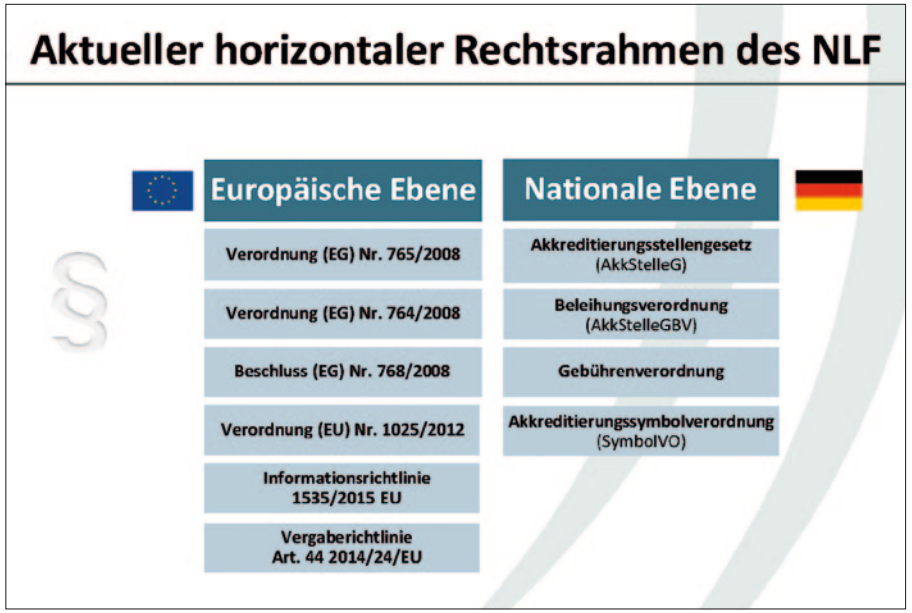


Abb. Kirmes Folie 5:

Die Qualitätsinfrastruktur gliedert sich in drei Säulen, nämlich Anforderungen, Vormarktprüfung und Marktüberwachung. Die Anforderungen sind entweder international (ISO), Supra-National (CEN) oder national (DIN). In der zweiten Säule der Qualitätsinfrastruktur bilden die Konformitätsbewertung und die Akkreditierung die wesentlichen Bausteine der WTO-Regelung.

Das gesamte System soll sich für die Globalisierung in der Wirtschaft wenn irgend möglich zur Zufriedenheit aller weiter entwickeln und damit letztlich Handelsbarrieren überflüssig machen. Auf dem Weg dahin sind natürlich Schwierigkeiten zu überwinden und Herausforderungen zu bestehen.

3. Wo liegen die Schwierigkeiten im Global Governance?

Die Verbraucher erwarten ein stimmiges System. Sie erwarten aber auch im Zweifel den Durchgriff des Staates.

Wenn alle Stakeholder sich verabredungsgemäß verhalten, kann der internationale Ansatz gelingen. Dabei wird die transnationale Legitimation durch Sachverstand gewährleistet, die Vertrauenswürdigkeit wird durch Konformitätsbewertung und Akkreditierung hergestellt. Schließlich erwarten die Verbraucher, dass eine Kennzeichnung auch wirklich zutrifft. Der Staat muss für die Verlässlichkeit verbraucherbezogener Produktkennzeichnung sorgen, indem er es garantiert.

Nachstehend findet sich in dem Bild ein Überblick über die verschiedenen Verfahren, um allen Anforderungen von der Akkreditierung bis zum Produkt gerecht werden zu können.

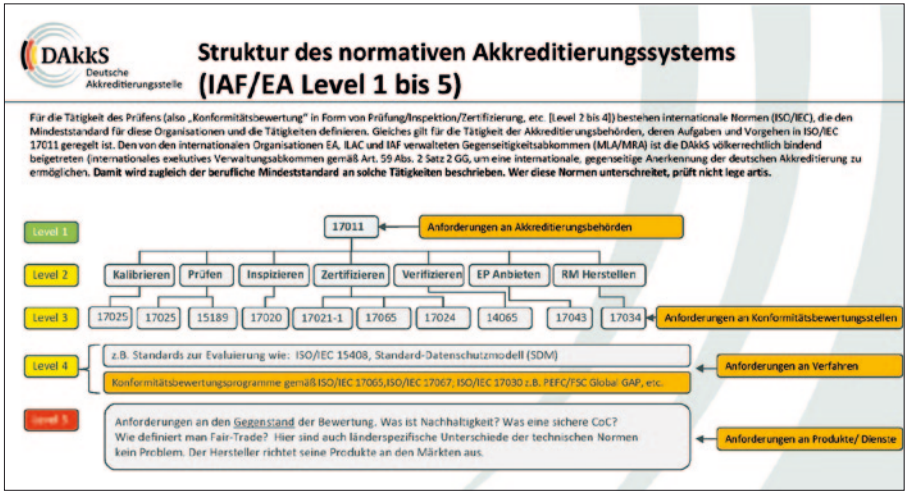


Abb. Kirmes Folie 15:

Akkreditierung ist ein Instrument des WTO-Rechts zur internationalen Harmonisierung und Anerkennung der Konformitätsbewertung, wobei Normung, Konformitätsbewertung und Technische Vorschriften zusammen betrachtet werden müssen. Internationale Abkommen helfen dabei, Handelsbarrieren abzubauen (ILAC- und IAF-Abkommen).

Für EU-Europa gilt grundsätzlich das gleiche Vorgehen, nur die rechtliche Verbindlichkeit ist stringenter gefasst, siehe nachstehendes Bild.

Die weitere Entwicklung wird permanent beobachtet; rechtzeitige Korrektur muss möglich sein.

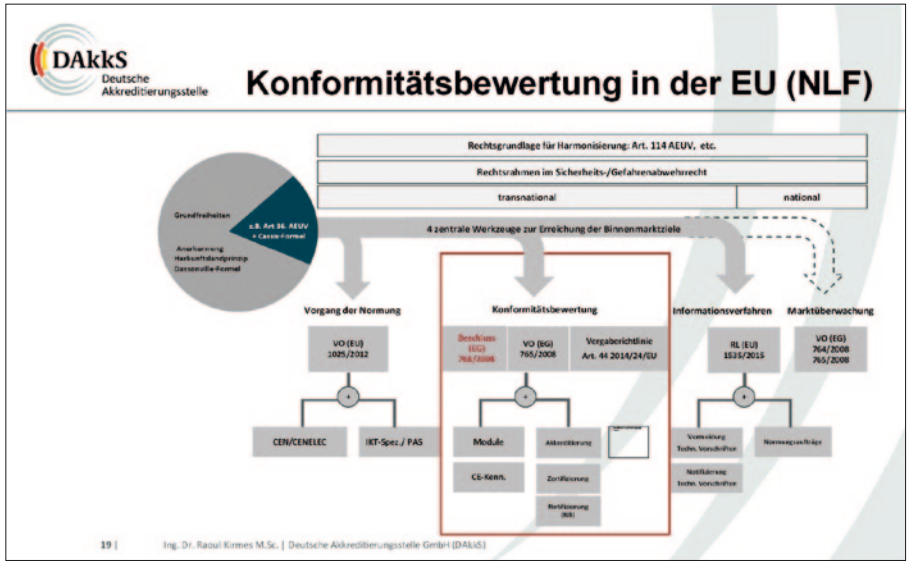


Abb. Kirmes Folie 19:

Schließlich soll in dem nachfolgenden Bild noch ein Überblick über die Zusammenhänge mit den Programmeignern die Vielschichtigkeit der gesamten Prozessketten verdeutlichen.

Ob es letztlich zur Zufriedenheit aller gelingen kann, einen weltweiten Handel auf vertrauensbasierten Tätigkeiten aufzubauen und zu erhalten, bleibt die Kernfrage für die WTO.

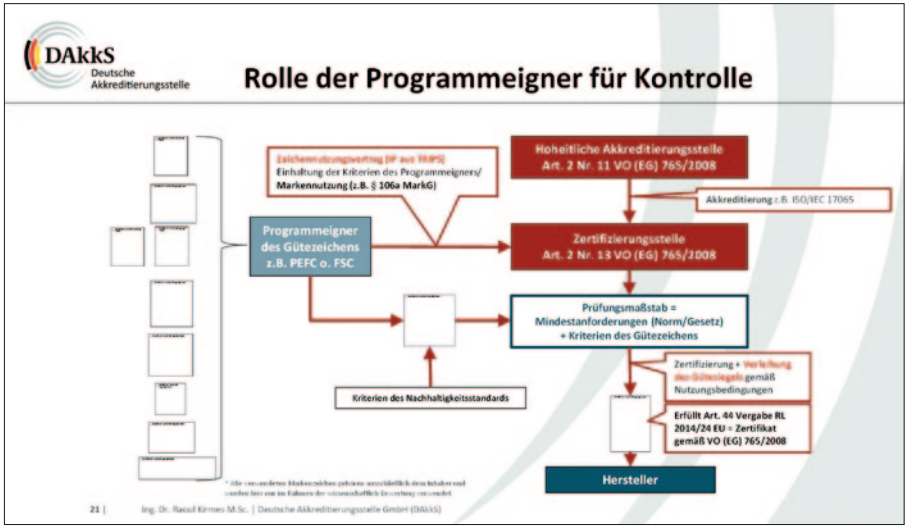


Abb. Kirmes Folie 21:

4. Drei Thesen und jeweils eine erste Antwort

Die DAkkS prüft die Prüfer!

These 1

Dass Prüf- und Zertifizierungsstellen private Organisationen sind, ist ein wichtiges Funktionsmerkmal für die transnationale Wirkung der Kontroll- und Integritätssysteme. Eine deutsche Behörde kann ja nicht selbst in Bangladesch Hersteller überprüfen!

Aber diesen Vorteilen stehen auch Risiken gegenüber. Der Preisdruck im Wettbewerb ist der Prüfqualität abträglich und die Prüfstellen sind potenziellen Unabhängigkeits-, Fraud- und Korruptionsrisiken ausgesetzt.

Antwort

Deshalb ist eine staatliche Überwachung durch die hoheitlichen Akkreditierungsstellen erforderlich.

These 2

Können die Qualität und Glaubwürdigkeit von Zertifikaten und Siegeln für Verbraucher durch veränderte gesetzliche Rahmenbedingungen erhöht werden?

Antwort

Derzeit ist ein massiver Wildwuchs unregulierter Gütesiegel und Labels zu beobachten. Dieser Wildwuchs bringt das ganze System in Gefahr, denn ist das Verbrauchervertrauen erst enttäuscht, scheitert auch der Funktionsmechanismus der marktbasierten Anreizsysteme für Gütesiegel und Zertifikate. Es bedarf deshalb umgehend regulativer Rahmenbedingungen zum Schutz der Vertrauenswürdigkeit dieser Systeme. Wer am Markt für sich in Anspruch nimmt, die Konformität für Verbraucherprodukte festzustellen, bedarf einer staatlichen Akkreditierung im Hinblick auf Kompetenz und Unabhängigkeit.

Die Akkreditierer der Staaten sichern das System über **Peer-Review** (Kreuzgutachten).

These 3

Ist eine Akkreditierungspflicht für Konformitätsbewertungsstellen, die Labels für Verbraucherprodukte ausgeben, eine Lösung ?

Antwort

Ja, denn die hoheitliche Akkreditierung stellt nach internationalen Standards für Akkreditierungsbehörden (ISO/IEC 17011) sicher, dass die Unabhängigkeit und Kompetenz der Prüfstelle gewährleistet ist und dass eine Prüfleistung durchgeführt wird, die zu reproduzierbaren und vergleichbaren Ergebnissen führt.
Dabei wird die Pluralität der verschiedenen technische Anforderungen (Normen), Sozial- und Nachhaltigkeitsstandards voll gewahrt. So wird ein Mindestmaß an Verbrauchervertrauen hergestellt. Fehlanreize durch „green and social washing" werden vermieden!

Auch hier gilt:
Abwarten, beobachten und bereit sein zum Eingriff.

Ceterum censeo: Digitalisierung geht uns alle an.

Cybersecurity-Probleme werden viel diskutiert. Es gibt Lösungsmöglichkeiten: man muss sie nur umsetzen!

Lesen Sie bitte den nachstehenden Artikel.

Digitalisierung

Einfügung des Herausgebers

LESSONS LEARNED – PISEA-ERGEBNISSE IN SAFETY AND IT-SECURITY

Dr. Hubert B. Keller

Vorbemerkung der Herausgeber: Dr. Hubert B. Keller war z.Zt. des Vortrages Leiter des Fachgebiets „Advanced Automation Technologies“ im KIT (Karlsruher Institut für Technologie), leitete direkt die Arbeitsgruppe „Reliable, Safe and Secure Software and Systems“, war Prinicpal Investigator in KASTEL (Karlsruher Kompetenzzentrum für angewandte Sicherheitstechnologie) und ist Vorsitzender von Ada Deutschland e.V. (Verein für sichere Software).
Er forscht über Sichere Software, Echtzeitsysteme und Maschinelle Intelligenz und ist Mitbegründer des GI Fachbereichs „Sicherheit – Schutz und Zuverlässigkeit“, er war Co-Chair der Sicherheitstagung der Gesellschaft für Informatik (GI) 2003, Co-Chair der Konferenzen Reliable Software Technologies Europe 2000 und 2013, der Automotive – Safety&Security Konferenzen seit 2004 und weiterer.

Als Autor von „Echtzeitsysteme“, Springer Verlag 2019, und „Maschinelle Intelligenz“, Vieweg Verlag 2000, sowie Mitautor von „Technical Safety- An Attribute of Quality“, Springer Verlag 2018, und engagierter Fachmann in mehreren weiteren Organisationen besitzt er eine hohe Expertise im Bereich Safety und Cyber Security.
Der Vortrag enthielt 68 Folien, die ein großes Maß an Details zur Safety und Cyber Security beinhalten und wegen der grundlegenden Bedeutung für die Weiterentwicklung in Deutschland in Gänze gelesen werden sollten. Daher wird der Vortrag auf www.forum46.eu in dem Bereich „Technologie und Gesellschaft“ veröffentlicht und steht dort neben der Dokumentation über diese 7. Berliner Gesamtkonferenz der Sicherheitsinstitutionen (BGKdSI).
Nachstehend die textuelle Fassung in gekürzter Version.

1. Einleitung

Unsere Gesellschaft stützt sich massiv auf eine vernetzte Automatisierung mit einer hohen Dezentralisierung. Beispiele sind Kritische Infrastrukturen wie Energie, Wasser, Verkehr etc. sowie auch die Lieferketten in der Industrie. Diese Vernetzung bietet enorme Entwicklungspotentiale, aber auch gleichzeitig hohe Security-Risiken. Seit Jahren sind zunehmend Schwachstellen in diesen Systemen festzustellen, die es Angreifer erlauben, sich in Systeme einzuklinken, diese zu übernehmen und zu zerstören oder aber hohe Geldforderungen zu stellen.

Dieser Vortrag widmet sich dem Thema „Lessons learned – PISEA Ergebnis in Safety und IT-Security" (PISEA - Programme for International Science and Engineering Assessment) und fragt „Wie sicher sind Kritische Infrastrukturen, Automatisierungslösungen, Smart Grids, Home Automation, smarte Geräte, etc.?“.

2. Angriffsszenarien

In Polen hackt ein 14-Jähriger Teenager eine Straßenbahn mit einer einfachen Fernbedienung. Dahinter steht, dass infrarotes Licht als Steuersystem eingesetzt wurde. „Die Weichen werden anscheinend per Infrarot gesteuert. Das bedeutet, dass er nur die Codes, vielleicht noch die Lichtfrequenz und die Amplitude, herausfinden musste.“ (siehe [1]). Welche Einstellung ist hier beim Entwurf der Sicherheit zu erkennen?

Als Ursachen wird in ([2]) genannt: „Transport command and control systems are commonly designed by engineers with little experience or knowledge about security using commodity electronics and a little native wit. The apparent ease with which Lodz's tram network was hacked, even by these low standards, is still a bit of an eye opener."

Obwohl dieser Angriff und die vorhandene Sicherheit sehr einfach waren, ist anhand des folgenden Bildes (aus [3]) zu sehen, dass es eine hohe Anzahl von Angriffen auf wichtige Bereiche des öffentlichen Lebens gibt.

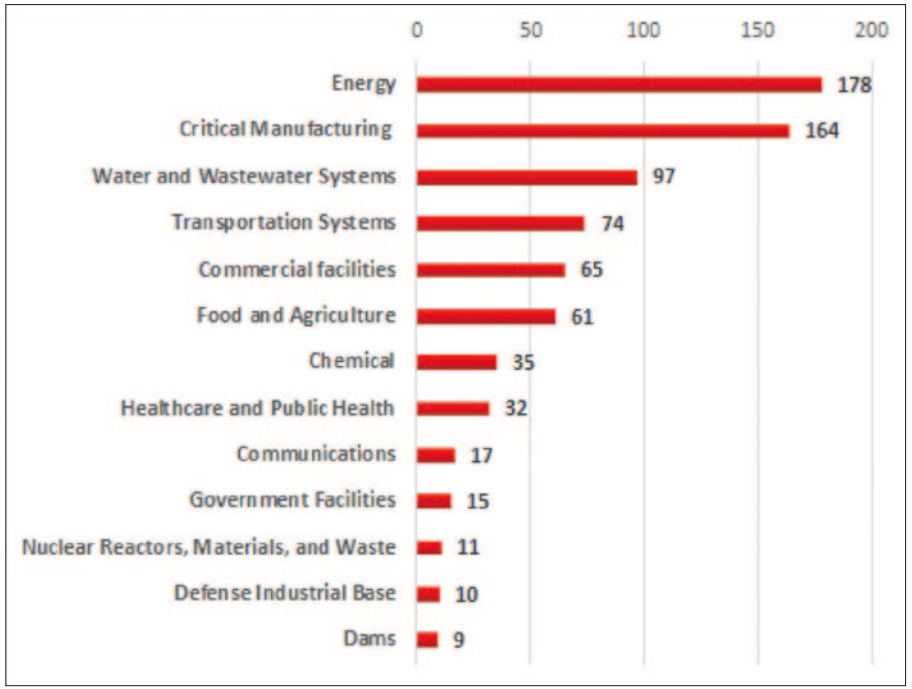


Bild 1: Angriffsbereiche (nach [3])

Beim Energiesektor mit dem zukünftig hoch verteilten und massiv über IKT verbundenen Komponenten bestehen zudem noch spezifische Angriffsvektoren (vgl. [4]).

Laut Cyber Security Assessment Netherlands - CSAN-4 ([5]) bietet sich ein düsteres Bild der Realität. Die IoT-Attacken 2017 zeigen einen Anstieg um 600% gegenüber 2016. Der erwartete Schaden 2019 wird 2 Billionen US-Dollar weltweit betragen. In Deutschland stieg er von 51,6 Mio. Euro 2016 auf 71,8 Mio. Euro 2017 an, wobei die erfasste Cyberkriminalität in Deutschland 85.960 Fälle in 2017 umfasste. Bei 20 Milliarden internetfähigen Geräten, Tendenz steigend, erfolgt alle 39 Sekunden weltweit ein Hackerangriff.
Die zugrundeliegenden Schwachstellen sind dabei von einer Art, die sich permanent fortsetzt. Dies

ist erkennbar an der hohen Zahl von wiederkehrenden Updates, im Bild 2 rot eingefärbt. Es werden Schwachstellen singulär repariert und nicht systematisch vermieden. Als Konsequenz gibt es ein Update für das Update oder Updates in Folge.

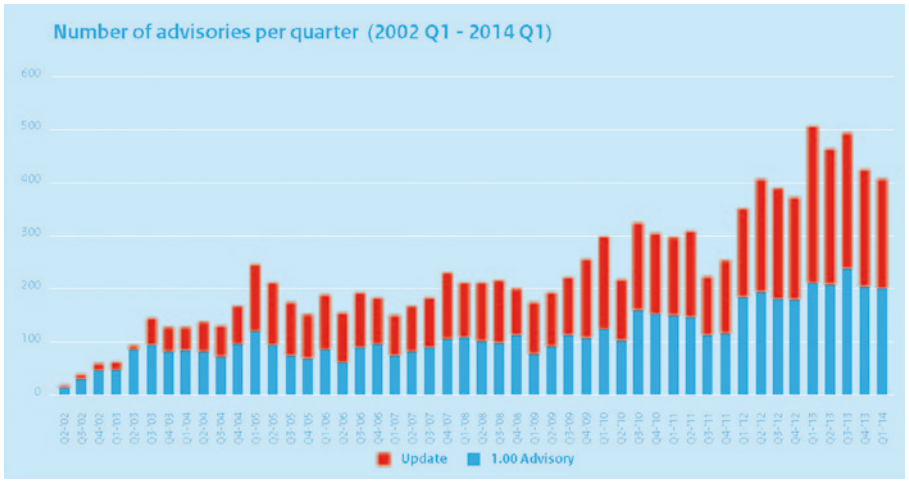


Bild 2: Update Problematik (nach [5])

Die Hacker benutzen dabei Werkzeuge (siehe Bild 3), welche standardmäßig viele Exploits beinhalten: „Overview of integrated exploits for products in 60 exploit kits (Hack Tools). Other sources also report the dominant presence of Java in the exploit market. Together with Java, Microsoft Internet Explorer and Adobe Flash and Adobe Reader/Acrobat account for 80 percent of the integrated exploits in exploit kits."

Mit diesen Werkzeugen ist es für Angreifer ein Leichtes, das Internet lahmzulegen. Am 21 Oktober 2016 erfolgte ein Angriff auf das Unternehmen Dyn, eine "switch-board operator company", als Teil des internationalen Domain Name System (DNS). Viele Internetseiten waren nicht mehr erreichbar. Der Grund war ein massiver Distributed Denial of Service (DDoS) Angriff durch die vorherige Übernahme von Tausenden von internetfähigen Geräten (siehe ([6]). Die Angreifer nutzten Schwachstellen aus, die Firmen aufgrund ihrer „speed-to-market"-Strategie, anstatt eine "security-by-design"-Strategie zu fahren, nicht behoben hatten. Die in Verkehr gebrachten anfälligen Geräte konnten von den Angreifern übernommen und eingesetzt werden (siehe ([6]).

Dies lässt sich auf „Kritische Infrastrukturen“ übertragen. Der Schutz von Öl, Gas, Energieerzeugung, -übertragung, Smart Grids und andere Bereiche ist zentrales Thema für alle Verantwortliche. Die Vernetzung all dieser Bereiche führt auch zu Safety-Problemen. Beispielsweise haben Forscher der University of Michigan gezeigt, wie schwach Verkehrsführungsanlagen abgesichert sind. Sie nutzen Schwachstellen in der kabellosen Kommunikation von Ampeln aus und übernahmen diese komplett. Katastrophale Konsequenzen wären ein leichtes Ergebnis (siehe ([6]).

Mit Industrie 4.0 sollen die Industriezweige noch stärker digitalisiert und vernetzt werden. Bei den gegebenen Schwachstellen stellt die Vernetzung mit Zulieferbetrieben über Enterprise Management Systemen bis hinunter in die Produktions- und Prozessebene ein riesiges Security-Problem dar. Im „Draft NISTIR 8276“ ([7]) wird dieses Thema intensiv diskutiert und die Frage nach der Resilienz der Supply Chains gestellt.

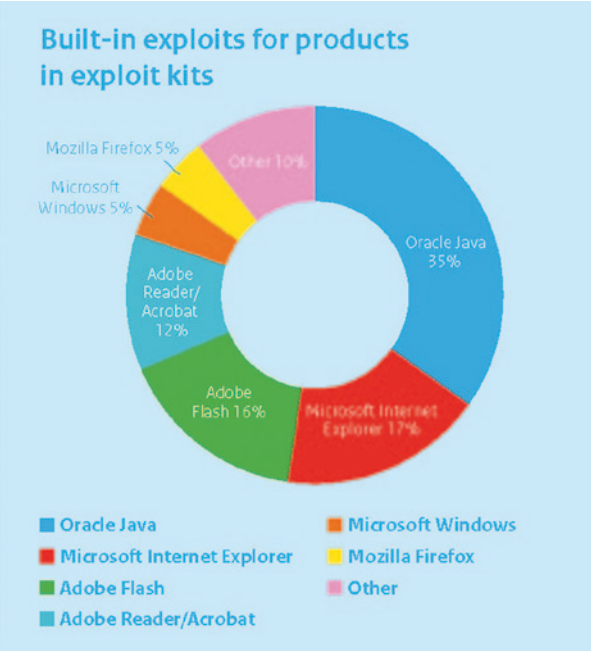


Bild 3: Produkt bezogene Exploit Kits (nach [5])

Dass dieses Thema höchst kritisch ist, zeigt ein dazu passender Fall, genannt ShadowHammer. 2018 wurde die Update-Funktionalität eines Computerherstellers (ASUS) gehackt und mit Schadsoftware versehen. Die kompromittierte Software wurde über das Update-Werkzeug auf der offiziellen Website des Herstellers verteilt und erreichte Millionen von Nutzern. Diese Aktion erfolgte als Reminiszenz an die Dragonfly-Gruppe, die seit 2013 industrielle Automatisierungssysteme auf die gleiche Art angriff (siehe hierzu [8] von Europol).

Im Januar 2019 hatte Kaspersky Lab diesen Angriff entdeckt. Ungefähr 500.000 Windows-Rechner waren betroffen und erhielten die Schadsoftware mit einem gültigen ASUS-Zertifikat. Die Schadsoftware war gezielt auf bestimmte Rechnersysteme ausgerichtet.

Dies sind keine isolierten Angriffe, die Strategie dahinter, „island hopping“ genannt, ist es, alle verbundenen Partner und Kunden zu erreichen (siehe ([9]).

Die Ausgestaltung der Kommunikationsinfrastruktur mit 5G wirft ebenfalls erhebliche Security-Probleme auf. Im Report der ENISA (siehe [10]) wird die nachfolgende Grafik von Bild 4 mit den darin genannten Bedrohungen aufgeführt.

Selbst der militärische Bereich ist von diesen Schwachstellen nicht verschont. Waffensysteme des Department of Defense (DoD) werden immer vernetzter und über IKT geführt. In der eingesetzten Software wurden betriebskritische Security-Schwachstellen entdeckt, die mit einfachen Mitteln ausgenutzt werden konnten. Die Systeme konnten komplett übernommen und unentdeckt genutzt werden (siehe ([11]).

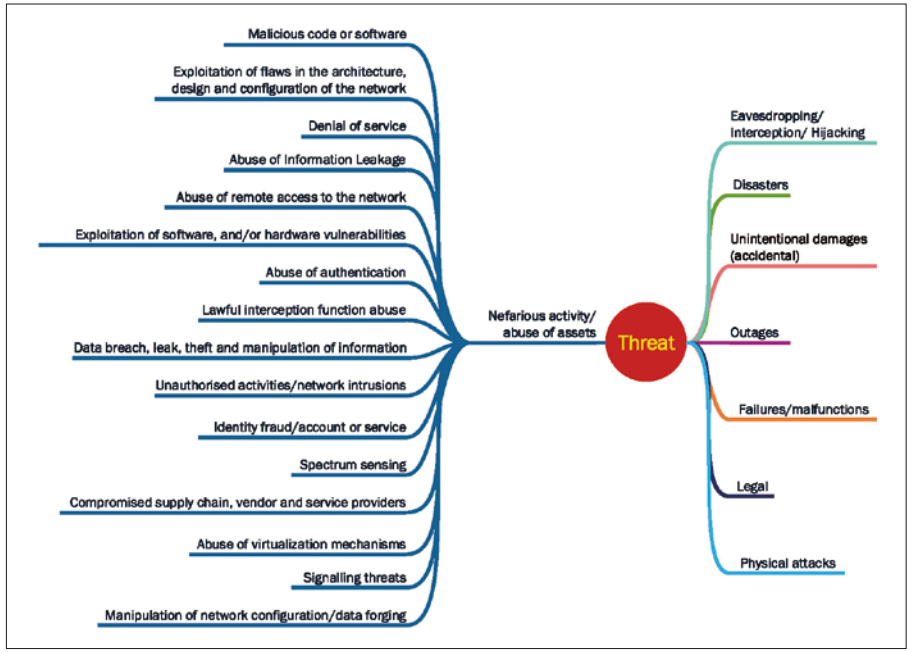


Bild 4: 5G-Schwachstellen (nach [10])

Es muss festgehalten werden, dass die existierenden Schwachstellen von vielen Akteuren mit unterschiedlichen Interessen und Zielsetzungen ausgenutzt werden. Falls nur Geld im Spiel wäre, könnte nur von einem finanziellen Schaden ausgegangen werden. Dies ist aber leider nicht immer so. Potente Angreifer interessieren sich entweder für Geld oder für wirtschaftlich oder politisch verwertbare Informationen (siehe ([5]).

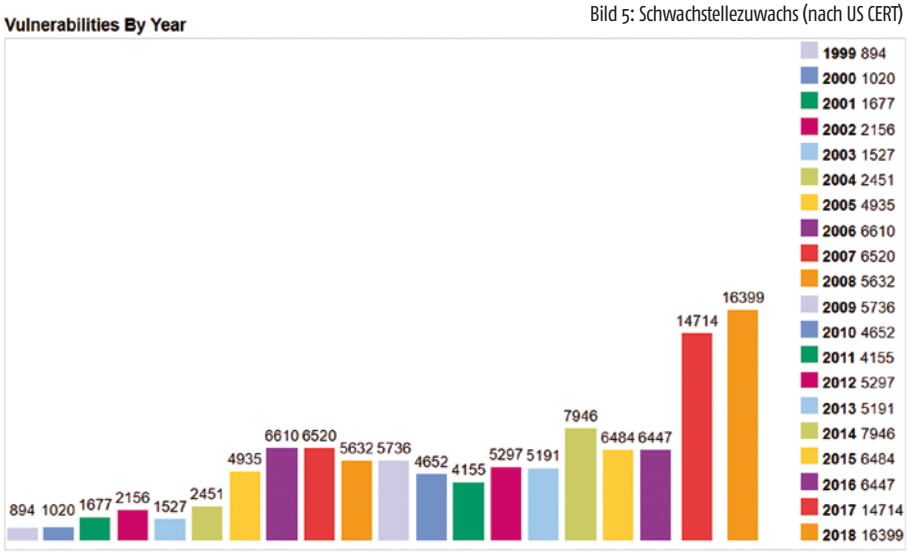
3. Schwachstellen und Einfallstore

Die Entwicklung der erkannten Schwachstellen zeigt eine stetige Zunahme (Bild 5, nach Daten des US CERT).

Insbesondere eigentlich aus der Informatik als gelöst betrachtete Probleme zeigen sich immer wieder in steigender Tendenz. Index Range Violations, Buffer Overflow oder Stack Overflow sind Schwachstellen, die es seit Jahrzehnten eigentlich nicht mehr geben dürfte. Typstrenge Sprachen mit entsprechenden Prüfungen zu Übersetzungs- und Laufzeit vermeiden diese Probleme grundsätzlich.

In den vorhandenen Implementierungen bleiben die Software Schwachstellen nach wie vor extrem hoch. Gerade auch in viel genutzter Standardsoftware. Security by Design ist nach wie vor keine Strategie in der industriellen Herstellung. Sprachen wie Java, die sich einer großen Beliebtheit erfreuen und in den Embedded-Markt drängen, bzw. C und C++ bringen gerade diese Schwachstellen in kritische

Bild 5: Schwachstellezuwachs (nach US CERT)



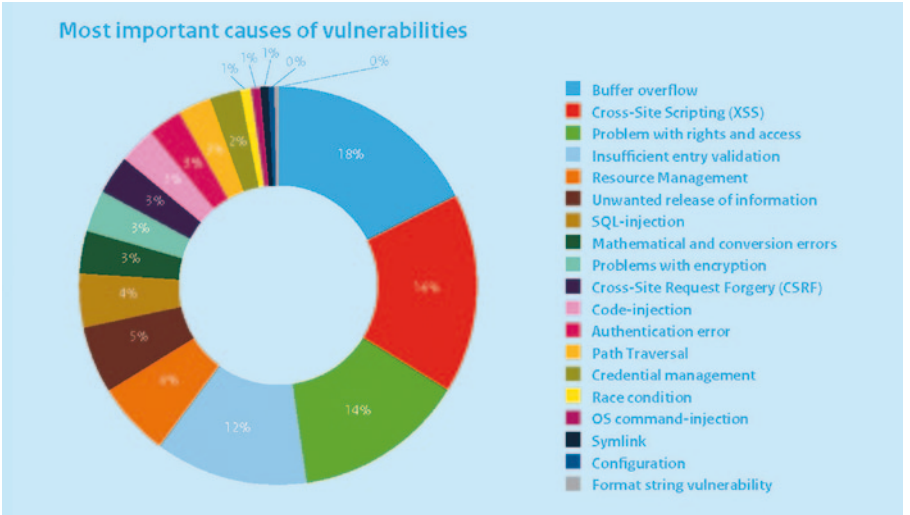


Bild 6: Ursachen von Schwachstellen (nach [5])

Bereiche. Hacker-Werkzeuge beinhalten Standardangriffsverfahren, die direkt auf Java Anwendungen abzielen (siehe [5] und Bild 6).

Im Bericht des NIST ([12]) sind die Aussagen eindeutig:

- „ ... 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.“

Aber auch die Implementierung von Fernzugriffsprotokollen zeigt massivste Schwachstellen. Im Mai 2019 wurde eine Microsoft security vulnerability CVE-2019-0708 (BlueKeep) entdeckt, die es Angreifer erlaubt, sich über RDP (Remote Desktop Protocol) sich zu verbinden und spezielle Bitstrings zu senden. Diese Schwachstelle erlaubt das Ausführen von Programmen auf dem Zielrechner ohne Aktion des Benutzers, ohne eine Datei hochzuladen, ohne Schadsoftware einzuschleusen. Der Rechner muss nur eingeschaltet sein! Mindestens 1 Million Zielrechner waren davon betroffen. (siehe hierzu ([8]).

Im Bereich der industriellen Automatisierung definiert die ISA 99, jetzt IEC 62443, eine Security Architektur basierend auf einer Segmentierung und Abschottung des Netzwerks. Dazu werden Secure Router, VPNs und Monitoring Systeme eingesetzt. Es bleibt die Frage ob das ausreichend ist, wenn SPS mit bekannten Schwachstellen direkt über das Internet erreichbar sind oder Router mit der gleichen Problematik eingesetzt werden. Im Energiebereich sind Schwachstellen wie bei Siemens SIPROTEC 4 and SIPROTEC Compact (Update B), 07/27/2017, „Advisory contains mitigation details for improper input validation, missing authorization, and improper authentication vulnerabilities in the Siemens SIPROTEC 4 and SIPROTEC Compact devices", regelmäßig auftretend (siehe http://ics-cert.us-cert.gov).

Da nützt ein Statement beispielsweise von Siemens wie "Digital transformation will only be successful if we succeed in ensuring the security of data and networked systems. Digitalization and cybersecurity are two sides of the same coin" wenig.

Auch die Meldung im Handelsblatt „Siemens, Daimler, Airbus, Telekom, TÜV: Allianz für Cyber-Sicherheit findet immer mehr Mitglieder" und „Hackerangriffe kosten Konzerne jedes Jahr Milliarden – und die Risiken steigen weiter. Ein Bündnis von 16 Konzernen hat nun Standards für die Sicherheit in ihren Lieferketten definiert" belegt noch wenig (siehe https://www.charteroftrust.com/).
Der Einsatz von VPNs kommt mit den nachfolgenden und immer wieder auftretenden Meldungen ebenfalls schnell an seine Grenzen (siehe Cybersecurity & Infrastructure Security Agency, USA, https://www.cisa.gov/):

- Juniper Networks Releases Security Updates
  Original release date: January 09, 2020
  Juniper Networks has released security updates to address multiple vulnerabilities in various Juniper products. A remote attacker could exploit some of these vulnerabilities to take control of an affected system.
- VMware Releases Security Updates
  Original release date: November 12, 2019
  VMware has released security updates to address vulnerabilities in ESXi, Workstation, and Fusion. An attacker could exploit some of these vulnerabilities to take control of an affected system.

Schaut man sich bei US CERT oder ICS CERT die Liste der firmenspezifischen Meldungen an, ist zu erkennen, dass die Anzahl der Schwachstellen nicht wirklich weniger wird. Stellvertretend für viele anderen Hersteller sei Siemens mit etwa 100 Schwachstellen im Zeitraum 2016 bis 2019 erwähnt.

4. Informatik-Erkenntnisse aus den Jahren 1970 und folgende

Die Entwicklung von Software ist historisch gut nachzuvollziehen. Ab 1955 erfolgte die Realisierung kleinster und kleiner Programme (elementare Algorithmen) auf noch wenig leistungsfähigen Rechnern. Die Programme waren leicht überblickbar, die Problemstellung elementar. Leistungsfähigere Prozessoren erlaubten dann Lösungen für größere Problemstellungen und Programme, aber ohne Ingenieurmäßiges Vorgehen. Es wurden viele Sprachen, je nach Problem bzw. Teilproblem, eingesetzt. Die Durchführung der Projekte war nicht systematisiert (kein Phasenzyklus), die Struktur der Programme ergab sich irgendwie und die Implementierung war höchst individuell und extrem optimiert.

Der Kollaps der Programmerstellung war somit programmiert, die Kosten im laufenden Betrieb für die Behebung von Fehlern oder die Anpassung an geänderte Anforderungen waren enorm. Die Wartbarkeit und Wiederverwendbarkeit von Programmen oder -Teilen war nicht möglich, ja die Fehlerbehebung produzierte selbst wieder Fehler. Teilweise wurde auf die Behebung von Fehlern verzichtet, da ein erkannter Fehler besser beherrschbar war, als die durch die Behebung entstehenden neuen Fehler. Dies führte zur sogenannten Software-Krise um ca. 1972.

Die Mathematik von Algorithmen war eigentlich schon immer eindeutig definiert. Auch die Informatik hatte klare Festlegungen. Jeder Algorithmus war für bestimmte Eingabedaten definiert und liefert nach endlichen Schritten auf einem Rechner die zugehörigen Ausgabedaten. Nicht zulässige Eingaben sind zu erkennen und als Fehler zu melden.

Die Idee der Spezifikation von Software ist es, in mathematischer und prüfbarer Weise das Verhalten von Software im Voraus zu beschreiben. Allerdings ergibt sich hier ein Problem. Das Programm darf nur und nur ausschließlich die Spezifikation realisieren und keine weiteren Freiheitsgrade. Daran halten sich aber gerade populäre Sprachen absolut nicht und führen höchst kritische Freiheitsgrade in die Implementierung ein, die sich dann als Schwachstellen äußern. Eine reine Prüfung auf die vorgegebene Spezifikation erkennt dies nicht.

Ein Fehler betrifft iPhones, ein anderer Windows und ein dritter betrifft Server mit Linux. Auf den ers-

ten Blick unterschiedliche Fehler, in Wirklichkeit aber die gleiche Ursache – unsichere Speicherzugriffe (siehe hierzu ([13]):

"By allowing these types of vulnerabilities, languages such as C and C++ have facilitated a nearly unending stream of critical computer security vulnerabilities for years."

Was passiert bei einer Liste von 10 Elementen, wenn das 11. Element abgefragt wird?
Normalerweise erwartet man die Fehlermeldung „Element nicht vorhanden ". Bei Speicherunsicheren Sprachen erhält man aber das, was in den Speicherstellen nach dem 10. Element steht. Manchmal Unsinn, manchmal aber direkt dort stehende Passwörter und Benutzerdaten.

„HeartBleed, which impacted 17 percent of the secure web servers on the internet, was a buffer-overflow exploit, letting you read 60 kilobytes past the end of a list, including passwords and other users' data" (siehe hierzu ([13]).

5. Entwicklungen anhand ausgewählter Beispiele

Am Software Engineering Institute der Carnegie Mellon University hat Robert C. Seacord Vorgaben für Secure Coding entwickelt (siehe ([14]):

- Validate input. Validate input from all untrusted data sources. Proper input validation can eliminate the vast majority of software vulnerabilities.
- Heed compiler warnings. Compile code using the highest warning level available for your compiler and eliminate warnings by modifying the code [C MSC00-A, C++ MSC00-A]. Use static and dynamic analysis tools to detect and eliminate additional security flaws.
- Architect and design for security policies. Create a software architecture and design your software to implement and enforce security policies.
- Keep it simple. Keep the design as simple and small as possible. Complex designs increase the likelihood that errors will be made in their implementation, configuration, and use.
- Default deny. Base access decisions on permission rather than exclusion. This means that, by default, access is denied.
- Adhere to the principle of least privilege. Every process should execute with the the least set of privileges necessary to complete the job.

- Sanitize data sent to other systems. Sanitize all data passed. Attackers may be able to invoke unused functionality in these components through the use of SQL, command, or other injection attacks. Because the calling process understands the context, it is responsible for sanitizing the data before invoking the subsystem.

Diese Vorgaben sollen die Schwachstellen von C / C++ einigermaßen beheben. Allerdings besitzen C und C++ weitere kritische Schwachstellen in der Sprachdefinition und gerade auch im Laufzeitsystem. Die Sprache Java besitzt weniger Schwachstellen als C und C++, hat aber ebenfalls noch sehr kritische Sprachdefizite wie Konvertierungsprobleme etc. (siehe [15]).
Dagegen war die Sprache Ada von Anfang an für höchste Zuverlässigkeit im Rahmen eines wissenschaftlichen Wettbewerbs entwickelt worden:

- Ada is an unusual language because it was developed in response to a detailed set of requirements.
- In the early 1970s no suitable language was found to fulfill these requirements.
- A competition was then created for companies to create a language meeting the government requirements: Readability, Efficiency, Provability, Expressiveness
- Winner was a team from France lead by Jean Ichbiah.
- Ada achieved ANSI standardization in 1980, and ISO standardization in 1983.

Als modulare und typstrenge Sprache gilt: Jede Variable hat einen statisch zugewiesenen Typ mit allen (!) Informationen zur Übersetzungszeit (!) und ist damit durch den Compiler prüfbar. Zur Laufzeit werden neu zugewiesene Werte automatisch auf Typkorrektheit geprüft. Es gibt keinen falschen Index, keinen Buffer Overflow usw. (siehe hierzu ([16] und]17[).
Die Sprachziele von Ada waren:

- Unterstützung der Zuverlässigkeit und Wartbarkeit von Programmen,
- Berücksichtigung des Programmierens als menschliche Tätigkeit (Teamarbeit) und
- Sicherstellung der Effizienz der Programme
- Lesbarkeit von Programmen hat Vorrang vor einfachen Schreibweise
- Variable müssen explizit mit ihrem Typ deklariert werden, Typ einer Variable ist fest
- Übersetzer kann falsche Verwendung zur Übersetzungszeit feststellen
- Laufzeitsystem ebenso bei dynamischer Zuweisung (Array mit Indexgrenzen!)

- Ada betrachtet Variablen und Typen mit mathematischer Präzision

Dass Defizite einer Sprache und eines Betriebssystems ausgeglichen werden müssen, fordert die Namur-Empfehlung NE 153 ([19]). Darüber hinaus lassen sich die Anforderungen der NE 153 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. Also:

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

Diese Empfehlung kann vom Autor gerne zur Verfügung gestellt werden. Die meisten Normen sind im Gegensatz dazu deskriptiv und nicht konstruktiv (vgl. Orientierungsleitfaden für Hersteller zur IEC 62443, ZVEI [18]). Security-Normen nehmen auch Wahrscheinlichkeiten z. B. über die Kompetenz eines Angreifers an, die so nicht wirklich existieren. Toolkits, zum Teil mit KI-Verfahren, bieten auch dem unbedarften Angreifer weitgehende Möglichkeiten (siehe Niederlande). Bestehende Normen sind z.B. die IEC 62443 (ehemals ISA99) oder die ISO 27001 sowie die Richtlinien von BSI, NIST, EU etc.

Neue Entwicklungen versuchen mit Methoden der Künstlichen Intelligenz (KI) die Sicherheit (Security) zu erhöhen. Dabei entsteht ein Wettlauf zwischen Angreifer und Schutzsystem. KI in der Cyber Security dient z. B. zur Analyse und zum Lernen von Normalverhalten, der Analyse und Erkennung von Anomalien (siehe NISTIR Report 8219c [20]). Auf Basis der Analyse von Bitstrings oder auch auf der Ebene symbolischer Elemente zur statischen Analyse wird versucht Angriffe zu erkennen. KI wird auch zur Klassifikation im Zugang (Security), aber gleichzeitig auch in intelligenten Hackertools eingesetzt.

Auf der anderen Seite stellt sich die Frage nach der Cyber Security von KI-Verfahren. Hier geht es z.B. um die Manipulierbarkeit von KI Verfahren, die Datenmanipulation (Bilder, Werte, Fake News, ...), die Fehlleitung der Bilderkennung im autonomen Fahren oder um die Provokation falscher Klassifikationen und nachfolgend falsche Handlungsableitungen.

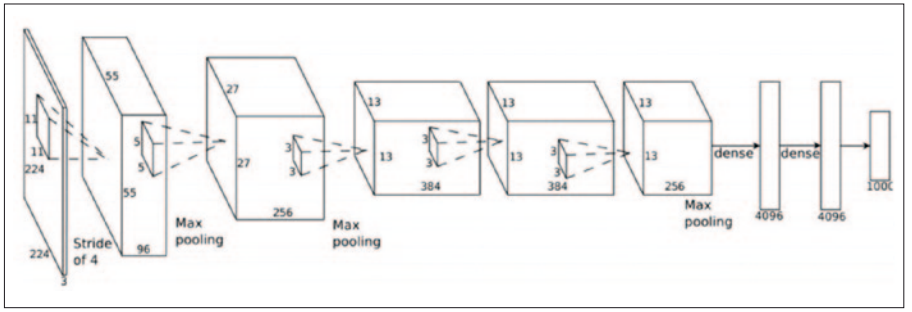


Bild 7: Schema Deep Learning (nach [21])

Gerade beim Einsatz des sogenannten Deep Learning sind Fragen der Manipulierbarkeit und der Robustheit noch nicht ausreichend erforscht. Das Deep Learning setzt Rosenblatts Perceptron letztlich nur auf einen neuen Level in der einsetzbaren Rechenleistung. Es erlaubt Bildanalysen über neuronale Netze mit vielen Hidden Layern und lokaler Zuständigkeit mit Faltungen (Filter, siehe Bild 7).

Das Ziel ist Eigenschaftselemente (Features) von Bildern zu extrahieren, daraus Objektteile zusammen zu führen und dann Objekte im Bild zu erkennen (Klassifikation). Dynamische Rückkopplungen erlauben auch den Einsatz für eine Verhaltensmodellierung (zeitlich). Umfangreich eingesetzt wird es für das „Bildverstehen" im Autonomen Fahrzeug. Dieses Bildverstehen wurde durch einfache farbige Muster (siehe Bild 8, linke Seite) nachhaltig gestört, so dass Personen mit diesem Farbmuster nicht mehr als

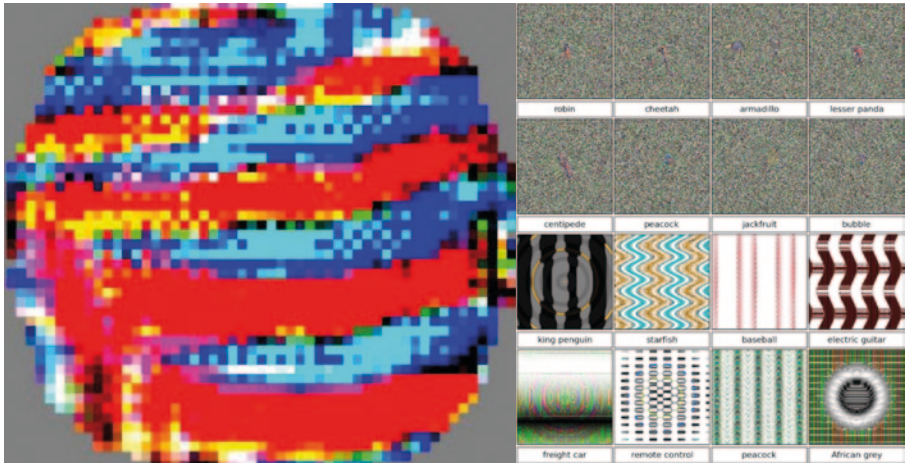


Bild 8: Manipulationsmuster (nach [22] und [23])

solche erkannt wurden (siehe [22]). Andere Forscher haben weitere „Störbilder" gefunden, die zu einer Fehlerkennung führen ([23]).

Allerdings ist der Autor der Ansicht, dass die Anwendbarkeit nur bei definierten Kontexten wie einer Paketverteilanlage mit Erkennungsraten bis zu 96% sinnvoll ist. Bei komplexen und hochdynamischen Kontexten wie ein Fahrzeugumfeld ist die Zuverlässigkeit und insbesondere die Robustheit bei Störungen, ob zufällig oder gezielt, kritisch zu sehen. Bild 9 zeigt diese Problematik.

6. Stakeholder für die Entwicklung sicherer Systeme

Betrachtet man die Welt der Stakeholder in diesem Themengebiet, so stellt man umfangreiche Aktivitäten in den USA fest. Dort sind insbesondere das US CERT, das ICS CERT, das NIST und Homeland Security etc. sehr aktiv in der Analyse der Problematik und der Festlegung von Richtlinien und Vorgaben.

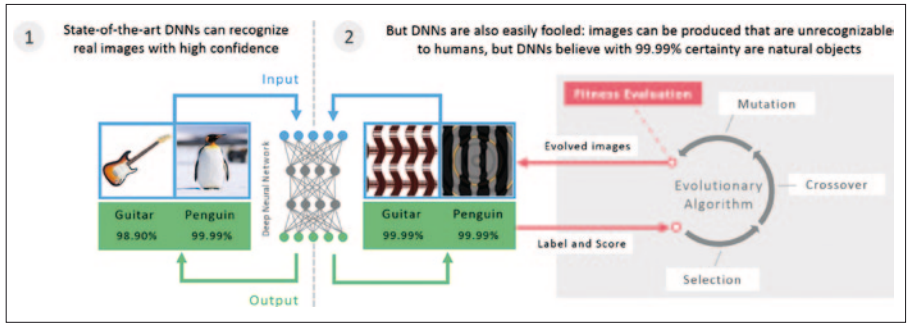


Bild 9: Schema Fehlklassifikation und Verbesserung durch EA (nach [23])

Auch ist die Datenbank des US CERT bzw. ICS CERT die einzig nahezu vollständige Datenbasis über erkannte Schwachstellen. Auch Kapersky Labs bezieht sich auf diese Datenbasis in ihren Berichten. Daneben gibt es das Software Engineering Institute der Carnegie Mellon University, das seit vielen Jahren im Bereich des Software Engineering einschließlich der Safety- und Security-Themen aktiv ist.

General Electric, ein US-amerikanisches Unternehmen, setzt in seiner Strategie für Cyber Security auf eine urdeutsche Erfindung, den L4 Kernel der ehemaligen und leider aufgelösten Gesellschaft für Mathematik und Datenverarbeitung in Bonn (GMD). General Electric hat in diesen deutschen Betriebssystemkern Security Features einbauen lassen.

In den Niederlanden gibt es das National Cyber Security Centre (NCSC). Es arbeitet zusammen mit der Wirtschaft, Regierungsbehörden und Wissenschaftlern um die niederländische Gesellschaft in der digitalen Welt zu schützen:

- The NCSC supports the central government and organisations in fulfilling an essential function for society by providing expertise and advice, response to threats and enhancing crisis management.
- In addition, the NCSC provides information and advice to citizens, the government and the business community relating to awareness and prevention.
- This means that the NCSC constitutes the central reporting and information point for IT threats and security incidents.
- The NCSC is part of the Cyber Security Department of the National Coordinator for Security and Counterterrorism [Nationaal Coördinator Terrorismebestrijding en Veiligheid] (NCTV).

In Deutschland existiert das Bundesamt für Sicherheit in der Informationstechnik (BSI). Es soll für die Gesellschaft den Schutz in der digitalen Welt absichern, aber nach dem geplanten IT-Sicherheitsgesetz 2.0 gleichzeitig auch Angriffsoptionen erarbeiten. Dies führt zu einem eklatanten Widerspruch in seiner Aufgabenstellung.

Daher hat die Gesellschaft für Informatik auf Basis einer Analyse der Fachgruppe Ada eine entsprechende Stellungnahme übermittelt. Diese Stellungnahme der Gesellschaft für Informatik – Fachgruppe ADA – Zuverlässige Software-Systeme vom 22.5.2019 ([24]) sieht einen Mangel an Gewaltenteilung beim Thema IT-Sicherheit und der Aufteilung der Verantwortung in voneinander gänzlich unabhängige Entitäten.

Es sind daher 3 Bereiche bzw. Verantwortungen klar zu trennen:

1. Hersteller

(Beispiele aus der Luftfahrt: Airbus, Boeing):

- stellen Produkte her, die Sicherheitskriterien erfüllen sollen
- Produkte müssen Sicherheitsstandards genügen und sich einer Zulassung unterziehen

2. Zulassungsbehörde

(Beispiele aus der Luftfahrt: Luftfahrt-Bundesamt LBA, FAA):

- definiert Standards für Sicherheitszertifikat oder Gebrauchszulassung

- akkreditiert die unabhängigen Gutachter/Testlabore
- Gutachter dürfen in keinem Abhängigkeitsverhältnis stehen

3. Organisation für die Untersuchung von IT-Sicherheitsvorfällen

(Beispiele aus der Luftfahrt:
Bundesstelle für Flugunfalluntersuchung BFU, NTSB):

- führt Buch über alle entdeckten IT-Sicherheitsvorfälle
- veröffentlicht diese nach gesetzlich zu definierender Vorgabe
- untersucht die Ursachen dieser Vorfälle zur Aufdeckung von Schwächen
- kann Empfehlungen für die Änderung der Standards und Vorschriften ableiten
- ist gänzlich unabhängig von Hersteller und Zulassungsbehörde
- technische Untersuchung soll Erkenntnisse gewinnen, um künftige Vorfälle und Störungen zu vermeiden

Die IT-Sicherheitsstandards können gemeinsam von allen interessierten Seiten entwickelt und nach öffentlicher Diskussion als anzuwendende Standards verabschiedet werden.

Die ICS Richtlinie des BSI (ICS-Kompendium) macht Vorgaben wie „Industrial Control Systems" abzusichern sind. Allerdings geht das BSI in keiner Weise auf die Implementierungsproblematik mit Index Range Violation, Buffer Overflow oder Stack Overflow und deren Absicherung ein. Ein Kompendium ohne Implementierungsvorgaben lässt daher eine sträfliche Lücke.

Die Politik glaubt, dass sie alle notwendigen Hintergründe weiß und entsprechende Projekte und Vorgaben machen kann. Leider scheint dies so nicht zu stimmen, die momentane Lage dürfte eher eine gewisse Ahnungslosigkeit von der realen Situation zeigen.

Die verschiedenen Institutionen und Gremien wie VDI, VDE ITG, ZVEI, usw. sind zwar aktiv, aber nicht gemeinsam und auch nicht koordiniert. Vieles wird parallel mit unterschiedlichen Interessen und Zielrichtungen verfolgt.

Die (Automatisierungs-) Industrie hat in ihrer Software immer noch Schwachstellen ohne Ende und eine Besserung ist nicht abzusehen, wie die permanenten Meldungen des US CERT bzw. ICS CERT zeigen.

Die Wissenschaft hat das Wissen um diese Problematik, aber wenig Ahnung von und Interesse an der Realität von konkreten Anwendungen. Leider ist dort immer noch das Ziel viele hochrangige Publikationen zu erzielen, um entsprechende Drittmittel akquirieren zu können. Dies ist dann eher einer Problem-Persistenz förderlich.

7. Resümee

Wenn PISEA, das hier vorgestellte Programme for International Science and Engineering Assessment, analog den PISEA-Studien auf den Erkenntnisstand und den Fortschritt im Bereich Cyber Security angewandt wird, so ist festzustellen, dass im Bereich „Science and Engineering" wenig „Lessons learned" für die reale Welt erkannt werden.

Forschungseinrichtungen sind massiv Drittmittel-orientiert und daher entweder an Publikationen oder am aktuellen Status der Industrie fixiert. Die Industrie will ihre aktuellen Produkte ohne weitere Aufwände verkaufen, bei neuen Produkten ist die „time to market"-Strategie und nicht die „design security"-Strategie vorrangig. Auch spielt das kaufmännische Denken mit der Preisorientierung eine zentrale Rolle und bestärkt damit die alte Software mit alten Schwächen. Neue Software verspricht nach aktuellen Daten von US CERT und der zu erwartenden neuen Norm von C und C++ keine Verbesserung. Ist das eine Ignoranz ohne Ende und wird nur ein Stempel im Sinne „zertifiziert, entspricht irgendeiner einer Norm" angestrebt?

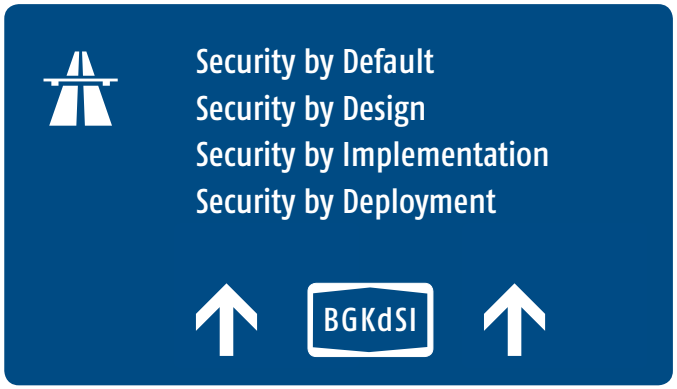
In vielen Bereichen scheint tatsächlich keine Wahrnehmung vorhanden zu sein, auf welche immanente Problemkomplexität wir zusteuern. Kritische Infrastrukturen, Verkehr der Zukunft mit Autonomen Fahrzeugen, Industrie 4.0, das Energiesystem der Zukunft mit virtuellen Kraftwerken und höchster Vernetzung, Home Automation, unsere gesamte Gesellschaft und Industrie funktionieren und leben mit automatisierungstechnischen und Software-basierten Funktionen (siehe [25]). Diese Funktionen sind zum gegenwärtigen Zeitpunkt keinesfalls als sicher und verlässlich einzustufen. Eine konstruktive Strategie um dieses Problem zu lösen ist noch nicht erkennbar, gleichwohl entsprechende Erkenntnisse vorliegen. Auch eine Qualitätsinfrastruktur, wie von DIN und anderen initiiert, stellt nur einen formalen Rahmen, aber keine inhaltliche Lösung dar.

Die Berliner Gesamtkonferenz der Sicherheitsinstitutionen (**BGKdSI**) versucht als transparente öffentliche Veranstaltung die hier vorgestellten Erkenntnisse zu Cyber Security in einem gesamten Sicher-

heitskontext mit Safety zu setzen und in eine reale Umsetzung zu bringen. Dazu müssen unabhängige Experten in einer unabhängigen Institution vereint werden, damit individuelle und einzelne institutionelle Sichtweisen koordinativ zusammengeführt werden und eine einheitliche, inhaltlich konstruktive Umsetzung erreicht wird. Möglicherweise ist die Gründung einer Dachorganisation wie eine **Deutsche Gesellschaft für Technik und Sicherheit** als gemeinsame Basis für alle existierenden Institutionen, Einrichtungen und Gremien zu etablieren.

Das Risiko ist eindeutig unterschätzt:
Konsequenzen in Cyber Security Kosten =
hohe Eintrittswahrscheinlichkeit **x** hoher Schaden **x** hohe Ignoranz **x** Unterschätzung der Angreifer

Die bisherige Vorgehensweise ist eindeutig wenig zielführend. Methodisch ist allerdings eine begründetet Basis vorhanden ((siehe [25]).



Einfügung des Herausgebers

Literaturreferenzen

(1) https://www.tecchannel.de/a/polen-teenager-hackt-strassenbahn-mit-fernbedienung,1744101, abgerufen am 10.02.2020

(2) https://www.theregister.co.uk/2008/01/11/tram_hack/, abgerufen am 10.02.2020

(3) Threat Landscape for Industrial Automation Systems in H2 2017 Kaspersky Lab ICS CERT, 2018. Bilder mit offizieller Genehmigung durch Olga Emel-yanova, Senior Editor, Kaspersky Lab, Olga.Emel-yanova@kaspersky.com, 39A/2 Leningradskoe shosse, Moscow, 125212, Russia, ics-cert.kaspersky.com.

(4) Elbez, G.; Keller, H. B.; Hagenmeyer, V.: A new classification of attacks against the cyber-physical security of smart grids. 2018. ARES 2018: International Conference on Availability, Reliability and Security, August 27–30, 2018, Hamburg, Germany, Art.-Nr. 63, ACME, New York (NY). doi:10.1145/3230833.3234689

(5) Cyber Security Assessment Netherlands - CSAN-4. National Cyber Security Centre, Turfmarkt 147 | 2511 DP The Hague, the Netherlands, PO Box 117 | 2501 CC The Hague, the Netherlands, T +31 (0)70 - 751 55 55 | F +31 (0)70 - 70 322 25 37, www.ncsc.nl | csbn@ncsc.nl, October 2014

(6) Future of Digital Economy and Society System Initiative, January 2017
Advancing Cyber Resilience Principles and Tools for Boards. In collaboration with The Boston Consulting Group and Hewlett Packard Enterprise

(7) Draft NISTIR 8276, Key Practices in Cyber Supply Chain Risk Management: Observations from Industry. National Institute of Standards and Technology Interagency or Internal Report 8276 31 pages (February 2021). This publication is available free of charge from: https://doi.org/10.6028/NIST.IR.8276.

(8) INTERNET ORGANISED CRIME THREAT ASSESSMENT (IOCTA) 2019, 09 October 2019, Europol, https://www.europol.europa.eu/sites/default/files/documents/iocta_2019.pdf, abgerufen am 10.02.2020

(9) "The Ominous Rise of 'Island Hopping' & Counter Incident Response Continues ", Carbon Black, 2019. Retrieved from: https://www.carbonblack.com/global-incident-response-threat-report/april-2019/.

(10) ENISA THREAT LANDSCAPE FOR 5G NETWORKS, November 2019. Threat assessment for the fifth generation of mobile telecommunications networks (5G)

(11) WEAPON SYSTEMS CYBERSECURITY, DOD Just Beginning to Grapple with Scale of Vulnerabilities, Report to the Committee on Armed Services, U.S. Senate, October 2018, GAO-19-128

(12) NIST - National Institute of Standards and Technology 2011, Source Code Security Analysis, Tool, Func-tional Specification Version 1.1"

(13) The Internet Has a Huge C/C++ Problem and Developers Don't Want to Deal With It. What do Heartbleed, WannaCry, and million dollar iPhone bugs have in common? by Alex Gaynor, Nov 15 2018, https://www.vice.com/en_us/contributor/alex-gaynor.

(14) Seacord. R. C. et al.: A Structured Approach to Classifying Security Vulnerabilities. TECHNICAL NOTE, CMU/SEI-2005-TN-003, January 2005

(15) Robert Seacord, ttps://www.securecoding.cert.org/confluence/display/seccode/Top+10+Secure+Coding+Practices, abgerufen am 10.02.2020

(16) John Barnes, Safe and Secure Software - An Invitation to Ada 2012

(17) Roderick Chapman & Yannick Moy, AdaCore Technologies for Cyber Security

(18) Orientierungsleitfaden für Hersteller zur IEC 62443, Herausgeber: ZVEI - Zentralverband Elektrotechnik und Elektronikindustrie e. V., Fachverband Automation, Lyoner Straße 9, 60528 Frankfurt am Main. Re-daktion: Lenkungskreis Automation Security, April 2017

(19) NAMUR Empfehlung NE 153: Automation Security 2020 – Anforderungen an Design, Implementierung und Betrieb künftigerindustrieller Automatisierungssysteme, NAMUR 2015.

(20) NISTIR Report 8219, Securing Manufacturing Industrial Control Systems: Behavioral Anomaly Detection

(21) Evgeny A. Smirnov*, Denis M. Timoshenko, Serge N. Andrianov: Comparison of Regularization Methods for ImageNet. Classification with Deep Convolutional Neural Networks. 2013 2nd AASRI Conference on Computational Intelligence and Bioinformatics

(22) Farbmuster MPI Tübingen, aus: Attacking Optical Flow. Anurag Ranjan, Joel Janai, Andreas Geiger, Michael J. Black (Max Planck Institute for Intelligent Systems bzw. University of Tübingen)

(23) Nguyen A, Yosinski J, Clune J. Deep Neural Networks are Easily Fooled: High Confidence Predictions for Unrecognizable Images. In Computer Vision and Pattern Recognition (CVPR '15), IEEE, 2015.

(24) Fachgruppe Ada, Gesellschaft für Informatik, https://www.safeware-engineering.org/site/assets/files/1134/pressemitteilung_der_gi_zur_stellungnahme_der_fg_ada.pdf. Abgerufen am 10.02.2020

(25) Keller, H. B.: Entwicklung von Echtzeitsystemen – Einführung in die Entwicklung zuverlässiger softwarebasierter Funktionen unter Echtzeitbedingungen. 2019. Springer Fachmedien Wiesbaden, Wiesbaden. doi:10.1007/978-3-658-26641-7

NUKLEARTECHNOLOGIE ALS VORREITER FÜR SICHERHEITSKONZEPTE

Holger Ludwig
Senior Adviser Nukleare Sicherheit
Framatom GmbH

1. Einleitung

Vorsorge ist besser als Nachsorge.

Zunächst wird auf die Sicherheitsprinzipien der „Väter" verwiesen, nämlich dass Prävention der Mitigation vorzuziehen ist, und dass Fehler in jedem Fall aufgefangen werden können müssen.Für die Sicherheitskonzepte bedeutet das, dass fehlerverzeihende Sicherheitskonzepte entwickelt werden müssen. In den fünfziger und sechziger Jahren des vorigen Jahrhunderts entstanden die Grundzüge dazu in den USA. In den siebziger und achtziger Jahren wurde dieses Sicherheitskonzept für die Kernkraftwerke in Deutschland mit einigen besonderen Ansätzen vertieft und vervollständigt. Das stellt sich wie nachstehend wiedergegeben dar:

Grundelemente des Sicherheitskonzeptes

Risikominimierung durch unverlierbare Eigenschaften.

Die Konstruktion des Reaktorkerns sieht vor, dass die Energieerzeugung durch die Kettenreaktion ein selbst stabilisierendes Verhalten aufweist

→ Inhärente Stabilität

Risikominimierung durch mehrere Barrieren.

Die Isolation der radioaktiven Stoffe gegenüber der Umwelt wird durch ein System von mehreren umschließenden Barrieren gewährleistet.

→ Barrierenkonzept

Diese Gewährleistung der ausreichenden Integrität und Funktion der Barrieren bei allen zu unterstellenden Zuständen und Ereignissen ist durch ein System gestaffelter Maßnahmen gegeben.

→ Konzept der Sicherheitsebenen

Risikominimierung durch systemische Sicherheitsebenen.

Die technischen Lösungen für Sicherheitseinrichtungen, die auch bei unterstellten Fehlern (technischem oder menschlichem Versagen) den Schutz durch Barrieren gewährleisten, wird durch die Auslegung sichergestellt

→ Auslegungsprinzipien für Sicherheitseinrichtungen

Eine im höchsten Maße **herausragende Rolle** spielt in dem Gesamtsystem das Barrierenkonzept. Es besteht aus fünf Teilen:.

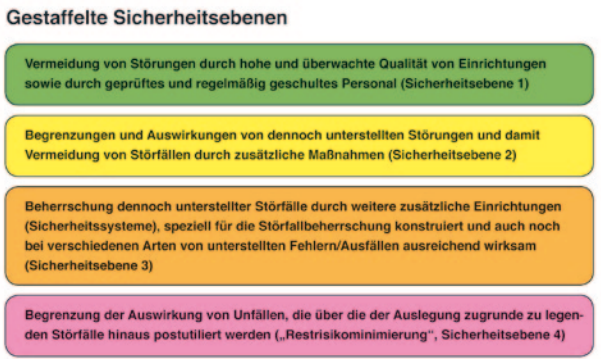
- der Brennstoffkeramik
- den Brennstabhüllrohre
- dem druckdichten Reaktorkühlsystem
- dem Sicherheitsbehälter
- den den Sicherheitsbehälter umgebende Stahlbetonstrukturen.

Wird die Zerstörung der ersten beiden Barrieren (Kristallgitter in der Keramik des Brennstoffs und Brennstabhüllrohre) verhindert, ist die Freisetzung von radioaktiven Stoffen in gefährlichem Umfang **physikalisch unmöglich**. Die Zerstörung der ersten beiden Barrieren ist nur möglich, wenn der Reaktorkern stark überhitzt wird. Solange der Reaktorkern mit Wasser bedeckt ist, also gekühlt ist, ist keinerlei Freisetzung von gefährdenden Mengen radioaktiver Stoffe in die Umgebung möglich.

Ein gestaffeltes Barrierensystem schützt zuverlässig.

Das Konzept der Sicherheitsebenen sorgt für einen sicheren Einschluss der radioaktiven Stoffe in sämtlichen Zuständen, angefangen vom Normalbetrieb, über den Wartungsbetrieb bis hin zu Brennstoffwechselbetrieb und Zwischenfälle sowie Unfällen.

Vom eigentlichen Reaktor gehen keine Gefahren aus.



Die Sicherheitskaskade

Inhärenz war in Tschernobyl nicht gegeben.

Die Notstromversorgung hätte oberhalb des KKW angeordnet sein müssen.

Ausfälle schon im Entstehen beherrschen.

2. Die Sicherheit der Kernkraftwerke in Deutschland / in der EU

Soweit es zu schweren Störfällen oder Unfällen in der Welt gekommen ist, war immer ein Abweichen von der Systematik bedeutsam, z.B. beim RBMK in Tschernobyl. Die Konstruktion des Reaktorkerns machte es möglich, dass es sich bei bestimmten Anlagenzuständen um kein selbststabilisierendes System mehr handelte. In Fukushima waren grundlegende Auslegungsfehler hinsichtlich der anzusetzenden Einwirkungen von Außen der eigentliche Grund für die Katastrophe. Fehlannahmen bei der Erdbeben- und Tsunamiauslegung führten zum nahezu gleichzeitigem Versagen von Sicherheitssystemen auf allen Sicherheitsebenen, das defence-in-depth- Prinzip konnte daher nicht zum Tragen kommen.
Wie eingangs erwähnt, sollen hier die besonderen Maßnahmen aus den sechziger und siebziger Jahren im einzelnen erläutert werden.

2.1 Die Maßnahmen im Einzelnen

Zusätzlich zu der Möglichkeit, Ausfälle auf der nächsten Sicherheitsebene auffangen zu können, sollten Ausfälle möglichst früh auf den jeweiligen gestaffelten Sicherheitsebenen vermieden oder hier beherrscht werden, d.h. wenn machbar Schäden **unmittelbar vermeiden, statt eingetretene Schäden erst auf der nächsten Stufe zu beherrschen.**

2.1.1 Ausschluss von Brüchen in Leitungen (Leck vor Bruch)

In den siebziger Jahren des vorigen Jahrhunderts waren Brüche in Rohrleitungen schon unwahrscheinlich, letztlich aber doch noch möglich. Es stellte sich die Frage, ob es durch weitere Forschungen möglich ist, einen Bruch- Ausschluss definitiv zu bestätigen.

Zusammengefasst kann das Ergebnis wie folgt beschrieben werden: Geeignete Materialien und qualifizierte Herstellungsverfahren sind

die Voraussetzung dafür,dass keine herstellungsbedingten Fehlstellen im Material vorliegen. In zähen Werkstoffen und bei niedriger Spannungsausnutzung sowie geringer Ermüdungsausnutzung ist sichergestellt, dass sich Risse nicht bilden oder allenfalls sehr langsam wachsen. Es schließt sich die Kontrolle der Randbedingungen im Betrieb an, gefolgt von regelmäßigen Überwachungsmaßnahmen. Somit ist die Bedingung „Leck vor Bruch" gegeben. Leckageüberwachung und regelmäßige Druckproben im kalten Betrieb vervollständigen das System, dass es zulässt, einen Bruch der Rohrleitungen auszuschließen.

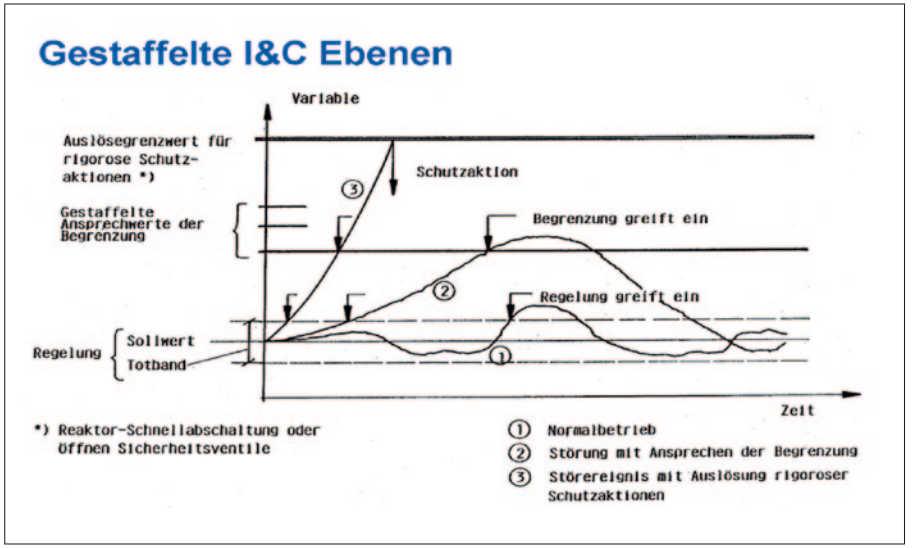
Die Erfahrungen in Deutschland bestätigten die Erwartungen an das System in vollem Umfang.

Materialforschung und -anwendung lassen mit Hilfe der Bruchmechanik Risse nicht mehr kritisch werden.

2.1.2 Weitere richtungweisende Entwicklungen

Nachstehend werden vier weitere Maßnahmen kurz genannt, die die Sicherheit in der betrieblichen Praxis der Kernkraftwerke erhöhen.

- Integritätskonzept für Dampferzeuger-Heizrohre
  Erfahrung: Kaum Leckagen, kein einziger Heizrohrbruch. etliche Dampferzeuger
  KWU-Konzept als Ersatz in Anlagen andere Hersteller eingebaut
- Leistungsreduktion/Abschaltung des Reaktors
  Ergebnis: Besonders zuverlässige Leistungsreduktion bei Anforderung
- Energieversorgung der Sicherheitssysteme bei Verlust der Verbundnetzanbindung
  Ergebnis: Ausfall der Drehstromversorgung der Sicherheitssysteme unwahrscheinlicher als bei anderen Anlagen
- Schutz und Optimierung von Sicherheitssystemen
  Vergleichsweise weitgehende Trennung von betrieblichen Systemen und Sicherheitssystemen entsprechend dem Konzept der gestaffelten Maßnahmen



Reaktorversagen wird technisch ausgeschlossen.

2.1.3 Weitere Auslegungsprinzipien

- Redundanzprinzip (Schutz gegen Einzelfehler)
- Diversitätsprinzip (Schutz gegen systematische Fehler und GVA)
- Automatisierung (Schutz gegen Fehlhandlungen)
- Wiederkehrende Prüfungen, Selbstüberwachung (Schutz gegen unerkannte Ausfälle und Fehler

3. Kritik an der Aufsicht und Ausblick

Seit Jahren wird das konsequente Bemühen, im gestaffelten Sicherheitskonzept Ausfälle möglichst früh zu vermeiden oder auffangen, in der staatlichen Atomaufsicht nicht richtig gewürdigt, wie folgende Beispiele zeigen.

Wo kein Wille ist, ist auch kein Weg!

Wir feilschen über Details in Nachweisen für ATWS (Ereignisse mit unterstellten Versagen des Schnellabschaltsystems), 2F-LOCA (Komplettabriss der Hauptkühlmittelleitung) oder StationBlackout, obwohl diese Ereignisse aufgrund der besonderen Vorsorgemaßnah-

men in Deutschland weit in der Sicherheitsebene 4 anzusiedeln, also nach „dem Maßstab der praktischen Vernunft“ auszuschließen sind, statt den Blick dort zu fokussieren, wo es nach probabilistischen und deterministischen Sicherheitsanalysen bedeutsamer wäre. Grund:

„International“ mache man das so (wobei die Unterschiede in der Vorbeugung nicht beachtet werden). Wir kumulieren Vorschriften für das Personal und drohen mit dem Staatsanwalt, statt uns um die Beseitigung des Unwesentlichen und damit um den – so wesentlichen –„Kavitationsschutz“ des Anlagenpersonals zu kümmern.

Im Land des Kalkar-Urteils verlässt man den eigenen Maßstab!

Das Prinzip „Vorbeugen – wo machbar – ist besser als aufräumen“ hat sich bewährt, wie der Rückblick bestätigt. Die Entwicklungen in dieser Richtung haben zur hohen Zuverlässigkeit der deutschen KKW beigetragen und damit

- zur im internationalen Vergleich hohen Verfügbarkeit und
- zu der Basis für ein hohes Sicherheitsniveau

Das Prinzip ist auch heute noch richtig und wegweisend!

Ein bewährtes Prinzip wird ohne Not missachtet.

SICHERHEIT IM STIHL-AKKU-SYSTEM
LEITGEDANKEN AUS DER ENTWICKLUNG

Dr. Holger Lochmann

1. Einleitung

Die ganz wesentlich in der Kernindustrie entwickelten Sicherheitselemente finden sich auch in anspruchsvollen Bauteilen, Baugruppen und Systemen im konventionellen Bereich. Es finden sich auch hier die Prinzipien der inhärenten Sicherheit, der Redundanz einschließlich in besonderen Fällen der diversifizierten Redundanz, des Human Factor Engineering, der passiven Sicherheit wie auch der funktionalen Sicherheit zusammengefasst in Managementsystemen.

Sicherheitsprinzipien anwenden – Vertrauen aufbauen.

Am Beispiel des Akku-Systems der Firma STIHL wird das nachfolgend dargestellt.

2. Das gestaffelte System

Im Kern des Systems befindet sich der Akku bzw. die Akku-Zelle, die inhärent sicher ist. Diese Sicherheit wird validiert gegen elektrische und mechanische Beanspruchungen aller Art.

Unverlierbare Eigenschaften.

Die aktive Sicherheit des Systems wird durch ein Batteriemanagement gesteuert, dass das Laden und Entladen von Batteriezellen parametrisiert und einschließlich Potenzialüberwachung und Temperaturmanagement überwacht und steuert.

Sicherheitsmanagementsysteme nutzen, Komplexität beherrschen.

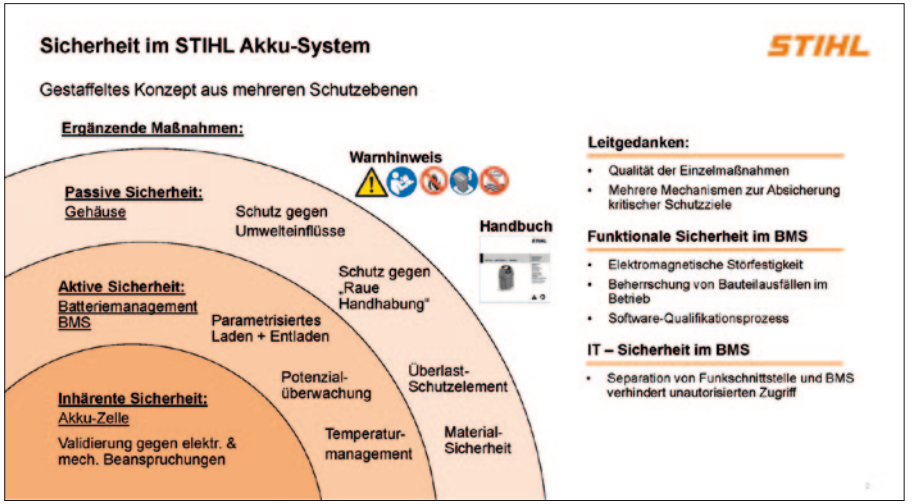
Die inhärente sowie die aktive Sicherheit werden noch ergänzt durch passive Elemente, die überwiegend den Schutz gegen Umwelteinflüsse und gegen „raue Behandlung“ abdecken. Zu diesem Bereich gehört auch noch ein Überlast-Schutzelement.

Passive Sicherheit immer gezielt einsetzen.

In allen Bereichen, also der inhärenten, der aktiven und der passiven Sicherheit werden nur Materialien eingesetzt, die ähnlich wie in der Kernindustrie Eigenschaften aufweisen, die Schäden von vornherein praktisch ausschließen.

Nachstehend ist dieser Zusammenhang in einem Bild dargestellt.

Materialforschung und Bruchmechanik ermöglichen den sicheren Ausschluss spezifischer Materialschädigungen.



Überbeanspruchungen können aufgefangen werden.

Zusammenfassend kann festgestellt werden, dass durch die Leitgedanken Qualität der Einzelmaßnahmen und mehrere Mechanismen zur Absicherung kritischer Schutzziele robuste Konstruktionen möglich werden. Die Funktionale Sicherheit wird durch elektromagnetische Störfestigkeit, Beherrschung von Bauteilausfällen im Betrieb und Software-Qualifikationsprozesse gewährleistet. Im IT-Bereich wird ein unautorisierten Zugriff durch eine getrennte Funkschnittstelle und das Batteriemanagementsystem gewährleistet.

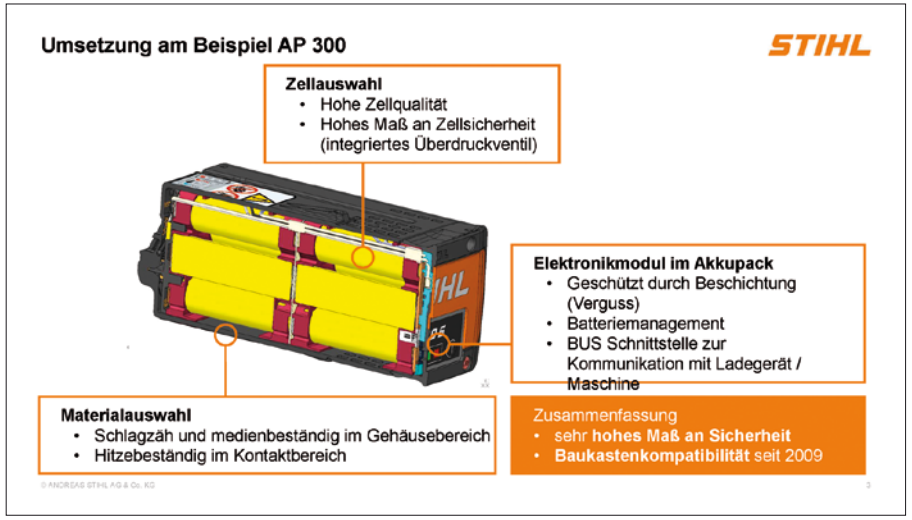
.

3. Ein Beispiel

Die Umsetzung am Beispiel AP 300 zeigt deutlich, dass die verschiedenen Elemente des Sicherheitssystems zu einem Bauteil führen, dass Alltagsbelastung garantiert aushält. Durch die gestaffelte Sicherheit ist auch gewährleistet, dass Überbeanspruchungen kaskadenartig abgefangen werden können.

4. Resümee

Bauteile und Geräte in der konventionellen Technik haben in punkto Sicherheitselemente von den Entwicklungen in der Kern-



Aufbau eines Akkus

industrie profitieren können. Auch hinsichtlich Verlässlichkeit und Wiederanlauf nach Störungen werden in gleichem Maße auch in diesem Bereich der Technik Standard.

Eine Rahmenrichtlinie zur Generierung und zumal von Sicherheit in allen Bereichen der Technik kann auf die Erfahrungen aus mehreren Fachbereichen aufbauen und sollte in Angriff genommen werden.

Zukünftig muss es eine Gesamtschau über alle Fachgebiete geben.

ARBEITEN 4.0

Armin Knopf
VBG Berlin

1. Einleitung

Die zurzeit wichtigsten Entwicklungen stellen sich wie folgt dar: Neue Technologien ziehen in das Arbeitsleben ein, deutliche Flexibilisierungen treten auf und nehmen auch noch zu, zusätzliche Anforderungen an die Führung stellen sich und neue Beschäftigungsformen ergänzen die bisherigen.

Welche Auswirkungen haben diese eingetretenen und sich verstärkenden Entwicklungen auf die Generierung der Sicherheit und ihren Erhalt?

Die Digitalisierung dringt in alle Lebensbereiche ein.

2. Die Entwicklungen im Detail

2.1 Neue Technologien

Zunächst sind die weitreichenden Technologien zu benennen, nämlich die durchgreifende allgemeine Digitalisierung und damit auch weltumspannende Informations- und Kommunikationstechnik. Dazu gehören selbstorganisierende Produktionssysteme – Stichwort Industrie 4.0 – Augmented Reality, kollaborierende Roboter, Wearables und Ambient Intelligence. Das Ganze fügt sich in die grundlegenden Veränderungen von Arbeit und bedingt sie andererseits. Datenbrillen in Lagersystemen erleichtern die Zuordnung und Exoskelette unterstützen die normale Körperkraft.

Und die Zukunft klopft auch schon an die Tür, nämlich die selbstfahrenden Autos. Mobiles und flexibles Arbeiten wird mithilfe der neuen Technologien einfach ermöglicht. Das bedeutet aber, dass der Mensch nur unterstützt und nicht ersetzt wird, was beim Planungs- und Entwicklungsprozess berücksichtigt werden muss. Sicherheit und Gesundheit der handelnden Menschen müssen im Vordergrund bleiben, insbesondere bei einem flexiblen Mitarbeitereinsatz (Arbeit auf Abruf).

Im digitalen Zwilling muss genauso Ordnung herrschen wie im Analogen.

2.2 Flexibilisierungen

Überall und jederzeit **kann** gearbeitet werden.

Muss das auch so sein?

Das wirklich neue an der Flexibilisierung liegt auf der Betonung, dass wirklich überall gearbeitet werden kann. Natürlich bezieht sich das nicht auf sämtliche Berufe, sondern nur auf die, die im Wesentlichen ein mobiles Endgerät (Laptop o.Ä.) für die Erfüllung der Aufgaben benötigen. Zu dem Begriff „überall" gesellt sich der Begriff „jederzeit". Und damit beginnen die Probleme hinsichtlich der Gesundheit und der Sicherheit. Wie sieht es mit den Arbeitszeiten aus? Wie sieht es mit den Erholungszeiten aus? Ist jederzeit Erreichbarkeit wirklich nötig? Wird es noch eine verlässliche Work-Life-Balance geben?

Die gestiegenen Handlungs- und Entscheidungsspielräume der Erwerbstätigen sind positiv zu werten, wie auch die räumliche Mobilität. Die Identifikationsmöglichkeit mit der Aufgabe ist sicher auch positiv zu werten. Die Probleme liegen eher bei der Vereinbarkeit von Arbeit und Privatleben, der möglichen Selbstausbeutung und ergonomische Probleme am Arbeitsplatz, Beispiel Berichtsabfassung im Hotel. So ist grundsätzlich langes Arbeiten mit einem Endgerät auf dem Schoß nicht empfehlenswert.

Chancen und Risiken ausbalancieren!

2.3 Anforderungen an die Führung

Die Aufgaben und Anforderungen an die Vorgesetzten ändern sich, es wird mehr indirekte Steuerung und Führung durch Kennzahlen und Ziele geben. Die Kommunikation wird sich zunehmend virtuell abspielen und damit eine Führung auf Distanz Platz greifen. So kann zum Beispiel eine Konstruktionsaufgabe in viel kürzerer Zeit erledigt werden, wenn man die erledigte Teilaufgabe am Abend einem anderen Team auf der Welt zuleitet, dass dann an der Fortsetzung wirkt. Wer ist der fachliche Ansprechpartner? Wer ist der Vorgesetzte?

Führungsmethoden anpassen, entwickeln und ausprobieren.

Man muss auch in diesem Bereich sehr deutlich einerseits die Chancen sehen und andererseits die Augen nicht vor den Risiken verschließen. Motivation und Arbeitszufriedenheit sowie Stolz können bei erfolgreichen Arbeiten durchaus wachsen, was aber eine positive Auseinandersetzung mit einer neuen Führungskultur voraussetzt.

Führungskultur setzt Zustimmung voraus.

2.4 Beschäftigungsformen in der Entwicklung

Die neuen Beschäftigungsformen sind ganz wesentlich kritisch zu betrachten. Der hohe Gewinn auf der Habenseite muss nachhaltig gespiegelt werden in durchsetzbaren Anforderungen an diese Beschäftigungsformen heute und in der Zukunft. Pflichten und vor allem die Rechte der Mitarbeiter müssen analog zu den heutigen Tarifverträgen in entsprechenden Verträgen niedergelegt werden, sodass Gelegenheitsbeschäftigung, Teilzeit, Zeitarbeit, Werkverträge und fehlende soziale Einbindung in adäquater Weise erfasst werden. Damit muss unter anderem sichergestellt werden, dass Scheinselbstständigkeit, prekäre Arbeitsbedingungen und die Aushebelung gesetzlicher Regelungen sicher vermieden werden.

Im digitalen Zwilling müssen die Rechte wie auch sonst üblich ausgehandelt werden.

3. Chancen und Risiken der Entwicklungen

Den Chancen der Entwicklung stehen entsprechende Risiken gegenüber, es handelt sich stets um eine Abwägung. So wird einerseits die Vereinbarkeit von Beruf und Familie deutlich verbessert, wie auf der anderen Seite die Gefahr der Selbstausbeutung besteht. Dies hängt ganz wesentlich von der Einstellung des Arbeitnehmers und von der Führung durch den Vorgesetzten ab. Der deutlich gestiegene Handlungs- und Entscheidungsspielraum der einzelnen Mitarbeiter kann Positives bewirken, vorausgesetzt, der Mitarbeiter ist zur Selbstorganisation unterwiesen und befähigt worden.

Eine Entwicklung ist angestoßen, es liegt an uns, ob sie positiv verlaufen wird.

4. Resümee

Eine umfassende Transformation der Gesellschaft ist in vollem Gange und sicher nicht aufhaltbar und schon gar nicht zurückführbar. Es kann also nur heißen, den Vorgang der Transformation von Anfang an, laufend und bis zum Schluss positiv zu moderieren – durch Politik und gesellschaftliche Kräfte. Dabei gilt selbstverständlich, dass die entstehenden Chancen verstärkt werden und die sich einstellenden Risiken verringert werden müssen. Antworten auf die zentralen Fragen der Arbeitsgestaltung müssen gefunden werden! Vielleicht ist es sinnvoll, eine Taskforce in der Administration unter Beteiligung aller gesellschaftlicher Kräfte einzusetzen.

Die Transformation wird moderiert. Reicht das nicht, muss geführt werden.

Ebenso müssen Erfolg versprechende Kommunikationskanäle der Ansprache für die Zukunft gefunden werden. Praxisbezogene Aus- und Weiterbildungskonzepte müssen entwickelt werden, die auch das Fachwissen von älteren Beschäftigten einbeziehen. Es ist eine Herausforderung und Aufgabe der gesetzlichen Unfallversicherung, Präventionskonzepte so weiter zu entwickeln, dass diese in einer digitalen, hoch technisierten und flexiblen Arbeitswelt wirksam werden.

Sämtliche Kommunikationsmöglichkeiten müssen ausgeschöpft werden.

FORTSETZUNG VON THEMEN DER BGKDSI

1. Weltkongress der Sicherheit

Die Konferenzleitung hat im Auftrag der BGKdSI Herrn Dipl. Wirtsch.-Ing. Ralph Appel, Direktor und geschäftsführendes Präsidiumsmitglied des VDI (Verein Deutscher Ingenieure e.V.), Geschäftsführer VDI GmbH, in einem Brief angetragen, dass zur Planung eines nächsten „Weltkongresses der Sicherheit" der VDI die Federführung übernehmen und in Kooperation mit weiteren Stakeholdern dessen Durchführung veranlassen möge. Gleiches Schreiben ging an den Präsidenten des VDI; telefonisch wurde auf Nachfrage mitgeteilt, dass der VDI andere Prioritäten setze.

2. Karte der Sicherheitslandschaft

Die Konferenz betrachtet die Erstellung einer Landkarte der Sicherheitsinstitutionen als laufende Aufgabe und erwartet bei nächster Gelegenheit die Vorstellung aus Österreich, das über eine solche Landkarte verfügt. Herr Dr. Ralph Hammer (Bundesministerium für Landwirtschaft, Regionen und Tourismus, Sektion IV – Telekommunikation, Post und Bergbau Stabstelle f. Sicherheitsforschung und Technologietransfer) ist grundsätzlich bereit, die Konferenz zu informieren; gegebenenfalls kann über eine Erweiterung bis hin zu einer D-A-CH- Landkarte diskutiert werden

3. Finanzierung der Berliner Gesamtkonferenz der Sicherheitsinstitutionen.

Die Konferenz wird von allen Akteuren geschätzt; ihre Fortsetzung etwa alle Jahre ist gewünscht und nötig. Mit einem gemeinsamen Zielverständnis kann so auch die Basis für ein konstruktives Element in Europa geschaffen werden. Statt unterschiedlicher Sicherheitsansätze muss auf eine einheitliche Vorgehensweise hingewirkt werden.

Anlässlich der nächsten Konferenz soll versucht werden, Vertreter von Institutionen mit finanziellen Entscheidungsbefugnissen einzuladen. Für die Zwischenzeit gilt das nachstehende Wort von Herrn Professor Dr. Banse:

Fortführung der BGKdSI als Initiative mit direkter finanzieller Unterstützung beteiligter Institutionen und bis auf Weiteres nach wie vor die Beauftragung des Forum46 e.V. zur Organisation und Dokumentation.

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

Die BGKdSI auf einen Blick

Die BGKdSI widmet sich den dringenden Fragen zu Chancen und Risiken der Technik mit Bezug zu den Wechselwirkungen von technischen und gesellschaftlichen Entwicklungen. Sie leistet damit einen Beitrag zu den Grundlagen unseres Miteinanders in der Zukunft vor dem Hintergrund des Innovationsklimas.

Der Anspruch des BGKdSI

Wir brauchen eine stärkere Vernetzung aller Institutionen in den Bereichen Technik, Wirtschaft, organisiertes Gemeinwesen und Administration um konstruktiv-kritisch in den politischen Raum hinein zu wirken. Eine allgemein etablierte und anerkannte Kultur der Sicherheit mit umfassenden und klaren Konzepten schützt und stärkt das Wertschöpfungspotenzial der Volkswirtschaft.

Der Fokus des BGKdSI

Ein wesentlicher Schwerpunkt ist die Sensibilisierung für die volkswirtschaftliche Dimension der Sicherheit. Dabei geht es auch um eine sachliche, fundierte Einschätzung von Risiken. Der Fokus liegt vor allem auf mittelständischen wertschöpfenden Strukturen sowie Kritischen Infrastrukturen (Kritis) unter Berücksichtigung der Wechselwirkungen von Mensch, Organisation und Technik im Kontext der Sicherheit „by Design"/„by Default".

Die Motivation der Akteure und Unterstützer der BGKdSI

Aus der BGKdSI heraus werden gegenüber Gesellschaft, Politik, Wirtschaft und Wissenschaft Impulse gesetzt. Es wird ein konstruktiv-kritischer, offener Austausch über Fachbereichsgrenzen hinweg gepflegt: Grundlage des Gedankenaustauschs ist die „Chatham House Rule". Der Wunsch, einander kennenzulernen und voneinander zu lernen, hat sich als eine bedeutende Motivation der Akteure herausgestellt.