Berliner Gesamtkonferenz der Sicherheitsinstitutionen

- Eine europäische Richtlinie zur Generierung von Sicherheit
- CyberSecurity – Bewertung und Handlungsstrategien
- Dutch Safety Board und Chemical Safety Board (USA)
- Risk assement as management task
- Industrie 4.0 zwischen Idee und Realität. Ein Ländervergleich
- Weltkongress der Sicherheit
- Erstellung einer Sicherheitslandkarte

FORUM TECHNOLOGIE & GESELLSCHAFT

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

BDI
Bundesverband der Deutschen Industrie e.V.

Förderverein Ada Deutschland e. V.

DEKRA
On the safe side.

Die Veranstaltung wurde ermöglicht durch die freundliche Unterstützung des Bundesverbandes der Deutschen Industrie e.V., des Fördervereins Ada Deutschland e.V. und der DEKRA

INHALT

GRUSS-ADRESSEN

Dipl.-Ing. Dirk Pinnow

Dr. Holtmann

Dr. Langenbach

Einleitung

Für die BGKdSI-Konferenzleitung begrüßte Dirk Pinnow die Anwesenden und dankte dem BDI, vertreten durch die Herren Dr. Holtmann und Wittenbrink für die **Unterstützung**.

Herr Dr. Holtmann betonte in seinem Grußwort, dass Sicherheit für den BDI als Spitzenorganisation der deutschen Industrie und industrienahen Dienstleister **von zentraler Bedeutung** sei, welche alle Bereiche erfasse. Er führte aus, dass der Erfolg der deutschen Volkswirtschaft auf einer komplexen Struktur industrieller Wertschöpfungsketten basiert, welche mehr als 100.000 große, mittlere und kleinere Unternehmen umfasst. Der BDI repräsentiert demnach mit seinen Mitgliedsunternehmen mehr als acht Millionen Arbeitnehmer. Er stellte kurz die Abteilung Umwelt, Technik und Nachhaltigkeit vor und benannte beispielsweise mehrere BDI-Arbeitskreise/-gruppen, welche sich mit **sicherheitsrelevanten Themen** befassen (AK Technikpolitik, AK Betriebssicherheit BDI/BDA, AK Arbeitsstoffe, AK Brandschutz, AHG Novelle Gefahrstoffverordnung, AHG NLF Cybersecurity, AK Cybersicherheit und Wirtschaftsschutz der Abteilung Digitalisierung sowie Datenschutz der Abteilung Recht).

Der BDI vertritt mehr als 100.000 Mitgliedsfirmen und damit mehr als 8.000.000 Arbeitnehmer.

Er gab den Hinweis, dass nach Stand vom Mai 2019 die **BDI-Broschüre zum Recht des technischen Arbeitsschutzes in neuer Auflage** erschienen ist – die enthaltenen Änderungen beträfen insbesondere die Aufhebung der 7. und 8. Produktsicherheitsverordnung. Innerhalb des BDI werde derzeit eine Positionierung diskutiert, um die Cyber-Sicherheit technischer Produkte mittels einer **konsistenten Regulierung auf EU-Ebene** zu regeln. Die Industrie sei sich der vielfältigen Gefahren für die Sicherheit von Institutionen (security) und Personen (safety) bewusst, welche sich aus der zunehmenden Anzahl und Vernetzung technischer Produkte ergeben. Insbesondere die Cyber-Sicherheit sei ein **„permanenter Prozess über den gesamten Produktlebenszyklus“** und bedür-

Die Cybersicherheit technischer Produkte steht im Focus der Aufmerksamkeit mit Blick auf EU-Regulierungen.

fe der ständigen Anstrengung von Herstellern, Integratoren, Betreibern und Privatanwendern. In diesem Zusammenhang spielten die Prinzipien **„security-by-design"** und **„security-by-default"** sowohl für den sogenannten B2C-, als auch den B2B-Bereich eine entscheidende Rolle. Ergebnisoffen diskutiert werde derzeit, inwiefern der **EU Cyber-Security Act** (CSA) eine ausreichende Lösung darstellt, ob der CSA um weitere Elemente des New Legislative Frameworks (NLF) erweitert werden sollte – oder inwiefern es zusätzlich eines Ansatzes zur Festschreibung von grundlegenden Cyber-Sicherheitsanforderungen jeweils in den bestehenden NLF-Verordnungen und -Richtlinien bedarf. Die langfristige Einführung einer „horizontalen Phänomenrichtlinie" für Cyber-Sicherheit werde indes nicht weiter verfolgt.

Der Cyber-Security Act wird augenblicklich noch ergebnisoffen diskutiert.

Herr Dr. Langenbach begrüßte die Teilnehmer für das DLR. Er dankte dem BDI als Gastgeber und führte aus, dass das DLR e.V. zwar „das Forschungszentrum der Bundesrepublik Deutschland für Luft- und Raumfahrt" sei – neben den beiden „großen" Buchstaben im Kürzel (L und R) forsche es aber auch zu „E" wie Energie und „V" wie Verkehr (s. e.V.). In Ergänzung dieser Forschungsschwerpunkte werde auch an den eben gerade für Luftfahrt, Raumfahrt, Energie und Verkehr zentralen Querschnittsthemen **Sicherheit und Digitalisierung** gearbeitet. Im Auftrag der Bundesregierung sei das DLR Raumfahrtmanagement für Planung und Umsetzung der deutschen und europäischen Raumfahrtaktivitäten zuständig, zudem fungiere es als Dachorganisation für einen der größten Projektträger Deutschlands.

Die Sicherheitskultur in der Luftfahrt ist Vorbild für andere Bereiche.

Die DLR-Forschung werde derzeit mit knapp **8.100 Mitarbeitern an 20 Standorten in Deutschland** betrieben – im Geschäftsjahr 2017 habe der Etat für Forschung und Betrieb rund eine Milliarde Euro betragen (ohne das verwaltete Raumfahrtbudget und die Fördermittel der Projektträger). „Das DLR war einer der Initiatoren der

Generierung von Sicherheit mit dem Direttissima-Ansatz

BGKdSI, nicht nur weil unser Portfolio von Technologien für Energieversorgung, Mobilität, Kommunikation bis hin zur Sicherheit reicht, sondern auch wegen der Erweiterung um unseren neuen **Querschnittsbereich Digitalisierung"**, erläuterte Dr. Langenbach. Dieser solle insbesondere zu den folgenden Themen signifikante Beiträge leisten: Digitalisierung in der Wirtschaft, Big and Smart Data / Data Science, Cyber-Sicherheit und Intelligente Mobilität. Schließlich wünscht er den versammelten Akteuren „interessante Vorträge, fruchtbare Diskussionen und viele anregende Gespräche".

EINE EUROPÄISCHE RICHTLINIE ZUR GENERIERUNG VON SICHERHEIT

Dr. Christian Langenbach

Die Optimierung der Flugzeuge erfolgt heute über Senkung des Treibstoffverbrauchs und die Nutzung faserverstärkter Werkstoffe.

Der äußere und innere Strukturaufbau moderner Verkehrsflugzeuge ist über die Zeit im Prinzip gleichgeblieben. So ähneln sich die Muster der Hersteller mehr und mehr, wie z.B. der Airbus A350 und als Pendant die Boeing 787 („Dreamliner"). Die Stellschrauben für die Optimierung moderner Flugzeuge, wie Treibstoffverbrauch oder der Einsatz von faserverstärkten Werkstoff, um das Gesamtgewicht noch deutlich zu verringern, sind für den normalen Betrachter versteckt.

Der Planungsprozess muss die robuste Ausgangsphase verwirklichen.

Zur Ausprägung einer expliziten Sicherheitskultur ist ein positiver Umgang mit Fehlern sowie die Fähigkeit, aus Erfolgen wie eben auch aus Fehlern zu lernen, erforderlich.Hierbei könnte die Luftfahrt den Vorreiter geben und dieses Vorgehen auch in andere Bereiche zu übertragen helfen.

Zur Generierung von Sicherheit empfiehlt sich der sogenannte „Direttissima-Ansatz": Einer „robusten Beurteilung der Ausgangslage" schließt sich hierbei das „Erkennen der künftigen Herausforderungen" an und führt zum „Setzen der richtigen Prioritäten". Vor dem Hintergrund des Produktlebenszyklus ist Technische Sicherheit durchgehend von der Konzeption bis hin zur Entsorgung permanent vorzusehen (s. Abb. 1).

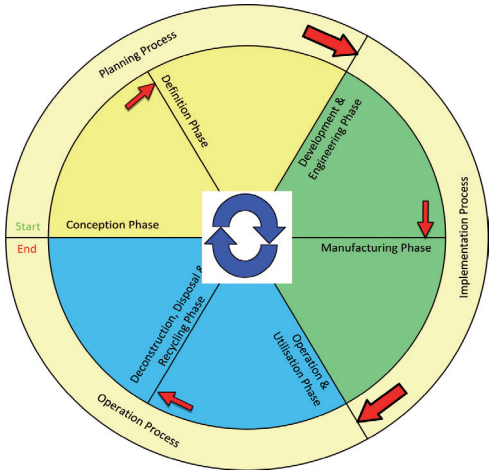


Abb. 1: Generierung Technischer Sicherheit von der Konzeption bis zur Entsorgung (Quelle: „Technical Safety – An Attribute of Quality", ISBN 978 3-319-68624-0).

Im Planungsprozess mit seinen beiden Elementen Konzeption und Definiton steht die robuste Beurteilung der Ausgangslage im Vordergrund. Die sicherheitsmethodische Vorgehensweise ist dabei zu abstrahieren und in Einzelkriterien darzustellen. Da es weder möglich, noch überhaupt ratsam ist, eine Sicherheitsmethodik ausschließlich und spezifisch für eine bestimmte Technologie zu schaffen. Die erarbeiteten Kriterien erlangen Allgemeingültigkeit in dem Sinne, dass sie für jedes Fachgebiet und jede Technologie gleichermaßen anwendbar werden. Diese allgemeine Gültigkeit bietet für die Anwendung folgende Vorteile:

Es muss gelingen, eine fachgebietsübergreifende Regelung zu schaffen.

- Die begutachtenden Tätigkeiten aufsichtführender Institutionen können während der Entwicklung nach den gleichen Kriterien und dem gleichen Handlungsschema erfolgen wie die technische Auslegung.
- Bei einheitlicher Einführung ermöglichen eine fachgebietsunabhängige und eine Kommunikation frei von Missverständnis zwischen den verschiedenen Fachgebieten. Letzteres ist besonders bei der Realisierung neuartiger Technologien unverzichtbar.

Ein Handlungsschema für sämtliche Fachgebiete

Im daran anschließenden Realisierungsprozess sollten die künftigen Herausforderungen zu erkennen sein. Der Projektstrukturplan muss Zuständigkeiten und Verantwortlichkeiten festlegen. Dabei sind " für jedes Element des Projektstrukturplans nach dem Qualitätsmerkmals „technische Sicherheit definiert werden. Das Umfasst ebenfalls die Erstellung, Abstimmung und Freigabe der Rahmenspezifikationen und das in Kraft setzen eines entsprechendes Konfigurationsmanagement. Idealerweise sollten bereits in dieser Prozessphase alle beteiligten Stellen und die aufsichtführenden Institutionen von Beginn an eigebunden sein.

Im Realisierungsprozess (Entwicklung und Konstruktion sowie Herstellung) muss das Qualitätsmerkmal „Technische Sicherheit“ Priorität haben.

Im Betriebsprozess, der auch den Rückbau und Entsorgung umfasst, stehen für das Sicherheitsmanagement bewährte Managementwerkzeuge zur Verfügung:

- Sicherheitsorganisation, geführt durch „Systemarchitekten“
- Critical Items List (Safety Hazard List)
- Risikomanagement (anhand einer Risk Management List)
- Reporting (öffentliche Sicherheit)
- regelmäßig angesetzte Sicherheitsreviews zu Konzipierung, Definition, Entwicklung, Bau und Nachweisführung (technische Qualifikation, technische Abnahme)

Eine europäische Richtlinie „Technische Sicherheit“ gibt das Handlungsschema für sämtliche Fachgebiete vor.

Eine so hergeleitete allgemeine Sicherheitsmethodik muss mit einer interdisziplinären Verständigung über die Begrifflichkeit einhergehen. Zur ingenieursmäßigen „Erzeugung von Sicherheit“ gilt es, alle Beteiligten einzubinden. Die Etablierung einer europäischen Richtlinie „Technische Sicherheit“ ist also sinnvoll. Sie ist gleichsam das „fehlende Puzzleteil“ bzw. der „Schlussstein“, um das metaphorische „Haus der Sicherheit“ zu komplettieren (s. Abb. 2).

Abb.2: Das Haus der Sicherheit (Quelle: nach klunke-coaching.de; © Europäische Union, 1995-2019)

Herr Törkel kommentierte, dass die Luftfahrt ein gutes Beispiel für einen holistischen Sicherheitsansatz sei – Safety und Security sollten von Deutschland zum Schwerpunkt der EU-Ratspräsidentschaft 2020 gemacht werden.

Herr Barz bestärkte Dr. Langenbachs Konklusion, dass nur noch ein Puzzleteil fehle, um das „Haus der Sicherheit" – im europäischen Rechtsrahmen – fertigzubauen. Herr Kalenberg bekundete Interesse an einer konkreten Umsetzungs-Idee.

CYBERSECURITY – BEWERTUNG UND HANDLUNGSSTRATEGIEN

Dr. Hubert B. Keller

Einführung

Im Safety Bereich gibt es anerkannte Risikobewertungsverfahren. Im Security Bereich stehen wir erst am Anfang. Die große Frage ist, wie wird das Cyber Security Risiko berechenbar gemacht und bewertet. Hierzu wird am Beispiel des Dokuments "Classification Method and Key Measures - Cybersecurity for Industrial Control Systems" der ANSSI (siehe Literaturverweis am Ende) eine Vorgehensweise erläutert.

Wie bewerten wir das Risiko im Bereich der Cyber Security?

Grundlagen

Für eine Kritikalitätseinstufung bzw. Risikobewertung werden einige grundlegende Feststellungen getroffen. Bei den Industrial Control Systems (ICS) wird im Ansatz der French Network and Information Security Agency (ANSSI) in folgende Klassen von Systemen unterschieden:

- Class 1: Auswirkung oder Wahrscheinlichkeit (Risiko) eines Angriffs ist niedrig
- Class 2: Auswirkung oder Wahrscheinlichkeit (Risiko) eines Angriffs ist merklich
- Class 3: Auswirkung oder Wahrscheinlichkeit (Risiko) eines Angriffs ist kritisch.

Einteilung in Risikoklassen

Die Einstufung bezieht sich dabei nicht auf das Unternehmen oder eine Einzelperson, sondern auf die Auswirkungen auf den gesamten Staat.

Die Ergebnisse der Risikobetrachtung beziehen sich auf Gesellschaft / Staat.

Weiterhin werden grundlegende Anforderungen definiert:

- Es ist eine Kette von Verantwortlichkeiten für alle ICS zu definieren.
- Eine Risikoanalyse ist durchzuführen. Bei Class 3 hat diese jährlich mit einem Zertifizierer zu erfolgen.

Die Teilaufgaben werden gemäß Risikoklassen definiert.

- Es hat eine Inventarisierung zu erfolgen in der logisch, physikalisch und Anwendungsorientiert alle Komponenten erfasst werden. Bei Class 2 erfolgt dies regelmäßig, zumindest bei Änderungen. Bei Class 3 erfolgt dies regelmäßig, aber mindestens einmal pro Jahr.
- Ein Anwendertraining mit einer Zertifizierung hat zu erfolgen. Bei Class 3 ist ein zertifizierter Anbieter zu verwenden.
- Es sind Audits (Prüfungen) durchzuführen. Bei Class 1 kann dies intern erfolgen, bei Class 2 extern. Bei Class 3 erfolgt dies mindestens einmal pro Jahr durch unabhängige zertifizierte Anbieter.
- Ein Monitoring ist als Prozess zu definieren. Bei Class 1 für alle Produkte mit dem Ziel regelmäßiger Updates, bei Class 2 zusätzlich zur Verbesserung der Schutzmechanismen. Bei Class 3 erfolgt dies erweitert um Bedrohungen, Angriffstechniken und Schutzmechanismen.

Die Summe aller Teilaufgaben deckt das Gefahrenspektrum komplatt ab.

- Eine Backup Strategie (neu aufsetzen oder fortsetzen) ist zu definieren, bei Class 2 mit einem Test der Effektivität. Bei Class 3 muss zusätzlich mit einer Abdeckung aller möglichen Vorfälle gearbeitet werden und zwar nicht nur Cyber Security.
- Es sind Safety / Notfallpläne zu definieren, um nutzbare Schwachstellen zu vermeiden. Risikoanalysen und zugeordnete Handlungen sind festzulegen. Die Nachverfolgbarkeit ist zu gewährleisten. Bei Class 3 darf es keine nachfolgenden Schwachstellen ergeben.
- Ein Meldungsmanagement ist zu definieren. Class 2 erfordert zusätzlich ein Krisenmanagement mit regelmäßiger Prüfung. Bei Class 3 ist einmal pro Jahr eine Prüfung erforderlich sowie die Meldung an die übergeordnete Behörde.

Außerdem sind erforderlich:

- Eine Netzwerk Segmentierung und -Abschottung,

- Eine Remote Diagnose und eine Wartung und ein Management
- Eine Einbruchsdetektion sowie Überwachungsmechanismen und
- Eine Security Abnahme.

Bewertungsverfahren

Bei der Risikobewertung werden folgende Größen miteinander verrechnet:

Komplettierung des Systems

- Konnektivität
- Funktionsleistung
- Zugangsverwaltung der Benutzer
- Kompetenz der Angreifer
- Auswirkungen eines erfolgreichen Angriffs

Die Konnektivität und Funktionsleistung der ICS ergeben eine Expositionseinstufung, die Expositionseinstufung, die Zugangsverwaltung der Benutzer und die Kompetenz der Angreifer ergeben eine Wahrscheinlichkeit für den Erfolg eines Angriffs und die Auswirkungen eines erfolgreichen Angriffs und die Angriffserfolgswahrscheinlichkeit ergeben die Klassifikation des Risikos bzw. der Kritikalität.

Expositionseinstufung und Wahrscheinlichkeit eines Angriffserfolges

Die Auswirkungen (Impact) auf Menschen wird in 5 Stufen unterteilt, von „Nicht signifikant – Vorfall gemeldet und keine medizinische Behandlung oder gesundheitliche Auswirkungen“ über „Minor – Meldung und gesundheitliche Auswirkung oder medizinische Behandlung“, „Moderat – dauerhafter Ausfall“, „Major – Todesfall“ bis zu „Katastrophal – mehrfache Todesfälle“.

Die Auswirkungen auf die Umwelt wird ebenfalls in 5 Stufen unterteilt, von „Nicht signifikant – begrenzte und nur vorübergehender Austritt höher als der Standard festlegt, keine Meldung erforderlich“, über „ Minor – begrenzte und nur vorübergehender Austritt höher als der Standard festlegt, Meldung rechtlich erforderlich, keine Konsequenzen für die Umwelt“, „Moderat – moderate, aber begrenzte Verschmutzung des Standorts“, „Major – signifikante Verschmutzung oder Verschmutzung der Umgebung, Menschen sind zu evakuieren“ bis zu „Katastrophal – bedeutende Verschmutzung mit langwierigen Konsequenzen für die Umwelt außerhalb des Standorts“.

Auswirkungen auf die Umwelt: von unbedeutend bis katastrophal (5 Stufen)

Die Auswirkungen durch die Unterbrechung der Dienste (Prozesse) werden auch in 5 Stufen unterteilt, von „Nicht signifikant – ernste Auswirkungen für etwa 1.000 Personen“, über „Minor – ernste Auswirkungen auf 10.000 Personen und Unterbrechung der lokalen Wirtschaft, „Moderat – ernste Auswirkungen auf 100.000 Personen und Unterbrechung der regionalen Wirtschaft, ernster zeitlicher Verlust der Infrastruktur“, „Major – ernste Auswirkungen auf 1.000.000 Personen und Unterbrechung der nationalen Wirtschaft, ernster zeitlicher Verlust kritischer Infrastrukturen, dauerhafter Verlust der überwiegenden Infrastruktur“ bis zu „Katastrophal – ernste Auswirkungen auf 10.000.000 Personen und Unterbrechung der nationalen Wirtschaft, dauerhafter Verlust kritischer Infrastrukturen“

Auswirkungen auf Prozesse: von nicht signifikant bis katastrophal (5 Stufen)

Die Wahrscheinlichkeit eines Angriffs wird in 4 Stufen festgelegt, von „Sehr niedrig“, über „Niedrig“, „Moderate“ bis zu „Stark (hoch)“. Hinzu kommen 5 Kompetenzlevel für den Angreifer, von „Ungezielt – Virus, Bot“, über „Amateur – Individuum mit begrenzten Möglichkeiten, nicht unbedingt mit Absicht einen Schaden zu verursachen, „Einzelner Angreifer – Individuum oder Organisation mit begrenzten Mitteln, aber mit einer definierten Zielvorstellung (gekündigter Mitarbeiter)“, „Private Organisation – Organisation mit erheblichen Mitteln (Terrorismus, Konkurrenzunternehmen mit unlauteren Methoden)“ bis zu „Staatliche Organisation – unbegrenzte Mittel und sehr klaren Zielvorstellungen“.

Die Wahrscheinlichkeit eines Angriffs wird in 4 Stufen eingeteilt.

Abhängig vom Funktionsumfang der ICS, werden 4 Stufen definiert, von „CIM 0 – es gibt keine Kommunikation“, über „CIM 1 – es handelt sich um programmierbare Steuerungen“, „CIM 2 – es handelt sich um SCADA Systeme (Supervisory Control and Data Acquisition)“, „CIM 3 – zusätzlich erfolgt die Anbindung an ein MES (Manufactoring Execution System)“ bis zu „CIM 4 – es existiert noch die übergeordnete Ebene eines ERP Systems (Enterprise Ressource Planning)“.

Ebenfalls wird die Kommunikationsmöglichkeit in 4 Stufen eingeteilt.

Die Konnektivität (Verbindung/Kommunikation) wird nach 5 Klassen gegliedert, von „C1 – es handelt sich um ein isoliertes System“, „C2 – hier liegt ein ICS verknüpft mit einem MIS vor“, „C3 – die Kommunikation erfolgt über drahtlose Verbindungen (wireless communication)“, „C4 – es handelt sich um ein verteiltes ICS mit PN (private network) und externer Eingriffsmöglichkeit“, bis zu „C5 – das ICS ist verteilt und die Kommunikation erfolgt über das Internet“.

Die Verbindungsmöglichkeiten werden in 5 Stufen eingeteilt, von isoliert bis Internet.

F1: Minimal Systems: CIM 0 und 1 ohne programmierbare Konsolen.
F2: Complex systems: CIM 0, CIM 1 und CIM 2 ohne programmierbare Konsolen und ohne Engeneering Workstations
F3: Very complex systems. Alle weiteren Kategorien

Anhand den Funktionalitätsstufen (F) und den Konnektivitätstufen wird dann ein Expositionsindex ermittelt. Die folgende Tabelle stellt diesen Index dar:

F3	Exposure 3	Exposure 3	Exposure 4	Exposure 4	Exposure 5
F2	Exposure 2	Exposure 2	Exposure 3	Exposure 4	Exposure 5
F1	Exposure 1	Exposure 2	Exposure 3	Exposure 4	Exposure 5
Funct./Conn.	C1	C2	C3	C4	C5

Nun wird die Benutzerzugriffsverwaltung ausgehend von der restriktivsten Stufe absteigend in 4 Stufen unterteilt, von „User 1 (keine unautorisierten Eingriffe) - autorisiert (Rechte), zertifiziert (geprüft), kontrolliert (Identität, Handlung)“, über „User 2 (dto.) – autorisiert, zertifiziert“, „User 3 (dto.), autorisiert“ bis zu „User 4 - nicht autorisierte Zugriffe sind möglich“.
Im nächsten Schritt wird nun nach der folgenden Formel die Wahrscheinlichkeit des Angriffs bzw. dessen Erfolg berechnet:

$$L = E + \left\lceil \frac{A + U - 2}{2} \right\rceil$$

Hier erfolgt die zusammenfassende Aussage zur Wahrscheinlichkeit eines (erfolgreichen) Angriffs!

L: Wahrscheinlichkeit, A: Angreifer, U: User, E: Exposition. Der Wert wird zur nächst höheren ganzen Zahl aufgerundet.
Aus der berechneten Wahrscheinlichkeit und den definierten Auswirkungen wird nun die Klasse der Systemeinstufung festgelegt.

5+	Class 2	Class 2	Class 3	Class 3
4	Class 2	Class 2	Class 2	Class 3
3	Class 1	Class 2	Class 2	Class 2
2	Class 1	Class 1	Class 2	Class 2
1	Class 1	Class 1	Class 1	Class 1
Impact/Likeliho	1	2	3	4+

Class 1 bedeutet Einfluss oder Risiko eines Angriffs ist niedrig, Class 2 Einfluss oder Risiko ist merklich und Class 3 Einfluss oder Risiko ist kritisch.

Kritik und Resümee

Das geschilderte Verfahren ist ein erster Ansatz, um Automatisierungssysteme von niedriger bis höchster Stufe hinsichtlich dem Risiko bei Cyber Angriffen einzuordnen.

Das Bewertungssystem ist ein Anfang, allerdings ist er hinsichtlich der Fähigkeit des Angreifers noch verbesserungsbedürftig.

Allerdings ist kritisch anzumerken, dass Angreifer im Darknet günstig leistungsfähige Tools erwerben können und damit auch Amateure aus Spieltrieb schwerwiegende Effekte erzielen können. Weiterhin ist festzuhalten, dass professionelle Angreifer sich Ziele aussuchen

und höchst professionell vorgehen. Meist geht es um hohe Geldbeträge und damit um lohnende Projekte. Die Exposition wird selbst nur grob eingeschätzt. Diese müsste für jede Systemkomponente durch eine umfangreiche Analyse erfolgen und im Detail und definiert werden.

Bei der Einstufung der Funktionalität fällt die Güte der Implementierung völlig unter den Tisch. Zwei Drittel der Schwachstellen für Angriffe resultieren aus der Implementierung. Damit ist nicht nur die Funktionalität im Sinne möglicher Auswirkungen von Eingriffen zu betrachten, sondern insbesondere die Schwachstellen der Implementierung. Die Betrachtung der Konnektivität ist wichtig, da Protokolle wie die ISO 61850 Schwachstellen haben, welche als Angriffsvektor verwendet werden können. Eine mögliche oder vorhandene Verschlüsselung und Identitätssicherung geht wertemäßig nicht ein.

Es gibt (leider) keine genügende Sicherheit der Implementierung; ohne Nachbesserung ist das ein Ausschlussfakt.

Literaturverweis

"Classification Method and Key Measures. Cybersecurity for Industrial Control Systems.
ANSSI 2014, Version 1.0" der Agence nationale de la sécurité des systems d'information. 51 Boulevard de la Tour-Maubourg, 75700 Paris 07 SP, France (www.ssi.gouv.fr)

DUTCH SAFETY BOARD UND CHEMICAL SAFETY BOARD (USA) – AUFGABEN UND ERGEBNISSE (DEUTSCH)

Prof. Dr. Hans J. Pasman

Das Dutch Safety Board ist seit 1909 aktiv und war zunächst nur im maritimen Bereich tätig. Es erfolgte dann eine Aufgabenerweiterung auf die Unfallauswertung für alle Verkehrsträger und schließlich wurde mit dem Kingdom Act (Kingdom Act, 2 December 2004, instituting a Safety Investigation Board (Kingdom Act concerning Safety Investigation Board) auch der Industriebereich integriert, nachdem die Explosion der Fabrik in Enschede im Jahr 2000 große Defizite in Sicherheitsbelangen aufgezeigt hatte. Es geht darum, die Sicherheit durch eine professionelle, unabhängige und transparente Untersuchung von Schadensfällen zu verbessern. Das Gesetz findet man unter der folgenden Adresse: www.safetyboard.nl/htm. Hervorzuheben ist u.a., dass das Board neben allen technischen und naturwissenschaftlichen Fähigkeiten auch über staatsanwaltliche Befugnisse verfügt.

Der Dutch Safety Board ist eine unabhängige staatliche Einrichtung auf der Basis eines Gesetzes. Er hat alle Befugnisse zur Untersuchung von sämtlichen Ereignissen (Unfällen im Verkehr bis hin zu Katastrophen) einschließlich staatsanwaltlichen.

Heute widmen sich rund 70 Mitarbeiter diesen volkswirtschaftlich bedeutenden Aufgaben, wobei das Board auch externe Ermittler einsetzen kann, um alle Teilfragestellungen von Schadensfällen professionell behandeln zu können. Die Erkenntnisse sind frei verfügbar; es werden Empfehlungen abgegeben, wobei das Board auch deren Beachtung nach Ablauf eines halben Jahres prüft. Bisher sind 77 Unglücke im Schiffsverkehr, 598 in der Luftfahrt, 30 im Eisenbahnverkehr und 45 in der Industrie untersucht worden.

Das Board hat rd. 70 Mitarbeiter, die bei Bedarf externe Ermittler einschalten. Es wird offiziell berichtet, gekoppelt mit Empfehlungen. Über https://www.onderzoeksraad.nl/page/336/dutch-safety-board kann ein detaillierter Einblick gewonnen werden.

Hierzu gab es Einblicke im Detail mit einem Video zum Flug MH17 (Abschuss über der Ukraine) und den Hinweis auf die Explosion der Shell-Raffinerie am 3. Juni 2004, vergl. dazu den Bericht des Dutch Safety Board vom Juli 2005 (06d47740485 9summery_shell_moerdijk.pdf).

Das Chemical Safety Board in den USA hat für den Chemiebereich den gleichen Auftrag und ist seit 1998 aktiv. Es handelt sich um eine Bundesagentur, die die chemische Sicherheit durch unabhängige Untersuchungen zum Schutz der Menschen und der Umwelt sichern und steigern soll. Rund 100 Untersuchungen sind abgeschlossen, acht sind augenblicklich in Bearbeitung. Auch hierzu wurden Beispiele zur Illustration gezeigt, insbesondere der Ölunfall 2010 im Golf von Mexiko (Deep Water Horizon).

Das Chemical Safety Board (USA) hat durch unabhängige Untersuchungen für mehr Sicherheit für Mensch und Tier zu sorgen.

Deutschland und die EU sollten ihre einzelnen Untersuchungsstellen zusammenführen.

Anmerkungen aus der Konferenz: in der Bundesrepublik Deutschland gibt es keine vergleichbare Institution, die vor allem unabhängig und fachlich entsprechend ausgestattet Untersuchungen zu Schadensfällen anstellen kann. Vielmehr haben wir in der Bundesrepublik Deutschland verschiedene Untersuchungsstellen, die auch noch unterschiedlichen rechtlichen Bedingungen unterliegen. Im Verkehrsbereich sind das folgende Stellen: Eisenbahn Bundesamt für den Schienenverkehr, Bundesanstalt für den Güterverkehr für den Straßenverkehr, Bundesstelle für Flugunfalluntersuchung und Bundesstelle für Seeunfalluntersuchung. Aus dem Bereich der Industrie gibt es die zentrale melde und Auswertestelle für Störungen und Störfälle.

RISIKOBEWERTUNG ALS MANAGEMENTAUFGABE – ENTWICKLUNGEN IM BEREICH SICHERHEIT UND GEFAHRENABWEHR, ANALYSE UND VORHERSAGE AUCH UNTER ANWENDUNG KÜNSTLICHER INTELLIGENZ

Prof. Dr. Hans J. Pasman

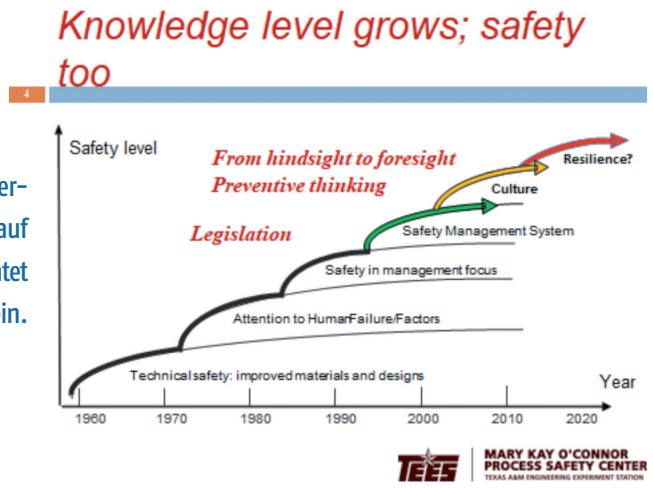
Am Anfang von Planungen/ Aufgaben in der Technik steht die Abschätzung eines Risikos.

Folgende Feststellung beschreibt die heutige Aufgabe, Sicherheit zu generieren und zu erhalten: man kann nur wissen, wie sicher eine Struktur, ein Werkzeug, ein Prozess oder eine Situation ist, wenn man weiß, welche Risiken damit verbunden sind. Demzufolge fängt man mit der Betrachtung des Risikos an, ermittelt die Unsicherheiten und die möglichen Barrieren, macht die Entscheidungsfindung transparent und kommuniziert die Ergebnisse mit sämtlichen Einschränkungen und Unsicherheiten. In der Zukunft wird man über eine Vielzahl von Daten und Analysen verfügen und kann sicher mithilfe der künstlichen Intelligenz wesentlich fundierter Aussagen zur Belastbarkeit von Strukturen und Systemen herleiten.

Man strebt demzufolge eine Sicherheitskultur an, die auf Belastbarkeit abzielt.

Eine (europäische) Sicherheitskultur muss heute auf Belastbarkeit ausgerichtet sein.

Das nachstehende Bild zeigt den Zeitverlauf der Entwicklungen der Maßnahmen zur gesteigerten Sicherheit.



Ein immer wieder auftauchendes Kommunikationsproblem ist der Gebrauch von Begriffen in der englischen Sprache, die nicht deckungsgleich in die deutsche Sprache zu übersetzen sind. Im Englischen wird zwischen den oft synonym erscheinenden Begriffen „hazard“, „risk“ und „danger“ unterschieden – siehe dazu „RISK MANAGEMENT IN A DYNAMIC SOCIETY: A MODELLING PROBLEM“ von Jens Rasmussen (1997). Bei der Analyse von Schadensfällen werden Kontextanalysen (Ziele, Stakeholder, Kriterien, Schlüsselelemente) leider zu oft vernachlässigt. In diesem Zusammenhang stellt die in vier Quadranten gegliederte „Rumsfeld Matrix“ eine Hilfe dar: In dieser wird das Risiko über der Beobachtbarkeit aufgetragen:

- Geringes Risiko bei geringer Beobachtbarkeit seien durch „known knowns“ gekennzeichnet,
- hohes Risiko bei geringer Beobachtbarkeit durch „known unknowns“,
- hohes Risiko bei geringer Beobachtbarkeit durch „known unknowns“,
- hohes Risiko bei hoher Beobachtbarkeit durch „unknown unknowns“...

Schließlich stellt sich die Frage, warum die Identifizierung von Szenarien so problematisch ist. Folgende Teilaspekte illustrieren die Problematik:

- Komplexität des sozi-technischen Systems, Dynamik des Organismus
- enge Kopplungen, Nichtlinearität und dysfunktionale Komponenten
- Inter Action und organisatorische Zwänge
- große Variabilität in der menschlichen Leistungsfähigkeit
- Viskosität der Organisationen (Bürokratie)
- falsches mentales Bild des Prozesses
- fehlerhafte Kommunikation innerhalb des Teams

Das Buch „Risk Management in a Dynamic Society: A Modelling Problem“ von Jens Rasmussen, 1997, bildet die Grundlage.

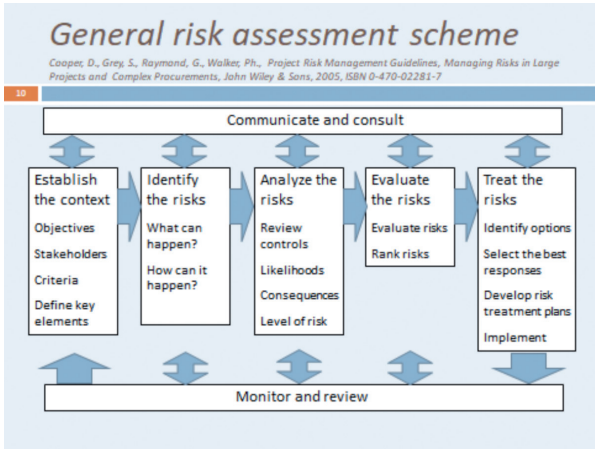
Analysen von Schadensfällen müssen zwingend von Kontextanalysen begleitet werden.

Die Identifizierung von Szenarien ist schwierig, muss aber geschafft werden.

- versteckte Konstruktionsfehler und Materialprobleme
- Unzulänglichkeiten bei der Wartung
- Domino-Effekte, Eskalation

Mögliche Lösung des Problems: Systemansatz

Die Lösung besteht in einem System-Ansatz.



Zu der Frage der Einbindung der technischen Abschätzungen in die ökonomischen wird eine Reihe von Literaturstellen angegeben.

Risikomanagement führt zu Risikominderung. Voraussetzung: Belastbarkeit ist hoch, alle Daten werden genutzt, auch soll KI aufgegriffen werden.

Schließlich führt die Risikobewertung dazu, zu erkennen, was, in welchem Umfang und wie oft schief gehen kann. Risikomanagement bedeutet, der Risikominderung Priorität einzuräumen. Man sollte keine hohe Genauigkeit der Vorhersage haben, man sollte auch nicht auf die Ergebnisse der Risikoanalyse ohne Unsicherheitsanalyse vertraut. Schließlich rettet die Belastbarkeit das Ges... man muss die besten Werkzeuge nutzen und gleichzeitig vermeiden, dass diese Werkzeuge black-boxes werden. Stets weiterdenken, weiter als bisher. Zukünftig erhalten wir große Datenmengen, die uns in vielerlei Hinsicht helfen werden, Informationen und damit wissen auch über heimtückische Trends und komplexe Wechselwirkungen zu bekommen. Stichwort: künstliche Intelligenz.

Der Beitrag von Herrn Prof. Dr. Hans J. Pasman liegt der Konferenz original in der englischen Sprache vor („Risk assessment as management task – Developments in safety and security analysis and prediction, also applying Artificial Intelligence") und kann ggf. von der Konferenzleitung angefordert werden. Sodann stellte er mit Videos einige vom Dutch Safety Board untersuchte Vorfälle vor.

Herr Ludwig führte aus, dass „Risk Assesment" immer wichtiger werde – es sei bereits in der Design-Phase möglich und helfe zudem, Wartungskosten einzusparen.

Professor Hennecke warf die Frage nach Kriterien für „Resilienz" auf.

Professor Pasman erläuterte, dass es hierzu noch Forschungsbedarf gebe.

Frau Seyerlein-Klug gab ihre Einschätzung wieder, dass „Risk Assesment" bisher nicht wirklich mitgedacht werde.

Risk Assesment muss auch durchgehend eingeführt werden, da es sich sicherheitlich **und** ökonomisch auszahlt.

INDUSTRIE 4.0 ZWISCHEN IDEE UND REALITÄT. EIN LÄNDERVERGLEICH

Prof. Dr. Gerhard Banse

Professor Banse stellte das Publikationsprojekt „Industrie 4.0 zwischen Idee und Realität. Ein Ländervergleich“ vor. Dies geht auf ein BMBF-Projekt aus dem Jahr 2014 zurück: „Internationale Zusammenarbeit in Bildung und Forschung, Region Mittelost-und Südeuropa“ – als ein Nebenziel ist die **Erstellung von „State-of-the-Art“-Länderreports** definiert worden. Das Publikationsprojekt ist mittels einer multidisziplinären Arbeitsgruppe durch Mitwirkende aus Deutschland, Polen, Slowenien und Tschechien umgesetzt worden – ergänzend kamen dann noch Analysen aus Österreich und Rumänien dazu. Ziel ist die Bereitstellung **vergleichender Länderreports zum Stand der Industrie 4.0** in den genannten Staaten. Hinzugefügt wurden noch spezifische Überlegungen zur Industrie 4.0 aus Sicht von Arbeitspsychologen und Beratern sowie der Technikfolgenabschätzung. Als ein Ergebnis des abschließenden Vergleichs der Situationen in den betreffenden Staaten sind noch weitergehende Fragen abgeleitet worden, welche weiterer Erforschung bedürfen.

Industrie 4.0 im Ländervergleich (D, PL, SLO CZ, A und RO)

Vergleichende Reports zum Stand von Industrie 4.0

Fortsetzung des Vergleichs durch F&E-Arbeiten

Ein Fazit: Industrie 4.0 als „Hype“ schwächt sich ab, denn sie werde zunehmend zur **Realität**. Einzelheiten sind dem Buch „Industrie 4.0 zwischen Idee und Realität. Ein Ländervergleich“ (Band 54 der Abhandlungen der Leibniz-Sozietät der Wissenschaften) zu entnehmen.

Industrie 4.0 ist Realität geworden.

Anschließend stellte Dr. Lingner das **Projekt „Industry 4.0 in Mittel- und Osteuropa. Die Perspektive der Technikfolgenabschätzung und des Vision Assessment“** vor. Bei diesem wurde der „Faktor Mensch“ in den Fokus gestellt, es geht um Bildungs- und erweiterte Sicherheitskultur.

Ein notwendiges Folgeprojekt fokussiert auf den Faktor Mensch; erweiterte Sicherheitskultur

PLANUNG „WELTKONGRESS DER SICHERHEIT“

Herr Kalenberg berichtet über die ursprüngliche Idee, mit dem „Weltkongress der Sicherheit“ an das Format „ARBEITSSCHUTZ AKTUELL 2020“ in Stuttgart anzudocken. Nach Rücksprache mit dem Präsidium eigne sich der Fokus 2020-2021 (Arbeitsschutz- Weltkongress in Toronto) nicht für so eine Kooperation – man könne aber ggf. über 2022 sprechen.

An die Konferenz „Arbeitsschutz aktuell 2020“ in Stuttgart konnte der „Weltkongreß Sicherheit“ nicht angedockt werden.

Dr. Keller merkte an, dass eine Vorbereitungsphase von mindestens zwei Jahren notwendig sei – und vorab die Klärung, welche Akteure einzubinden seien. Über den BDI könne man evtl. die großen Industrie-Unternehmen einbinden. Diese Einbindung der Wirtschaft sei entscheidend – z.B. um zu erörtern, wem die Daten gehören. Ihm gehe es um die Diskussion der Sicherheit von Produkten hinsichtlich Nutzern und Herstellern.

Für den Weltkongreß Sicherheit ist nach Klärung der Randbedingungen eine Vorlaufzeit von mind. 2 Jahren einzuplanen.

Dr. Schulz-Forberg verwies auf die Seiten 64 und 65 der vorliegenden Broschüre zur 5. BGKdSI-Auflage: Der Weltkongress würde Deutschland guttun – in dessen Rahmen könne z.B. auch der sichere Umgang mit Daten diskutiert werden. Ein Thema könnten zudem defekte Brücken in Deutschland sein – hierzu lägen ausreichend Daten vor, eine Schadensbehebung sei dringend geboten.

Professor Banse schlug als Kompromiss vor, einen deutschen Kongress der Sicherheit mit internationaler Beteiligung einzuberufen. Bezugnehmend auf die Seite 65 der Broschüre regte er an, die dort aufgelisteten Inhalte zu konkretisieren – es gehe dabei um „drängende Fragen“. Dr. Holtmann schlug vor, unter BDI-Mitgliedern ein Stimmungsbild einzuholen.

Ob Weltkongreß oder deutscher Kongreß, erst muss der Wille da sein

Herr Kalenberg merkte die Notwendigkeit an, zuvor ein Thesenpapier als Aufriss zu erstellen.

Dr. Langenbach ergänzte, dass herauszuarbeiten sei, „wo der Schuh drückt“.

Konkretes Ziel für den Kongreß aufstellen, Schwerpunkte wie Normen benennen

Herr Wittenbrink warf die Frage nach dem Kongressziel und dem Nutzen auf.

Herr Ludwig nannte Standards als einen möglichen Schwerpunkt.

Dr. Schwuchow schlug Akzeptanzfragen vor und führte in diesem Zusammenhang digitale Gebäudemodelle an. Zudem geht es um die Abwägung von Geldeinsparung vs. Lebensrettung. Man müsse die Politiker mitnehmen. Zur Frage defekter Brücken verwies er auf das jährlich stattfindende „Dresdner Brückenbausymposium“.

Politik und Versicherer müssen eingebunden werden. (Unfälle und Unfallkosten)

Professor Hennecke brachte die Unfallstatistik ein – Wegeunfälle seien z.B. eine große Stellschraube für Sicherheit.

Herr Knopf erläuterte, dass nach Erkenntnissen der Versicherer mit rund 80 Prozent Arbeitsunfällen und 20 Prozent Wegeunfällen zu rechnen sei.

ZWISCHENSTANDSBERICHT ZUR ERSTELLUNG EINER UMFASSENDEN SICHERHEITSLANDKARTE FÜR DEUTSCHLAND / DIE D-A-CH-REGION

Mit der Sicherheitslandkarte startete die BGKdSI.

Dr. Schulz-Forberg warf einen Blick zurück auf die Anfänge der BGKdSI: Dr. Dennis Göge als den Sicherheitskoordinator des DLR bestätigte, dass es keine Übersicht über alle mit dem Thema Sicherheit in Deutschland befassten Institutionen gibt. Der VDI/VDE-Arbeitskreis hat sich sodann mit dem Thema befasst und mit Dr. Göge hat das zum Auftakt der BGKdSI geführt. Auf Seite 5 der vorliegenden BGKdSI-Broschüre sind die **Hauptkriterien einer relevanten Sicherheitsinstitution** zu finden, nämlich:

1. Ständige Aufgabe, ständiger Auftrag, gewählte Mission.

2. Sicherheit als ein Schwerpunkt in der Institution.

In Österreich gibt es eine Landkarte! Gegebenenfalls kann auch über eine Karte der Region D-A-CH nachgedacht werden.

Dieser bei der vorherigen Auflage definierte Fokus erlaubt auch die Festlegung von Unterkriterien und Gewichtungen. Zur Orientierung könne die österreichische Website „kiras.at" dienen; Herr Dr. Ralph Hammer von der Stabsstelle für Technologietransfer und Sicherheitsforschung / Bundesministerium für Verkehr, Innovation und Technologie in Wien ist grundsätzlich zur Mitwirkung bei der Planung bereit. Ein mögliches Ziel gemeinsamer Aktivitäten kann eine **Sicherheitslandkarte für die sogenannte D-A-CH-Region** sein.

Dr. Holtmann riet dazu, die Erfahrungen der Österreicher zu nutzen – insbesondere gelte es dann, für die **notwendige Pflege der Website** zu sorgen.

Dr. Schulz-Forberg verwies darauf, dass für die weitere Sondierung eine **Finanzierung** benötigt werde. Er regte an, dass es zu einem direkten Austausch der Herren Dr. Hammer und Dr. Holtmann kommen könnte; auch wolle er Rücksprache mit dem VdTÜV nehmen.

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 unter stützen,

- 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

EINE FRUCHTBARE KOOPERATION

FORUM46 und AKSi

Das FORUM46 fördert die interdisziplinäre Zusammenarbeit an den Nahtstellen von Kunst, Wirtschaft, Wissenschaft und Zivilgesellschaft und hilft damit Innovationspotenziale aufzudecken.

Der AKSi widmet sich den dringenden Fragen zu Chancen und Risiken der Technik mit Bezug zu den Wechselwirkungen von technischen und gesellschaftlichen Entwicklungen unserer Zeit und sieht sich dabei in einer Wächterfunktion für Sicherheitsbelange

FORUM 46
INTERDISZIPLINÄRES FORUM FÜR EUROPA

VDI/VDE-Arbeitskreis Sicherheit (AKSi)
Bezirksverein Berlin-Brandenburg

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.