Methodischer Ansatz für ein interdisziplinäres Konzept zur Sicherheitstechnik

Dipl.-Ing. Wolf-Dieter Pilz VDI
[Vorsitzender des VDI-Ausschusses „Technische Sicherheit“]

34. Sicherheitswissenschaftliches Kolloquium
10. Juli 2007
Bergische Universität Wuppertal - Institut ASER e.V.

Erwartungshaltung der globalen Märkte

- **Deutsche Ingenieursleistungen werden weltweit unter dem Begriff „Made in Germany“ subsumiert.**
- **„Made in Germany“ steht hierbei für Qualität und Sicherheit der industriellen Erzeugnisse aus Deutschland.**
- **Die Märkte der Welt erwarten:**
  - ⇒ Innovative Technologie,
  - ⇒ angemessene Lebensdauer,
  - ⇒ uneingeschränkte Gebrauchstauglichkeit,
  - ⇒ Zuverlässigkeit,
  - ⇒ wirtschaftliche Verfügbarkeit und
  - ⇒ **Technische Sicherheit**.
- **Diese Erwartungen richten sich an alle Ingenieure, – bisher jedoch in fachspezifisch unterschiedlicher Ausprägung.**

„Technische Sicherheit“ im Umfeld „Technik“

- **Technik = Anwendung der Ingenieurswissenschaften**
- **Ingenieurswissenschaften sind eine „Wachstumsbranche“**
- **Die Zahl der Fachdisziplinen nimmt ständig zu**
- **Der Wissensumfang innerhalb der Fachdisziplinen wächst**
- **Technik bedarf eines zweckdienlichen Managements**
- **Technisches Management ist gängige Praxis bei:**
  - ⇒ Technischen Projekte,
  - ⇒ Technologischer Innovation,
  - ⇒ Qualität (z.B. gemäß DIN EN ISO 9000),
  - ⇒ Technische Zuverlässigkeit (einschl. wirtschaftlicher Verfügbarkeit),
- **Technisches Management erfolgt meist interdisziplinär**

Interdisziplinäre Technik – das ist doch bekannt!

- **Die Technik gliedert sich sowohl nach Branchen als auch nach technischen Fachdisziplinen, wie sie sich z.B. in den Fachgliederungen des Vereins Deutscher Ingenieure reflektieren.**
- **Bei technologischen Innovationen wirken die technischen Fachdisziplinen meist zusammen, was gelegentlich zu neuen Fachdisziplinen führt.**
- **Der VDI fördert das interdisziplinäre Zusammenwirken der technischen Fachdisziplinen untereinander:**
  - ⇒ „Grundsatzfragen von Forschung, Technologie und Innovation“,
  - ⇒ „Technikbewertung“,
  - ⇒ „VDI-Gesellschaft Systementwicklung und Projektgestaltung“.

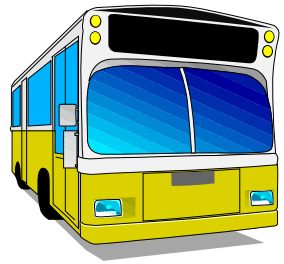
Interdisziplinäre Sicherheitstechnik – was ist das?

- **Die Sicherheitstechnik ist k e i n e eigenständige technische Fachdisziplin; sie ist in diesen jeweils integriert, die sich ihrerseits im Recht abbilden.**
- **Die Grundsätze des „Human Factors Engineering“ *) sind weder in den technischen Fachdisziplinen noch im „Sicherheitsrecht“ durchgängig und systematisch entfaltet.**
- **Technologische Innovationen bedingen nicht nur den interdisziplinären Rückgriff auf die verschiedenen technischen Fachdisziplinen, sondern auch auf**
  - ⇒ das „Sicherheitsrecht“ und das
  - ⇒ „Human Factors Engineering“.

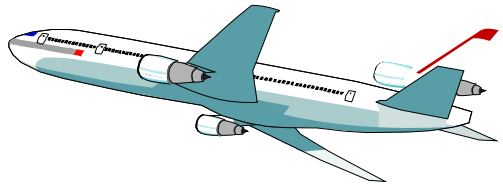
*) Neues Konzept der Beteiligung humanwissenschaftlicher Erkenntnisse in technische Entwicklungsprozesse (bislang nicht konsequent genutzt).

Beispiele für Sicherheitsrecht und -technik im Technikfeld „Verkehrssysteme“ (1)

- **Sicherheit bei Straßenfahrzeugen:**
  - ⇒ Straßenverkehrs-Zulassungs-Ordnung,
  - ⇒ Kraftfahrt-Bundesamt,
  - ⇒ Stand der Technik (unbestimmte Verweisung in Rechtsvorschriften),
  - ⇒ Sicherheitsverantwortung: Halter (bzw. Hersteller).

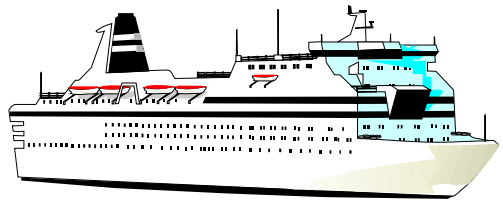


- **Sicherheit bei Luftfahrzeugen:**
  - ⇒ Prüfordnung für Luftfahrtgerät,
  - ⇒ Luftfahrt-Bundesamt,
  - ⇒ Zulassungsverfahren (zugel. Luftfahrtbetrieb, Joint Airworthiness Reg.),
  - ⇒ Sicherheitsverantwortung: Hersteller (bzw. Betreiber).

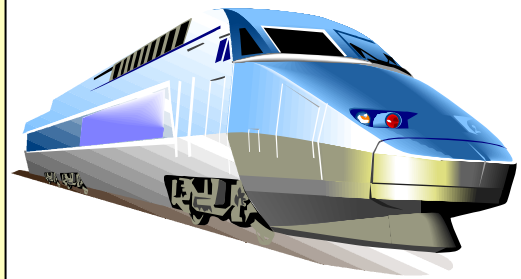


Beispiele für Sicherheitsrecht und -technik im Technikfeld „Verkehrssysteme“ (2)

- **Sicherheit bei Seefahrzeugen:**
  - ⇒ Seerecht (überschneidende nationale und internationale Regelungen),
  - ⇒ konkurrierende Behörden (und Gerichte),
  - ⇒ Schiffsregisterordnung (und weitere),
  - ⇒ Sicherheitsverantwortung: Betreiber (bzw. nationaler Hersteller).



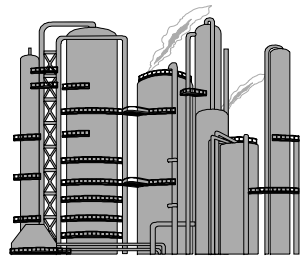
- **Sicherheit bei Bahnfahrzeugen:**
  - ⇒ Eisenbahn-Bau- und Betriebsordnung,
  - ⇒ Eisenbahn-Bundesamt,
  - ⇒ Bau- und Durchführungsverordnungen, Technische Regelwerke,
  - ⇒ Sicherheitsverantwortung: Betreiber.



Beispiele für Sicherheitsrecht und -technik im Technikfeld „Bau- und Anlagentechnik“

- **Sicherheit bei Bauwerken:**
  - ⇒ Bauordnungsrecht (Landesbauordnungen),
  - ⇒ Bauaufsichtsbehörden, Baugenehmigung,
  - ⇒ Bautechnische unabhängige Prüfung,
  - ⇒ Technische Baubestimmungen (DIN-Normen),
  - ⇒ Bauaufsichtliche Zulassungen (Deutsches Institut für Bautechnik, Berlin).
  - ⇒ Anerkannte Prüf- und Zertifizierungsstellen

- **Sicherheit bei Anlagen:**
  - ⇒ Umweltschutzrecht & Raumordnungsrecht,
  - ⇒ Baurecht & Immissionsschutzrecht,
  - ⇒ Gefahrstoff- und Chemikalienverbotsverordnung,
  - ⇒ Gewerbeaufsicht & Technische Überwachung,
  - ⇒ Sachverständige der verschiedensten Art,
  - ⇒ Genehmigungen mit Konzentrationswirkung.



Problematik der Sicherheitstechnik

Sachstand der Sicherheitstechnik

Anwendungsspezifisch rechtliche Ausprägung der Sicherheitstechnik:

- **Rechtsgrundlagen sind je nach Technikfeld unterschiedlich geartet,**
- **Zuständigkeiten von Aufsichtsbehörden bzw. hinzugezogenen aufsichtführenden Institutionen variieren ebenfalls.**
- **Anwendung des Stands der Technik:**
  - ⇒ Rechtsverordnungen mit unbestimmter Verweisung auf Technische Regelwerke (allgemein anerkannter Stand der Technik),
  - ⇒ Bau- und Durchführungsverordnungen mit direkter Verweisung auf einschlägig anwendbare technische Regelwerke;
  - ⇒ Sicherheit durch Vollnormung ⇔ versagensanalytisch basierte Sicherheitstechnik.
- **Unterschiedliche Zuordnung der Sicherheitsverantwortung in der Rechtsanwendung:**
  - ⇒ Hersteller, Eigentümer (Halter), Betreiber, (höhere Gewalt).
- **Änderungspotenzial**

Auswirkung bei technologischer Fortentwicklung

Sicherheitstechnik bei technologischer Fortentwicklung:

- **Rechtsgrundlagen sind zuordenbar,**
- **Aufsichtsbehörde bzw. aufsichtführende Institution sind für den betreffenden Anwendungsfall festgelegt.**
- **Anwendung des Stands der Technik:**
  - ⇒ Rechtsverordnungen (Verweisung auf den Stand der Technik bleibt gültig),
  - ⇒ Sicherheitstechnische Anwendbarkeit der Normung jedoch fraglich ⇒ Klärung durch versagensanalytisch basierte Sicherheitstechnik möglich,
  - ⇒ Kein rechtlicher Zwang zur Klärung der sicherheitstechnischen Anwendbarkeit der Normung,
  - ⇒ Problematik: Meinungsvielfalt bei der Aufsichtführung.
- **Unterschiedliche Zuordnung der Sicherheitsverantwortung in der Rechtsanwendung:**
  - ⇒ Hersteller, Eigentümer (Halter), Betreiber.

Auswirkung bei technologischen Innovationsvorhaben

Sicherheitstechnik bei technologischen Innovationsvorhaben:

- **Rechtsgrundlagen sind nicht zuordenbar:**
  - ⇒ Verlegenheitslösungen ⇒ z.B. Gesetz über den Bau und den Betrieb von Versuchsanlagen zur Erprobung von Techniken für den spurgeführten Verkehr (Versuchsanlagengesetz)
- **Aufsichtsbehörde bzw. aufsichtführende Institution sind für den einzelnen Anwendungsfall festzulegen**
- **Anwendung des Stands der Technik:**
  - ⇒ Keine erschöpfenden Rechtsverordnungen (alleinige Verweisung auf den Stand der Technik ist hier sicherheitstechnisch fragwürdig)
  - ⇒ Keine Normung ⇒ Zwang zu versagensanalytisch basierter Sicherheitstechnik
  - ⇒ Problematik: Meinungsvielfalt bei der Aufsichtführung
- **Zuordnung der Sicherheitsverantwortung bleibt beim Entwickler bzw. Hersteller**

Heutige „Struktur“ von Sicherheitsrecht und -technik

- **Allen beispielhaft aufgezählten Anwendungsbereichen des Rechts ist gemeinsam, dass sie auf der Basis von Regeln (Rechtvorschriften und Normen) strukturiert sind, die nationale, europäische oder internationale Gültigkeit haben.**
- **Prüfungen und Zulassungen/Genehmigungen sowie Kontrollen sind unterschiedlich gefasst, ohne dass hierfür ein begründeter Anlass erkennbar ist.**
- **Die Überwachung (Aufsicht) ist ebenso wenig gleichartig geregelt; die primäre Sicherheitsverantwortung ist bei verschiedenen Institutionen (Betreiber, Hersteller) angesiedelt.**
- **Eine klare und rechtsübergreifende Zuordnung fehlt.**

Beobachtungen nach Stör- oder Unfällen

- **Die Sicherheitstechnik in der Bundesrepublik Deutschland setzt einen weltweit anerkannt hohen Standard.**
- **Dennoch melden sich unmittelbar nach einem folgenschweren Stör- oder Unfall oft „Experten“ zu Wort, die vorgeben zu wissen, dass sich der betreffende Vorfall angeblich aufgrund von „Sicherheitsmängeln“ ereignet habe.**
- **Bei den verunfallten Systemen handelt es sich allerdings um hochkomplexe Systeme, deren Sicherheitstechnik nicht nur gleichermaßen komplex, sondern auch interdisziplinär weit gefächert ist.**
- **Nicht einmal ein Experte aus dem Technikfeld „Bahnverkehr“ verfügt heutzutage über die erforderliche Sachkenntnis, um das Kausalitätsgeflecht eines Stör- oder Unfalls bei einem Magnetbahn-System sachgerecht werten zu können.**

Ansatz zur Problemlösung

Aufgaben für den Bereich der Sicherheitstechnik

- **Anwendbare Regeln und Verfahren auf dem Gebiet von Sicherheitstechnik (und -recht) müssen optimiert und harmonisiert werden.**
- **Die Denkschrift des VDI: Qualitätsmerkmal „Technische Sicherheit“ stellt ein harmonisiertes und interdisziplinär anwendbares sicherheitsmethodische Konzept vor, das als Basis gedacht ist.**
- **Hierzu sind nicht nur nationale, sondern auch europäische und ggf. internationale Anstrengungen erforderlich.**

VDI-Ausschuss „Technische Sicherheit“ (1)

<u>Zielvorgaben</u>
[auf dem Weg der industrialisierten Welt zur Globalisierung]:

- **„Sicherheit in der Technik“ geht alle an,**
- **Interdisziplinäre Zusammenarbeit gewinnt an Bedeutung: innerhalb der Technik, mit dem Recht, mit der Wirtschaft,**
- **Unterschiedliche „Sicherheit“ in verschiedenen Technikfeldern?**
  - ⇒ von außen betrachtet: Unterschiede der Sicherheitskonzepte,
  - ⇒ von innen betrachtet: Gemeinsamkeiten der Sicherheitskonzepte.
- **Herausforderung für die Zukunft:**
  - ⇒ Das **„verdeckte Gemeinsame“** gemeinsam fortentwickeln;
  - ⇒ Interdisziplinäres Zusammenwirken (insbesondere unter Einbindung von Juristen).

VDI-Ausschuss „Technische Sicherheit“ (2)

Aufgabenstellung:

- **Interdisziplinäres Zusammenwirken aller betroffenen Disziplinen und Technikfelder**
  [der VDI-Ausschuss ist bereits interdisziplinär besetzt]**,**
- **Harmonisierung der Sicherheitstechnik durch technikübergreifende Offenlegung des „verdeckten Gemeinsamen” als interdisziplinäre Aufgabe,**
- **Entwicklung auf dem Gebiet der Sicherheitstechnik zur Verbesserung sicherheitsmethodischer Vorgehenskonzepte und Rückkopplung in die einzelnen Technikfelder.**
- **Betrachtung der Technischen Sicherheit über den gesamten Produkt-Lebenszyklus unter Einschluss des „Human Factors Engineering“.**

Zum Begriff „Sicherheit“ – im Allgemeinen

- **Sicherheit gehört zu den Grundbedürfnissen des Menschen und ist als Rechtsgut eingeführt.**
- **Technische Sicherheit eines neuen Produkts, einer neuen Anlage, eines neuen Systems oder eines neuen Prozesses, – verallgemeinert als neue Gestaltungsaufgabe –, bedarf der Nachweisführung.**
- **Nachweisführungen in der Sicherheitstechnik haben prognostischen Charakter. Derartige Prognosen beruhen auf dem Stand der Technik bzw. dem Stand von Wissenschaft und Technik.**

Zum Begriff „Sicherheit“ – in der Technik

In der Technik bedeutet „Sicherheit“:

- **das Qualitätsmerkmal für verlässliche technische Beschaffenheit von Werkstoffen und Strukturen (im Sinne von Beschaffenheitsmerkmal),**
- **das Qualitätsmerkmal für zuverlässige Beherrschbarkeit der vorgesehenen Funktionsabläufe (im Sinne von technischen Prozessmerkmalen),**
- **die gesicherte Verfügbarkeit von Sicherungsfunktionen beim Auftreten von Störungen und Funktionsversagen,**
- **die rückverfolgbar dokumentierte und kommunizierte Nachweisführung (eine Zusicherung allein bleibt hier ohne Sinn), sowie**
- **die vorsorglich geplante Begrenzung möglicher Auswirkungen,**
- **Systematische Rückkoppelung von Versagensereignissen in die weitere Entwicklung und Herstellung betroffener Produkte.**

Zielgerichtetes Vorgehen bei der Sicherheitstechnik

Aspekte des Technischen Managements:

- **Projektmanagement** (Technik – Kosten – Termine)
- **Qualitätsmanagement**
- **Sicherheitsmanagement:**
  - ⇒ Einvernehmen zu den sicherheitstechnischen Grundsätzen
  - ⇒ Interdisziplinarität
  - ⇒ Erzeugen von Sicherheit (Methodisches Vorgehenskonzept)
  - ⇒ Grenzen der Sicherheit
  - ⇒ Überprüfbarkeit von Sicherheit
- **Sicherheit = gesellschaftspolitisches Ziel**
- **Technische Sicherheit = Kompetenz und Aufgabe der Ingenieure**
- **Hoheitliche Aufsichtführung**
  („sachverständiger Anwalt“ der Öffentlichkeit)

Erzeugen von Sicherheit

Einvernehmen zum Begriff „Sicherheit“

Das Normenwerk des DIN weist zwischen 100 und 150 Definitionen des Begriffs „Sicherheit“ aus, die je nach Technikfeld teils recht unterschiedlich ausfallen.

Vorschlag nach DIN 31 000:

- **Sicherheit ist eine Sachlage, bei der das Risiko nicht größer als das Grenzrisiko ist.**
- **Grenzrisiko ist das größte noch vertretbare Risiko eines bestimmten technischen Vorgangs oder Zustands.**

Ferner gilt die grundsätzliche Erkenntnis:

- **Technische Sicherheit lässt sich in ein System „nicht hineinprüfen“.**
- **Technische Sicherheit muss in ein System „hineinentwickelt“ und „hineingebaut“ werden.**

Ist das Erzeugen von Sicherheit noch verbesserbar?

- **In allen Technikfeldern ist der erreichte Stand an Technischer Sicherheit außerordentlich hoch.**
- **Bei technologischer Fortentwicklung ist die Technische Sicherheit nicht immer von vornherein gänzlich überschaubar, denn für technologische Innovationsvorhaben gibt es keinen „anerkannten Stand der Sicherheitstechnik“ und kein Vorgehenskonzept zur systematischen Generierung von Technischer Sicherheit.**
- **Innovation auf dem Gebiet der Sicherheitstechnik zur Verbesserung sicherheitsmethodischer Vorgehenskonzepte muss allgemein an die Entwicklung der Technik gekoppelt werden.**

Was tut der Verein Deutscher Ingenieure?

- **Der Verein Deutscher Ingenieure hat das Thema „Sicherheit in der Technik“ aufgegriffen, um den aktuellen Sachstand zur Sicherheit technischer Einrichtungen bewusst zu machen.**
- **Unsere Rechtsordnung macht zwar sicherheitsrechtliche Vorgaben für die Sicherheitstechnik, verfolgt dabei jedoch kein anwendungsübergreifendes einheitliches Konzept.**
- **Es liegt deshalb nahe, die historisch nach Branchen unterschiedlich gewachsenen und anwendungsspezifisch verschiedenartig praktizierten Vorgehenskonzepte in Sicherheitstechnik und -recht zu einem interdisziplinären sicherheitsmethodischen Vorgehenskonzept zusammenzuführen.**

Aufgabenstellung für den Verein Deutscher Ingenieure

Auf diese Herausforderung gibt der Verein Deutscher Ingenieure die gebotenen Antworten, – und zwar mit folgenden Schwerpunkten:

- **Interdisziplinäres Zusammenwirken aller betroffenen Disziplinen und Technikfelder,**
- **Technikübergreifende Harmonisierung durch Offenlegung des „verdeckten Gemeinsamen",**
- **Rückführung und Anwendung der gefundenen technikübergreifenden Verallgemeinerung in die einzelnen Technikfelder,**
- **Betrachtung des gesamten Lebenszyklus eines Produkts – von der ersten Idee bis zur endgültigen Entsorgung,**
- **Lösung des scheinbaren Zielkonflikts zwischen Sicherheit und Wirtschaftlichkeit.**

Zielvorgaben zur Lösung der Aufgabenstellung

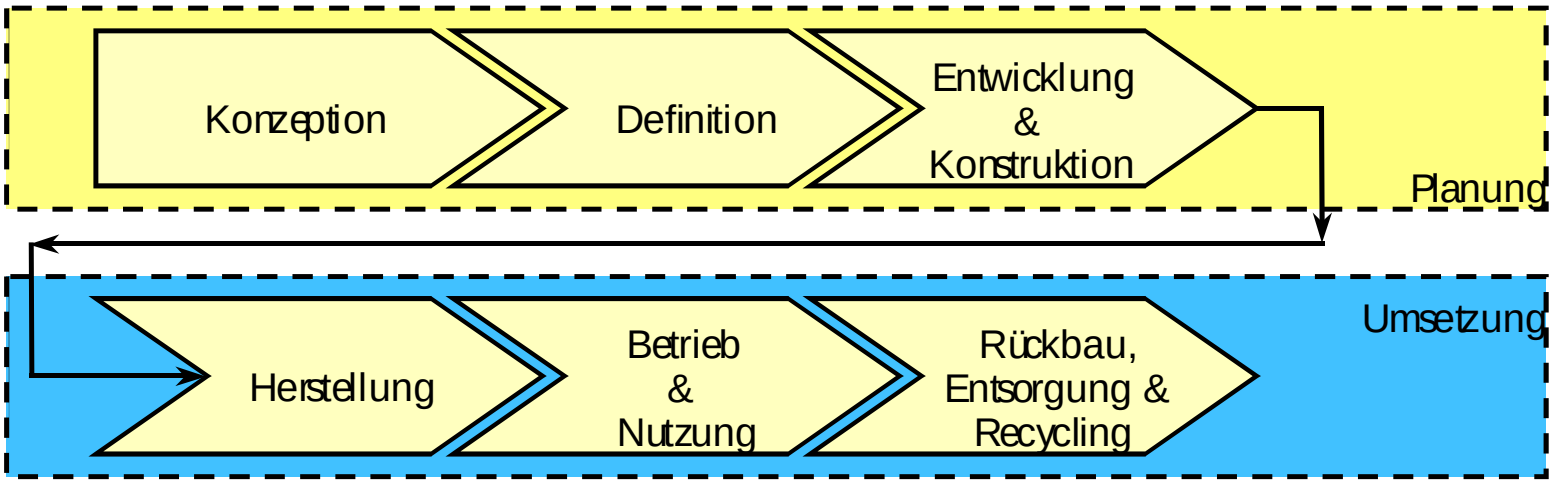
Die industrialisierte Welt befindet sich auf dem Weg der zur Globalisierung. Daraus resultieren besondere Zielvorgaben:

- **„Sicherheit in der Technik“ geht alle an.**
- **Interdisziplinäre Zusammenarbeit gewinnt an Bedeutung: innerhalb der Technik, mit dem Recht, mit der Wirtschaft.**
- **Unterschiedliche „Sicherheit“ in verschiedenen Technikfeldern?**
  - ⇒ von außen betrachtet: Unterschiede der Sicherheitskonzepte,
  - ⇒ von innen betrachtet: Gemeinsamkeiten der Sicherheitskonzepte.
- **Herausforderung für die Zukunft:**
  - ⇒ Das „verdeckte Gemeinsame“ gemeinsam fortentwickeln;
  - ⇒ Interdisziplinäres Zusammenwirken (insbesondere unter Einbindung von Juristen).

Produkt-Lebenszyklus

Anwendung des Phasenkonzepts zur Erzeugung und Überprüfung von Sicherheit in der Technik:

- **Ein Phasenkonzept erleichtert nicht nur das technische Management, sondern sichert in besonderem Maße auch das ordnungsgemäße Verfolgen und Überwachen der vorgegebenen Sicherheitsziele.**
- **Die Phasen eines Produkt-Lebenszyklus können wie folgt dargestellt werden:**



Human Factors Engineering (1)

Noch dreht sich die Diskussion um Entwurf und Konstruktion neuer technischer Anlagen fast ausschließlich um technische Probleme, während die Perspektiven des Human Factors Engineering dabei eine nur untergeordnete Rolle spielen.

- **Sicher muss in den allerersten Phasen einer technischen Konzeption den grundlegenden technischen Designkriterien eine Priorität eingeräumt werden.**
- **Sämtliche komplexen Anlagen werden aber ausnahmslos aus technischen und menschlichen Komponenten bestehen.**
- **Die Entwurfsprinzipien für derartige Systeme fordern Entwicklungs- und Entwurfsprozesse, bei denen zum frühest möglichen Zeitpunkt die Optimierung von Mensch-Maschine-Nahtstellen als gemeinsame Optimierung sowohl der Technik- als auch der Human-Komponenten konzeptbestimmend einsetzt.**

Human Factors Engineering (2)

- **Analysen gravierender Ereignisse zeigen, dass auch dem Steuerungspotential menschlichen Handelns bei der Minderung von allfälligen nachteiligen oder verheerenden Folgen der Unfälle eine eminente Bedeutung zukommt.**
- **Als "Human Factors" sind sämtliche Faktoren zu begreifen, die den Menschen in seiner Interaktion mit einem technischen System beeinflussen bzw. die von Menschen beeinflusst werden.**
- **Organisatorische Faktoren, Arbeitsteilung, vorgängige Managemententscheidungen und sogar inter-organisationale Beziehungen sind hier von Relevanz im Sinne eines umfassenden holistischen Verständnisses von „Human Factors".**

Grenzen der Sicherheit

Vorstellungen der Gesellschaft – technische Wirklichkeit

Vorstellungen der Gesellschaft:

- **Störfälle, die zur Überschreitung vorsorglich festgelegter Grenzwerte führen, werden in der Öffentlichkeit meist als unmittelbare Bedrohung der körperlichen Unversehrtheit empfunden.**
- **Der Begriff „Restrisiko“ (verbleibende Unsicherheit) ist zwar besonders einprägsam, jedoch ingenieurswissenschaftlich nicht fassbar.**

Technische Wirklichkeit:

- **Zielvorstellungen zum Thema „Sicherheit in der Technik“ sind herauszuarbeiten, die eine solide Basis für ingenieurwissenschaftliches Handeln zu bieten vermögen.**
- **Der ingenieurswissenschaftlichen Betrachtungsweise muss der ihr gebührende Stellenwert zukommen.**

Sicherheit – Grenzrisiko, Grenzwerte (1)

Die Ansichten über Nutzen und Risiken von Technik sind inhomogen:

- **Eine Bevölkerung am Existenzminimum wird und muss ausschließlich um seine Selbsterhaltung kämpfen, also dem Nutzen Vorrang geben.**
- **Das verfeinerte Empfinden für die Risiken von Technik darf als Charakteristikum einer saturierten Gesellschaft gelten.**

Akzeptanz-Grundsatz misst sich am Grenzrisikos:

- **Absolute Sicherheit im Sinne eines Null-Risiko (Risikoverbot) kann nicht gefordert werden, weil es prinzipiell nicht möglich ist.**
- **Verschiedene technische Einrichtungen sollten kein unterschiedliches Verhältnis von Risiko zu Nutzen für zu schützende Rechtsgüter darstellen (Risikoäquivalenz).**
- **Bei Ausweitung von Grenzwerten in alle Lebensbereiche hinein wird es immer wichtiger, technische Sicherheit so zu gestalten und zu vermitteln, dass sie die Erwartungen der Gesellschaft erfüllen.**

Sicherheit – Grenzrisiko, Grenzwerte (2)

Das Fazit lautet:

- **Die Bestimmung der Grenzen mit sicherheitstechnischer Machbarkeit basiert auf Verantwortung, Akzeptanz, Kompromissen, dem Maßstab der praktischen Vernunft, politischer Durchsetzbarkeit und letztendlich auf ethischen Normen.**
- **Die Festlegung der technischen Sicherheit basiert auf Praktikabilität, Kostenbewusstsein, Risikobereitschaft und dem Fortschritt durch Forschung und Entwicklung.**
- **Die Ziehung von Grenzen stellt ein positives und notwendiges Gebot dar:**
  - ⇒ Es bedeutet Gewinn, ethische Aufgabe, sinnvoller Verzicht und
  - ⇒ keineswegs Schwäche, Defizit und Mangel.

Überprüfbarkeit der Sicherheit

Technische Sicherheit – eine interdisziplinäre Aufgabe

Zu beachtende Grundsätze:

- **Technische Sicherheit lässt sich in ein System „nicht hineinprüfen“.**
- **Technische Sicherheit muss in ein System „hineinentwickelt“ und „hineingebaut“ werden.**
- **Technische Sicherheit bedarf – insbesondere bei technologischer Innovation und Fortentwicklung – des interdisziplinären Einvernehmens.**
- **Technische Sicherheit braucht nicht in Widerspruch zur Wirtschaftlichkeit technischer Einrichtungen stehen.**
- **Technische Sicherheit ist ein Qualitätsmerkmal, das sachgerechtes technisches Management erfordert.**
- **Technische Sicherheit muss nachweislich den – sachlich begründeten – Belangen der Öffentlichkeit entsprechen.**
- **Die Öffentlichkeit bedarf eines „fachkundigen Anwalts“ für technische Sicherheit ⇒ d.h. aufsichtführender Institutionen.**

Sicherheitstechnische Überprüfung (1)

Sicherheit ist nur insoweit zu gewährleisten, wie sie auch überprüfbar ist.

Mögliche Verantwortlichkeiten:

- **Prüfungen in eigener Verantwortung (Eigenprüfung),**
- **Prüfungen durch einen Auftraggeber/Kunden in ggf. ergänzender Verantwortung oder**
- **Prüfungen durch einen unabhängigen Dritten, der in der Regel keinerlei Verantwortung für ordnungsgemäß erzeugte Sicherheit übernimmt; hierbei kann es sich entweder um**
  - ⇒ den Staat, eine hoheitlich für ihn wirkende Prüfstelle oder
  - ⇒ eine privatwirtschaftlich tätige Prüfstelle

  handeln.
- **Hoheitliche – und fachkompetente – Überwachung**

Sicherheitstechnische Überprüfung (2)

Die Wirksamkeit von Prüfmaßnahmen wird durch folgende Faktoren bedingt:

- **den Grad der Unabhängigkeit der Prüfung vom betroffenen Vorgang,**
- **die technisch/fachliche Qualifikation des Prüfpersonals,**
- **die Intensität der Überprüfung (Häufigkeit und Umfang von Prüfungen),**
- **den Beurteilungskriterien und Maßnahmen bei negativen Prüfergebnissen,**
- **den Einsatz mehrfacher unabhängiger Prüfungen, wobei je nach Erfordernis der Qualitätssicherung folgende Abstufung möglich ist (z.B. in Anlehnung an DIN EN ISO 9000 „Qualitätsmanagementsysteme“):**
  - ⇒ nur Herstellerprüfungen,
  - ⇒ betriebsextern geregelte Herstellerprüfungen zusammen mit Fremdprüfungen oder Abnahmeprüfungen,
  - ⇒ betriebsextern geregelte Herstellerprüfungen zusammen mit Fremdprüfungen sowie Abnahmeprüfungen oder einer zweiten unabhängigen Fremdprüfung.

Einbeziehen der Gesellschaft

Qualitätsmanagement gegen sicherheitskritisches Versagen

- **Problematik internationaler und nationaler Entwicklungen**
- **Sicherheit und Legislative**
- **Sicherheit und Deregulierung**
- **Sicherheit und Wirtschaft**
- **Sicherheit und Zuständigkeitsverteilungen**
- **Sicherheit als vorrangiges Qualitätsmerkmal**
- **Qualitätsmanagement als Vorgehenskonzept für das Sicherheitsmanagement**
- **Konfigurationssteuerungs- und Änderungsverfahren**
- **Der Mensch als Kriterium für das Sicherheitsmanagement**

Kommunikation Technischer Sicherheit mit der Öffentlichkeit

Bringschuld der Wissenschaft zu verständlicher Kommunikation der bestehenden Risiken.

Berücksichtigung der psychologischen Faktoren bei der Wahrnehmung von Gefahren:

- **Freiwilligkeit**
- **Kontrollierbarkeit**
- **Katastrophenpotential**
- **Betroffenheit**
- **Bekanntheit / Gewohnheit**

Proaktive Kommunikation:

- **Glaubwürdige und unmissverständliche Information**
- **Kein Vertuschen**
- **Kein Widerspruch zwischen Aussagen und Handeln**
- **Kein verspätetes Reagieren auf öffentliche Beschuldigung**

Empfehlung

Interdisziplinär ganzheitliches Vorgehenskonzept

Das verdeckte Gemeinsame suchen – und finden

Sicherheitsmethodisches Vorgehenskonzept

Sicherheitsmethodisches Vorgehenskonzept (1)

Konzeptionelle Kernbestandteile:

- **Generierung technischer Integrität auf der Basis natürlicher Integrität (als Vorbedingung für sicherheitsgerechte Produkt-Gestaltung)**
- **Analyse des sicherheitskritischen Versagensverhaltens**
- **Versagensausschluss aufgrund unverlierbarer Eigenschaften (z.B. in Form eines anerkannten Festigkeitsnachweises)**
- **Sicherungsmaßnahmen gegen gefährliche Versagensfolgen (z.B. in Form einer elektrischen Sicherung in Stromnetzen)**
- **Begrenzung der Eintrittswahrscheinlichkeit gefährlicher Versagensformen**
- **Behandlung von Einfach- und (sequentiellem) Mehrfachversagen**
- **Berücksichtigung von Sicherheitsverzugszeiten (z.B. bei der Konzipierung von Zielbremsungen)**
- **Konzipierung nachweislich zugänglicher Rettungs- und Fluchtpfade**

Sicherheitsmethodisches Vorgehenskonzept (2)

Konzeptionelle Zusatzbestandteile:

- **Definition des jeweils „sicheren Zustandes“ bzw. des „sicheren Verhaltens“ des Systems**
  (d.h. der „fail safe“- bzw. „fail operational“-Bedingung)
- **Analyse der sequentiellen Mehrfach-Versagensformen**
  (unter Einbeziehung der deterministischen Versagensvorkehrungen)
- **Folge- und Wechselwirkungen von auslösenden Versagensformen**
  (z.B. in Form von Kaskadeneffekten)
- **Auswirkung der sicherheitstechnischen Vorkehrungsmaßnahmen auf die technische Zuverlässigkeit und Verfügbarkeit des Systems**
- **Definition der technischen Sicherheits- und Sicherungsmaßnahmen**
- **Definition der betrieblichen Sicherungsmaßnahmen**
  (als Mensch-Maschine-System mit gesicherter Erkennbarkeit von Anzeigen)
- **Organisation des sicherheitstechnischen Qualitätsmanagements**
  (das mit hinreichenden Eingriffsrechten ausgestattet sein muss)

Teilmethodik: Versagensanalyse

- **Erfassen des Versagensverhaltens (FMECA, FMEA):**
  - ⇒ Funktionsbaum (nach VDI 2221 … 2223):
    - — Top-Funktion(en)
    - — Funktionselemente
    - — Verknüpfungen
  - ⇒ Versagensursachen:
    - — Zufallsausfall
    - — Umwelteinfluss
    - — menschlicher Irrtum
  - ⇒ Formen des Versagens von Funktionselementen (standardisierbar):
    - — Funktionsaufbau (kontrolliert, zeitlich, sachlich, …)
    - — Funktionsverlauf (sachlich, beständig, kontrollierbar, …)
    - — Funktionsabschluss (zeitlich, kontrolliert)
  - ⇒ Klassifizierung:
    - — katastrophal
    - — **sicherheitskritisch**, …

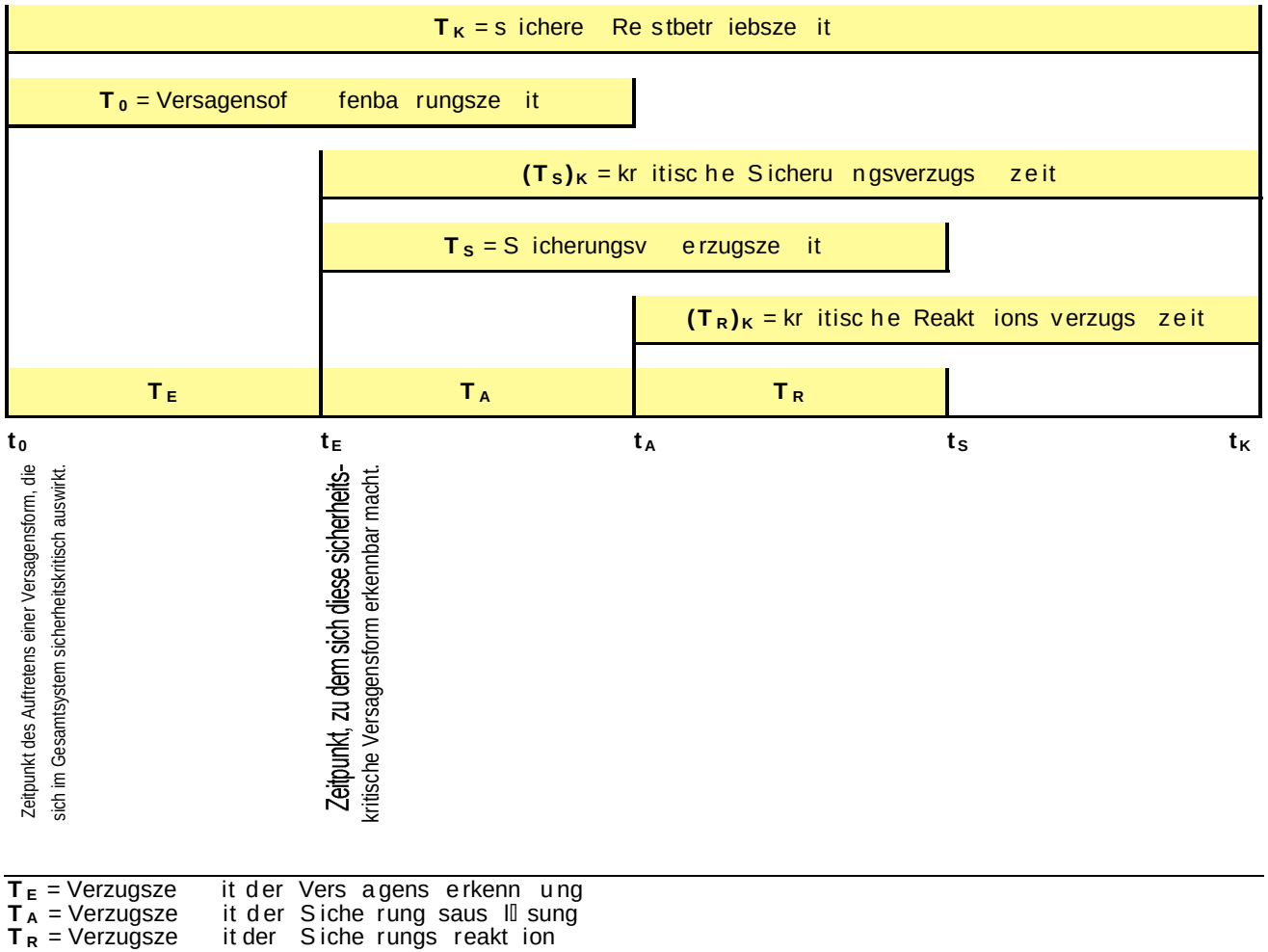
Teilmethodik: Sicherungsverzugszeiten (1)

Bei der technischen Gestaltung sicherheitsrelevanter Systemkomponenten ist folgende Aspekte auf zu achten:

- **In der Regel verbleibt auch nach dem Auftreten eines Versagens eine gewisse Zeitspanne, ehe das Versagensverhalten im Gesamtsystem nicht mehr beherrschbar wird.**
- **Ausreichende Reaktionszeit nutzen, um die vorgesehenen technischen bzw. operationellen Sicherungsmaßnahmen gegen die Folgen eines sicherheitskritischen Versagens wirksam werden zu lassen.**
- **Von der „sicheren Restbetriebszeit“ und den zeitlichen Möglichkeiten für Versagenserkennung und (System-) Sicherung hängt die Entscheidung ab, ob eine Hemmung der (System-) Funktion notwendig ist, oder ob eine Versagens- (Stör-) Meldung (Störanzeige) ausreicht, mit der geeignete operationelle Sicherungsmaßnahmen ausgelöst werden.**

Die zeitlichen Zusammenhänge sind in nachfolgender Folie dargestellt:

Teilmethodik: Sicherungsverzugszeiten (2)



T_E = Verzugszeit der Versagenserkennung
T_A = Verzugszeit der Sicherungsauslösung
T_R = Verzugszeit der Sicherungsreaktion

Vorteile interdisziplinären Vorgehens (1)

Für den Bereich der Technik selbst:

- **Umfassend anwendbares Vorgehenskonzept deckt unterschiedliche anwendungsspezifische Vorgehenskonzepte ab**
- **Verbesserung des interdisziplinären Zusammenwirkens von Ingenieuren aus verschiedenen technischen Fachgebieten**
  (mit einheitlichem Fachterminologie auf dem Gebiet der Sicherheitstechnik)
- **Die in einer Unzahl von – teils widersprüchlichen – Rechtsvorschriften und technischen Regelwerken verborgenen sicherheitstechnischen Vorgehenskonzepte lassen sich systematisch aufdecken – und ggf. fortentwickeln**
- **Für technologische Innovationsvorhaben steht ein sicherheitstechnisch effizientes, ganzheitlich und interdisziplinär anwendbares Vorgehens-konzept zur Verfügung**

Für die Rechtsanwendung der Sicherheitstechnik:

- **Verbesserung der Kommunikation zwischen Technik und Recht**

Vorteile interdisziplinären Vorgehens (2)

Mit einem interdisziplinär geeigneten Vorgehenskonzept für die Sicherheitstechnik werden auch weitgesteckte Ziele erreichbar:

Vorteile interdisziplinären Vorgehens (3)

Interdisziplinäre Sicherheitstechnik:

- Weiterentwicklung bewährter Techniken
- Technische Neuentwicklungen
- Konzipierung von Fail safe- und Fail operational-Einrichtungen
- Verbesserung der interdisziplinären Kommunikationsfähigkeit
- Systematisierung der sicherheitstechnischen Nachweisführung
- Wirtschaftlichen Verbesserung der Systemverfügbarkeit
- Gestaltung von Rettungspfaden und -einrichtungen
- Einwirkungen (z.B. Brandschutz)
- Betriebliche Unfallverhütung

Schlussbemerkungen

Ausblick (1)

Der Markt reicht mit seinen Mechanismen für sich alleine nicht aus, technische Sicherheit von Erzeugnissen zu gewährleisten!

Die Denkschrift des Vereins Deutscher Ingenieure:
Das Qualitätsmerkmal „Technische Sicherheit“
wird in Kürze veröffentlicht.

—

- **Auf der Grundlage dieser Denkschrift wird der VDI-Ausschuss „Technische Sicherheit“ ein sicherheitsmethodisches Konzept entwickeln, – mit dem Ziel interdisziplinärer Anwendung und allgemeiner Anerkennung (Standard).**

Ausblick (2)

Die Idee für ein interdisziplinäre nutzbares, sicherheitsmethodisches Vorgehenskonzept liegt somit vor.

Es liegt an den Ingenieuren, das Konzept abschließend zu definieren und auszubauen, sowie für alle Technikfelder zugänglich zu machen!