Berliner Gesamtkonferenz der Sicherheitsinstitutionen

Zu Gast beim VDE-Elektrotechnischen Verein (ETV) Bezirksverein Berlin-Brandenburg im VDE

- Östereichische Sicherheitsforschung und ihre Sicherheitslandkarte
- PISEA – aktuelle Erkenntnisse zu Safety und IT-Security
- Sicherheit im Bauwesen – über die Veränderungen bei der GruSiBau
- Sicherheitsherausforderungen aus DWV-Sicht
- Aufgabenfeld „Sicherheit" im DLR
- Das Dutch Safety Board (DSB) als Vorbild für Deutschland
- Work and Results of the Dutch Safety Board
- Leistungsübersicht der ci-tec GmbH Karlsruhe

FORUM TECHNOLOGIE & GESELLSCHAFT

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

DEKRA
On the safe side.

ci·tec

VDE Berlin-Brandenburg (ETV)

Die Veranstaltung wurde ermöglicht durch die freundliche Unterstützung der DEKRA, der ci-tec und dem VDE Berlin-Brandenburg.

Für den Druckkostenzuschuss danken wir Christian Peuker, Geschäftsführer Advanced Lift Consultants GMBH.

INHALT

GRUSSWORTE

Dipl.-Ing. Dirk Pinnow
Dipl.-Ing. Carsten Pinnow

Dipl.-Ing. (TU) Dirk Pinnow begrüßte die Anwesenden namens der BGKdSI-Konferenzleitung und drückte seine Freude über die jetzt wieder mögliche Präsenzveranstaltung und die substanzielle Beteiligung an dem Format der Berliner Gesamtkonferenz der Sicherheitsinstitutionen aus.

Sicherheit muss stets und stärker in den Fokus.

Die BGKdSI widmet sich bekanntermaßen 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 stets abzusichernden positiven Innovationsklimas. Wir brauchen eine stärkere Vernetzung aller Institutionen in den Bereichen Technik, Wirtschaft, organisiertes Gemeinwesen und Administration, um konstruktivkritisch in den politischen Raum hineinzuwirken. Eine allgemein etablierte und anerkannte Kultur der Sicherheit mit umfassenden und klaren Konzepten schützt und stärkt das Wertschöpfungspotenzial der Volkswirtschaft.

Der Elektrotechnische Verein in Berlin.

Dipl.-Ing. (TU) Carsten Pinnow begrüßte als Vorsitzender des VDE-Elektrotechnischer Verein (ETV) e.V., Bezirksverein Berlin-Brandenburg im VDE die Teilnehmer als Gastgeber und gab in seinem Grußwort einen kurzen Abriss über den am 20. Dezember 1879 in Berlin im damaligen Reichspostgebäude in der Leipziger Straße (heute: Museum für Kommunikation Berlin) gegründeten Elektrotechnischen Verein (ETV).

Unter den Gründern befanden sich Dr. Werner von Siemens und Dr. Heinrich von Stephan. Mit anfänglich 36 Mitgliedern wurden schnell weitere aus ganz Deutschland und dem Ausland gewonnen. Weitere Regionalvereine wurden gegründet, bis dann 1893

der VDE (Verband der Elektrotechnik Elektronik Informationstechnik e.V.) ins Leben gerufen wurde. Zu den ETV-Mitgliedern und Vortragenden des Vereins gehörten bedeutende Persönlichkeiten ihrer Zeit wie Gustav Robert Kirchhoff, Albert Einstein, Thomas Alva Edison und Lord Kelvin.

Der ETV fühle sich dem damaligen Gründungsimpuls mehr denn je verpflichtet, *„als in Berlin engagierte Repräsentanten der Wirtschaft, Behörden, Wissenschaft und auch des Militärs die Notwendigkeit erkannten, bei der nutzbringenden Erschließung eines auch durchaus strategisch relevanten, volkswirtschaftlich bedeutsamen neuen Technologiegebietes zu kooperieren, methodisch vorzugehen und Wissenstransfer zwischen Grundlagen- sowie Anwendungsforschung zu ermöglichen“*.

Wissenstransfer und Kooperation stärken die Wirkung von Anwendungs- und Grundlagenforschung.

Wenn heute im Zuge der Digitalen Transformation, also der Durchdringung fast aller Lebensbereiche mit Informations- und Kommunikationstechnik quasi wieder „Neuland“ betreten werde und dieses systematisch erschlossen werden solle, sei abermals enge Kooperation gefragt. Die Stichworte „Internet der Dinge und Dienste“ sowie „Embedded Systems“, „Autonome Systeme“, „Künstliche Intelligenz“, „Big Data“ sowie „Robotic Process Automation“ usw. steckten grob die Vielfalt der Herausforderungen ab – Sicherheit im umfänglichen Verständnis werde dabei immer eine zentrale Rolle spielen: Sicherheit sei notwendige, wenngleich noch lange nicht hinreichende Bedingung für eine erfolgreiche „Industrie 4.0“ oder gar „Gesellschaft 4.0“.

In der Gesellschaft 4.0 ist die Sicherheitsgestaltung deutlich wichtiger geworden.

Abschließend betonte Carsten Pinnow, dass wir vor „gewaltigen wissenschaftlichen, technischen, gesellschaftlichen und kulturellen Herausforderungen“ stehen und der ETV sich sachlich und kompetent in die Diskussion um die besten, sichersten und umweltverträglichsten Lösungen einbringen möchte. Er wiederholte gegenüber den BGKdSI-Akteuren seinen Appell aus dem Jubiläumsjahr an alle mit der Digitalen Transformation befassten Organisationen – Unternehmen, Vereine wie Verbände –, die Kooperation zu suchen und Berlin, Deutschland, ja Europa in eine Art neuer Gründerzeit zu führen. Berlin habe einst als „Elektropolis“ und zugleich als einer der bedeutendsten Industriestandorte im kontinentalen Europa gegolten – „unsere Vorfahren, darunter auch die ETV-Gründer, haben bemerkenswerten Mut und Weitsicht beweisen, woran wir uns immer wieder ein Beispiel nehmen sollten!“ Ihr Vorbild gelte es in zeitgemäßer Weise adaptieren.

Digitale Transformation mit allumfassender Kooperation voranbringen. Aus Berlin wieder Elektropolis machen!

VORSTELLUNG DER ÖSTEREICHISCHEN SICHERHEITSFORSCHUNG UND IHRES VERNETZUNGSINSTRUMETS SICHERHEITSLANDKARTE

Dipl.-Ing. Dirk Pinnow

Das Funktionieren des Systems aus Recht und Norm ist für die Sicherheit konstitutiv.

Dirk Pinnow berichtete über die Website „kiras.at“. Dabei führte er aus, dass das Projekt einer Sicherheitslandkarte (zunächst für Deutschland) ein wesentliches Motiv zur Gründung des heutigen VDI/VDE-Arbeitskreises Sicherheit (AKSi) war und einige Kollegen, so auch der anwesende BGKdSI-Akteur Armin Knopf, sich hierzu mit grundlegenden Recherchen befasst hatten, so dass dieser Themenkomplex schließlich die BGKdSI seit ihrer Einrichtung begleitet hat – nunmehr erweitert als Idee einer **„D-A-CH-Sicherheitslandkarte“** für das deutschsprachige Europa. Die Konferenz kam überein, diese Thematik auf der weiteren Agenda der Konferenzreihe zu belassen und bei einer Folgeveranstaltung mit Dr. Hammer zu vertiefen.

Link 1: „Die österreichische Sicherheitsklammer“
https://www.kiras.at/.

Die Sicherheitsforschungslandkarte KIRAS

Sie wurde im Dezember 2009 vom damaligen österreichischen Bundesministerium für Verkehr, Innovation und Technologie eingerichtet, mit dem erklärten Ziel,

- Anwender (Bedarfsträger wie Bundesministerien, Landesbehörden, „Blaulicht“-Organisationen, Betreiber Kritischer Infrastrukturen)
- Forscher
- Unternehmen
- Geistes-, Sozial und Kulturwissenschaftler

auf dieser Internetplattform ihren Bedarf sowie ihre Fähigkeiten darstellen zu lassen und so die Schaffung von Konsortien für KIRAS-Projekte dank einfacher Bedienung zu erleichtern. Bisher haben über 500 Institutionen diese kostenlose Möglichkeit der Repräsentation wahrgenommen.

SICHERHEIT ALS EIGENSCHAFT TECHNISCHER SYSTEME UND DIE ABHÄNGIGKEIT VON DER CYBER SECURITY

Eine Empfehlung der Berliner Gesamtkonferenz der Sicherheitsinstitutionen (BGKdSI)

Dr. Hubert B. Keller

Herr Dr. Hubert B. Keller hat unter dem Titel „PISEA – aktuelle Erkenntnisse in Safety und IT-Security" umfangreiche Daten bereitgestellt, beurteilt und das in 46 Folien der Konferenz zur Kenntnis gebracht. Diese diskutierte das Thema mit der allgemeinen Fragestellung, warum hören eigentlich Politik und Wirtschaft nicht auf diese durchdringenden Warnsignale? Die Konferenz war sich einig, dass man beim Studieren der Folien eigentlich die Alarmglocken hören muss. Aus diesem Grund wird der komplette Vortrag auf der Website des Forum46 (www.forum46.eu) bekanntgemacht werden.

1. Einleitung

Cyber-Angriffe nehmen stark zu.

Heutige technische Systeme aller Art bestehen in großen Teilen aus Software bzw. softwarebasierte Funktionen. Die Zuverlässigkeit dieser Systeme hängt daher stark vom korrekten Funktionieren dieser Software ab. Aufgrund der mittlerweile stark vorhandenen Vernetzung und der vorhandenen Schwachstellen in der Software sind Cyber-Angriffe in großem Umfang und mit erheblichen Auswirkungen quasi schon normal.

2. Vorhandene Informationen

Die Gesellschaft erwartet die Beherrschbarkeit der Sicherheitslage, professioneller Eingriff des Staates kann nötig werden.

Die Bitkom-Studie vom 5.8.2021 über Cyber-Kriminalität (https://www.bitkom.org/Presse/Presseinformation/Angriffsziel-deutsche-Wirtschaft-mehr-als-220-Milliarden-Euro-Schaden-pro-Jahr) geht von einem Gesamtschaden von 223 Milliarden Euro p.a durch Diebstahl, Spionage und Sabotage für die deutsche Wirtschaft aus. 2018 / 2019 waren es dagegen „nur" 103 Milliarden Euro p.a. Die Studie zeigt, dass neun von zehn Unternehmen (88 Prozent) 2020 / 2021 von Angriffen betroffen waren (2018 / 2019 waren es drei Viertel = 75 Prozent).

Absolut korrekte und zielgerichtete Vorgehensweise muss die bisherige oft nachlässige Vorgehensweise in der Programmierung ablösen.

Vernetzte Systeme wie Kritische Infrastrukturen, Lieferketten, Chemische Industrie und zukünftig auch Autonome Fahrzeuge sind damit hoch gefährdet. Die Ursachen der Cyber-Angreifbarkeit liegen in drei wesentlichen Bereichen:

- Dem inkorrekten Benutzermanagement mit falschen Identitäten oder Rechten
- Den unsicheren Kommunikationsprotokollen mit falschen Identitäten oder manipulierten Daten
- Den inhärenten Implementierungsfehlern durch falsche Programmierung, fehlende Prüfung oder schlichtweg durch die Wahl der falschen Programmiersprache

CISA – die Cybersecurity and Infrastructure Security Agency publiziert regelmäßig Hinweise auf aufgetretene / erkannte und ausgenutzte Schwachstellen in der Software von technischen Systemen oder in der Automatisierung (https://www.cisa.gov/uscert/ncas/current-activity/2022/10/13/cisa-releases-twenty-five-industrial-control-systems-advisories).

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

ICS-CERT – das CERT für Industrial Computer Systems veröffentlicht ebenfalls Hinweise, wie z. B. vom 14.5.2022 mit 30 Hinweisen. CISA veröffentlicht das sogenannte Vulnerability Summary for the Week, hier vom 10.10.2022. 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.

Eine verbindliche Handlungsanleitung zur Vermeidung von Fehlern wird benötigt.

Folgende Security-Schwachstellen treten dabei immer wieder in den Vordergrund (beispielhafte Aufzählung):

In der Kommunikation z.B.
- Cleartext Transmission of Sensitive Information

In der Benutzerverwaltung z. B.
- authentication bypass vulnerability
- privilege escalation vulnerability
- multiple vulnerabilities
- Improper Authentication

In der programmtechnischen Realisierung z. B.
- Remote Code Execution Vulnerability
- insufficient validation of user-supplied input

Logische Maßnahmen durchsetzen, gegebenenfalls fehlerhaftes Vorgehen ahnden.

- Improper Input Validation
- Classic Buffer Overflow
- Stack-based Buffer Overflow
- Out-of-bounds Write
- Out-of-bounds Read
- Null Pointer Dereference
- Integer Overflow to Buffer Overflow
- Double Free
- Use After Free

Im Bereich der Programmierung und den damit zusammenhängenden Schwachstellen, welche für Cyber-Angriffe ausgenutzt werden, gibt es solche, **welche seit Jahren konstant und dominant vorherrschen.**

Diese 2022 CWE Top 25 Most Dangerous Software Weaknesses sind leicht zu finden, auszunutzen und können es Angreifern ermöglichen, ein technisches System von der Software-Seite komplett zu übernehmen, Daten zu entwenden bzw. zu manipulieren oder auch Anwendungen und Funktionen zu blockieren. **Gerade bei Kritischen Infrastrukturen führt dies zu gefährlichen Situationen.** Krankenhäuser müssen ohne Krankendaten arbeiten, Wasserwerke sind außer Funktion oder auch Energieversorgungen sind gefährdet.

3. Die 25 kritischsten Schwachstellen

Diese 25 kritischsten Schwachstellen sind unter https://cwe.mitre.org/top25/archive/2022/2022_cwe_top25.html#cwe_top_25 aufgeführt. Das nachfolgende Bild zeigt, dass diese im Wesentlichen seit Jahren stabil dominant sind. Es zeigt auch in Konsequenz, dass diese Erkenntnisse nicht in der Praxis umgesetzt werden.

Da diese Schwachstellen auch Security Router, virtuelle Maschinen etc. betreffen, welche in Systemen der Automatisierung, Betriebsführung und Lieferkettenvernetzung eingesetzt werden, ist die Situation als deutlich kritisch zu bewerten.

4. Notwendiges Vorgehen

Die Frage lautet also, wie diese Schwachstellen effektiv und wirtschaftlich vertretbar und nachhaltig behoben werden können. Eine singuläre Reparatur einzeln erkannter Schwachstellen ist sicher nicht zielführend.

Grundsätzlich sind folgende Forderungen zu erfüllen:

Es muss zwingend eine ganzheitliche Reparatur am System erfolgen! Systemführung?

- Im Design der Architektur des Gesamtsystems
  - Security by Design im Sinne Security muss ganz am Anfang im Entwurf berücksichtigt werden

- In der Benutzerverwaltung
  - Strenge Authentifizierung des Benutzers
  - Minimale Rechtevergabe an den Nutzer
  - Nur absolut notwendige Software einsetzen, damit keine Seiteneffekte entstehen können

- Bei Kommunikationsprotokollen und der Verschlüsselung
  - Identifikation des Kommunikationspartners sichern (z. B. durch eine Hash ID)
  - Zuverlässigkeit des Protokolls sicherstellen, um Man-in-the-Middle-Attacken zu vermeiden
  - Verschlüsselung der Übertragung um eine Manipulation der Daten (Kommando und Daten) zu vermeiden
  - Zeitliche Gültigkeit des Schlüssels nach Risiko festlegen

Laufende Überwachung organisieren und korrigierend eingreifen; Systemführerschaft etablieren.

- In der Implementierung
  - Den Code durch automatische Analysen auf Einhaltung von Vorgaben prüfen lassen (formale Verifikation durch SPARK, wo möglich)
  - sichere Algorithmen verwenden bzw. updaten
  - sichere Programmiersprache verwenden (wegen inhärente Defizite kein C/C++, kein Java)
  - jedes Eingabedatum syntaktisch und semantisch prüfen
  - die Vorgaben von Seacord und der NUMUR-Vorgaben (NE153) umsetzen

Bei Cloud und Micro Cloud Services muss der Rechtefluss überwacht und geprüft werden. Da Security eine Architektureigenschaft ist, muss dies im agilen Vorgehen berücksichtigt werden. Auch die eingesetzten Betriebssysteme müssen hinsichtlich den genannten Schwachstellen untersucht und entsprechend ertüchtigt werden.

Alle Beteiligten „einschwören"!

Bei allen Beteiligten ist ein Sicherheits-Bewusstsein zu entwickeln. Dies betrifft direkt die Entwicklung, das Management, aber auch die Politik und die Gesellschaft allgemein.

Langfristig ausschließlich sichere Software-Lösungen verwenden. In der Übergangszeit mit der Einhegung von gefährdeten Teilen arbeiten.

Existierende Software sollte langfristig durch sichere Versionen ersetzt werden. Aus ökonomischen Gründen ist in einer Übergangszeit eine umgebende Schutzsoftware (Gartenzaun) zu realisieren, die jede Eingabe von Informationen in ein System von außen auf syntaktische und semantische Korrektheit prüft. Die dazu notwendigen Informationen (Kommandos, Parameter etc.) sind in aller Regel in den Engineering-Werkzeugen verfügbar.

5. Schlussfolgerung

Für Software-Systeme aus Deutschland soll wieder klar sein, dass sie sicher sind; Alleinstellungsmerkmal.

Der Mehrwert der getroffenen Maßnahmen wäre

- eine erhebliche Absicherung Kritischer Infrastrukturen,
- eine Ertüchtigung aller technischen Systeme,
- eine nachhaltige Zuverlässigkeit der eingesetzten Software

alles bei gleichzeitiger Reduzierung der Kosten im Cyber-Security-Bereich.

SICHERHEIT IM BAUWESEN – ÜBER DIE VERÄNDERUNGEN BEI GruSiBau

Neuauflage, Änderungen im Vergleich zur Erstfassung

Dr.-Ing. Ronald Schwuchow

GruSiBau bildet die „Bibel“ für die Sicherheitsanforderungen im Bauwesen.

1. Zusammenfassung

Die unter dem Namen GruSiBau bekannte Leitlinie „Grundlagen zur Festlegung von Sicherheitsanforderungen für Bauliche Anlagen“ ist seit 1981 in Kraft. Seit über vier Jahrzehnten war es die “Bibel“ im Bauwesen in Deutschland und in großen Teilen von Europa. Eine Überarbeitung und damit eine Anpassung an die Änderungen innerhalb des Bauwesens in den letzten 40 Jahren war geboten und hat ihren Niederschlag 2022 in einem Grundsatzpapier des DIBt (Deutsches Institut für Bautechnik) gefunden. Mit den nachstehenden Adressen sind die Papiere aufzurufen:

Mit der Aufnahme von Weiterentwicklungen von 40 Jahren wird die GruSiBau als „Bibel“ fortgeschrieben.

https://www.dibt.de/de/aktuelles/meldungen/nachricht-detail/meldung/vier-jahrzehnte-grusibau-ein-vorschlag-fuer-eine-fortschreibung

https://www.dibt.de/fileadmin/dibt-website/Dokumente/Allgemein/Vorschlag_Grusibau_2_0.pdf

Das Deutsche Institut für Bautechnik (DIBt) nimmt einen großen Aufgabenkatalog professionell wahr.

Das Deutsche Institut für Bautechnik ist 1968 gegründet worden und beruht auf einem Abkommen der Länder mit dem Bund. Zur Erfüllung der Aufgaben im Bereich des öffentlichen Rechts arbeitet die Behörde als Technische Zentralstelle im Bauwesen, wobei die Wirkung über Deutschland hinaus reicht. So genannte Euro-Codes sind im Bauwesen europaweit eingeführt und partizipieren von den Arbeiten des DIBt. In Deutschland fungiert die Behörde als Zulassungsstelle für genormte Bauprodukte und Bauarten, sie ist technische Bewertungstelle auch für technische Bewertungen in Europa. Für das Land Berlin ist sie zudem für Zustimmungen im Einzelfall und vorhabenbezogene Bauart-Genehmigungen zuständig und ist bautechnisches Prüfamt.

2. Das DIBt

Das DIBt fungiert als Deutsche Zulassungsstelle für nicht genormte Bauprodukte und Bauarten, als Technische Bewertungsstelle (für Europäische Technische Bewertungen). Es kann die Zustimmung im Einzelfall und vorhaben-bezogene Bauartgenehmigungen für das Land Berlin aussprechen, Gutachten über die Einhaltung von Bauwerksanforderungen für Produkte und Gutachten auf Antrag der Länder oder des Bundes abgeben. Es ist das Bautechnisches Prüfamt. Ferner führt es die Aufgaben im sogenannten DIBt-Abkommen (einschl. Verwaltungsabkommen) aus, die zwischen den Bundesländern und dem Bund festgelegt wurden.

Es gibt 19 Aufgabenschwerpunkte, die von der Zulassungserteilung für innovative Bauprodukte über die Marktüberwachung bis hin zu Aufgaben im Bereich der Energieeffizienz von Gebäuden reichen. Es gibt kein vergleichbares bzw. weiteres Institut in Deutschland.

Das DIBt ist auch Anerkennungsstelle und notifizierende Behörde für Drittstellen und ist Gemeinsame Marktüberwachungsbehörde der Länder.

Ferner gehört zu seinen Aufgaben die Erstellung und Veröffentlichung der Muster-Verwaltungsvorschrift Technische Baubestimmungen (MW TB), die Anregung, Vergabe und Betreuung bautechnischer Untersuchungen sowie Bewertung von Bauforschungsberichten, die Registrierstelle für Energieausweise und Inspektionsberichte für Klimaanlagen nach dem Gebäudeenergiegesetz (GEG) sowie die Produktinfostelle für das Bauwesen. Zuletzt muss genannt werden, dass das DIBt die zuständige Behörde für den Schutz vor Radioaktivität in Bauprodukten gem. Strahlenschutzgesetz ist.

Das DIBt übt mit seinen Aufgaben verlässlich die Funktion einer zentralen Bewertungsstelle in einem föderalen Staat aus, von allen Ländern und dem Bund getragen.

Das Institut kann darüber hinaus:

Im europäischen und internationalen Raum arbeitet die fachlich orientierte Behörde mit.

- an der Ausarbeitung technischer Richtlinien und technischer Regeln im nationalen, europäischen und internationalen Bereich mitwirken
- in Gremien der Europäischen Kommission sowie sonstigen europäischen und internationalen Gremien mitarbeiten

3. GruSiBau 2022, Neuauflage (2 / 2)

Die Neuauflage der GruSiBau greift sämtliche Erkenntnisse der Zwischenzeit auf und führt darüber hinaus erweiterte Analysen ein, die auch in anderen Technikbereichen Betrachtung finden.

Ziel der Neuauflage ist die Fortschreibung der Erkenntnisse. Damit werden die Grundlagen für an Normung Beteiligte auf nationaler Ebene aktualisiert verfügbar gemacht; international nachvollziehbare, wissenschaftlich fundierte Vorschläge für die nächste Stufe der Eurocodes bereitgestellt.
Besonders hervorzuheben sind Betrachtungen zu „versteckten Sicherheiten“, zu nichtlinearen Grenzzuständen, zur Sensitivitätsanalyse und zu Aspekten der Geotechnik.

Damit wurde ein Beitrag zur Diskussion über die „Fortschreibung der Grundlagen der Sicherheitstheorie“ geleistet und der Fachöffentlichkeit vorgestellt. Eine parallele Betrachtung des vorgelegten Vorschlags und weiterer Ansätze, die bei der Überarbeitung der Eurocodes zur Anwendung kommen, erscheint sinnvoll und kann neue Potentiale und Forschungsperspektiven erschließen.

Sämtliche Vorgänge werden vom DIBt transparent der Öffentlichkeit zugänglich gemacht; die Ergebnisse der verschiedenen Arbeitsgruppen werden ebenfalls öffentlich bekannt gemacht, bevor dann nach diesen Fachgesprächen der neue Rechtsstatus veröffentlicht wird.

4. Ausblick aus Sicht der BGKdSI

Die verbindliche Umsetzung der GruSiBau ist in naher Zukunft zu erwarten und wird eine Bereicherung bei der Bearbeitung von Planungen im Bauwesen bringen.

Die Veröffentlichung „Technical Safety – An Attribute of Quality, An Interdisciplinary Approach and Guideline", ISBN 978-3-319-68624-0 ISBN 978-3-319-68625-7, (© Springer International Publishing AG 2018) ist der VDI-Gesellschaft für das Bauwesen vorgestellt worden und hat dort bezüglich der Abläufe in den Phasen des Lebenszyklus umfassende Zustimmung erhalten. Dabei geben die sechs Phasen Konzeption, Definition, Entwicklung und Konstruktion, Herstellung und Betrieb, Rückbau, Entsorgung und Recycling einen detaillierten Einblick in die gesamte Vorgehensweise. Eine deutschsprachige Version ist beim Beuth Verlag zu erhalten: „Das Qualitätsmerkmal „Technische Sicherheit" Denkansatz und Leitfaden" (ISBN 978-3-410-26296-4).

Die GruSiBau ist ein ganzheitlicher Ansatz.

Eine Sensitivitätsanalyse wie jetzt in der GruSiBau vorgesehen ist in diesem Ablauf (noch) nicht vorgesehen und sollte wegen der Bedeutung nicht nur für das Bauwesen grundsätzlich bedacht werden und ggf. in allen Fachbereichen eingeführt werden.

Die Sensitivitätsanalyse stärkt in jedem System dessen Resilienz.

SICHERHEITSHERAUSFORDERUNGEN AUS DWV-SICHT

Werner Diwald

1. Einleitung

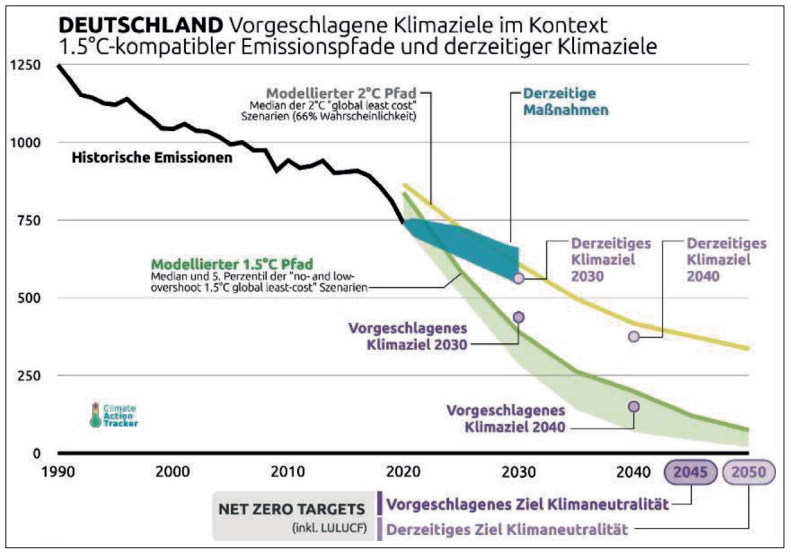
Die Technische Sicherheit und die Energetische Versorgungssicherheit müssen in allen nachfolgenden Bereichen erzeugt, auf Dauer vorgehalten und ggf. gestärkt werden. Der Gesamt-Prozess beginnt mit dem Planungsprozess, gefolgt vom Realisierungsprozess und endet mit dem Betriebsprozess. Auf die Erzeugung von Wasserstoff folgt fast immer die Speicherung. Die Nutzung einschließlich langfristiger Lagerung bzw. Umwandlung beinhalten auch stets den Transport. Die großen Bereiche der Anwendung sind Industrie, Mobilität und Gebäude.

Die Wasserstoff-Wirtschaft ist die Avantgarde!

2. Die Lage

Die Technische Sicherheit ist selbstbestimmt, während die energetische Versorgungssicherheit weitestgehend fremdbestimmt ist. Nach dem 24.2.2022 (Russlands Angriff auf die Ukraine) ist das deutlich für jedermann erkennbar, was zu enormen Anstrengungen zur Milderung dieses Zustandes führen muss.

Auf der Basis von technischer Sicherheit muss die Versorgungssicherheit gewonnen werden



Grüner Wasserstoff macht unabhängig, kostet aber finanzielle Anstrengungen.

Die EU-Kommission schätzt, dass bis 2030 zusätzlich 15 Millionen Tonnen erneuerbarer Wasserstoff 25-50 Mrd. m³ pro Jahr importiertes russisches Gas ersetzen können (10 Mio. Tonnen importierter erneuerbarer Wasserstoff aus verschiedenen Quellen und 5 Mio. Tonnen mehr in Europa produzierter erneuerbarer Wasserstoff, zusätzlich zu den bereits geplanten 5 Mio. Tonnen), was aber mit mehr als 500 Mrd. EUR Investitionen bis 2030 abgegolten werden muss.

Die Versorgungssicherheit mit Grünem Wasserstoff ist herstellbar, allerdings ist sie nur mit **gemeinsamem Handeln** erreichbar.

Grüner Wasserstoff kann überall erzeugt werden, günstig aber in Gegenden mit viel Sonne und viel Wind bei wenig Eigenbedarf.

Um diese Versorgungssicherheit für Grünen Wasserstoff herzustellen und dann langfristig zu garantieren, müssen alle Beteiligten wirklich gemeinsame Anstrengungen unternehmen und auf Dauer beibehalten. Die Vorteile einer Europäischen Grünen Wasserstoffunion liegen auf der Hand. Es gibt viele Orte auf der Welt, an denen die Kosten für die Produktion von Grünem Wasserstoff niedrig sind – sogar niedriger als für einige fossile Energieträger. Als ein interessantes Beispiel sei hier Westafrika genannt: Viel Sonne, viel Wind und ein niedriger Eigenbedarf der Bevölkerung, so dass die Produktion als Überschuss anderweitig genutzt werden kann.

Die Transportsicherheit ist ein entscheidender Faktor in der Sicherheit des Gesamtsystems.

Allerdings ist die Produktion allein noch nicht der Schlüssel für eine Versorgungssicherheit in Europa. Hier tritt in den Vordergrund der Transport vom Ort der Produktion zum Ort der Verwendung. Und dabei gilt es insbesondere, die Technische Sicherheit, die Wirtschaftlichkeit und die Nachhaltigkeit zu maximieren.

3. Die Aufgaben

Die Versorgungssicherheit in Europa wird einhergehen mit der Industrie- und Wirtschaftsentwicklung auf unserem Kontinent, wenn die geopolitische Stabilisierung in und um die EU herum gelingt. Dazu muss die Europäische Grüne Wasserstoffunion ihren bedeutenden Beitrag leisten. Insbesondere sind sämtliche möglichen Produktionsstandorte zu vernetzen, also neben schon vorhandenen Verbindungen auch solche in den südeuropäischen Raum.

Für eine europäische und grüne Wasserstoff-Union müssen alle Produktionsstandorte vernetzt werden.

Man muss sich klarwerden, dass Sonne und Wind handelbare Werte darstellen und gelungene oder geplante Prozesse des Strukturwandels für alle Energieträger von herausragender Bedeutung sind.

Sonne und Wind als Basis für ein neues Wirtschaftswunder.

Mit den angeschobenen und geplanten Projekten in der EU kann es gut gelingen, und zwar im besten Fall so, dass ein neues Wirtschaftswunder Platz greift.

4. Aussicht

Bündeln wir günstige Produktionen mit nachhaltigen und wirtschaftlichen Transporten derart, dass in den Produktionsstandorten der Grüne Wasserstoff ausreichend zur Verfügung steht, dann gelingt ein Beitrag zur Klimaschonung nebst langfristiger Wirtschaftlichkeit. Die politischen Weichenstellungen für Technische Sicherheit und Versorgungssicherheit sind erkennbar im genügenden Umfang gestellt. Die Wasserstoffmarktwirtschaft wird greifen, politisch mutiges und weitsichtiges Handeln auf Dauer vorausgesetzt.

Der Hochlauf der Wasserstoffwirtschaft gelingt mit guter Politik.

Klimaziele erreichen und Energieversorgung sichern.

5. Anmerkung aus Sicht der BGKdSI

Der Deutsche Wasserstoff-Verband e.V. (DWV)1 vertritt seit 1996 die Interessen seiner Mitglieder für die Förderung eines schnellen Markthochlaufs des Energieträgers Wasserstoff und der Brennstoffzellentechnologie. Das Ziel ist, die Grüne Wasserstoff-Marktwirtschaft als Bestandteil einer nachhaltigen, wirtschaftlichen und versorgungssicheren Energiewirtschaft voranzutreiben. So können die Klimaziele effizient erreicht und gleichzeitig der Erhalt der Versorgungssicherheit gewährleistet werden.

Der DWV sorgt für die richtigen Rahmenbedingungen.

Wasserstoff, der mit erneuerbaren Energien erzeugt wird, nimmt dabei eine entscheidende zentrale Rolle ein. Im Mittelpunkt der Verbandsaktivitäten stehen die Implementierung und Optimierung der erforderlichen marktwirtschaftlichen, technologischen und ordnungsrechtlichen Rahmenbedingungen für die Wasserstoffwirtschaft in den Bereichen Anlagenbau, Erzeugung, Transportinfrastruktur und Anwendungstechnologien.

In der deutschen Wirtschaft stellt der DWV eine feste Größe dar.

Um diese Herausforderungen global zu lösen, setzt sich der DWV auch für eine internationale nachhaltige Zusammenarbeit ein. Die 400 persönlichen Mitglieder und über 180 Mitgliedsinstitutionen und -unternehmen stehen für bundesweit mehr als 1,5 Millionen Arbeitsplätze. Der Verband repräsentiert somit einen bedeutenden Teil der deutschen Wirtschaft.

SICHERHEITS- UND VERTEIDIGUNGSFORSCHUNG IM DEUTSCHEN ZENTRUM FÜR LUFT- UND RAUMFAHRT

Michael Langerbeins

1. Einleitung

Das DLR.

Michael Langerbeins vom Deutschen Institut für Luft und Raumfahrt stellt zunächst das DLR vor, was in der Praxis der Konferenz die Kontinuität der Mitarbeit des DLR darstellt:

Das DLR beschäftigt über 10.000 Mitarbeiter deutschlandweit an 30 Standorten in 55 Instituten und Einrichtungen sowie 178 Großforschungsanlagen.

Sicherheitsforschung in der Wehrtechnik und im zivilen Bereich.

Es gliedert sich weiter in Wehrtechnische und Zivile Sicherheitsforschung, wobei die erste sich weiter untergliedert in Satellitentechnik und Sensorik, Luftgestützte Plattformen & Mensch-Maschine-Interaktion, Wirkung, Werkstoffe und Cyber-Sicherheit sowie Reaktionsschnelle Satellitenverbringung. Die zivile Seite enthält Sicherheit und Dual-Use sowie Maritime Sicherheit.

Zivile Sicherheitsforschung mit rund 11 Millionen Euro pro Jahr.

Die zivile Sicherheitsforschung im DLR umfasst aber weit mehr als die aktuell 25 aus dem DLR-Programm Zivile Sicherheitsforschung mit einem Volumen von rund elf Millionen Euro p.a. finanzierten Projekte – Beispiel: DLR-Zentrum für satellitengestützte Kriseninformation (ZKI) als Einrichtung der Raumfahrt.

Es gibt auch sog. Fokus-Projekte, die gemeinsam mit Behörden und Organisationen für Sicherheitsaufgaben (BOS) durchgeführt werden (z.B. SiFoPolis mit BKA, PHYLAXmit BPol, Livelage mit Fw Duisburg etc.).

Das erste Institut für den Schutz maritimer Infrastrukturen wird seit 2017 aufgebaut, seit 2019 wird das zweite Institut dazu errichtet.

Dual-Use Themen werden eng mit der Wehrtechnischen Forschung abgestimmt und teilweise gemeinsam finanziert (z.B. Detektion

von Gefahrstoffen, Weltraumlage etc.), also eine optimale Ausnutzung von Synergien.

Als Beispiele aus der Maritimen Sicherheitsforschung seien hier die Projekte TRAGVIS (u.a. Seenotrettungsunterstützung und Schlechtwettersichtverfahren) und DEoL (Drohnendetektion mittels Erweiterung optischer Lernverfahren) und eine Unterstützung der Polizei bei einem Castor-Transport per Schiff genannt. ([14]):

Aus der maritimen Sicherheitsforschung: Drohnendetektion und Polizei-Unterstützung bei Castortransporten.

2. Institut für den Schutz terrestrischer Infrastrukturen

Das Institut für den Schutz terrestrischer Infrastrukturen ist 2019 gegründet worden. Mit Stand 10/2022 gibt es ca. 50 MA an verschiedenen Standorten, Hauptsitz: Sankt Augustin. Es forscht im Bereich der

- Resilienz- und Risikomethodik
- von Detektionssystemen
- zu Digitalen Zwillingen für Infrastrukturen
- und der Simulationsmethoden für Digitale Zwillinge

Es bestehen Kooperationen mit Hochschulen, insb. UniBw München, und Partnerschaften mit Industrie und BOS.

Das Aufgabenfeld ist weit gefasst, es reicht vom Schutz und der Rettung des Menschen mit Optischer Aufklärung, Kooperationen & Soforthilfe über den Schutz kritischer Infrastrukturen (Gefahrstoffdetektion Technologietransfer) bis zum Schutz vor Kriminalität und Terrorismus (Polizeistreifenoptimierung, Kooperationen).

Im weiten Spektrum der Arbeiten ist auch die Gefahrstoff-Detektion enthalten.

3. Aufgaben und Kompetenzen in der wehrtechnischen Forschung

Hier sind drei Bereiche festzuhalten:

- Beiträge zur Bedarfsdeckung und Schließung von Fähigkeitslücken der Bundeswehr sowie für den Erhalt und Ausbau von militärischen Fähigkeiten
- Verfahren und Anlagen zur Demonstration, Erprobung und Bewertung wehrtechnische relevanter Technologien
- Mission: Beiträge für Erhalt und Ausbau der Analyse und Bewertungsfähigkeit des BMVg, PlgABw, BAAINBw, und der nachgeordneten Dienststellen

Enge Zusammen- und Zuarbeit mit ministeriellen Stellen.

Die Umsetzung / Themen der wehrtechnischen Forschung im Einzelnen:

- umfasst mehr als 42 Technologievorhaben sowie multi- und interdisziplinäre Projekte
- befasst sich mit Forschung- und Entwicklungsarbeiten für
- bemannte- und unbemannte Plattformen
- Interaktion zwischen Menschen und Maschine
- unterschiedliche Sensorik, u.a. Laser, Radar und Optik
- luft- sowie raumgestützte Gesamtsysteme

Fokus: aus Forschungsaktivitäten erzielter Erkenntnisgewinn und Überführung in die Anwendung

Das Dutch Safety Board (DSB) als Vorbild für Deutschland

Dr.-Ing. Bernd Schulz-Forberg
Forum46 e.V.

1. Einleitung

Der Nobelpreisträger Svante Pääbo ist für seine Forschungen auf dem Gebiet der Paläogenetik ausgezeichnet worden Seine Ausführungen belegen u.a., dass der Homo Sapiens in der Lage ist, **Koalitionen einzugehen und Kompromisses zu schließen**. Wir leben in einer Gesellschaft, die sich bis heute gut fortentwickelt hat und insbesondere in den westlichen Industrienationen an einen Wendepunkt angekommen zu sein scheint. Die Erkenntnis, dass man den Bereich der Technik nicht mehr isoliert betrachten kann, setzt sich durch, wenn auch langsam. Wir leben in einer **sozio-technischen Gesellschaft**, will sagen, wir müssen alle interessierten Gruppen in der Gesellschaft zusammenbringen, um diese sozio-technische Gesellschaft gemeinsam weiterzuentwickeln.

Technik muss Teil des sozio-technischen Systems sein.

2. Das Lernen aus Ereignissen

Das Lernen aus einzelnen Ereignissen (Zwischenfälle, Unfälle, Katastrophen) stand im Vordergrund und ist bis heute von herausragender Bedeutung, insbesondere vor dem Hintergrund des Einflusses auf die Regelfortentwicklung bei sehr einschneidenden Ereignissen bzw. bei der Häufung ähnlicher Ereignisse.

Lernen aus Ereignissen.

Der Lerneffekt in Sachen Technik und Organisation wird durch die größere Anzahl von Ereignissen, also auch der Beinahe-Ereignisse, gestärkt. Raumzeitlich weit vor den auftretenden Ereignissen sind häufig Design-, Konstruktions-, Wartungs- und Managementfehler gelagert, die einen Einfluss auf die Ausprägung des beobachtbaren Ereignisses haben. Es stellt sich daher die zusätzliche Aufgabe, diese Fehler vorbeugend zu vermeiden.

Auslösende Elemente und vorlaufende Fehlhandlungen müssen zusammen betrachtet werden.

Menschen lernen aus Erfahrung, hauptsächlich aus Fehlern; Organisationen lernen aus Ereignissen einschließlich Beinahe-Ereignis-

sen, die systematisch analysiert werden müssen. Eine **Neuausrichtung der Fehlerkultur** in Deutschland hin zu einer **Lernkultur** ist das Gebot der Zeit. Ein erstmalig auftretender Fehler muss so breit als irgend möglich kommuniziert werden, und bei der Ahndung des Fehlers ist ggf. der gewonnenen Lerneffekt zu berücksichtigen.

Von der Fehlerkultur hin zur Lernkultur

Die nichtmeldepflichtigen und die Beinahe-Ereignisse sind von besonderer Bedeutung, weil in ihnen ein hohes Erkenntnis-Potenzial steckt. Es gilt bei sämtlichen Ereignisanalysen darauf zu achten, dass die unmittelbar auslösenden Faktoren für ein Ereignis bekannt und gewichtet werden, ihre Zusammenhänge und Abhängigkeiten analysiert werden und diese dann vor allem in Zusammenhang mit systemimmanenten Schwachstellen gebracht werden, die zusammen mit den auslösenden Faktoren die ganze Matrix der Faktoren beschreiben. Dazu müssen die Strukturen der Ereignisdaten und auch die der Auswertung stärker normiert werden.

Vor dem Hintergrund der oft nachhaltigen Folgen von Ereignissen und Störfällen ist es humane Pflicht, die Ressourcen für die Datenerfassung, ihre Strukturierung und letztlich auch ihre Verbreitung bereit zu stellen, was für die volkswirtschaftliche Gesamtrechnung (VGR) sicher als Nutzen beschrieben werden kann. Sämtliche Ereignisdaten aus allen Technik- bzw. Rechtbereichen müssen primär einer fachlichen Analyse zugeführt werden, so dass die Erkenntnisse aus dem Handeln in der Technik, unabhängig vom Rechtsbereich, in ihren Auswirkungen bekannt werden und Analogiebetrachtungen erfolgen können.

Fachliche Bewertung geht vor rechtliche Würdigung.

Vor dem Hintergrund der SEVESO-Richtlinien und der darin u.a. geforderten **Risikoanalyse** soll noch auf die notwendige Behandlung des Begriffes Risiko in seiner vielfältigen Ausprägung hingewiesen werden. Hier gibt es Nachbarstaaten in Europa, die diese Methodik schon entwickelt und angewendet haben, z. B. das Vereinigte Königreich, die Niederlande und die Schweiz. Der Gesundheitsbereich in Deutschland hat schon eine Institutionalisierung vorgenommen in Form eines Bundesinstituts für Risikobewertung. Er hat genauso wie der Anlagenbereich die Risikokommunikation aufgegriffen. Auch im Bereich des Verkehrsrechtes gibt es gute Anfänge und Ansätze, ganz zu schweigen von den Verkehrsträgern Luft und See im Besonderen. Allerdings müssen wir in Deutschland noch die Ressortgrenzen durchlässiger machen, damit Technikfelder untereinander den Austausch pflegen und die Datenlage optimieren können.

Risikobetrachtungen ermöglichen und Ressort-Grenzen durchlässig machen.

3. Beispiele

Hier folgt eine beispielhafte Aufzählung von Ereignissen, um die Bedeutung des Anliegens zu unterstreichen.

- **The 2017 MAERSK Cyber Incident**
  (Ein Cyberangriff auf die Reederei konnte nur durch einen zufälligen Stromausfall einer Maersk-Depandanz in Afrika finanziell in Grenzen gehalten werden)

- **Aircraft Accident Report**
  (Die FAA der USA haben den Beinahe-Flugunfall einer Tristar auf ungenügende Überwachung und mangelhafte Ausbildung der Servicekräfte zurückgeführt)

- **Petrobras**
  (Die Bohrinsel war durch Fehlhandlungen des Managements stark vorgeschädigt, eine Begehung durch Det Norske Veritas konnte den Totalausfall der Plattform nicht verhindern)

- **Brustimplantate**
  (Billige Brustimplantate führten zu Personenschäden; der TÜV war nur beauftragt, das Verfahren zu überprüfen, nicht also selbst Prüfungen vorzunehmen)

- **Magnetschwebebahn im Emsland**
  (Der Transrapid-Unfall mit mehreren Toten wurde von juristischer Seite untersucht und falsche Schuldige zeitnah gefunden; die eigentlichen Fehlhandlungen – mehrere – wurden nicht festgestellt)

Eine einheitliche Ereignis-Behandlung muss geplant und umgesetzt werden.

4. Fazit

Hier schließt sich der Kreis und es wird deutlich, dass in den soziotechnischen Systemen sämtliche Einflussfaktoren gebührend berücksichtigt werden müssen, um tragfähige Ergebnisse und damit Erkenntnisse zu gewinnen. Das Dutch Safety Board der Niederlande sollte auf Übertragbarkeit für Deutschland geprüft werden, wobei die Größenunterschiede beider Staaten zu berücksichtigen sind, wie auch der föderale Aufbau Deutschlands einzubeziehen ist.

WORK AND RESULTS OF THE DUTCH SAFETY BOARD

Arbeitsweise und Ergebnisse des niederländischen Sicherheitsrates

Lex van Delden [1]

[1] Investigationsprozess im Dutch Safety Board
(Der Vortrag „Work and Results of the Dutch Safety Board" von Lex van Delden wird auf der Website des Forum46: https://www.forum46.eu bekannt gemacht.)

1. Einleitung (Einschub von der BGKdSI)

Nach 20 Jahren findet in der BGKdSI ein Austausch unter Fachleuten statt!

Im Jahr 2004 hat Herr Pieter van Vollenhoven als damaliger Leiter des Dutch Safety Board (DSB) in der Bundesanstalt für Materialforschung und -prüfung (BAM) das DSB vorgestellt und angeregt, dass die Bundesrepublik Deutschland sich an diesem Beispiel orientieren möge und anschließend zusammen mit den Niederlanden diese Konstruktion der Ereignisbehandlung in der EU vorstellen könnte. Der damalige Präsident der BAM wie auch der damalige Vorsitzende der Störfallkommission des BMU sagten eine Verfolgung der Angelegenheit zu.

„Gut Ding will Weile haben."

2. Geschichte und Gründung des niederländischen Sicherheitsrates

Ausgehend von spektakulären Unfällen bzw. einer auffälligen Häufung von kleineren Unfällen hat die Gesellschaft in den Niederlanden die nachstehenden Organisationen nach und nach ins Leben gerufen:

1909: Seeschifffahrtsgericht der Niederlande
1939: Binnenschifffahrt-Ausschuss für Unfälle
1932: Ausschuss für Zivilluftfahrt
1956: Ausschuss zur Untersuchung von Eisenbahnunfällen
1977: Ausschuss für Straßenverkehrssicherheit
1999: Verkehrssicherheitsrat
2005: Ausschuss für Verkehrssicherheit, Einsetzung des DSB am 7. Februar 2005

Alle Ereignisse aus sämtlichen Verkehrsbereichen werden zentral untersucht.

Der vorläufige Abschluss im Jahre 2005 fasst demzufolge alle Ereignis-Untersuchungen auf sämtlichen Verkehrsträgern zusammen: Unerwünschte Vorkommnisse wurden von Fall zu Fall untersucht, einzelne Verkehrssicherheitsausschüsse wurden gegründet, und dann erfolgte eine Zusammenfassung in einem einzigen Verkehrssicherheitsausschuss. Letztlich erfolgte die Gründung des niederländischen Sicherheitsausschusses nach den Motti: unabhängige staatliche Organisation, aus Ereignissen lernen und keine Schuld- und Haftungsfragen behandeln.

Der DSB ist eine unabhängige staatliche Einrichtung für sämtliche Ereignis-Untersuchungen.

3. Struktur des niederländischen Sicherheitsrates

Ein Generaldirektor wird unterstützt von einem Kommunikationsmanager und einem Verwaltungsmanager sowie zwei Leitern von entsprechenden Ermittlungsbüros.

In den Abteilungen werden die Ermittlungen im Einzelnen behandelt, wobei auch Chemieanlagen und das Bauwesen im DSB untersucht werden. Die Mission lautet in allen Abteilungen, die Sicherheit in den Niederlanden zu steigern und zu stärken. Die Betonung liegt immer auf der Unabhängigkeit, der Transparenz und der Professionalität.

Zwei Ratsmitglieder werden von sieben assoziierten Ratsmitgliedern unterstützt, ferner stehen dem Büro des Generaldirektors vier weitere Manager zur Verfügung. Insgesamt sind mehr als 70 Personen beschäftigt, in der Mehrzahl handelt sich dabei um Ermittler. Man arbeitet in 15 Sektoren und Domänen und verfolgt gemeinsam die Steigerung der Sicherheit in den Niederlanden aufgrund von Unabhängigkeit, Transparenz und Professionalität.

Professionalität, Unabhängigkeit und Transparenz sind gewährleistet.

4. Internationaler und nationaler Rechtsrahmen

Im internationalen Bereich handelt das DSB in den Sektoren Luftfahrt, Schifffahrt, Eisenbahn, Chemische Industrie und Verteidigung.

Im nationalen Bereich greifen die Dekrete des Kingdom Act Dutch Safety Board sowie weitere übliche staatlichen Regelungen. Das gesetzliche Rahmenwerk stellt somit sicher, dass nur verpflichtende

und zulässige Untersuchungen vorgenommen werden. Die Unabhängigkeit der Untersuchung ist garantiert, die Ermittlungsbefugnisse sind ausreichend, wobei auch der Schutz vor unzulässigen Untersuchungsinformation für andere gewährleistet ist. Die Zielrichtung ist stets, die fachlichen Gründe für das Ereignis festzustellen und demzufolge nicht die Schuld-und Haftungsfrage zu klären. Die notwendige Koordinierung mit Staatsanwaltschaft, Polizei und Verteidigung ist in jedem Einzelfall vorzunehmen.

Die Federführung liegt beim DSB, der gegebenenfalls die Koordination mit Staatsanwalt, Polizei und Verteidigung organisiert.

Die Aufgabe besteht also darin, eine Einzeluntersuchung vorzunehmen bzw. eine Kategorie von Ereignissen zu untersuchen und die jeweiligen Konsequenzen abzuschätzen. Als Ziel gilt in jedem Fall, die Verhinderung ähnlicher Vorkommnisse und die Begrenzung der Folgen. Das Ergebnis der Arbeiten wird im Bericht niedergelegt und falls erforderlich werden Empfehlungen ausgesprochen

Die DSB-Untersuchungen werden in einem öffentlichen Bericht vorgelegt; ggf. mit Empfehlungen.

5. Ermittlungsbefugnisse

Die Befugnisse der Ermittler sind weitreichend und beginnen mit der Konservierung des Zustandes eines Ereignisses durch die Behörde. Wenn nötig, können Objekte für die Untersuchungen zur Verfügung gestellt werden. Ferner ist der Zugang der Ermittler zu allen Orten einschließlich von Mannschaftsquartieren auf Schiffen jederzeit möglich. Man hat das Recht, jegliche Information zu erbitten und relevante Daten und Dokumente für die Inspektion einzusehen. Alle Objekte können inspiziert werden und gegebenenfalls können Proben entnommen werden.

Die Ermittler des DSB haben umfassende Befugnisse.

Jedermann ist verpflichtet, mit den Ermittlern zu kooperieren, wobei die Ausnahmen restriktiv festgelegt sind. Schließlich ist die Nicht-Kooperation nach Art.184 des niederländischen Strafgesetzbuches zu ahnden.

Die Ermittler müssen offiziell unterstützt werden; Nichtbeachtung ist strafbar.

6. Schutz von Untersuchungsinformationen

Sensitive Daten können gegebenenfalls geschützt werden und demzufolge nicht Bestandteil des Berichts der Ermittler sein. Endgültige Berichte sind für die Öffentlichkeit, alle Informationen aus den Ermittlungen nicht. Der Abschlussbericht kann nicht als Beweismittel verwendet werden.

Sensitive Daten können geschützt werden.

Datenaufzeichnungen, Ermittler, Zeugen oder Sachverständiger in Gerichtsverfahren sind geschützt. Es gibt keine Anzeigen von Straftaten, die während der Ermittlungen festgestellt wurden und es gilt eine Verschwiegenheitspflicht für die an der Untersuchung Beteiligten.

Die Verschwiegenheitspflicht ist gegeben.

Datenschreiber sind nicht als Beweismittel in Gerichtsverfahren zugelassen, eine Einsichtnahme kann nicht verlangt werden. Ausnahmen bestehen bei Geiselnahme, Mord, Totschlag und Terrorismus.

Zusammenfassend kann herausgestellt werden, dass die obligatorischen Ermittlungen stets eine Garantie für unabhängige Untersuchungen garantieren und die Ermittler über weitreichende Befugnisse verfügen. Zeugen und ggf. weiteres Personal sind stets ausreichend geschützt. Zudem wird generell ohne Schuld- und Haftungsbelange ermittelt. Insbesondere durch diese Stellung des DSB wird das Lernen aus Ereignissen sehr gefördert.

Ausnahmen zur Einsichtnahme nur bei Kapitalverbrechen.

7. Ermittlungsverfahren

Das Verfahren läuft folgendermaßen ab: Bevor die eigentliche Untersuchung eingeleitet wird, muss geprüft werden, ob es sich um eine verpflichtete Untersuchung handelt. Dann wird der Schwerpunkt der Untersuchung festgelegt und ein Aktionsplan aufgestellt. Anderenfalls erörtert der Ausschuss zunächst die Vor- und Nachteile

Unabhängige Ermittlungen steigern das Lernen aus Ereignissen.

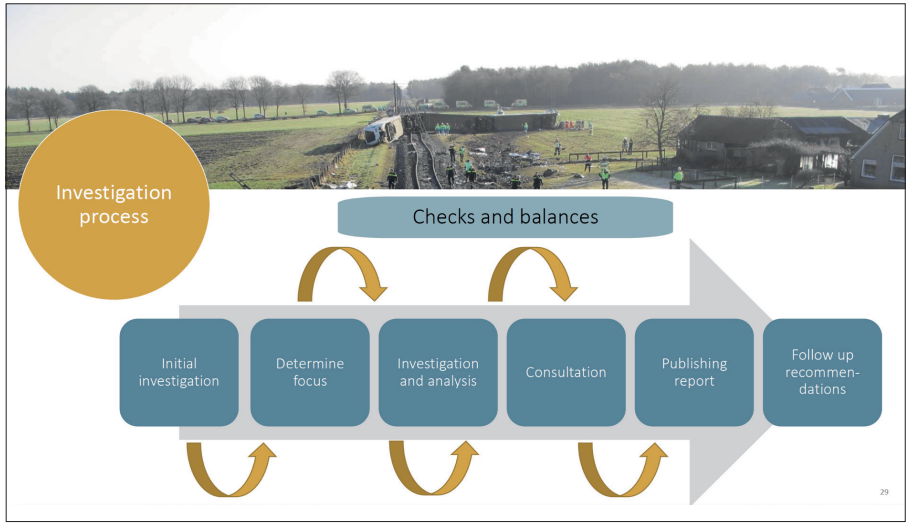
einer Untersuchung. Wird eine Untersuchung befürwortet, werden wie o.a. der Schwerpunkt und der Aktionsplan festgelegt. Fast alle unsere Untersuchungen sind eine Kombination aus Vor-Ort- und Schreibtisch-Recherchen, einschließlich zahlreicher Interviews mit beteiligten Personen und Organisationen. Das Dokument, in dem der Schwerpunkt der Untersuchung, die zu behandelnden Fragen und der Aktionsplan beschrieben sind, wird von einer ausgewählten Anzahl von Kollegen überprüft, die nicht an der Untersuchung beteiligt sind. Ihre Rolle ist die des „Advokaten des Teufels", der gegen die Idee/den Plan argumentiert, um den eigentlichen Ermittlern zu helfen, einen besser begründeten Ermittlungsplan zu erstellen. Dieselbe Routine wird durchgeführt, wenn das Untersuchungsteam einen ersten Entwurf eines Berichts verfasst hat und kurz vor dem endgültigen Entwurf eines Berichts. Darüber hinaus werden bei bestimmten Untersuchungen zusätzliche Ermittler mit speziellen Fachkenntnissen eingeschaltet.

Nach der Planungsphase folgt die Ermittlungsphase; am Schreibtisch oder vor Ort.

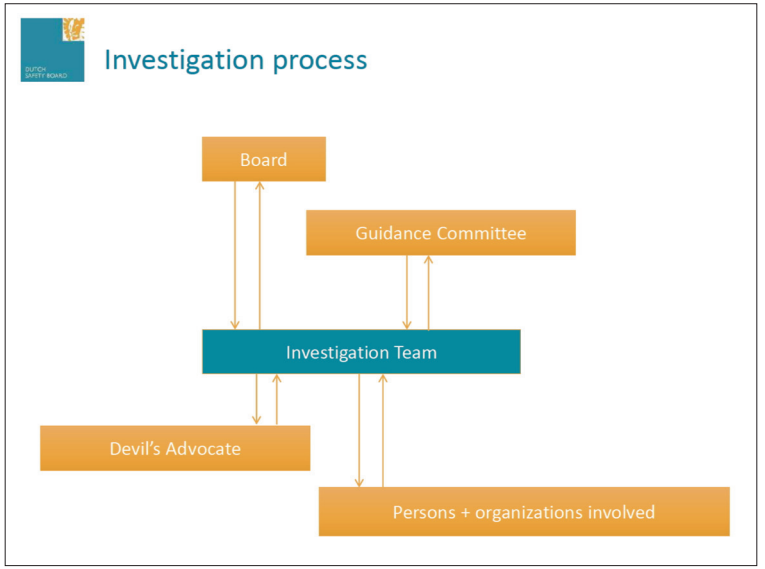
„Des Teufels Advokat"

Die Ermittlung schließt mit einem Bericht ab; Empfehlungen werden langfristig beobachtet.

Das nachstehende Bild ergibt einen Überblick über die einzelnen Schritte im Ermittlungsverfahren:



Abschließend ergibt das nachstehende Bild einen sehr generellen Überblick über die verschiedenen beteiligten Institutionen an dem Ermittlungsprozess.



8. Fallstricke

Herausragendes Ziel der Untersuchungen ist stets das Lernen aus den Ereignissen wie auch die Verringerung der Folgen.

Das Vertrauen in Professionalität, Unabhängigkeit und Transparenz muss ständig neu erworben werden.

In der öffentlichen Debatte und in den Sozialen Medien können aber Missdeutungen die Oberhand gewinnen und letztlich Argwohn gegen die Untersuchungen erzeugen. Ermittlungen in unbekannten Gefilden führen leicht zu einem Verlust an Vertrauenswürdigkeit und das Infragestellen der Unabhängigkeit des DSB. Ungenügende Expertise kann auch die Glaubwürdigkeit und die Vertrauenswürdigkeit beschädigen. Eine derartige Schräglage in der Öffentlichkeit kann auch die Fokussierung auf die Frage von Schuld und Haftung in den Vordergrund stellen und damit den eigentlichen Lerneffekt reduzieren.

Leistungsüberblick der ci-tec GmbH Karlsruhe (Dr. Hubert B. Keller, ci-tec)

Wir optimieren Ihre Prozesse.

Wir entwickeln **nachhaltige und innovative Lösungen**, die den neuesten Stand der Wissenschaft und Technik in die industrielle Praxis überführen. So unterhalten wir **langjährige, partnerschaftliche Kundenbeziehungen** zu Industrieunternehmen weltweit, die ihre Anlagen mit unseren Lösungen klimafreundlicher, ressourcen-schonender, effizienter und damit auch rentabler machen.

Energieeinsparung, Erhöhung der Laufzeiten, Steigerung des Durchsatzes, Sicherung der Produktqualität und letztlich erhebliche Kosteneinsparungen sind mit unseren Lösungen direkt erreichbar. Unser System **inspect pro control** realisiert für Sie auf Basis von Infrarot-Sensor/Daten messbare Einsparpotenziale in Ihren thermischen Prozessen wie Sonderabfall, Zement, Zink, Siliziumherstellung etc. Überzeugen Sie sich von unserem System bei einem unserer Partner vor Ort oder durch eine Testmessung bei Ihnen.

Unsere Expertise beinhaltet den Einsatz von **Verfahren der künstlichen Intelligenz (KI)** auf Ihren Prozessdaten, um datenbasierte Analysen, Modellierungen und Optimierungspotenziale zu generieren. Zudem unterstützen wir Sie in der Transformation zur **Dekarbonisierung** Ihrer Prozesse. Ob Wasserstoff oder andere regenerative Energieträger, wir bieten Ihnen forschungsbasierte Dienstleistungen zur Anpassung Ihrer Prozesse an.

KI-Engineering

Methoden der Künstlichen Intelligenz eröffnen neue Möglichkeiten, das Potential bereits vorhandener Daten auszuschöpfen und Systeme/Prozesse datengetrieben zu analysieren und zu optimieren. So können in allen Arten von Anlagen kontinuierlich gemessene Sensordaten intelligent verknüpft werden, um aussagekräftige **Kenngrößen** für die aktuelle System-/Prozessqualität in Echtzeit zu berechnen. Insbesondere dort, wo z. B. die Prozessführung sich auf stichprobenartige Laborbewertungen der produzierten Produktqualität stützt, bietet die Ergänzung der Laboranalyse um eine kontinuierliche **Echtzeit-Schätzung** der relevanten Qualitätsmerkmale einen erheblichen Mehrwert für die Optimierung und ggf. sogar neue, innovative Regelungsmöglichkeiten. Aber auch bei Bauwerken kann auf Basis von nicht invasiven Messdaten eine **Zustandsanalyse** erfolgen. Unsere KI Expertise stützt sich auf jahrelange Erfahrung und umfangreiche Projekte.

Kontakt: ci-tec GmbH, info@ci-tec.de, Beuthenerstraße 16, 76139 Karlsruhe, www.ci-tec.de

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 in der Wagnisgesellschaft 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.