TS529-Schulz-Forberg

Das Qualitätsmerkmal „Technische Sicherheit“

Diskurs zwischen Risikovermeidung und Sicherheitsmanagement

Bernd Schulz-Forberg, Berlin

Immer wieder auftretende Zwischenfälle und Unfälle bis hin zu spektakulären Störfällen mit großer öffentlicher Wirkung verlangen eine kritische Überprüfung der Methoden zur Erzeugung von Sicherheit. Diese wird häufig genug nur in den sehr spezifischen Fachdisziplinen vorgenommen. Der hohe Grad der Differenzierung in Fachdisziplinen erfordert in zunehmendem Maße die Einführung von Managementsystemen, wie dies im Bereich der Planung und des Betriebs schon selbstverständlich ist. Die Sicherheitstechnik selbst bildet keine eigenständige Fachdisziplin, vielmehr werden sicherheitstechnische Belange jeweils in den Rechtsbereichen und den zugeordneten Fachdisziplinen angesprochen, wobei auch von Fall zu Fall schon die Managementsysteme für das Qualitätsmerkmal Technische Sicherheit Platz greifen. Damit ergibt sich heute ein recht uneinheitliches Bild der Sicherheitstechnik. Ein geschlossenes sicherheitsmethodisches Konzept als gültiger Rahmen für alle Fachdisziplinen kann hier Abhilfe schaffen.

Der Verein Deutscher Ingenieure (VDI) hat hierzu die Initiative ergriffen: Die Publikation „Das Qualitätsmerkmal Technische Sicherheit – Denkansatz und Leitfaden“[1)] beschreibt unter Hinweis auf die Ausgangslage und den Werdegang diese Zielstellung. Der Diskurs zu dieser Veröffentlichung wird gerade gestartet. Anhand des damit vorliegenden Denkansatzes und Leitfadens kann und soll auf vielen Ebenen diskutiert werden. Am Ende des Diskurses sollen dann allgemein und jederzeit anwendbare Regeln zur Erzeugung und Erhaltung Technischer Sicherheit aufgestellt werden.

Die VDI-Publikation

Einführung

Erzeugung der Technischen Sicherheit

Die Publikation zur Technischen Sicherheit baut auf der im Jahre 2010 erschienenen Denkschrift (www.vdi.de/technik/fachthemen/technische-sicherheit/) auf. Diese widmet sich zunächst dem Erzeugen des Qualitätsmerkmals Technische Sicherheit. Hervorzuheben ist die Strukturierung einer empfehlenden Vorgehensweise nach einem den gesamten Lebenszyklus umfassenden Phasenkonzept. Das Konzept gliedert sich in drei Bereiche (**Bild 1**):

– den Planungsprozess, mit den Elementen Konzeption und Definition,
– den Realisierungsprozess, mit den Elementen Entwicklung und Konstruktion sowie Herstellung,
– den Betriebsprozess, gebildet aus den Elementen Betrieb und Nutzung, sowie Rückbau und Entsorgung.

Grenzen der Sicherheit

Folgerichtig werden auch die Grenzen der Sicherheit, aus erkenntnistheoretischer Sicht wie auch aus der Abwägung von Chancen und Risiken heraus, behandelt. Die Denkschrift stellt dabei erwartungsgemäß fest, dass es keine absolute Sicherheit geben kann. So wird u. a. ausgeführt, dass der Maßstab für die größten noch vertretbaren Schäden nicht nur durch das Schutzbedürfnis der betrachteten Rechtsgüter bestimmt wird,

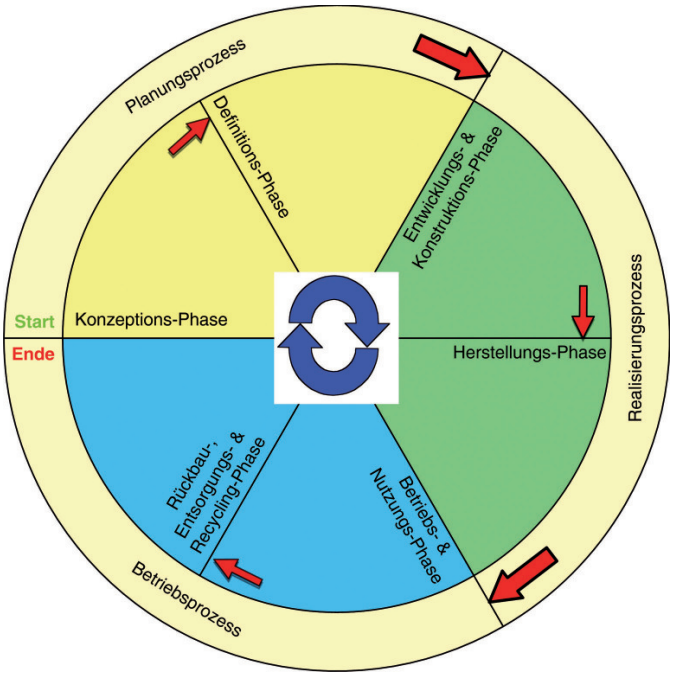

Bild 1 Lebenszyklus von Produkten (Phasenkreis).

[1)] Das Qualitätsmerkmal „Technische Sicherheit“. Hrsg.: VDI. Berlin: Beuth Verlag 2016.

sondern auch durch die Absicht, gesellschaftliche Bedürfnisse zu befriedigen, wobei es im Allgemeinen einer Abwägung im gesellschaftlichen Konsensbedarf (Risikosteuerung).

Überprüfbarkeit der Sicherheit

In einem umfangreichen Kapitel befasst sich die Denkschrift mit der Überprüfbarkeit der Sicherheit. Prüfung ist nicht etwa nur wegen der Kontrolle nötig, sondern auch wegen der Selbstvergewisserung der Akteure. Ausgeführt wird die Strukturierung der Prüfung für übliche Güter, Anlagen und Verfahren, aber insbesondere auch für innovative Vorhaben. In jedem Fall muss für alle Fachdisziplinen der Mensch stärker als bislang eingeführt berücksichtigt werden, weshalb besondere Betonung auf den Bereich des Human Factor Engineering (HFE) gelegt wird. Hervorzuheben ist darüber hinaus, dass ein durchgängiges Sicherheitscontrolling über alle Phasen des Lebenszyklus empfohlen wird.

Gesellschaftliche Betrachtungen

Die Denkschrift geht im Kapitel „Gesellschaftliche Betrachtungen“ u. a. darauf ein, dass Deutschland mit den Begriffen Qualität und Sicherheit im Markt gesehen wird und diese Karte nicht verspielt werden darf. Dazu wird betont, dass sich der Staat nicht nur auf die Regelsetzung und die Strafandrohung beschränken darf. Er muss vielmehr mit der Vorgabe der Normen und Strukturen im erforderlichen Maß durch aktives Handeln gleichzeitig deren Erfüllung und Einhaltung sicherstellen. Es ist zwar politischer Wille, bisher staatliche Aufgaben vermehrt in die Hände privater Einrichtungen bzw. der Wirtschaft zu geben, dennoch muss die erforderliche Balance zwischen Durchführungs- und Gewährleistungsverantwortung des Staates eingehalten werden. Es bedarf einer adäquaten Ausrichtung der staatlichen Aufgaben in den sich ändernden Prüf- und Genehmigungssystemen.

Empfehlungen

In den Empfehlungen wird insbesondere angeregt, den Bereich der Sicherheit wieder verstärkt in die Ausbildungs- und Lehrangebote der bildenden Institutionen zu tragen, eine Kommunikationsinitiative in Richtung Öffentlichkeit vorzusehen, ein durchgängiges Informationsmanagement zu etablieren und letztlich über die Schaffung eines Technikrats nachzudenken.

Schlussbemerkungen

In den Schlussbemerkungen betont die Denkschrift, dass der VDI das erforderliche interdisziplinär aufgebaute Methodenkonzept erarbeitet, wobei der breit angelegte Diskurs in der Gesellschaft als Voraussetzung angesehen wird. Die Arbeiten müssen deutlich über den nationalen Rahmen hinaus zielen, damit auch die möglichen Schwächen im europäischen System ausgeglichen werden können, wie auch Beispielwirkungen für internationale Konventionen im Sicherheitsbereich erzielt werden können. Das Methodenkonzept ist nun als Bestandteil der VDI-Publikation in Form eines Leitfadens fertiggestellt. Die Publikation enthält also den Denkschriftteil und einen Leitfaden zur fachgebietsübergreifenden Generierung von Technischer Sicherheit.

Eckpunkte

Erwartung der Märkte

Deutsche Ingenieursleistungen werden weltweit unter dem Begriff „Made in Germany“ am Markt platziert, was für Qualität und Sicherheit der industriellen Erzeugnisse aus Deutschland steht. Die Märkte der Welt erwarten: Innovative Technologie, angemessene Lebensdauer, uneingeschränkte Gebrauchstauglichkeit, Zuverlässigkeit, wirtschaftliche Verfügbarkeit und Technische Sicherheit, also gezielte Anwendung der Ingenieurswissenschaften.

Dazu ist ein zweckdienliches Management gängige Praxis. Technisches Management erfolgt meist interdisziplinär und ist damit eine gute Basis für ein integriertes Sicherheitsmanagementsystem(SMS).

Rechtsgrundlagen

Die Rechtsgrundlagen sind je nach Technikfeld unterschiedlich geartet, die Zuständigkeiten von Aufsichtsbehörden bzw. hinzugezogenen aufsichtführenden Institutionen variieren ebenfalls. Die Rechtsverordnungen beziehen sich mit unbestimmter Verweisung auf die allgemein anerkannten Regeln der Technik, den Stand der Technik oder den Stand von Wissenschaft und Technik (**Bild 2**).

Sondergebiete generieren Sicherheit durch Vollnormung oder durch versagensanalytisch basierte Sicherheitstechnik. Die Sicherheitsverantwortung in der Rechtsanwendung obliegt dem Hersteller, dem Eigentümer (Halter) oder dem Betreiber, (höhere Gewalt).

Technologische Weiterentwicklung

Sicherheitstechnik bei technologischer Fortentwicklung adaptiert die o. a. Regularien. Also sind die Rechtsgrundlagen zuordenbar, die Aufsichtsbehörde bzw. aufsichtführende Institution sind für den betreffenden Anwendungsfall festgelegt und die Anwendung des Stands der Technik wird genauso gehandhabt. Die sicherheitstechnische Anwendbarkeit der Normung ist jedoch fraglich, während Sicherheitstechnik durch versagensanalytisches Vorgehen möglich bleibt. Problematisch sind demzufolge die Meinungsvielfalt bei der Aufsichtführung und die unterschiedliche Zuordnung der Sicherheitsverantwortung.

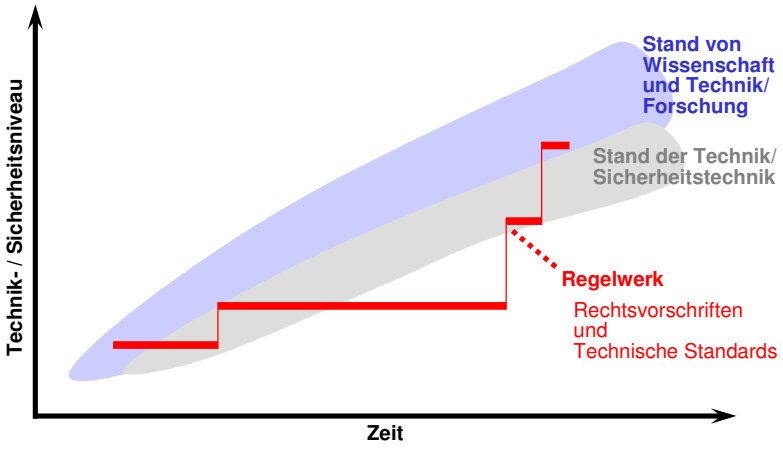

Bild 2 Zeitliche Entwicklung der Regeln und des Standes der Technik.

Technologische Innovationen

Sicherheitstechnik bei technologischen Innovationsvorhaben bedingt zunächst die Klärung der Rechtsgrundlagen. Verlegenheitslösungen wie z. B. das Gesetz über den Bau und den Betrieb von Versuchsanlagen zur Erprobung von Techniken für den spurgeführten Verkehr (Versuchsanlagengesetz) sind oft nicht zielführend. Ferner ist die Aufsichtsbehörde bzw. aufsichtführende Institution für den einzelnen Anwendungsfall festzulegen und die alleinige Anwendung des Stands der Technik ist hier fragwürdig. Zutreffende Normen gibt es nicht, also besteht der Zwang zu versagensanalytisch basierter Sicherheitstechnik. Problematisch ist auch hier die Meinungsvielfalt bei der Aufsichtsführung. Die Zuordnung der Sicherheitsverantwortung bleibt beim Entwickler bzw. Hersteller.

Unterschiedliche Regelungen

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

Sicherheit in der Technik umfasst Merkmale für die verlässliche technische Beschaffenheit von Werkstoffen und Strukturen (im Sinne von Beschaffenheitsmerkmal), für die 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 sowie die vorsorglich geplante Begrenzung möglicher Auswirkungen, die systematische Rückkoppelung von Versagensereignissen in die weitere Entwicklung und Herstellung betroffener Produkte.

Menschlicher Einfluss in allen Phasen

Die Anwendung des Phasenkonzepts zur Erzeugung und Überprüfung von Sicherheit gewährleistet in besonderem Maße das ordnungsgemäße Verfolgen und Überwachen der vorgegebenen Sicherheitsziele.

In den allerersten Phasen einer technischen Konzeption muss den grundlegenden technischen Designkriterien Priorität eingeräumt werden.

Sämtliche komplexe 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. Analysen gravierender Ereignisse zeigen, dass auch dem Steuerungspotenzial 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 im Sinne eines umfassenden, holistischen Verständnisses von „Human Factors“ (sozio-technische Systeme) von Relevanz.

Risikosteuerung als gesellschaftlicher Prozess

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 umfassendere Empfinden für die Risiken von Technik darf als Charakteristikum einer saturierten Gesellschaft gelten. Absolute Sicherheit im Sinne eines Null-Risikos (Risikoverbot) kann nicht gefordert werden, weil es prinzipiell nicht möglich ist. Verschiedene technische Einrichtungen sollten aber 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.

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 aber auch 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. Die Wirksamkeit von Prüfmaßnahmen wird durch 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 und den Einsatz mehrfacher unabhängiger Prüfungen bedingt.

Kommunikation

Die verständliche Kommunikation zur Technischen Sicherheit mit der Öffentlichkeit ist eine Bringschuld von Wissenschaft und Technik. Dabei sind psychologische Faktoren zu berücksichtigen: Freiwilligkeit, Kontrollierbarkeit, Katastrophenpotenzial, Betroffenheit, Bekanntheit/Gewohnheit, proaktive Kommunikation[2)], glaubwürdige und unmissverständliche Information, kein Vertuschen, kein Widerspruch zwischen Aussagen und Handeln und kein verspätetes Reagieren auf öffentliche Beschuldigung.

Interdisziplinäres Vorgehen

Die Vorteile des interdisziplinären Vorgehens ergeben sich wie folgt: Für den Bereich der Technik selbst deckt ein umfassend anwendbares Vorgehenskonzept unterschiedliche anwendungsspezifische Vorgehenskonzepte ab, es führt zu einer Verbesserung des interdisziplinären Zusammenwirkens von Ingenieuren aus ver-

[2)] *Morgan, G.* et. al. (2002): Risk communication: A mental models approach, Cambridge University Press. *All we have to do get the numbers right. All we have to do is tell our audience the numbers. All we have to do is explain what we mean by the numbers. All we have to do is show our audience that we have accepted similar risks in the past. All we have to do is show our audience it's a good deal for them. All we have to do treat our audience nicely. All we have to do is make our audience partners.*

schiedenen technischen Fachgebieten (mit einheitlichem Fachterminologie auf dem Gebiet der Sicherheitstechnik) und die in einer Vielzahl von – teils widersprüchlichen – Rechtsvorschriften und technischen Regelwerken verborgenen sicherheitstechnischen Vorgehenskonzepte lassen sich systematisch aufdecken und ggf. fortentwickeln. Ferner steht für technologische Innovationsvorhaben ein sicherheitstechnisch effizientes, ganzheitlich und interdisziplinär anwendbares Vorgehenskonzept zur Verfügung.

Für die Rechtsanwendung der Sicherheitstechnik ergibt sich eine Verbesserung der Kommunikation zwischen Technik und Recht.

Mit einem interdisziplinär geeigneten Vorgehenskonzept für die Sicherheitstechnik werden auch weitgesteckte Ziele wie interdisziplinäre Sicherheitstechnik, Weiterentwicklung bewährter Techniken, technische Neuentwicklungen, Konzipierung von „fail-safe"- und „fail-operational"-Einrichtungen, Verbesserung der interdisziplinären Kommunikationsfähigkeit, Systematisierung der sicherheitstechnischen Nachweisführung, wirtschaftliche Verbesserung der Systemverfügbarkeit, Gestaltung von Rettungspfaden und -einrichtungen und betriebliche Unfallverhütung erreichbar.

Bestandteile des Vorgehenskonzepts

Das sicherheitsmethodische Vorgehenskonzept besteht aus konzeptionellen Kern- und Zusatzbestandteilen.

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 (sequenziellem) Mehrfachversagen,
- Berücksichtigung von Sicherheitsverzugszeiten (z. B. bei der Konzipierung von Zielbremsungen),
- Konzipierung nachweislich zugänglicher Rettungs- und Fluchtpfade.

Zusatzbestandteile:

- Definition des jeweils „sicheren Zustands" bzw. des „sicheren Verhaltens" des Systems (d. h. der „fail-safe"- bzw. „fail-operational"-Bedingung),
- Analyse der sequenziellen 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).

Aufgabe

Die Kernaufgaben lassen sich wie folgt beschreiben: Harmonisierung der Sicherheitstechnik als interdisziplinäre Aufgabe, Entwicklung auf dem Gebiet der Sicherheitstechnik zur Verbesserung sicherheitsmethodischer Vorgehenskonzepte und Rückkopplung in die einzelnen Technikfelder. Dazu ist die Betrachtung der Technischen Sicherheit über den gesamten Produkt-Lebenszyklus unter Einschluss des „Human Factors Engineering" als konstitutiv zu verstehen. Sicherheit gehört zu den Grundbedürfnissen des Menschen und ist als Rechtsgut eingeführt. Dabei bedarf die Technische Sicherheit eines neuen Produkts, einer neuen Anlage, eines neuen Systems oder eines neuen Prozesses der Nachweisführung. Technologische Innovationen bedingen nicht nur den interdisziplinären Rückgriff auf die verschiedenen technischen Fachdisziplinen, sondern auch auf das „Sicherheitsrecht" und das „Human Factors Engineering". Die Grundsätze des „Human Factors Engineering" sind heute weder in den technischen Fachdisziplinen noch im „Sicherheitsrecht" durchgängig und systematisch entfaltet.

Der Leitfaden als Handlungsanleitung

Motiv und Nutzen

Nach öffentlichkeitswirksamen Unfällen wird in den Medien und häufig auch in der Politik reflexartig spekuliert, dass die Regeln nicht ausreichen und schleunigst verbessert werden müssten. Dabei spielt es keine Rolle, ob tatsächlich die Regeln nicht ausreichen oder es sich nur um ein Vollzugsdefizit handelt. Aus einer Alarmierungsstimmung heraus neigt die Gesellschaft dann dazu, sogar „Verschlimmbesserungen" ins Auge zu fassen.

Daneben gibt es im Bereich der Luft- und Raumfahrttechnik versagensanalytische Vorgehensweisen. Klingt die Aufregung nach einem Unfall ab, wendet man sich der sachlichen Aufarbeitung zu. Ist demzufolge eine Regel anzupassen, so wird dies im Rahmen der Rechtsordnung der Bundesrepublik Deutschland sachgemäß durchgeführt. So ist beispielsweise die Auslegung von Druckbehältern für Wasserstoff nach dem Unfall in Hanau im Jahre 1991 ergänzt worden[3)]. So gut und so richtig diese Vorgehensweise für den betroffenen Technikbereich ist, so führt sie doch dazu, dass die Unterschiede in den verschiedenen Technikbereichen weiter zunehmen, denn es wird nur in diesem Technikbereich eine Anpassung vorgenommen und eine Verallgemeinerung für andere Technikbereiche in der Regel nicht betrachtet.

Bei innovativen Technologien wirkt sich das bisherige Verhalten besonders nachteilig aus, da aus jedem Technikbereich heraus der Stand der Technik bzw. der Stand von Wissenschaft und Technik für das innovative Vorhaben gesondert ermittelt wird und eine Verallgemeinerung für andere Bereiche kaum vorgenommen wird. Diese Schwachstelle im Technikrecht muss überwunden werden. Eine fachgebietsübergreifende Vorgehensweise zur Generierung und zum Erhalt von Sicherheit ist geboten.

In fast allen Technikbereichen gibt es normative Regelwerke, anhand derer sich die notwendige Sicherheit bestimmen lässt. Vom Bauwesen über das Verkehrswesen und die chemische

[3)] Bericht SFK-GS-15 „Bewertung der Regelungsbedürftigkeit im Bereich der Wasserstofftechnologie des Arbeitskreises Wasserstoff-Technologie der Störfall-Kommission. Hrsg.: Störfallkommission. Bonn 1998. Siehe www.kasbmu.de/publikationen/sfk/sfk_gs_15.pdf

Verfahrenstechnik bis hin zur Elektrotechnik liegen anwendungsspezifische Sicherheitskonzepte vor. Da gibt es Bauvorschriften, Betriebsanweisungen, Instandhaltungsanweisungen und Auflagen zur Nachrüstung, alle aber anwendungsspezifisch. Auch die Vorgehensweisen – normativ oder versagensanalytisch – müssen zusammengeführt werden.

Im Gefahrguttransport beispielsweise war der Unfall in Herborn einer von mehreren Anlässen für eine durchgreifende Regelverbesserung. Diese führte aber zunächst zu einer „Verschlimmbesserung". Die Nachrüstung von Koffertanks mit der sog. Bauchbinde half zwar, die Alarmierungsstimmung in der Politik zu beenden, sorgte aber für zum Teil kontraproduktive Maßnahmen. Letztlich konnte diese „Verschlimmbesserung" aber aufgelöst werden durch den Forschungsbericht 203 der Bundesanstalt für Materialforschung und -prüfung (BAM), der im Zusammenhang mit dem § 7 des Gefahrgutsgesetzes zu einer Entspannung in Bezug auf die Fahrwegbestimmung führte, da diese technische Begründung in einer noch heute gültigen Ausnahmegenehmigung aufgenommen wurde.

Betrachtet man den Unfall in Herborn in Zusammenhang mit den Unfällen in Los Alfaques und Ingoldstadt, so waren es diese Anlässe, die zu der durchgreifenden Regelverbesserung im ADR[4)] führten.

Generelle Überlegungen

Ausgehend von der Vorgabe „Freiheit von unvertretbaren Risiken" müssen die sicherheitsrelevanten Qualitätsmerkmale eines Produkts oder Systems bei der Gestaltung und Realisierung von Sicherheit ausgerichtet werden. Dazu gehören das Emissionsverhalten, die passiven Beschaffenheitsmerkmale und die aktiven Funktionsmerkmale.

Beim Emissionsverhalten muss zwischen unerwünschten Nebenwirkungen und notwendigen Nutzfunktionen unterschieden werden. Die erforderlichen Schutzmaßnahmen vor unerwünschten Nebenwirkungen lassen sich grundsätzlich anhand der allgemein anerkannten Regeln der Technik bestimmen. In besonderen Fällen wie dem Immissionsschutz und dem Strahlenschutz wird ein Verweis auf den Stand der Technik bzw. den Stand von Wissenschaft und Technik vorgenommen. Bei den Nutzfunktionen gibt es risikofreie, risikoarme und risikobehaftete Ausbreitungsbereiche, denen entsprechende Schutzmaßnahmen zugeordnet werden. Darüber hinaus gibt es stellenweise Minimierungsgebote.

Passive Beschaffenheitsmerkmale gelten als unverlierbar. Man unterscheidet unverlierbare und technisch unverlierbare Beschaffenheitsmerkmale, also z. B. die Schwerkraft oder die geführte bruchsichere Druckfeder. Zusammengefasst ergeben die passiven unverlierbaren Beschaffenheitsmerkmale inhärente Sicherheit, die mit zugeordnetem Aufwand nachgewiesen werden muss.

Aktive Funktionsmerkmale können verloren gehen, wobei das stochastische Versagen durch geeignete Verfahren zu behandeln ist. Gebräuchlich ist hier die redundante Auslegung, bis hin zur diversitären Redundanz. Es gilt hierbei, zwei unterschiedliche Sicherheitskonzepte gegeneinander abzuwägen:

- „fail-safe": Bei einem Versagen eines aktiven Funktionsmerkmals wird das technische Erzeugnis in einen definierbaren „sicheren Zustand" überführt (wie z. B. Zwangsbremsung). Infolge einer solchen Sicherheitsmaßnahme wird die laufende Betriebsfunktion beendet.
- „fail operational": Bei einem Versagen eines aktiven Funktionsmerkmals wird das technische Erzeugnis in ein funktionell eingeschränktes, aber „sicheres Funktionsverhalten" überführt. Bei einer derartigen Sicherheitsmaßnahme wird die laufende Betriebsfunktion in eingeschränkter Form fortgeführt (wie z. B. die Notlandung, d. h. die Landung auf dem nächsterreichbaren Flughafen).

Je komplexer Produkte, Anlagen oder Systeme aufgebaut sind, desto unverzichtbarer wird ein geeignetes Instrumentarium aus Managementsystemen. Dazu werden optimal die Konzeptions- und Definitionsphase (Planungsprozess), die Entwicklungs-, Konstruktions- und Herstellungsphase (Realisierungsprozess) sowie die Betriebs- bzw. Nutzungsphase und die Rückbau-, Entsorgungs- und Recyclingphase (Betriebsphase) in einem zentral geführten Konfigurationsmanagement zusammengeführt. Das darin integrierte Sicherheitsmanagementsystem muss dazu unter eine eigene Verantwortung gestellt werden, die zentral alle Ebenen der Projekt- bzw. Systemstruktur erfasst. Ein derartiges Phasenkonzept erleichtert nicht nur das technische Management, sondern sichert in besonderem Maße auch die notwendigen organisatorischen Managementmaßnahmen und führt letztlich dazu, dass das ordnungsgemäße Verfolgen und Überwachen der vorgegebenen Ziele erst möglich wird.

Für alle Phasen gilt, dass an vorrangiger Stelle sicherzustellen ist, dass die Struktur und Ausformung der Sicherheitsdokumentation (des „safety case", auch „safety assessment" nach IEC 1508 oder nach DIN EN ISO 12100 „Technische Unterlagen" genannt) folgenden acht Punkten entspricht:

- In allen Phasen müssen die technischen Vorgaben eindeutig, klar verständlich und nachvollziehbar sein.
- Die Randbedingungen, unter denen die Antworten zur Bildung des „safety case" gegeben werden, müssen für jede Phase von den zuständigen und verantwortlich handelnden Personen eindeutig beschrieben und auch begründet werden.
- Die herangezogenen Bewertungsmaßstäbe müssen nachvollziehbar dargestellt werden, wobei das zugrunde gelegte Regelwerk aus gesetzlichen und technischen Bestimmungen konkret zu benennen ist. Die ggf. notwendige Bezugnahme auf den Stand der Technik oder den Stand von Wissenschaft und Technik ist zu integrieren.
- Die Antworten auf die phasenspezifischen Fragestellungen müssen klar zwischen Tatsachen, Angaben der handelnden Personen, Berechnungen, Annahmen, Prüfergebnissen und Schlussfolgerungen unterscheiden. Darüber hinaus ist die Bewertung getrennt zu führen.
- Unterschiede in den Bewertungen in den Phasen sind von den verantwortlich handelnden Personen deutlich hervorzuheben und zu begründen.
- Schlussfolgerungen müssen transparent und vollständig nachvollziehbar sowie in sich schlüssig sein.
- Der „safety case" ergibt sich aus den einzelnen Phasen des Produkt-Lebenszyklus und muss aus sich heraus verständlich und nachvollziehbar sein.
- Die Dokumentation muss vollständig sein und insbesondere alle rekursiven Iterationsschritte enthalten. Die Transparenz über alle drei Prozesse muss durchgehend gewährleistet sein. Der Interessenschutz kann besondere organisatorische Maßnahmen notwendig machen, ohne jedoch das

[4)] ADR: Accord européen relatif au transport international des marchandises dangereuses par Route; Europäische Übereinkommen über die internationale Beförderung gefährlicher Güter auf der Straße.

Interesse „Öffentlich-Technischer Sicherheit“ unzumutbar zu beeinträchtigen.

Systematik

Mit der Veröffentlichung der Sicherheitsnorm DIN 31004-1 „Begriffe der Sicherheitstechnik – Grundbegriffe” wird der Begriff der Sicherheit mit dem des Risikos in Zusammenhang gesetzt. Die Betrachtung des Risikos ist eine probabilistische Sicht auf stochastische Versagensformen von technischen Erzeugnissen und somit Bestandteil des allgemein anerkannten Stands der Technik. Bei der probabilistischen Betrachtung von Sicherheit steht die Häufigkeit eines Schadenseintritts (Wahrscheinlichkeitsannahme) verknüpft mit dem möglichen Ausmaß des Schadens im Fokus. Hierbei wird auf das „größte noch vertretbare Risiko“ (Betrachtung des Grenzrisikos) Bezug genommen. Jedoch lässt sich dabei das größte noch vertretbare Risiko nicht absolut definieren. Es ist vielmehr ein Ergebnis aus kulturellen, gesellschaftlichen, technischen, wirtschaftlichen und ggf. versicherungsrechtlichen Erwägungen. Durch entsprechende Maßnahmen wird das tatsächlich festgestellte Risiko so weit reduziert, bis es als vertretbar eingeschätzt wird. Dabei muss stets bewusst sein, dass Maßnahmen zur Reduzierung eines Risikos in aller Regel weitere, anders geartete Risiken[5)] induzieren können, die ihrerseits zur Erhöhung des Gesamtrisikos führen.

Der deterministischen Betrachtung von Sicherheit liegt eine maximal auftretende Auswirkung bei einem Schadensfall bzw. einer maximalen Einwirkung beim Belastungsfall zugrunde („worst case“-Betrachtung). Für diesen „worst case“ wird die Bemessung der Struktur (technische Gestaltung) bzw. der erforderlichen Sicherheitsmaßnahmen vorgenommen, das Prinzip des Versagensausschluss wird angewandt.

Beide Betrachtungsweisen sind anerkannte Grundlagen der Ingenieurswissenschaften und enthalten in Teilen Elemente der jeweils anderen Betrachtungsweise. Für die sicherheitstechnische Anwendung erfolgt die Betrachtungsweise entsprechend der einmal gewählten Präferenz „worst case“ oder „Grenzrisiko“. Die einmal gewählte Betrachtungsweise ist konsequent beizubehalten – bei gegenseitigem Ausschluss auf makroskopischer Ebene.

Zur einzuhaltenden Systematik gehört auch die Überwachung als Bindeglied zwischen Sicherheitstechnik und Technikrecht. Hier befinden wir uns in einer Umbruchsituation in Europa, da der Staat zunehmend Aufgaben zur Sicherheit von seinen Institutionen in die Wirtschaft verlagert. Eine sorgfältige Beobachtung dieses Vorgehens innerhalb der Europäischen Union und auch global ist insofern gefordert, als die öffentlich technische Sicherheit tangiert ist, die der Staat stets zu garantieren hat. Schließlich ist die technische Sicherheit genauso zu werten wie die innere und äußere Sicherheit des Staates. Bei der Verlagerung von Überwachungsaufgaben in den Markt bietet sich eine Bilanzierung mit der Betrachtung des Risikos an, um begründet von den Durchführungsaufgaben des Staates in den reinen Gewährleistungsbereich überzuleiten. Die obersten Bundes- und Landesbehörden sowie die nachgeschalteten Behörden müssen so weit wie nötig ihre Funktionen weiterhin wahrnehmen, wie daneben nur so weit wie möglich diese Funktionen in den Markt gegeben werden sollten. Insofern ist konkret das Handeln der Europäischen Kommission im Rahmen des Neuen Konzepts und des Gesamtkonzepts zu beobachten, um gegebenenfalls steuernd eingreifen zu können.

Vor diesem Hintergrund sind die Hersteller technischer Einrichtungen bei der Erzeugung der Technischen Sicherheit im Bereich der überwiegenden Gewährleistungsverantwortung des Staates besonders auf ein gut organisiertes, sorgfältiges und zweckmäßiges sowie systematisches Vorgehen angewiesen, das ihnen mit diesem Leitfaden an die Hand gegeben wird.

Ziele der Sicherheitstechnik

Um Sicherheit von technischen Systemen über eine bestimmte Dauer hinweg zu generieren und zu erhalten, müssen die Systeme in ihrer Gesamtheit analysiert werden. Die bekannten Verhaltensanalysen FMECA, FMEA oder HAZOP[6)] können beispielsweise für die Feststellung und Bewertung funktionaler Abhängigkeiten und Wechselwirkungen von Einheiten, Komponenten und Bauteilen hinsichtlich der Nutzung herangezogen werden. Zweckdienlicherweise benutzt man dazu eine sicherheitstechnische Rahmenspezifikation, die optimal nach folgenden Gesichtspunkten gegliedert wird:

– Sicherheitsmethodik (methodischer Rahmen, um alle Problemstellungen hinsichtlich sicherer technischer Systeme zu bearbeiten),
– Sicherheitskonzept (systemübergreifenden Darstellung sämtlicher Zusammenhänge, die Auswirkungen auf Versagensmöglichkeiten haben können),
– sicherheitstechnische Anforderungen (Zuordnung entsprechender Vorgaben für die bei Baueinheiten des Systems) und Nachweisführung.

Die Rahmenspezifikationen „Sicherheitstechnik“ ist die fachliche Plattform für die Erstellung der Spezifikation für alle Baueinheiten. Sie wird auch als Handlungs- und Entscheidungsrahmen für die Durchführung aller Arbeiten herangezogen, die für das Zusammenwirken aller beteiligten Unternehmen, insbesondere im Sinne juristischer Personen, mit aufsichtsführenden Institutionen von Bedeutung sind. Dabei sind zeitlich zufällige und umgebungsbedingte Versagensfälle zu berücksichtigen.

Als Voraussetzungen für ein sicherheitsmethodisches Vorgehen sind Sicherheitsdefinition, Sicherheitsengineering und Sicherheitsmanagement zu nennen. Durch einfaches Versagen eines Funktionselements darf kein sicherheitskritisches Versagen im Gesamtsystem vorkommen, und die Wahrscheinlichkeit für ein Mehrfachversagen, das zu einem sicherheitskritischen Versagen im Gesamtsystem führen kann, darf einen bestimmten Grenzwert nicht überschreiten. Diese Grenzwerte sind einsatzspezifisch und müssen so bestimmt werden, dass mögliche Abweichungen vom bestimmungsgemäßen Betrieb durch fahrlässigen Umgang kein sicherheitskritisches Versagen im System herbeiführen.

Sämtliche sicherheitstechnischen Tätigkeiten müssen nach nachstehender Abfolge erfolgen: Ausschluss von sicherheitskritischen Versagensfällen (Versagensausschluss aufgrund natürlicher oder technischer Integrität, wobei es sich hier um deterministische Maßnahmen gegen Einfachversagen han-

[5)] Nach 9/11 haben in den USA viele Menschen das Flugzeug gemieden und dafür den Pkw benutzt. Es gab zusätzliche Tote im Straßenverkehr, und zwar in der Größenordnung der Katastrophe von 9/11.

[6)] FMECA: US-amerikanische Norm MIL-STD-1629A „Procedures for Performing a Failure Mode, Effect and Criticality Analysis“, 24. November 1980, FMEA – Fehlermöglichkeits- und Einflussanalyse. DGQ-Band 13-11. 5. Aufl. Frankfurt a. M. 2012. HAZOP: BS IEC 61882: Hazard and operability studies (HAZOP studies) – Application guide. British Standards Institution 2001.

delt[7], Ausschluss der Folgen sicherheitskritischer Versagensfälle und Begrenzung ihrer Wahrscheinlichkeit durch die Anwendung der Zuverlässigkeitstechnik.

Herausforderungen der Zeit

Software-basierte Funktionalität

Moderne Technik und Systeme besitzen mittlerweile einen merklichen Anteil softwarebasierter Funktionen. Daher kommt Software in der Betrachtung von Technischer Sicherheit eine immer größer werdende Bedeutung zu und muss wie ein Produkt betrachtet werden.

Sicherheit von Software ist ausschließlich durch besonders ausgewählte konstruktive und organisatorische Maßnahmen zu erreichen. Daher ist die Herstellung von Software ebenfalls analog hinsichtlich der sicherheitsgerechten Vorgehensweise zu planen.

Technische Sicherheit softwarebasierter Funktionen bedingt eine frühe integrative Behandlung, denn die technische Sicherheit von Produkten und Systemen basiert in rasant zunehmendem Maße nicht zuletzt auf der IT-Sicherheit. Sehr wesentlich ist eine Programmiersprache, die Zuverlässigkeit und Sicherheit unterstützt, semantisch und syntaktisch vollständig definiert ist und die Umsetzung des Softwaremodells in allen Eigenschaften umfassend unterstützt sowie Fehler vermeidet bzw. erkennt. Ferner ist die Programmstruktur algorithmisch beherrschbar zu gestalten, was eine Beschränkung der Komplexität nach sich zieht. Besondere Aufmerksamkeit ist den offenen Systemen zu widmen, die an der Schnittstelle rückwirkungsfrei mit externer Software interagieren können. Zur mentalen Beherrschung der Komplexität von Software basierten Funktionen ist eine durchschaubare und mental beherrschbare Funktionsauslegung zu realisieren. Intelligentes Verhalten über interpretative Algorithmen muss vorhersagbar und verlässlich sein (deterministisch in exaktem Kontext). Dies gilt insbesondere für die Kombination von komplexen Funktionen wie z. B. bei heutigen Assistenzsystemen im Auto.

Bei softwarebasierten Systemen ist Sicherheit als zweiseitige Eigenschaft überlebenswichtig, nämlich als Betriebs- wie auch als Informationssicherheit.

Human Factors

Sämtliche Faktoren der Interaktion des Menschen mit einem technischen System gelten über den gesamten Produkt-Lebenszyklus als Human Factors. Es fallen also nicht nur die Handlungsfehler im Betrieb unter diese Kategorie, sondern auch alle in den vorlaufenden Phasen. Schließlich ist auch der Produktentwickler nur ein Mensch. Geeignete sozio-technische Systeme müssen demzufolge einerseits die unverzichtbaren Potenziale wie auch die unveränderlichen Einschränkungen des Menschen berücksichtigen[8]. Eine angemessene Fehlerkultur erkennt einen Fehler als Lernchance und fragt nicht: „Wie konntest Du nur?“, sondern: „Wie konnte es dazu kommen?” Wir müssen von einer Fehlerkultur in eine Lernkultur überleiten. Heute werden drei Modelle der Einbeziehung von HFE-Experten verwendet:

(a) Integriertes Modell: Hier ist der HFE-Fachmann (Arbeitswissenschaftler, Psychologe, Mediziner) von Anfang an im Entwurfsteam integriert.

(b) Intermittierendes Beteiligungsmodell: Hier wird der HFE-Experte in kritischen Entwurfsphasen hinzugezogen. Dies gibt die Möglichkeit, erfahrene Operateure (z. B. Piloten, Wartungspersonal.) einzubeziehen.

(c) Post hoc Beteiligungsmodell: Des Weiteren ist es von Nutzen, bei hochkomplexen Systemen eine partizipative Integration des zukünftigen Nutzers anzustreben.

Die Ausgestaltung des Zusammenwirkens von Mensch und Maschine muss in der Sicherheitskonzeption angelegt sein, wobei die Spannbreite von dominanter Maschine bis zum dominierenden Menschen reicht; Eingriffsmöglichkeiten können aber auch kooperativ vergeben werden.

Unterstützendes Management

Managementverfahren sind unabdingbare Voraussetzung für die Erzeugung von und den Erhalt der Sicherheit in allen Phasen des Produktlebenszyklus. Folgende Verfahrensweisen werden zielführend eingesetzt: Projektmanagement, Konfigurationsmanagement und Projektdefinition (mit Projektstrukturierung und -spezifizierung), Zuverlässigkeitstechnik, Umgebungsengineering, Herstellung und Prüfung, Qualitätsmanagement, Nachweisführung, zweckdienliches Beanstandungs- und Bauabweichungswesens, Instandhaltung sowie sicherer Betrieb mit Erstellung und Verfolgung von Instandhaltungsvorschriften sowie Betriebsvorschriften.

Im Leitfaden werden die Prinzipien und maßgebenden Kriterien für alle Phasen des Lebenszyklus aufgeführt; eine über dieses Maß hinausgehende hinreichende Vertiefung ist der einschlägigen Fachliteratur zu entnehmen. Folgerichtig werden nur die wichtigsten Voraussetzungen, Zuständigkeiten und Methoden quasi als Checkliste dargestellt. Alle Festlegungen sind rechtzeitig zu treffen, schriftlich festzulegen und für den gesamten Produkt-Lebenszyklus anzuwenden.

Für das Projektmanagement ist neben der schriftlichen Festlegung insbesondere zu kontrollieren, ob alle vertraglichen Festlegungen in sich konsistent sind und die Festlegung der zuständigen natürlichen oder auch juristischen Personen in Bezug auf technische, terminliche und kostenmäßige Zuständigkeit erfolgt ist. Es folgen die organisatorischen Zuständigkeiten und die Bereitstellung der einzusetzenden Arbeitsmittel, Methoden und Vorgehensweisen.

Für das sicherheitsbezogene Konfigurationsmanagement ist analog vorzugehen, insbesondere ist zu kontrollieren, dass der Auftraggeber und die aufsichtführenden Institutionen in den Informationsfluss des Konfigurationsmanagements eingebunden sind. Wie beim Projektmanagement ist auch hier die Festlegung der organisatorischen Zuständigkeiten im Unternehmen sowie die Bereitstellung einzusetzender Arbeitsmittel, Methoden und Vorgehensweisen schriftlich zu fixieren.

Im Rahmen der Zuverlässigkeitstechnik wird auf das VDI-Handbuch „Verlässlichkeit“ erwiesen und hier insbesondere auf die Richtlinie VDI 4003 „Verlässlichkeitsmanagement“. Insbesondere ist die Festlegung von Bedeutung, für welche Baueinheiten der Projektstruktur ein deterministisch begründbarer Versagensausschluss gelten soll.

Zum Umgebungsengineering und für die Festlegung wird auf die Richtlinie VDI 4005, Blatt 1 bis 5 verwiesen. Alle Gesichtspunkte und Anforderungen hinsichtlich ursprünglicher und objektbeeinflusster Umgebung werden erfasst und qualita-

[7] Eine Grundlage dafür findet sich in der Ausarbeitung „Darstellung des sicherheitsgerechten Gestalten im Bauwesen und im Anlagenbau“ im Abschnitt 4.4.

[8] siehe „Saarbrücker Erklärung“ anlässlich des World Congress on Safety of Modern Technical Systems, Saarbrücken 2001.

tiv und quantitativ bestimmt, so z. B. elektromagnetische Verträglichkeit und Blitzschutz.

Für die Realisierung ist insbesondere über die üblichen Festlegungen hinaus die Rückverfolgbarkeit von herausragender Bedeutung, ebenso die Einbindung des Auftraggebers in die Planung des Prüfablaufs einschließlich der sog. mandatory inspection points, also der Abnahmeprüfungen. Diese Punkte sind Bestandteile des Freigabeverfahrens.

Bei unbeabsichtigten Abweichungen von den Spezifikationen (Beanstandungen) und einmalig beabsichtigten Abweichungen (Bauabweichungen) sind die schriftliche Festlegung und die Kommunikation von herausragender Wichtigkeit.

Bei den einzusetzenden Arbeitsmitteln, Methoden und Vorgehensweisen ist insbesondere auf die Einbindung von IT-Programmen zu achten.

Als Voraussetzung für die sicherheitsbezogenen Prüfungen gilt, dass das Unternehmen gemäß DIN ISO 9001 zertifiziert ist. Die Protokollierung der Prüfungen erfolgt mit personeller Zertifizierung und Zuteilung von Prüfstempeln. Selbstverständlich ist auf die geeigneten Mess- und Prüfmittel mit entsprechenden Eich- und Kalibrierungszyklen zurückzugreifen. Im Zuge der Prüfungen ist es notwendig, die „lessons learned" zentral zu erfassen, lückenlos zu dokumentieren und für die Prozessverbesserung bereitzustellen.

Ein sicherheitsgerechtes Beanstandungs- und Bauabweichungswesen ist zu etablieren, wobei eine besondere Bedeutung der Kontrolle und der Dokumentation des Entscheidungsablaufs zukommt. Überschau- und nachvollziehbar werden die Aktionen aus diesem Bereich durch regelmäßige Audits.

Die sicherheitsgerechte Instandhaltung ist eine wesentliche Voraussetzung für die über die Lebensdauer eines Produkts zu erhaltende Sicherheit. Beanstandungen und Bauabweichungen müssen regelmäßig durch das Prüflesen bekannt gemacht werden.

Für den Betrieb gilt, dass zweckdienliche und sicherheitsgerechte Betriebsvorschriften geplant, angewendet und jederzeit beachtet werden. Das bezieht sich sowohl auf den Regelbetrieb wie auf den Ersatzbetrieb und muss unter Einbindung der Auftraggeber, der mitwirkenden Unternehmen und der aufsichtführenden Institutionen abgeklärt sein. Zweckdienlicherweise wird ein Betriebs-Logbuch vorgehalten. Für das Management der sicheren Entsorgung, des Rückbaus und des Recyclings gelten die Voraussetzungen und Checklisten wie für den sicheren Betrieb analog.

Das Handlungsschema

Das Handlungsschema ist ein sicherheitsmethodisches Ablaufdiagramm (**Bild 3**) mit detaillierten Beschreibungen, das fachgebietsübergreifend die ersten drei Phasen im Lebenszyklus eines Produkts umreißt. Es handelt sich um die Konzepti-on-, Definitions- und Entwicklungsphase, also Phasen, die man zusammengefasst auch als Software-Phasen bezeichnen kann[9)].

Für Planer, Entwickler, Hersteller, Betreiber, Genehmigungsbehörden und sonstige aufsichtführende Institutionen und deren Sachverständige würde es heute schon die sicherheitstechnische Überwachung erleichtern, wenn Ähnliches und Gleichlautendes in Sicherheitsvorgaben vereinheitlicht würde. Darüber hinaus würde die Öffentlichkeit – nicht nur bei Unfällen – einer einheitlichen Sicherheitsphilosophie mehr Verständnis entgegenbringen als der heutigen Normenvielfalt.

Zum besseren Verständnis wird das Handlungsschema zunächst in Einzelheiten zerlegt.

Deterministik

Zu Beginn werden die Versagensformen ermittelt (**Bild 4**), wobei die Handlungsschritte 1.1-1.4 (Auswahl der Baueinheit, Versagensanalyse, Klassifizierung der Auswirkungen und sicherheitskritisches Versagen durch Einfach-Versagen oder Mehrfach-Versagen) betrachtet werden müssen. Es folgt dann eine Entscheidung gemäß der Frage, ob es sich bei dem Produkt/System bzw. einer Baueinheit um die ausschließliche Möglichkeit eines Einfach-Versagens handelt. Bei positiver Antwort ist man dann im Bereich der Deterministik. Nehmen wir den klassischen Fall einer Baueinheit aus dem Brückenbau und betrachten das Auflager. Hier wirkt die Masse, die die Auflagekraft ergibt, die es durch Baumaßnahmen abzufangen gilt. Ist dies sachgemäß ausgeführt, ist der Nachweis ausreichender Sicherheit erbracht, d. h. die Phasen 1 bis 3 sind erfolgreich durchlaufen.

Ein Beispiel aus dem Transport gefährlicher Güter ist die Auslegung des Transportbehälters Castor für Brennelemente. Wegen der grundsätzlich unbegrenzt hohen Menge an Radioaktivität für den Transport in so genannten Typ B-Behältern werden diese nach dem Prinzip des Worst case ausgelegt. Einfach-Versagen ist damit begründbar durch unverlierbare technisch bedingte Eigenschaften ausgeschlossen (**Bild 5**). Der Worst case besteht hierbei aus einem 9-m-Fall auf ein unnachgiebiges Fundament, einem Penetrationsversuch aus 1 m Höhe auf einen Dorn, einem halbstündigen Feuer von 800 °C und einem Eintauchtest in Wasser. Der Nachweis kann dabei entweder durch Berechnungen, Versuchen oder durch Analogiebetrachtungen erfolgen. Für den sehr kritischen Fall der Stoßbeanspruchung aus 9 m sind die Berechnungsgrundlagen auch heute noch nicht ausreichend, weshalb mindestens ein Versuch verifiziert werden muss. Man kann auch auf die Ähnlichkeitsmechanik zurückgreifen, wird aber in der Regel auch zur Überzeugung der aufsichtsführenden Institutionen und der Öffentlichkeit einen Prototyptest durchführen müssen.

Probabilistik

Je komplexer eine technische Einrichtung bzw. je anspruchsvoller der jeweilige Einsatzzweck (Missionsprofil) ist, desto notwendiger ist es, dass auf Beschaffenheit (passive Eigenschaftsmerkmale) und Funktionsverhalten (aktive Eigenschaftsmerkmale) Verlass besteht.

Dies setzt vor allem voraus, dass sowohl die natürlichen als auch die objektbeeinflussten Umgebungseinflüsse (Umwelt-Engineering) und deren Wirkungen auf das technische Erzeugnis ermittelt und berücksichtigt werden, ebenso wie das probabilistische Versagensverhalten, wobei hier nicht das „technische Risiko" angesprochen ist, sondern die gezielte Beeinflussung der „Überlebens-Wahrscheinlichkeit" des betrachteten technischen Erzeugnisses. Probabilistische Vorgehensweisen ersetzen keinesfalls die bewährten deterministischen Vorgehensweisen, sondern ergänzen sie bei entsprechendem Bedarf. Man denke nur an den Brand eines Zuges im Tunnel. Das Konzept der Zielbremsung nutzt die kinetische Energie eines mit Betriebsgeschwindigkeit fahrenden Zuges, um ihn mittels einer elektronischen Regelungseinrichtung so gezielt abzubremsen, dass er an einer Stelle zum Stehen kommt, die für Rettungskräfte zugänglich ist. Für diese Regelungseinrichtung

[9)] Am Ende des Leitfadens findet sich ein Ablaufdiagramm aus dem Bereich des Bauwesens und des Anlagenbaus, das alle sechs Phasen des Lebenszyklus eines Produkts beschreibt.

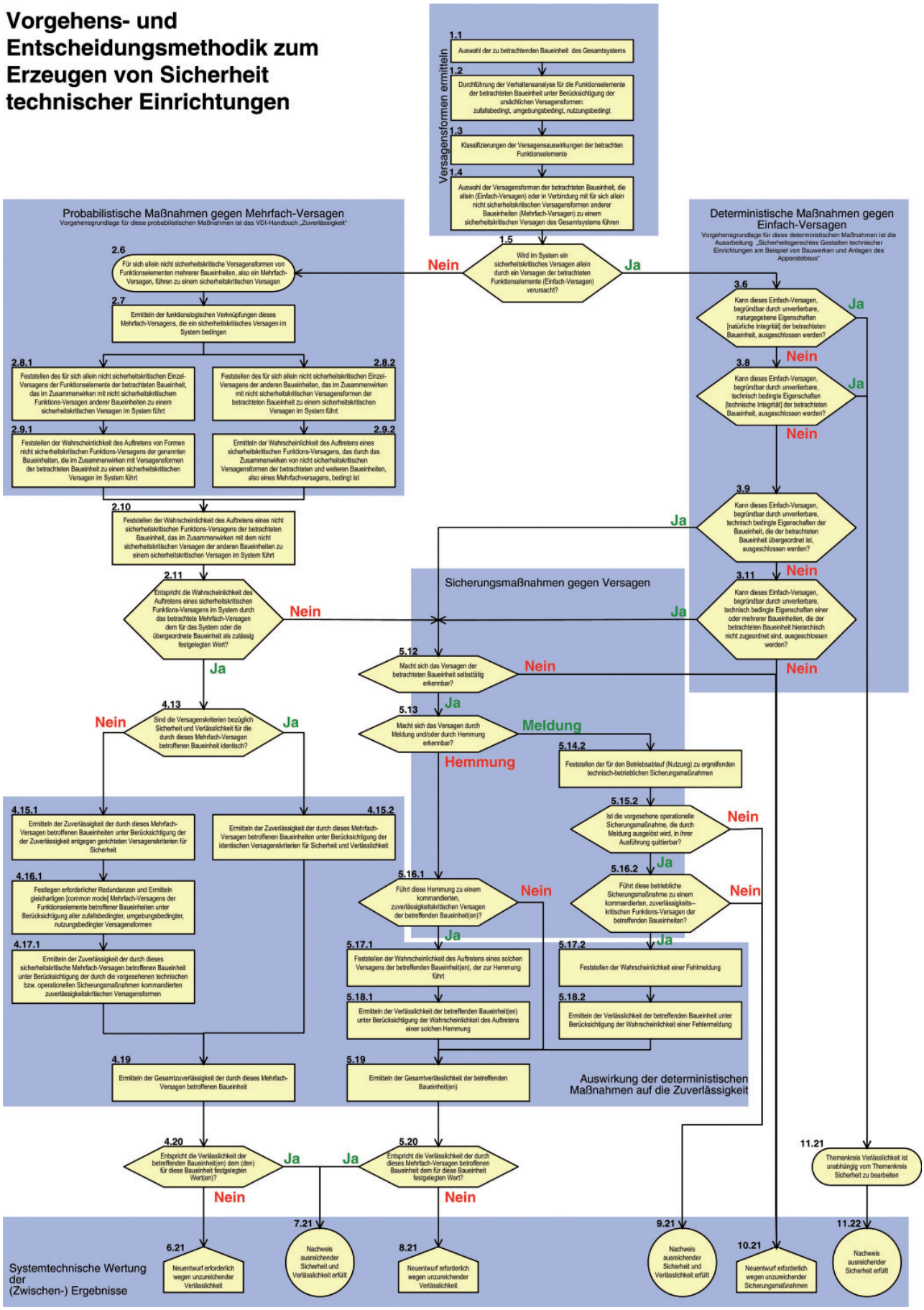

Bild 3 Fachgebietsübergreifender Handlungsablauf der ersten drei Phasen.

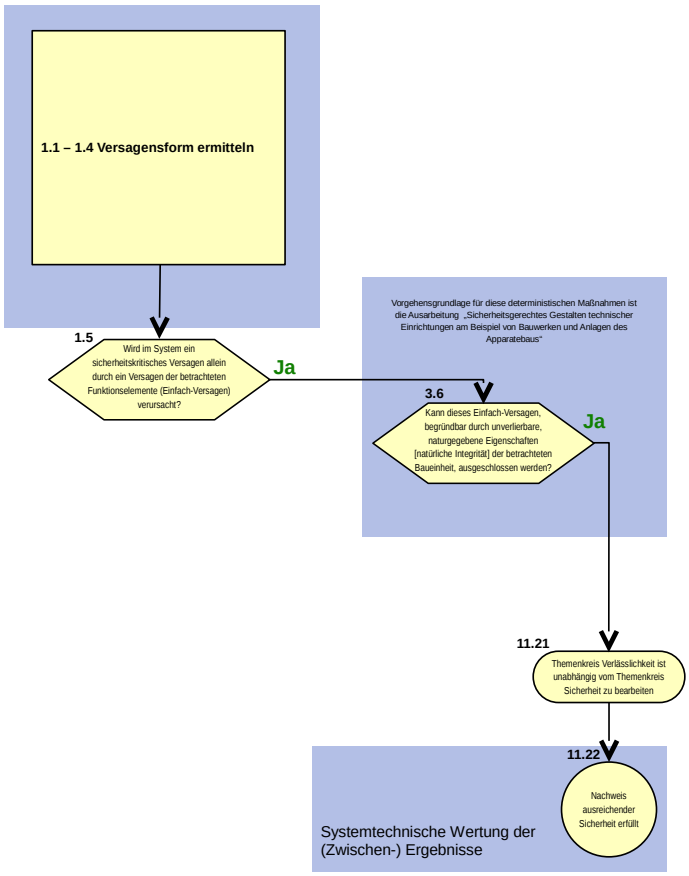

Bild 4 Ausschnitt aus dem Handlungsablauf (unverlierbare **naturgegebene** Eigenschaften).

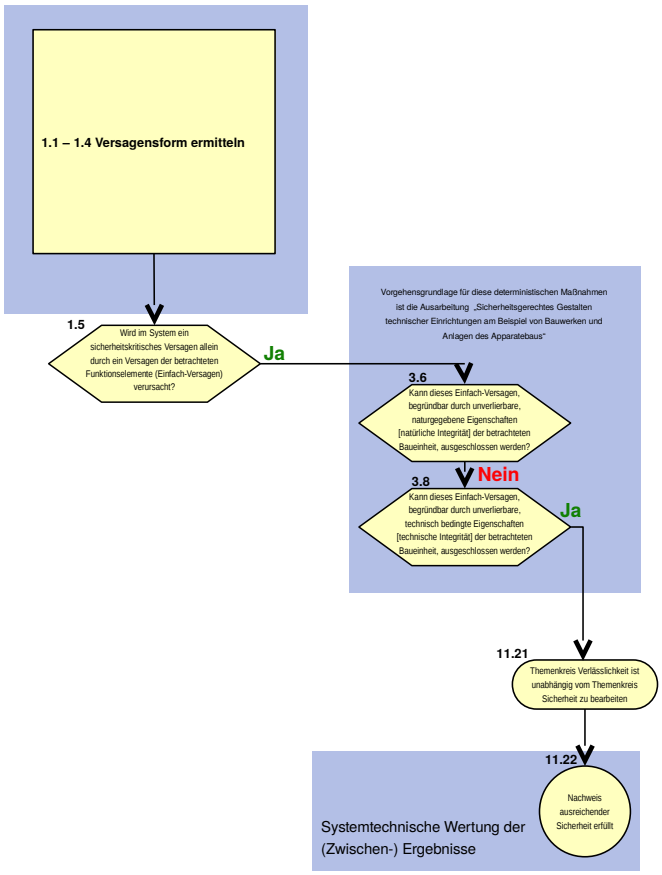

Bild 5 Ausschnitt aus dem Handlungsablauf (unverlierbare **technische** Eigenschaften).

käme dann die probabilistische Vorgehensweise (Zuverlässigkeitstechnik) zur Anwendung.

Zusammenfassung zum Handlungsschema

Das im VDI Ausschuss „Technische Sicherheit"erarbeitete Handlungsschema steht für die Fachwelt wie für die Öffentlichkeit zur Verfügung. Für alle Fachgebiete werden damit alle Vorgehensweisen – von der deterministischen über die semi-probabilistische bis hin zur probabilistischen – für die ersten drei Phasen des Lebenszyklus zusammengestellt. Da alle Vorgehensweisen in einem Schema dargestellt werden, ist dieses zwangsläufig kompliziert, aber vollständig.

Im Handlungsschema werden Handlungs- und Entscheidungsschritte angegeben, mit denen Ursachen und Auswirkungen von Versagensfällen systematisch ermittelt werden (1.n). Handlungs- und Entscheidungsschritte in der probabilistischen Betrachtungsweise sind mit 2.n bezeichnet. Die Entscheidungsschritte 3.n gelten für die deterministischen Betrachtungsweise. Um die stochastisch erfassbaren Auswirkungen von Vorkehrungsmaßnahmen auf die Verlässlichkeit abhandeln zu können, gibt es die Schritte 4.n. Gleiche Abschätzungen hinsichtlich der Vorkehrungsmaßnahmen im Bereich der Deterministik werden durch die Schritte 5.n ermöglicht. Schließlich werden für die Beurteilung der technischen Auslegung noch die Schritte 6.n bis 11.n im Handlungsschema aufgeführt.

Einzelheiten dazu sind in einem umfangreichen Kapitel abgehandelt und müssen hinsichtlich des Verständnisses anhand des Handlungsschemas intensiv erarbeitet werden.

Das Schema muss für jeden einzelnen Anwendungsfall richtiggehend erarbeitet werden, d. h. die Geschäftsleitung, die F&E-Abteilung, die aufsichtsführenden Institutionen, die Prüf- und Zertifizierungsstellen sowie die Anwender der komplexen Produkte oder Systeme müssen den Inhalt für sich erarbeiten, um ihn dann für ihre Zwecke mit Beispielen für alle in der Wertschöpfungskette Handelnden verständlich zu machen. Für das Bauwesen und den Anlagenbau ist ein spezielles Handlungsschema beigefügt, das sämtliche sechs Phasen des Produktlebenszyklus umfasst: die dazu notwendigen Erläuterungen beziehen sich auf das Bauwesen ausschließlich.

Der VDI hält sich als Ansprechpartner zur Verfügung, um Fragen und Anregungen aufzugreifen und letztlich zu prüfen, inwieweit eine VDI-Richtlinie zielführend sein kann. Parallel zu diesem Diskurs in Deutschland wird die VDI-Publikation in Europa bekannt zu machen sein, um auch aus dieser Ebene Anregungen entgegenzunehmen.

Fazit

Das sicherheitsmethodischer Handlungsschema bedingt, dass:

– die Übertragung der systematisch erarbeiteten Sicherheitskonzepte in Projekt- und Systemspezifikationen erfolgt,
– die systembezogenen Anforderungen an die Gestaltung des gesamten Systems und seiner Baueinheiten bzw. Funktionselemente übernommen werden,
– die Festlegung von Sicherheitsanforderungen für die Nachweisführung abgebildet werden,

– die Sicherheitsanforderungen zur Erlangung von Betriebsgenehmigungen übertragen werden und
–die Erfassung und Auswertung aller auftretenden sicherheitskritischen Versagensformen für den gesamten Produkt-Lebenszyklus als „lessons learned“ zu Erfahrungsrückführung benutzt werden („experience feed back“).

Die Vorgehens- und Entscheidungsmethodik (Handlungsschema) bildet die geeignete Arbeitsgrundlage, um Entscheidungen zur Angemessenheit sicherheitstechnischer

Gestaltungsmerkmale systematisch zu entwickeln und zu beurteilen. Das gilt für die ersten drei Phasen des Produktlebenszyklus für alle Fachbereiche; für das Bauwesen und den Anlagenbau ist ein Handlungsschema über alle sechs Phasen aufgestellt und speziell für das Bauwesen mit der VDI-Gesellschaft GBG (Bauen und Gebäudetechnik) beraten worden. Das Handlungsschema wird damit der Herausforderung gerecht, die unterschiedlichen Vorgehensweisen in verschiedenen Fachdisziplinen zu überwinden. Zu diesem Zweck wird das empirische Erfahrungswissen auf dem Gebiet der „Technischen Sicherheit“ methodisch zusammengefügt und das bestehende Regelwerk systematisch kodifiziert werden müssen. Gleichzeitig kann die scheinbar gegensätzliche Zielsetzung „Sicherheit“ und wirtschaftlich sinnvolle „Verlässlichkeit“ als ganzheitliches Systemkonzept in Angriff genommen werden.

Botschaft

Das mit dieser Publikation angebotene Handlungsschema zur Erzeugung von Sicherheit in allen Fachbereichen der Technik ist grundsätzlich auch unabhängig von jeglicher Rechtsnorm anwendbar. Es ist insbesondere für die Wirtschaft wichtig, sich die Technik des Handlungsschemas zu erarbeiten, da die Sicherheitsverantwortung oft ganz aber sicher zum Teil bei dem Hersteller verbleibt. In der Versagensanalyse können die Einwirkungen von außen und von innen festgelegt werden, wobei das sog. Grenzrisiko als gesellschaftliches Konstrukt zur Anwendung kommt.

In der Gestaltung eines geschlossenen Regelwerks aus Rechtsnorm und technischer Norm findet man häufig neben dem Verweis auf konkrete Normen den Verweis auf den Stand der Technik bzw. den Stand von Wissenschaft und Technik. Die VDI-Richtlinien sind Bestandteil des Bereichs der technischen Normen und beschreiben im abgeschlossenen Regelwerk einen möglichen Weg. Der ist dann der gebräuchliche und mit Privilegien hinsichtlich der Beweisführung ausgestattete[10]. Aber neben diesem Weg sind andere grundsätzlich zulässig und diese geben damit Innovationen ihren Raum.

Der Markt mit seinen Mechanismen reicht für sich alleine allerdings nicht aus, technische Sicherheit von Erzeugnissen zu gewährleisten. Der VDI als Sprecher für die Technik möchte den Diskurs über das Handlungsschema im Hinblick auf eine Verbindlichkeit beginnen, und dabei alle Stakeholder einbinden, also Staat, Wirtschaft und Verbraucher. Der Binnenmarkt in Europa und die fortschreitende Globalisierung bedingen, dass die Diskussion auch auf europäischer und globaler Ebene angestoßen werden muss. TS 529

[10] *Schepel, H.; Falke, J.*: Legal aspects of standardisation in the member states of the EC and EFTA, Luxemburg: Publication office 2000.

Autor

Dr.-Ing. **Bernd Schulz-Forberg**, stellvertretender Vorsitzender des VDI-Ausschusses Technische Sicherheit, Berlin.