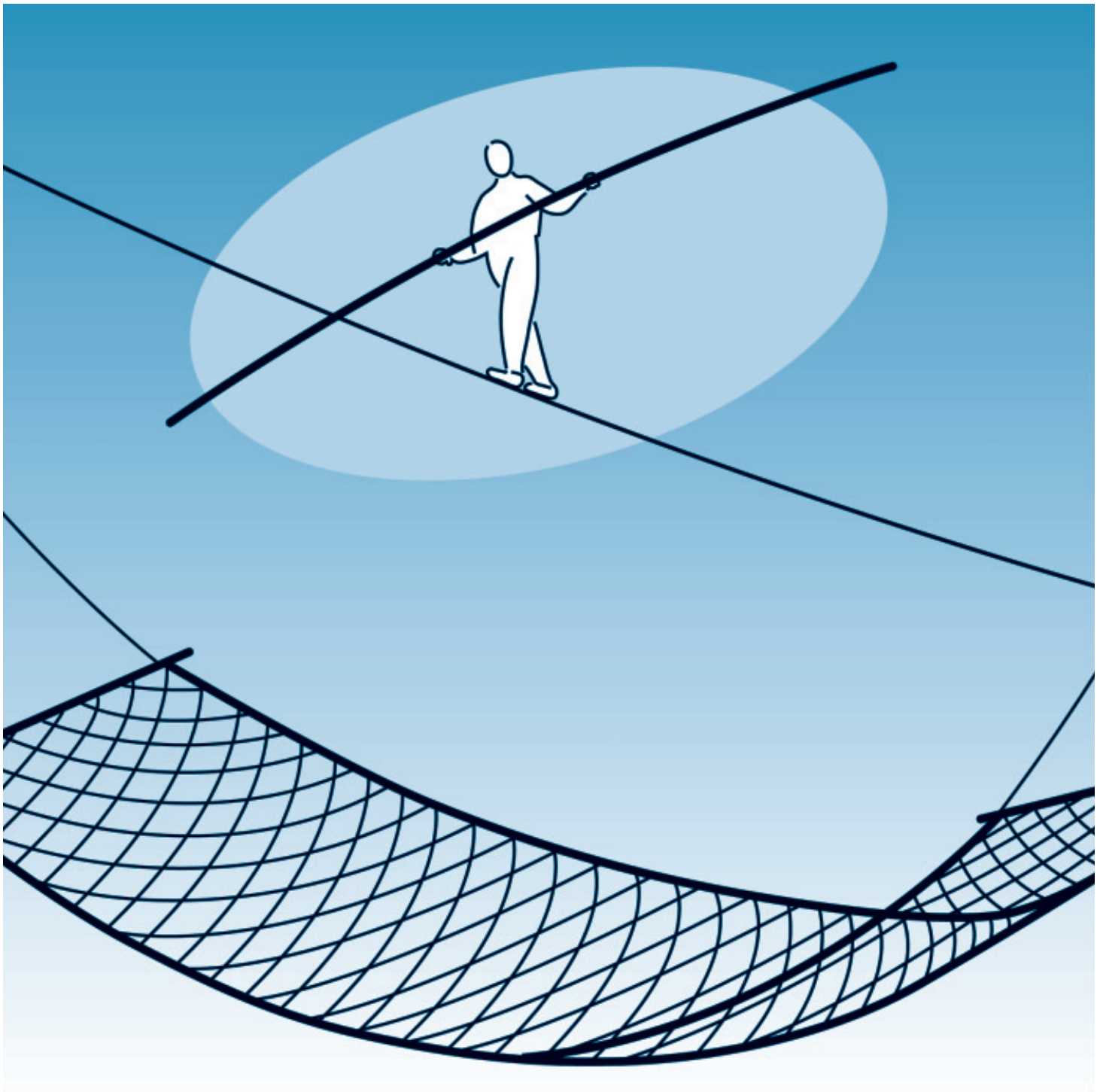
VDI

Qualitätsmerkmal „Technische Sicherheit"

Eine Denkschrift des Vereins Deutscher Ingenieure



Qualitätsmerkmal

„Technische Sicherheit"

- Eine Denkschrift

des Vereins Deutscher Ingenieure -

- INHALT -

1 Bedarf für ein sicherheitsmethodisches Konzept

1.1 Sicherheitstechnischer Handlungsbedarf

Das vergangene Jahrhundert war durch epochale technische Errungenschaften gekennzeichnet. Beide Weltkriege verursachten verheerende Verwüstungen, beschleunigten aber auch den technischen Fortschritt, der sich vor allen Dingen während der Wiederaufbauphase nach dem 2. Weltkrieg zeigte. Neuartige Technologien wurden entwickelt und werden ständig weiterentwickelt. Längst ist der weltumspannende Luftverkehr zur Realität geworden; die Raumfahrt hat sich zum ertragsfähigen Wirtschaftszweig entwickelt; die Mikroelektronik und die Computertechnik sind selbst aus der häuslichen Lebenssphäre nicht mehr wegzudenken. Allerdings vergrößerte sich infolge dieses technologischen Fortschritts auch die Zahl der Technikfelder; so werden heute an den Technischen Universitäten und Fachhochschulen Technikfelder gelehrt, an deren Existenz vor einem halben Jahrhundert noch nicht einmal zu denken war. Selbstverständlich entwickelte sich parallel zum technologischen Fortschritt auch die Sicherheitstechnik kontinuierlich weiter – allerdings spezifisch für die einzelnen Technikfelder. Eine der maßgeblichen Ursachen für diese anwendungsbezogene – sozusagen nach Technikfeldern strukturierte – Sicherheitstechnik ist in unserer Rechtsordnung zu suchen, weil die Rechtsgrundlagen der Sicherheitstechnik ebenfalls nach Technikfeldern strukturiert sind: Baurecht, Eisenbahngesetz, Luftverkehrsgesetz, Atomgesetz, Versuchsanlagengesetz – nur um einige zu nennen.

Bis heute hat die Zahl der technischen Fachdisziplinen bereits derart zugenommen, dass das gesamte Wissensgebiet der Technik unübersehbar und schlecht handhabbar geworden wäre, wenn nicht gleichzeitig fachgebietsübergreifende Managementmethoden und systemtechnische Arbeitsweisen eingeführt worden wären, um Planung, Verfolgung (Monitoring) und Nachweisführung in den verschiedenen technischen Fachdisziplinen nach einem ganzheitlichen Vorgehenskonzept vorzunehmen. Seit vier Jahrzehnten finden diese – unter dem Begriff interdisziplinäres Teamwork erfasste – fachgebietsübergreifenden Managementmethoden und systemtechnischen Arbeitsweisen immer weitere Anwendung. Kein größeres Vorhaben, das sich heutzutage über viele Jahre hinziehen kann, wird mehr ohne Einsatz eines zentralen Projektmanagements abgewickelt.

Mit zunehmender Globalisierung steigt auch der Zwang zum internationalisierten, über die Staatsgrenzen hinweg agierenden, multilingual befähigten Projektmanagement. Die Welt der Technik scheint keine Grenzen mehr zu kennen. Und doch gibt es diese Grenzen, und zwar auf dem Gebiet der Sicherheitstechnik. Hier gelten, abgesehen von den bereits existierenden europäischen Regelungen (die vornehmlich jedoch die Freizügigkeit des Warenverkehrs sicherstellen sollen), noch die national unterschiedlichen Rechtsordnungen. Denen ist gemein, dass nach ihrem Selbstverständnis die Sicherheitstechnik nach anwendungsbezogenen Technikfeldern strukturiert ist.

Anfang der siebziger Jahre des vergangenen Jahrhunderts kamen gesellschaftspolitische Vorstellungen auf, die den Bürgern ein „risikofreies“ Leben zu ermöglichen schienen. Im Mittelpunkt dieser Entwicklung stand häufig ein öffentlicher Diskurs über großtechnische und technologisch innovative Einrichtungen, wobei vor allem deren Sicherheit bzw. Sicherheitsfähigkeit als zweifelhaft dargestellt wurde. Insbesondere bei technologischen Innovationen wurde mehr über potenzielle Risiken und vorgeblich unerwünschte Nebenwirkungen diskutiert als über den eigentlichen Nutzen für die Bevölkerung und die wirtschaftlich-sozialen Chancen. Die Folge war, dass über die Sicherheit derartiger Einrichtungen letztendlich nicht mehr die technische, sondern zunehmend die rechtliche Kompetenz entschied. Über die gutachtlichen Aussagen der hinzugezogenen technischen Sachverständigen offenbarte sich auch die abträgliche Situation der heutigen Sicherheitstechnik, die je nach Anwendungsfeld unterschiedlich geprägte Konzepte vorsieht. Selbst das beispielhafte Normenwerk des Deutschen Instituts für Normung (DIN) weist eine bemerkenswerte Vielzahl unterschied licher Begriffsbestimmungen für „Sicherheit“ und „Technische Sicherheit“ auf.

Vor etwa zwei Jahrzehnten begannen in der Europäischen Gemeinschaft die Anstrengungen, den freien Warenverkehr bei Konsum- und Investitionsgütern zu realisieren. Damit einher ging die Frage, wie die Sicherheit für die Menschen, die die Güter nutzen, gewährleistet werden kann. Das zu dieser Zeit noch überwiegend nationalstaatlich ausgerichtete Instrumentarium der Sicherheitsüberwachung und -zulassung führte eher dazu, Handelshemmnisse aufzubauen, statt diese zu vermeiden. Die Europäische Kommission schuf deshalb mit dem „Neuen Konzept“ [New Approach] und dem „Gesamtkonzept“ [Global Approach] einen Maßnahmenkatalog, mit dem im operativen Bereich weitgehende Unabhängigkeit von nationalstaatlichen Stellen erreicht werden sollte. Geschaffen wurde dies mit dem Instrument der Konformitätserklärung, die dem

Modulbeschluss des Rates der Europäischen Union entsprechend entweder durch den Hersteller selbst oder durch die so genannten „Benannten Stellen“ abgegeben wird. Das Sicherheitsniveau selbst wird dabei durch die Europäischen Richtlinien vorgegeben und überwiegend durch mandatierte technische Normen konkretisiert. Wie wirkungsvoll dieser Maßnahmenkatalog letztlich ist, darüber teilen sich die Meinungen. Offensichtlich wurde bereits erkannt, dass das „Neue Konzept“ und das „Gesamtkonzept“ deutliche Schwächen aufweisen und zum Teil weit hinter der Wirksamkeit des abgelösten Systems stehen. Diese Schwächen, die den mit Sicherheitsfragen befassten Experten bereits bei der Einführung bekannt waren, sind vielfältig und die Europäische Kommission bessert zurzeit nach. Über die produktbezogenen Richtlinien hinaus gilt die „Richtlinie über die allgemeine Produktsicherheit“ 2001/95/EG vom 03.12.01 (veröffentlicht im Amtsblatt Nr. L 011 vom 15.01.02); diese regelt, dass alle Produkte, die innerhalb des Europäischen Wirtschaftsraums in Verkehr gebracht werden, sicher sein müssen. Wie dies sicherzustellen ist, bedarf allerdings weiterer Regelung.

Sowohl in der Luftfahrttechnik als auch der Raumfahrttechnik wird das System des „Neuen Konzepts“ nach wie vor durch die international bzw. europäisch vorgeschriebenen Prüfungen zur Flugzulassung bzw. durch abschließende Systemprüfungen ergänzt. So bestimmen auch die im Eisenbahnwesen eingeführten Interoperabilitätsrichtlinien, dass mit der Inbetriebnahmegenehmigung durch die nationale Sicherheitsbehörde das System des „Neuen Konzepts“ durch eine abschließende Systemprüfung ergänzt wird.

Es besteht also hinreichend Handlungsbedarf für ein sicherheitsmethodisch ganzheitliches Konzept, in welchem die verdeckten Gemeinsamkeiten der bereits bestehenden, allerdings anwendungsspezifisch begrenzten Sicherheitskonzepte zu einem interdisziplinär anwendbaren Gesamtkonzept zusammengefügt sind. Der Verein Deutscher Ingenieure (VDI) verfügt über die interdisziplinäre Fachkompetenz, ein derartiges sicherheitsmethodisches Konzept ganzheitlich auszuarbeiten und vorzustellen.

1.2 Einführung in den Themenkreis Sicherheitstechnik

In Wahrnehmung hoheitlicher Dienste hatten – zumindest in der Bundesrepublik Deutschland – staatliche Institutionen und Anstalten bisher sicherheitstechnische Nachweisführungen durchgeführt und sich so an der Beherrschung technischer

Risiken aktiv beteiligt. Die einschlägigen Richtlinien der Europäischen Union (EU) sehen inzwischen vor, dass diese sicherheitstechnischen Nachweisführungen zunehmend dem freien Markt überlassen bleiben und vom Staat nur noch überwacht werden. Die dazu erforderliche Fachkompetenz auf dem Gebiet der „Technischen Sicherheit“, die bisher überwiegend bei hoheitlich wirkenden Stellen gebündelt war, muss jetzt auf dem freien Markt beschafft werden. Mit dieser Denkschrift des Vereins Deutscher Ingenieure (VDI) soll zum Erhalt und zur Verbreitung dieser sicherheitstechnischen Fachkompetenz ein sicherheitsmethodisches Konzept angeregt werden, das in umfangreicher Bezugnahme auf die allgemein anerkannten Technischen Regelwerke sowie definierte Zielvorstellungen eine solide Basis für ingenieurwissenschaftliches Handeln auf dem Gebiet der Sicherheitstechnik bietet. Dieses sicherheitsmethodische Konzept ist gleichermaßen anwendbar für die Pflege und Weiterentwicklung bestehender Technikfelder (wie beispielsweise Bauwesen, Verkehrswesen, chemische Verfahrenstechnik, Energietechnik, Luftfahrttechnik, Anlagenbau, Maschinenbau, Elektrotechnik) wie zur Konzipierung und sicherheitstechnisch beherrschten Entwicklung neuartiger Technologien.

Unter „Technischer Sicherheit” wird begrifflich verstanden, dass ein technisches System, eine Anlage, ein Produkt über einen geplanten Zeitraum (gegebenenfalls die geplante Lebensdauer) hinweg die vorgesehenen Funktionen erfüllt und bei bestimmungsgemäßer Nutzung keine geschützten Rechtsgüter verletzt, d.h. weder Personen noch Sachen geschädigt werden, soweit dafür das System, die Anlage oder das Produkt ursächlich sein können. Die Zuverlässigkeit der Funktion über die vorgesehene Lebensdauer ist kein notwendiger Bestandteil der Sicherheit, sofern der Verlust der Funktion zu keinem unsicheren Zustand führt.

Sicherheit hat im Rahmen der Technologie-Diskussion nicht nur die Bedeutung von Technischer Sicherheit. Bezieht man sich auf den allgemeinen Sprachgebrauch, so fühlt sich ein Mensch dann sicher, wenn er sich nicht bedroht glaubt. Die Bedrohung muss keineswegs existentieller Natur sein. Bereits ein drohender Verlust an Lebensqualität kann eine Technik-Voreingenommenheit auslösen. Auch die Fremdbestimmung der eigenen Lebensführung und das damit verbundene Abhängigkeitsgefühl von nicht frei gewählten Bedingungen (Autonomie-Verlust) kann in einer freiheitlichen Wohlstandsgesellschaft zu aversiven Reaktionen einzelner Gruppen führen, wenn über Grenzen der Sicherheit zu diskutieren ist.

Einerseits sind in Teilen der Ingenieurwissenschaften aber auch der Biowissenschaften die Entscheidungsgrundlagen hierzu schwächer entwickelt, andererseits sind die Vorstellungen von Sicherheit in der Öffentlichkeit so breit angelegt, dass sich eine hinreichende Akzeptanz nur auf der Basis eines Risikominimierungsgebots – einer Eingrenzung mit akzeptiertem Grenzrisiko – herstellen lässt. Sinnfällig drückt sich die Verbrauchererwartung in der Vorstellung vom Reinheitsgebot aus, welches sich zumindest auf die unmittelbaren Lebensgrundlagen wie Nahrungsmittel, Trinkwasser und Luft erstreckt. Technologien, die bei offensichtlichem Nutzen, wie z.B. Konservierung, Verarbeitbarkeit, dieses Reinheitsgebot verletzen, werden soweit toleriert, als die Einhaltung gesetzlich festgelegter Schwellenwerte für etwaige Kontaminationen nur bei vorschriftsmäßiger Anwendung zu gewährleisten ist (Beispiel: „Gute landwirtschaftliche Praxis"). Der Abstand zur darüber liegenden gesundheitlichen Toleranzschwelle kann jedoch mehrere Größenordnungen betragen. Es gilt die Regel, Grenzwerte so hoch wie nötig, aber so niedrig wie möglich festzusetzen.

Hier müssen sich unter dieser Perspektive die sicherheitstechnischen Überlegungen im übertragenen Sinn auch auf die Sicherstellung der Verbrauchererwartung beziehen. Störfälle, die eine Überschreitung von Schwellenwerten verursachen, werden in der Öffentlichkeit meist als unmittelbare Bedrohung der körperlichen Unversehrtheit empfunden. Die Reaktion der staatlichen Aufsicht verstärkt erfahrungsgemäß diesen Eindruck, insbesondere dann, wenn für eine Abwägung der Verhältnismäßigkeit der Mittel zur Gefahrenabwehr kein ausreichender Spielraum gegeben ist.

Bei den Grundzügen eines allgemeinen sicherheitsmethodischen Konzeptes kann die besondere Ausprägung des Umgangs mit der „verbleibenden Unsicherheit", die als stehender Begriff beispielsweise ein besonderes Merkmal der Biowissenschaften ist, in der Diskussion über Nutzen und Schaden beim Risikomanagement zwar nicht ausgelassen, aber auch nicht vertieft werden. Es muss klargestellt sein, dass es sich hier um eine interdisziplinäre, sicherheitswissenschaftliche Leitlinie handelt. Im Interesse präziser Aussagen sind die Argumentationslinien und Begriffe dieser VDI-Denkschrift den Ingenieurwissenschaften entlehnt.

1.3 Gründe für diese Denkschrift

Spektakuläre Störfälle und Unfälle mit großer öffentlicher Wirkung werfen immer wieder die Frage nach hinreichender Sicherheit von technischen Einrichtungen auf. In derartigen Fällen neigen manche Medien dazu, in ihren Nachrichten nur das Ereignis selbst anzusprechen, gleichzeitig aber voreilige Schuldzuweisungen vorzunehmen. Es entspricht einer oft erlebten Mentalität, beim Versagen schnell einen Schuldigen zu finden. Dementsprechend finden sich auch immer wieder Sachverständige, die diese These nach Möglichkeit stützen. Im nächsten Schritt wird dann sofort auch gefragt, ob die Gesetze, Rechtsverordnungen, Überwachungsvorschriften und Regelwerke ausreichen, um die erwartete Sicherheit zu gewährleisten.

Diese typische Vorgehensweise lässt außer Acht, dass

- es 100%-ige Sicherheit nicht gibt, wobei die Grenzen der Sicherheit immer zu beachten sind,
- Sicherheit erzeugt, also entwickelt und hergestellt werden muss, bevor sie bei der Nutzung erhalten und überwacht werden kann,
- komplexe Sachverhalte meistens keinen mono-kausalen Zusammenhang bei Störfällen und Unfällen erkennen lassen, und vielmehr nichtvorhersehbare Ereignisse und unbekannte Einflüsse oder bisher nicht erkannte Verkettungen mehrerer Einflussfaktoren vorliegen, die zu Schäden führen.

Sicherheit wird in den meisten Fällen unter Anwendung einschlägiger Normen und Regelwerke und bestehender gesetzlicher Vorschriften geschaffen. Mit Rechenmodellen und analytischen Methoden werden Sicherheitskonzepte entwickelt. In diese Konzepte fließen auch langjährige empirische Erfahrungen ein, wie sie in unterschiedlichsten Anwendungsbereichen (Bauwesen, Verkehrs wesen, chemische Verfahrenstechnik, Energietechnik, Luftfahrttechnik, An lagenbau, Maschinenbau, Elektrotechnik und dergleichen mehr) spezifisch gewonnen wurden. Darin ist auch einer der Gründe zu sehen, weshalb es bisher noch kein anwendungsübergreifend einheitliches Sicherheitskonzept gibt.

So bestimmen unterschiedliche Sicherheitskonzepte die Entwicklung, Konstruktion, Auslegung und Herstellung der jeweiligen technischen Einrichtung. Für deren Betrieb werden detaillierte Betriebsanweisungen, Betriebsvorschriften und Instandhaltungsanweisungen sowie Auflagen zur Nachrüstung entwickelt. Auch

die Überwachung des Betriebs durch die Betreiber und sonstigen mit der Überwachung betrauten Stellen wird klar geregelt.

Die Konzeption, die Entwicklung, die Herstellung, der Betrieb, die Außerdienststellung und die Überwachung technischer Einrichtungen erfordern in besonderer Weise die Kompetenz von Ingenieuren. Mit dieser Denkschrift beabsichtigt der Verein Deutscher Ingenieure (VDI), diese Thematik aufzugreifen, um den Sachstand zur Sicherheit technischer Einrichtungen zunächst der Fachöffentlichkeit vorzustellen. Darüber hinaus werden Problembereiche aufgezeigt, wie zum Beispiel

- rechtliche Bewertungen, Beurteilungen und Urteile, die die Sicherheit beeinflussen,
- nicht vorhersehbare Vorkommnisse und Verkettungen, die zu Störungen und zum Versagen technischer Einrichtungen führen,
- der Mensch als Entwickler, Hersteller, Nutzer, Bediener und Überwacher, der zwar selbst nicht fehlerlos arbeitet, jedoch die Sicherheit entscheidend beeinflusst.

Hieraus werden Empfehlungen für ein fachübergreifendes Sicherheitskonzept abgeleitet, wie unterschiedlichste Sicherheitskonzepte auch in Zukunft gestaltet und weiterentwickelt werden müssen und wie hierbei das Zusammenspiel aller Beteiligten zu organisieren ist.

1.4 Rahmenbedingungen für Technische Sicherheit

Die Einsicht in und das Verständnis von Grenzen der Technischen Sicherheit resultieren aus einer Reihe von Sachverhalten wie beispielsweise Eintrittswahrscheinlichkeit, Schadenserwartung, Versagen, Wahrnehmung und Risiko, deren Stellenwert einer grundsätzlichen und verbindlichen Klärung bedarf. Technische Sicherheit begrenzt sich durch die Eintrittswahrscheinlichkeit eines Schadens oder fallweise des Versagens einer Anlage. Dieser Sachverhalt wird üblicherweise unter dem Begriff „Risiko“ subsumiert. Es ist jedoch ein vielschichtiger Begriff (siehe auch Abschnitt 3.3), weil er durch eine sehr unterschiedliche und sich stetig ändernde Wahrnehmung modifiziert wird.

Der Umgang mit Risiken, die nicht hinreichend bekannt oder nicht beherrschbar sind, stellt ein Problem dar; Schwierigkeiten treten auch auf, wenn über die Bewertung eines Risikos stark unterschiedliche Auffassungen herrschen. In diesen Fällen ist die erforderliche Vorsorge im Wesentlichen eine gesellschaftspolitische Entscheidung. In Betracht kommen vor allem Gefährdungen aus der Natur, aus natürlicher Umwelt, aus technischer Umwelt, durch menschliche Unzulänglichkeit und Fehlleistungen:

- Solche Gefährdungen aus natürlicher Umwelt können z.B. entstehen durch:
  - klimatische Einwirkungen in allen am Standort möglichen Formen (Wind, Schnee, Eis, Temperaturen usw.),
  - physikalische Einwirkungen (wie z.B. Blitzschlag, Erdbeben),
  - Verminderung von Widerständen von Bauteilen durch Korrosion, Ermüdung und Alterung.

- Gefährdungen aus technischer Umwelt können z.B. entstehen durch:
  - Überschreitung der planmäßigen Eigengewichte und Nutzlasten,
  - Einwirkungen aus technischer Umwelt (benachbarte Bebauung, Fahrzeugstoß, physikalische Einwirkungen, chemische Einwirkungen),
  - Verminderung von elektrischen Widerständen durch Korrosion, Ermüdung und Alterung,
  - herstellungsbedingte Unterschreitung der rechnerisch ermittelten Anforderungen an Bauteile und Tragwerke,
  - außergewöhnliche Einwirkungen aufgrund der Nutzung (Brand, Explosionen).

Menschliche Unzulänglichkeit und Fehlleistungen können ursächlich eine Gefährdung hervorrufen, oder sie behindern eine erfolgreiche Abwendung von Gefährdungen. Hierzu zählen alle Entscheidungen, Handlungen und Unterlassungen bei der Planung, Ausführung und Nutzung, denen einen Reihe von Faktoren zugrunde liegen kann, z.B.

- subjektiv nicht erkannte oder objektiv nicht bekannte Gefährdungen,
- unzureichender Wissensstand,
- Informationslücken, Missverständnisse,

- durch politischen Zwang oder falsch verstandene Sparsamkeit bedingte Fehlentscheidungen,
- Fahrlässigkeit.

Gefährdungen können auch durch vorsätzliche, aber nichtergründbare menschliche Handlungen entstehen.

Im Hinblick auf die möglichen Folgen, die Häufigkeit und die Dauer von Gefährdungen sowie die Art der zur Abwendung erforderlichen Maßnahmen kann unterschieden werden zwischen:

- ständigen Situationen, deren Dauer von gleicher Größenordnung ist wie die Nutzungsdauer des betroffenen Systems oder der Anlage (bestimmungsgemäßer Verlauf des Betriebes),
- vorübergehenden Situationen mit kurzer Dauer und großer Auftretenswahrscheinlichkeit (gegebenenfalls korrigierbare Störung des bestimmungsgemäßen Betriebs),
- außergewöhnlichen Situationen aufgrund von außergewöhnlichen Einwirkungen oder bei lokalem Versagen, mit kurzer Dauer und geringer Auftretenswahrscheinlichkeit, mit großen Wiederholungszeiten und großem Gefährdungspotenzial (siehe Tabelle 1: Gefährdungsklassen).

1.5 Ordnungsrechtliche Grundlagen der Technischen Sicherheit

Technische Sicherheit basiert weitgehend auf den Ingenieur- und Naturwissenschaften und wird durch das einschlägige Ordnungsrecht administriert. Die Sicherheit technischer Anlagen wird mit Methoden erzeugt, die systematisch gestaffelte Sicherheitsvorkehrungen (siehe Tabelle 1: Gefährdungsklassen) vorsehen. Diese werden sowohl durch technische Maßnahmen als auch durch organisatorische Vorkehrungen gebildet. Für technische Maßnahmen existieren häufig detaillierte Vorschriften, welche die Anforderungen an solche Maßnahmen wie Sicherheitsaufschläge, Grad der Redundanz, bereitzustellende Diversität oder Prüfungen regeln. Zu den technischen und organisatorischen Maßnahmen werden Grenzwerte, Prüfvorschriften und Managementsysteme in Form von Gesetzen und häufig in untergesetzlichen Regelwerken gefordert und angewendet. Die öffentlich-technische Sicherheit für den Bürger erfordert damit allgemein, dass durch die Nutzung der Technik

- der Mensch in seinem Recht auf Leben und körperliche Unversehrtheit nicht unzumutbar beeinträchtigt wird,
- die Umwelt nicht unzumutbar oder z.B. durch Gefahrstoffe nicht unzulässig oder irreversibel geschädigt wird und
- sonstige geschützte Rechtsgüter (Eigentum Dritter) nicht verletzt werden.

Die Gewähr für öffentlich-technische Sicherheit gehört demzufolge in die Verantwortung des einzelnen Nationalstaates und in Teilbereichen zunehmend in die der Europäischen Union, gegebenenfalls sogar der Vereinten Nationen. Die öffentlich-technische Sicherheit ist der Teil der Sicherheit, der durch das systematische Individual- und das Kollektivrisiko aus der aktiven und insbesondere der passiven Nutzung von technischen Produkten, Anlagen und Systemen sowie den zugehörigen Prozessen gekennzeichnet ist, für dessen Regulierung der Staat die Verantwortung trägt. Die staatliche Verantwortung für die Sicherheit seiner Bürger vor Risiken aus natur- und ingenieurwissenschaftlicher Forschung und Entwicklung, insbesondere der Anwendung daraus gewonnener Ergebnisse und technischer Vollzugsweisen ist insgesamt gegeben und wird hier als öffentlich-technische Sicherheit bezeichnet und übergreifend auch so verstanden.

Die Gewährleistung der öffentlich-technischen Sicherheit in einem sich ständig verändernden technischen und industriellen Umfeld ist in ihrer heutigen Bedeutung und Komplexität nicht anders zu werten als die Vorsorge des Staates für seine innere und äußere Sicherheit. Technische Anlagen müssen somit der objektiven Rechtsordnung entsprechen. Sie wird erfüllt durch Rechtssetzungen im Bereich der Technik, wie z.B. durch spezielle gesetzliche Regelungen, Verordnungen, Richtlinien und technische Regeln. Eine Gefahr für die öffentliche Sicherheit oder Ordnung liegt dann vor, wenn ein Sachverhalt oder ein Ereignis bei ungehindertem Verlauf des objektiv zu erwartenden Geschehens mit Wahrscheinlichkeit ein zu schützendes Gut schädigen wird (2. Senat des Bundesverfassungsgericht in seinem Beschluss vom 08.08.78, Az: 2 BvL 8/77, so genanntes Kalkar-Urteil).

Grundsätzlich ist zwischen einer konkreten, also fassbaren und einer abstrakten, also nur vorstellbaren Gefahr zu unterscheiden. Beide Gefahrenbegriffe stellen, was den zu erwartenden Schadenseintritt angeht, gleiche Anforderungen an die Wahrscheinlichkeit. Der Unterschied zwischen konkret und abstrakt liegt in der Betrachtungsweise. Die konkrete Gefahr ist auf den Einzelfall bezogen, wobei der Zeitpunkt des möglichen Eintritts eines Schadens nicht unmittelbar bevor-

stehen muss. Dieser Zeitpunkt liegt aber nicht in so weiter Ferne, dass er nicht mehr überschaubar ist.

Eine Gefahr gilt dann als gegeben, wenn eine Betrachtung für bestimmte Arten von Verhaltensweisen oder Zuständen zu dem Ergebnis führt, dass im Einzelfall mit hinreichender Wahrscheinlichkeit ein Schaden einzutreten pflegt. Deshalb muss Anlass bestehen, solchen Gefahren auch mit generell-abstrakten Mitteln, z.B. im Technikrecht selbst oder durch technische Regeln, vorzubeugen. Dann kann auf den Nachweis der Eintrittswahrscheinlichkeit im Einzelfall verzichtet werden. Gefahren, die bei Überschreitung von allgemein anerkannten Schwellenwerten erkannt werden, sind eindeutig konkreter Natur.

Die notwendigerweise unbestimmt formulierten Rechtsanforderungen an die Technische Sicherheit von technischen Systemen und Anlagen müssen durch technische Regeln konkretisiert werden, die nicht von rechtskompetenten Gremien, sondern von Fachleuten der entsprechenden technischen Fachsparten bestimmt werden.

Die erforderlichen staatlichen Maßnahmen richten sich primär nach dem inhärenten Schadenspotenzial der jeweiligen technischen Produkte, Prozesse, Anlagen und Systeme, einschließlich ihrer Folgewirkungen. Sie reichen von legislativen Rahmenvorgaben über Zulassungs- und Überwachungsfunktionen bis zu unmittelbaren staatlichen Eingriffsmaßnahmen.

Der Staat hat die Pflicht, in seiner Fürsorge Schaden für die Gesellschaft als Ganzes, aber auch für den einzelnen Menschen möglichst zu vermeiden und in jedem Fall zu begrenzen. Dabei kann jedoch nicht nur das Sicherheitsbedürfnis der betrachteten Rechtsgüter, z.B. Mensch und Umwelt, bestimmt werden; es bedarf vielmehr einer Abwägung zwischen ihrer Nützlichkeit bzw. Notwendigkeit für die Gesellschaft und den Risiken der Technik, was in eine Risikosteuerung mündet.

1.6 Ethische Grundsätze

Technische Sicherheit wird im Wesentlichen von Ingenieuren und Naturwissenschaftlern erarbeitet, wenngleich in zunehmendem Maße auch humanwissenschaftliche Disziplinen an Einfluss gewinnen. In ihrer Verantwortung dafür folgen sie nicht nur den Vorschriften der gültigen Rechtsordnung, sondern vor

allem auch den ethisch-moralischen Grundsätzen, die sich in den Jahrtausenden der abendländischen Geschichte herausgebildet haben. So ist die Ingenieurverantwortung verankert in ethischen Grundnormen und daraus sich entwickelnden moralischen Verpflichtungen.

In Wahrnehmung der Ingenieurverantwortung hat sich der Verein Deutscher Ingenieure zu folgenden ethischen Grundsätzen für den Ingenieurberuf verpflichtet (Düsseldorf im März 2002):

„Die Ingenieurinnen und Ingenieure

- verantworten allein oder mitverantwortlich die Folgen ihrer beruflichen Arbeit sowie die sorgfältige Wahrnehmung ihrer spezifischen Pflichten,
- bekennen sich zu ihrer Bringpflicht für sinnvolle technische Erfindungen und nachhaltige Lösungen,
- sind sich der Zusammenhänge technischer, gesellschaftlicher, ökonomischer und ökologischer Systeme und deren Wirkung in der Zukunft bewusst,
- vermeiden Handlungsfolgen, die zu Sachzwängen und zur Einschränkung selbstverantwortlichen Handelns führen,
- orientieren sich an den Grundsätzen allgemein moralischer Verantwortung und achten das Arbeits-, Umwelt- und Technikrecht,
- diskutieren widerstreitende Wertvorstellungen fach- und kulturübergreifend,
- suchen in berufsmoralischen Konfliktfällen institutionelle Unterstützung,
- wirken an der Auslegung und Fortschreibung rechtlicher und politischer Vorgaben mit,
- verpflichten sich zur ständigen Weiterbildung und
- engagieren sich bei der technologischen Aufklärung in Aus- und Weiterbildung an Schulen, Hochschulen, in Unternehmen und Verbänden.“

Im Alltag wird allerdings zwischen Ethik und Moral nur unscharf unterschieden. Innerhalb der Philosophie hat es sich dagegen eingebürgert, Ethik und Moral klar voneinander abzugrenzen. Demnach ist Ethik die wissenschaftliche Beschäftigung mit den verschiedenen Aspekten der Moral; der Gegenstand der Ethik ist die Moral. Die Ethik beschäftigt sich sowohl mit grundlegenden Fragen hinsichtlich der Natur der Moral und der möglichen Begründung moralischer Normen („Metaethik“) als auch mit Fragen der inhaltlichen Beschaffenheit moralischer Werte und Normen („normative Ethik“), also mit dem Guten und dem

Schlechten. Zu den wichtigsten Fragen der normativen Ethik gehört die Frage, inwieweit Folgenüberlegungen bei der moralischen Beurteilung von menschlichen Handlungen eine Rolle spielen dürfen oder müssen. Moralische Normen für sich allein genommen reichen zur Rechtfertigung bestimmter Handlungen und Strategien in keinem Fall aus. Um Schaden zu vermeiden und Nutzen zu bewirken, bedarf guter Wille stets der Ergänzung durch Sachkompetenz und Prognosefähigkeit.

Der Moral-Begriff umfasst objektive und subjektive Teile. Zu den objektiven Komponenten gehören die Normen, Prinzipien und Wertvorstellungen, die dem einzelnen Individuum gesellschaftlich vorgegeben sind und sich zum Teil im Rechtssystem niedergeschlagen haben. Hierzu gehören ebenso die Institutionen, die diese Normen setzen (z.B. Report 31 „Ethische Ingenieurverantwortung – Handlungsspielräume und Perspektiven der Kodifizierung“, VDI-Hauptgruppe Mensch und Technik, Düsseldorf, 2000 und „Ethik und Kernenergie – Expertise für den Fachausschuss Kerntechnik [FA-KT] der VDI-Gesellschaft Energietechnik [VDI-GET], Düsseldorf, Mai 2006) bekräftigen oder sanktionieren (Familie, Medien, Politik, Gerichte). Auf der subjektiven Seite entsprechen den objektiv vorgegebenen Normen einerseits die persönlichen Maxime, Leitsätze und Ideale und andererseits die moralischen Einstellungen, Motive, Gefühle und die Handlungsbereitschaft des Individuums. Die Grenze zwischen Ethik und Moral ist in der Praxis fließend. Wer moralisch handelt, hat in der Regel auch eine Vorstellung davon, welchen Sinn und welche Funktion die moralischen Normen haben, die er befolgt und vertritt, und wie diese Normen begründet sind. Mehr oder minder bewusst ausgesprochen gilt das selbstverständlich auch für die Verantwortung der Ingenieure in ihrer Alltagsarbeit und für das Vertrauen in ihre Arbeit.

Längerfristige Planungen müssen sich aus Verständigungsprozessen über Werte und Strategien zu ihrer Umsetzung ergeben, sie dürfen nicht „von oben“ diktiert werden. Eine solche Strategie empfiehlt sich schon aus pragmatischen Gesichtspunkten (Risikomanagement). Ein Diktat führt nahezu unausweichlich zu Glaubwürdigkeits-, Vertrauens- und Legitimationskrisen von Industrie, Politik und Bürokratie und trägt entscheidend zur Polarisierung der Standpunkte bei. Statt einer schleichenden Einführung neuer Technologien mittels Administration bei einer nachträglichen Sicherung der Akzeptanz durch geeignete Public Relations-Maßnahmen, sollte die Akzeptanz in einer diskursiv geführten, jedoch einer fachlich streng orientierten Vorgehensweise bei der Sicherheitstechnik von

vornherein abgesichert sein. Sie stellt eine wesentliche, vielleicht sogar zwingende Bedingung der Akzeptabilität einer demokratisch legitimierten Industriepolitik dar. Viele Diskussionen in Industriegesellschaften sind unbefriedigend, weil sie auf vorgefassten Meinungen und einseitigen Darstellungen des lückenhaften Sachstands beruhen und von indifferenten ethischen Vorstellungen ausgehen.

2 Erzeugen von Sicherheit

2.1 Sicherheitstechnische Prinzipien

2.1.1 Sicherheit – eine interdisziplinäre Aufgabe

Der Mensch strebt mit Hilfe der von ihm geschaffenen technischen Mittel eine stetige Erweiterung und Vervollkommnung seiner Möglichkeiten an. Dieser kulturgeschichtlich belegbare Umstand stellt eine in sich begründete Herausforderung an jeden Ingenieur dar, eine seiner vorrangigen Aufgabenstellungen bei der Realisierung zukünftiger technologischer Aufgaben darin zu sehen, dem ständigen Streben der menschlichen Gesellschaft nach Vervollkommnung der Sicherheit technischer Erzeugnisse gerecht zu werden. Dabei besteht die eigentliche Aufgabe darin, dass sich der Mensch die Technik als Assistenzfunktion zueigen macht, indem er die Verbindung in so genannten Mensch-Maschine-Systemen bzw. sozio-technischen Systemen herstellt. Dieser Herausforderung kommt umso mehr Bedeutung zu, weil Ingenieure in der allgemeinen Öffentlichkeit einen zunehmenden Mangel an Wissen über naturwissenschaftliche und technische Zusammenhänge beobachten müssen, der zu einem daraus resultierenden und häufig erschreckenden Misstrauen gegenüber der Technik geführt hat. Deshalb müssen Ingenieure bestrebt sein, ihr fachliches Können auf dem Sicherheitsgebiet allgemein fassbar und auch für Nichttechniker verständlich zu machen, damit das Unbehagen der Öffentlichkeit gegenüber technischen Einrichtungen beseitigt oder aber soweit begrenzt wird, dass keine unreflektierte Technikfeindlichkeit aufkommt.

Unfälle und Störfälle bieten immer wieder Anlass, deren Ursachen zu ergründen und abzustellen. Dabei ist die Wirksamkeit der bewährten und allgemein anerkannten sicherheitstechnischen Vorkehrungsmaßnahmen zu prüfen. Der Verein Deutscher Ingenieure unterstreicht erneut deutlich das Pflichtverständnis der Ingenieure, das Sachgebiet Technische Sicherheit ständig weiter zu entwickeln, dessen Anwendbarkeit zu vereinfachen und für Nichttechniker verständlich zu machen.

In diesem Zusammenhang stellen sich allerdings Fragen wie:

- Wird der Sicherheit moderner komplexer sozio-technischer Systeme heute keine ausreichende Bedeutung zugemessen?
- Wird der Wirtschaftlichkeit zunehmend Vorrang vor der Sicherheit eingeräumt?
- Finden die einschlägigen technischen Regelwerke keine hinreichende Beachtung mehr?
- Sind die einschlägigen technischen Regelwerke nicht mehr ausreichend zielführend?
- Setzt man sich über Gesetze und Rechtsverordnungen hinweg?
- Mangelt es an der Überwachung durch Behörden und aufsichtführende Institutionen?
- Welche Bedeutung hat der Mensch auf den unterschiedlichen Handlungsebenen?
- Sind das Verständnis und die Beurteilung technischer Gesetzmäßigkeiten unterentwickelt (weil es z.B. an der Vermittlung schulischen Wissens mangelt)?

Im Hinblick auf die möglichen Folgen von Gefährdungen erscheint es zweckmäßig, bei Systemen oder Anlagen im normalen Erfahrungsbereich drei Gefährdungsklassen zu unterscheiden (siehe Tabelle 1). Dabei ist sowohl dem Sicherheitsbedürfnis der Öffentlichkeit (Gefahr für Leib und Leben, sowie Gefährdung für die Umwelt; Bedeutung des Systems oder der Anlage) als auch wirtschaftlichen Gesichtspunkten (mögliche wirtschaftliche Folgen, Nutzungsanforderungen) Rechnung zu tragen, wobei dem erstgenannten Kriterium Vorrang gegeben wird. Bei den einzelnen Gefährdungsklassen ist, entsprechend den möglichen Folgen von Gefährdungen, ein unterschiedlicher Gesamtaufwand bei der Festlegung von Maßnahmen zu ihrer Abwendung erforderlich.

Grundsätzlich sind Anlagenteile und Bauelemente entsprechend ihrer Bedeutung für die Beschaffenheit und Gebrauchsfähigkeit einer technischen Anlage bzw. eines Produkts unterschiedlich zu klassifizieren. Vereinfachend können alle wichtigen Teile eines Systems oder einer technischen Anlage im Bereich einzelner Maßnahmen einer dieser Gefährdungsklassen zugeordnet werden. Jedes Sicherheitskonzept sollte sich mit seinen Maßnahmen an diesen Gefährdungsklassen orientieren.

Mögliche Folgen von Gefährdungen, die		
vorwiegend die Beschaffenheit betreffen	**vorwiegend die Gebrauchsfähigkeit betreffen**	**Gefährdungs-Klasse**
Große Bedeutung des Systems oder der Anlage für die Öffentlichkeit; Gefahr für viele Menschenleben	Große wirtschaftliche Folgen, große Beeinträchtigung der Nutzung; Kaskadeneffekte	3
Gefahr für Menschenleben und/oder beachtliche wirtschaftliche Folgen	Erhebliche wirtschaftliche Folgen, beachtliche Beeinträchtigung der Nutzung	2
Keine Gefahr für Menschenleben und geringe wirtschaftliche Folgen	Geringe wirtschaftliche Folgen, geringe Beeinträchtigung der Nutzung	1
Besteht bei Verlust der Gebrauchsfähigkeit Gefahr für Leib und Leben (z.B. Undichtigkeit von Behältern und Leitungen mit Gefahrstoffen), so wird dieser wie ein Verlust der erforderlichen Beschaffenheit behandelt		

Tabelle 1: Gefährdungsklassen

Die sicherheitstechnischen Errungenschaften sind bisher schon stets adäquat zu den zugrunde liegenden technologischen Innovationsleistungen gewesen. Allerdings scheinen sich Sicherheitstechnik und Sicherheitsrecht allmählich einer geordneten Anwendbarkeit zu entziehen. Insbesondere bei modernen, technologisch innovativen und komplexen Systemen erschweren heute folgende Sachverhalte die wirksamste sicherheitstechnische Lösung:

- Die Fülle an technischen Regelwerken, die häufig fach- und anwendungsspezifische Unterschiede aufweisen,
- die rein anwendungsspezifisch gültigen Rechtsvorschriften und Zuständigkeiten aufsichtführender Institutionen,
- die fach- und anwendungsspezifisch unterschiedliche Meinungsvielfalt unter Fachleuten sowie
- die in jeder technischen Fachdisziplin gepflegte Fachsprache.

Auch im Bereich der klassischen, bisher beherrschten Technik kündigen sich Beeinträchtigungen an, weil

- erfahrenes Fachpersonal entweder nicht mehr selbst zur Verfügung steht bzw. nicht in ausreichendem Maß Gelegenheit hatte, das eigene Wissen um Sachgrundlagen und Sachzusammenhänge an nachfolgende Ingenieurgenerationen weiterzugeben,
- das Wissen um die sicherheitsmethodischen Bezüge in technischen Regelwerken im ständig zunehmenden Umfang des Ingenieurwissens allmählich untergeht,
- im Zuge von Rationalisierungsvorhaben zwar auch Änderungen technischer Konzepte vorgenommen werden, ohne die zugehörigen sicherheitstechnischen Vorkehrungsmaßnahmen methodisch anzupassen.

Unsere Rechtsordnung macht zwar rechtliche Vorgaben für die Sicherheitstechnik, verfolgt dabei jedoch kein anwendungsübergreifendes einheitliches Konzept. Dies erschwert den ausführenden Ingenieuren das interdisziplinäre Zusammenwirken auf dem Gebiet der Sicherheitstechnik. Die politischen Gegner des Ausbaus und der Modernisierung der technisch-industriell geprägten Infrastruktur neigen dazu, technische Sicherheitskonzepte nicht mehr durch sachkundige Ingenieure, sondern durch Gerichte überprüfen zu lassen. Hier kommt es dann häufig zu Kompromissen, bei deren politisch ausgerichteter Festlegung sogar sicherheitstechnische Unzulänglichkeiten in Kauf genommen werden.

Kann die sich abzeichnende Überregulierung und Bürokratisierung bei der Sicherheitstechnik und beim Sicherheitsrecht noch abgewendet und in sachgerechtere Bahnen gelenkt werden? Hat der Staat nicht sogar die Pflicht, bei Deregulierung und Liberalisierung den Fortfall von Regelungen durch andere Sicherheitsprinzipien wie z.B. eine gleichartig durchgreifende Marktaufsicht zu kompensieren?

Auf diese Fragen versucht auch der Verein Deutscher Ingenieure Antworten zu geben. Dabei sind folgende Schwerpunkte zu behandeln:

- Zunehmender Zwang zum interdisziplinären Zusammenwirken aller betroffenen Disziplinen und in allen Technikfeldern,

- Technikübergreifende Verallgemeinerung der verschiedenen sicherheitstechnischen Konzepte durch Finden des „verdeckten Gemeinsamen”,
- Anschließende 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 (siehe Abschnitt 2.1.2),
- Wechselspiel zwischen Sicherheit und den Grenzen der Machbarkeit einerseits und der Wirtschaftlichkeit andererseits.

Im Zuge der Entwicklung innovativer Technologien sind selbstverständlich auch die dazugehörigen sicherheitstechnischen Konzepte auszuarbeiten. Zu diesem Zweck sind bereits vorhandene Sicherheitskonzepte auf verdeckte Gemeinsamkeiten zu untersuchen und zu einem sicherheitsmethodischen Konzept zusammenzufügen. In ein derartiges Konzept einzubeziehen sind die bewährten Erkenntnisse der Sicherheitstechnik, die sich vom vornehmlich empirisch gewachsenen Anwendungsbereich z.B. der Bahntechnik bis hin zum analytisch geprägten Anwendungsbereich wie etwa der Luft- und Raumfahrttechnik erstrecken, die vom deterministischen Konzept (dieses Konzept beruht auf klassischen „wenn - dann”-Beziehungen mit direkt nachvollziehbarer Kausalität des Eintretens von Ereignissen; siehe Abschnitt 2.2.4) bis zum probabilistischen Konzept (dieses Konzept beruht auf Wahrscheinlichkeitsbetrachtungen möglicher Ereignisse sowie auf dem Betrachten des möglichen Eintretens; siehe Abschnitt 2.2.4) der Zuverlässigkeit reichen sowie die sicherheitstechnische Vollnormung in den Bereichen Bau- und Elektrotechnik ebenso berücksichtigen wie die versagensanalytisch basierte Sicherheitstechnik im Bereich der Luft- und Raumfahrttechnik.

Hier geht es darum, wie sich die historisch unterschiedlich gewachsenen und anwendungsspezifisch verschiedenartig praktizierten Konzepte in Sicherheitstechnik und -recht zu einem einzigen interdisziplinären sicherheitsmethodischen Konzept zusammenführen lassen. Der Rückgriff auf die hier vorgestellte Methodik für ein interdisziplinäres Konzept auf dem Gebiet der Sicherheitstechnik (siehe Abschnitt 2.3) erleichtert sowohl die Kommunikationsfähigkeit als auch das interdisziplinäre Zusammenwirken zwischen den verschiedenen technischen Fachdisziplinen ebenso wie zwischen Ingenieuren, Vertretern von Wirtschaft, Politik, Justiz und den Mitbürgern. Dies wiederum wird sich bei technologischen Innovationsvorhaben ebenso vorteilhaft auswirken, wie es dem Verständnis für sicherheitstechnische Konzepte förderlich ist. Damit lässt sich verhin-

dern, dass sicherheitstechnische Belange, die bei Entwicklung und Herstellung noch in der gebotenen Art und Weise Berücksichtigung gefunden hatten, aus dem Ingenieurbewusstsein verdrängt werden, sobald an technischen Geräten, Anlagen bzw. Systemen Verbesserungen oder sonstige Änderungen vorgenommen werden.

Mit den in der 2. Hälfte des vergangenen Jahrhunderts zu beachtlicher Reife gebrachten Technologien höchster Komplexität und großen Nutzungs-Potenzials ist erstmals nachgewiesen worden, dass durch systemtechnisch orientierte Arbeitsweisen auch umfassend gestellte Ingenieuraufgaben zielsicher zu bewältigen sind. Die Methodik, systemtechnisch zu arbeiten, wird in diesem Beitrag vorgestellt (siehe Abschnitt 2.3). Bei konsequenter Anwendung erlaubt es dieses Konzept, die oft nicht deckungsgleichen Zielvorgaben Sicherheit, Zuverlässigkeit und Verfügbarkeit wirtschaftlich in ein System zu implementieren. Dies ist eine Ingenieuraufgabe, deren allgemein anwendbare Lösung zwischen Sicherheit und Wirtschaftlichkeit als Optimierungsaufgabe sowohl bei der Erstellung von Sicherheitskonzepten als auch im Technikbetrieb in interdisziplinärer Zusammenarbeit gefunden werden muss.

2.1.2 Anwendung des systemtechnischen Phasenkonzepts

Damit insbesondere bei komplex strukturierten, technologisch innovativen bzw. sicherheitstechnisch anspruchsvollen Systemen, Anlagen oder Produkten hinreichende Durchschaubarkeit der technischen und organisatorischen Sachverhalte stets erhalten bleibt, wird deren gesamter Lebenszyklus in Zeitabschnitte unterteilt, die nachfolgend als Phasen bezeichnet werden. Durch eine solche Unterteilung in Sach- und Zeitabschnitte lassen sich zu Beginn jeder dieser überschaubar gemachten Phasen klare Ziele, zu beachtende Randbedingungen, sonstige Vorgaben und Handlungsanweisungen festlegen. Zum Abschluss jeder einzelnen Phase lassen sich dann die erzielten Ergebnisse auf Erfüllung der gesetzten Ziele und Vorgaben überprüfen. Anhand der so festgestellten Ergebnisse werden so die Ziele, zu beachtende Randbedingungen, sonstige Vorgaben und Handlungsanweisungen für die sich jeweils anschließende Phase vorgegeben. 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.

Die Phasen eines Produkt-Lebenszyklus können wie folgt dargestellt werden:

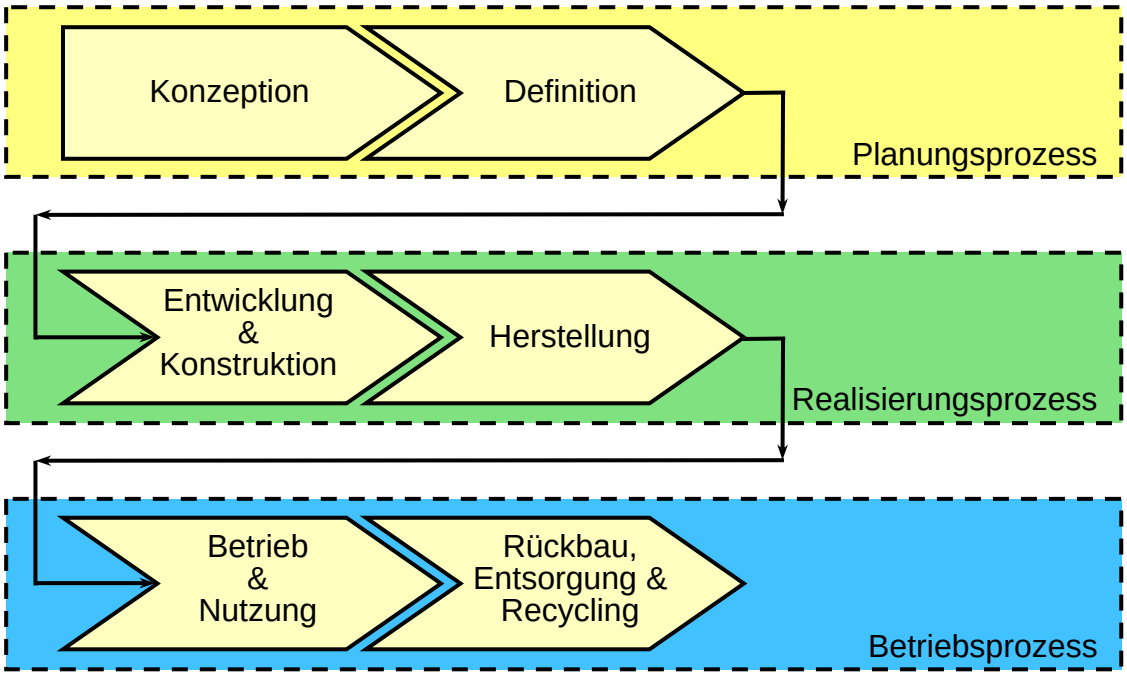


Abbildung 1: Phasen eines Produkt-Lebenszyklus

Wegen der unerlässlichen Durchschaubarkeit der Sachzusammenhänge sind die Darlegungen in dieser Denkschrift auf das vorstehend dargelegte Phasenkonzept ausgerichtet. Der Themenkreis Technische Sicherheit ist in dieses Phasenkonzept einzubinden. Das gilt nicht nur für das Erzeugen von Sicherheit in jeder einzelnen Phase des Lebenszyklus, sondern auch für deren Überprüfbarkeit.

Technische Sicherheit gehört zu den herausragenden Merkmalen eines Systems, einer Anlage oder eines Produkts. Technische Sicherheit zu erzeugen, stellt eine Aufgabe für Ingenieure und gegebenenfalls für Naturwissenschaftler dar, die sich weder von selbst noch nebenbei erledigen lässt. Mehr noch als alle anderen technischen Fachdisziplinen erfordert das Erzeugen und Nachweisen Technischer Sicherheit nicht nur Fachkunde der beteiligten Ingenieure und Naturwissenschaftler, sondern auch besondere Aufmerksamkeit und Sorgfalt des technisch-industriellen Managements. Dies bedeutet, dass der sicherheitstechnische Prozess über den gesamten Lebenszyklus – einschließlich etwaiger Nachrüstungen sowie von Maßnahmen zur Lebensdauer-Verlängerung – eines Systems, einer Anlage oder eines Produkts derselben Sorgfalt und Aufmerksamkeit bedarf wie das übrige Projekt. Aus diesem Grund bedürfen alle Aspekte und Merkmale

der Technischen Sicherheit in jeder einzelnen Phase dieses Lebenszyklus sachgerechter und fachkundiger Planung, ordnungsgemäßer Verfolgung und lückenloser Nachweisführung. Ein derartiger Prozess des Planens, des Verfolgens und des Nachweisens, der sich über den gesamten Lebenszyklus eines Systems, einer Anlage oder eines Produkts erstreckt, wird gemeinhin als „Controlling" bezeichnet. Da es sich in diesem Fall um das Controlling im Fachgebiet Technische Sicherheit handelt, ist die zutreffende Bezeichnung hierfür „Sicherheits-Controlling".

2.1.3 Die Rolle des Menschen bei der Sicherheit komplexer sozio-technischer Systeme

Störfälle und Unfälle der letzten Jahre haben in manchen Bereichen eines immer deutlicher werden lassen: der mögliche Nutzeffekt zusätzlicher Verbesserungen an technischen Systemkomponenten in hochkomplexen Anlagen großen Gefährdungspotenzials nimmt angesichts jahrzehntelanger Verbesserungen in diesem Bereich zunehmend ab. Mit dieser Tatsache zusammenhängend steigt die relative Bedeutung von Personalhandlungen bei der Auslösung von Stör- und Unfällen an. Es wäre jedoch eine unzulässige Vereinfachung, hierbei immer nur den unmittelbar an der Mensch-Maschine-Nahtstelle tätigen Operateur im Auge zu haben. Aus dem Prinzip tief gestaffelten Systemschutzes, das ja bei komplexen technischen Systemen immer angewandt wird, folgt logisch, dass ein individueller Einzelfehler nicht zu einem schwerwiegenden Stör- oder Unfall führen darf, was diverse Barrieren technischer oder organisatorischer Art zu verhindern haben. Nur dort, wo Schwachstellen im System unerkannt schlummern und eine unglückliche (oft stochastisch bedingte) Konstellation von aversiven Bedingungen auftritt, kann durch die Interaktion von Individuen und dem technischen System ein Stör- oder Unfallpfad durch individuelle Einzelfehler an der Mensch-Maschine-Nahtstelle („man machine interface", MMI) ausgelöst und beschritten werden. Dann kommt es zu negativ bewerteten Ereignissen.

Mit dem so genannten Phasenkonzept (siehe Abschnitt 2.1.2) lässt sich der gesamte „Produkt-Lebenszyklus" von technischen Einrichtungen umfassend, auch im Detail, berücksichtigen – und zwar von der Konzeption, über Definition, Entwicklung und Konstruktion, Herstellung, Betrieb und Nutzung bis zum Rückbau einschließlich Entsorgung und Recycling. In sämtlichen Phasen dieser Kette trägt menschliches Handeln zur (Un-) Zuverlässigkeit und (Un-) Sicherheit technischer Systeme maßgeblich bei. Es handelt sich hier also darum, in

sämtlichen Phasen des Lebenszyklus eines Produktes bzw. einer Dienstleistung einer entsprechenden Qualitätssicherung Rechnung zu tragen. Des Weiteren zeigen Analysen gravierender Ereignisse, dass auch dem Steuerungspotenzial menschlichen Handelns bei der Minderung von allfälligen nachteiligen oder verheerenden Folgen der Unfälle eine eminente Bedeutung zukommt. Der Bereich „Human Factors" (HF) wird eine sich immer mehr aufdrängende Problematik, die gezielte Antworten verlangt. Insoweit hat der menschliche Beitrag zu Sicherheit und Zuverlässigkeit sozio-technischer Systeme einen hohen Stellenwert.

Als „Human Factors" sind also sämtliche Faktoren über den gesamten Produkt-Lebenszyklus zu begreifen, die den Menschen in seiner Interaktion mit einem technischen System beeinflussen bzw. die von Menschen beeinflusst werden. Insofern ist der unbedachte und vielfach anzutreffende synonyme Gebrauch von „Human Factors" und „menschlichem Fehler" oder gar „menschlichem Versagen" unzulässig, ebenso wie die traditionelle Eingrenzung des ergonomischen Aspekts der MMI. Organisatorische Faktoren, Arbeitsteilung, vorgängige Managemententscheidungen und sogar inter-organisationale Beziehungen sind hier von Relevanz im Sinne eines umfassenden holistischen Verständnisses von „Human Factors".

Der menschliche Beitrag zu Zuverlässigkeit und Sicherheit sozio-technischer Systeme erfolgt unter Randbedingungen, die einerseits unverzichtbare Potenziale ebenso bieten wie unveränderliche Einschränkungen. Beide sind im Systemdesign zu berücksichtigen, denn „im Mittelpunkt aller von Menschen für Menschen errichteten Systeme muss der Mensch mit seinen naturgemäßen Fähigkeiten und Begrenzungen stehen" („Saarbrücker Erklärung" anlässlich des World Congress on Safety of Modern Technical Systems, Saarbrücken, 2001). Diese Fähigkeit macht ihn grundsätzlich der Maschine überlegen; insoweit kompensiert seine Lernfähigkeit die Fehleranfälligkeit und ist für sicherheitsgerichtetes Handeln eine wichtige Komponente.

Handlungsfehler sind definiert als das Nichterreichen eines Handlungsziels. Ein Widerspruch in sich wäre daher anzunehmen, dass jemand bewusst einen Fehler begehen könnte. Ob eine Fehlhandlung vorlag, lässt sich also immer erst im Nachhinein und nach Abklärung der Möglichkeit eines „korrekten", zielgerichteten Handelns beurteilen. So gesehen widerspricht die weit verbreitete Automatik der Schuldzuschreibung („menschliches Versagen") für einen Fehler dem

von Sicherheitswissenschaftlern geforderten „Menschenrecht auf Fehler". Eine angemessene Fehlerkultur erkennt einen Fehler als Lernchance und fragt nicht: „Wie konntest Du nur?", sondern: „Wie konnte es dazu kommen?"

Handlungsfehler entstehen aus vielfältigen Bedingungen, insbesondere aus überforderter mentaler Kapazität zur Informationsverarbeitung, aus unangemessenen Aufmerksamkeitsanforderungen, aus monotoner Arbeit, aus angeborenen oder erlernten (den anstehenden Aufgaben unangemessenen) Verhaltensstereotypien, aus Wissensbegrenzungen. All dies sind möglicherweise die menschliche Handlungskapazität überschreitende Belastungen und Beanspruchungen. Beidem, dem naturgemäß gegebenen menschlichen Potenzial sowie den menschlichen Begrenzungen, ist im Interesse der Vermeidung von Schäden für Menschen und Umwelt beim jeweiligen Systemdesign Rechnung zu tragen. Dies kann z.B. durch fehlertolerante Konstruktionen und Gestaltung geschehen.

Ein besonderer Stellenwert kommt hier der Automatisierung sozio-technischer Systeme zu, die aus technischer Perspektive oft ein Maximum anstrebt, um den „fehleranfälligen" Menschen möglichst auszuschließen. Tatsächlich dürfte jedoch der Beitrag des Menschen umso notwendiger werden je komplexer Systeme werden. Bainbridge spricht hier von den „Ironien der Automatisierung" (Ironies of automation, in J. Rasmussen, K. Duncan, J. Leplat (Eds), New technology and human error, Chichester: Wiley, S. 281…283, 1987). Zum einen ist der Entwickler eines Systems in aller Regel ein Mensch, der ebenfalls fehleranfällig ist und die korrekte Nutzung des entwickelten Systems dadurch negativ beeinflussen kann, denn er hinterlässt nach seiner maximalen Automatisierungsstrategie dem Operateur nur Aufgaben, die nicht mehr automatisierbar sind. Es entsteht, was vergleichbar mit dem ist, was Psychologen die „gelernte Hilflosigkeit" genannt haben: der Mangel an Gebrauch von motorischen oder kognitiven Fähigkeiten wird dann zum Problem, wenn ein unvorhergesehenes Ereignis entsteht und vom ungeübten Operateur neue Verhaltensweisen gefordert werden. Ähnlich wird eine durch umfassende Automatisierung verbleibende reine Kontrolltätigkeit einer Anlage durch die nachgewiesene menschliche Schwäche beeinträchtigt, langfristig aufmerksam zu bleiben.

Des Weiteren können komplexe Entscheidungssituationen zum Problem werden. Sofern alle notwendigen Elemente einer Entscheidung im Produktionsprozess spezifiziert werden können, kann die automatisierte computer-unterstützte Entscheidung schneller und mehrdimensionaler als durch den Operateur erfolgen.

Was dem Operateur dann aber verbleibt, ist möglicherweise das Ergebnis einer Entscheidung auf einer Metaebene zu beurteilen, deren Algorithmus er nicht oder nur unzulänglich versteht. Automatik kann somit Systemversagen überlagern und der korrekten Diagnose sowie Behebung entziehen. Was also zu fordern ist, wäre nicht maximale, sondern angemessene Automatisierung, die dem Menschen Lern- und Funktionsfähigkeit erlaubt, damit optimal gestaltete Sicherheitsfunktionen erzeugt werden.

2.2 Vorgehensweisen für ein interdisziplinäres sicherheitsmethodisches Konzept

2.2.1 Grundzüge

Die nachfolgende Darstellung gibt einen allgemeinen Überblick über die grundsätzlich gültige Vorgehensweise bei den erforderlichen Systemarbeiten zur Sicherheitstechnik – insbesondere im Hinblick auf die öffentliche Sicherheit. Das hier angesprochene interdisziplinäre „Sicherheitsmethodische Konzept" wird konkret zu gegebener Zeit in einem gesonderten Dokument vorgestellt. Als Grundlage für dessen Ausarbeitung werden folgende Grundsätze herangezogen:

2.2.1.1 Allgemeine Vereinbarungen zur Sicherheitstechnik

Grundsätzlich gilt, dass das sicherheitsgerechte Gestalten technischer Systeme so zu erfolgen hat, dass diese dem zeitgemäßen Stand der öffentlichen Sicherheit gerecht werden. Dies gilt jedoch nicht in dieser grundsätzlichen Forderung, wenn bei der Erprobung des Systems und seiner Baueinheiten die Sicherheit – nach den Erfordernissen eines Versuchsbetriebs – vorübergehend durch spezifische Maßnahmen gewährleistet wird.

Bei der sicherheitsgerechten Gestaltung eines technischen Systems sind folgende sicherheitstechnische Auslegungskriterien zu vereinbaren:

- Der Mensch muss mit seinen naturgemäßen Fähigkeiten und Unzulänglichkeiten im Mittelpunkt stehen. Dies erfordert unter anderem eine benutzerfreundliche Gestaltung von technischen Systemen.
- Ein Einzel-Versagen darf im Gesamtsystem kein sicherheitskritisches Versagen verursachen oder begünstigen.

Ist eine technische Auslegung, die dieser Forderung gerecht wird, nicht möglich, gilt:

- Verknüpfungen von Versagensfällen in Baueinheiten (Versagensmechanismen, Kausalketten) – einschließlich menschlicher Bedienungsfehler –, die zu einem sicherheitskritischen Versagen im Gesamtsystem führen können, müssen durch aktive oder passive Selbstprüfung erkennbar gemacht werden.

Ist auch hier eine technische Auslegung, die dieser Forderung gerecht wird, nicht möglich (z.B. weil dann die Zuverlässigkeit beeinträchtigt wird), gilt zusätzlich:

- Die Wahrscheinlichkeit für ein Mehrfach-Versagen (z.B. für ein zeitgleiches Einzel-Versagen verschiedener Baueinheiten), das zu einem sicherheitskritischen Versagen im Gesamtsystem führen kann, darf einen bestimmten, jeweils auf den Einsatz bezogenen Grenzwert nicht überschreiten.

  Die Festlegung derartiger Grenzwerte ist abhängig von den stochastischen Gegebenheiten des Versagensverhaltens der jeweils betroffenen Baueinheiten und dem – spezifizierten – Grenzwert, der für das Gesamtsystem als angemessen betrachtet wird.

Ein sicherheitsmethodisches Vorgehenskonzept zur sicherheitsgerechten Gestaltung von Produkten und technischen Einrichtungen setzt auch voraus, dass bei allen sicherheitstechnisch erforderlichen Tätigkeiten auch die folgenden Grundsätze berücksichtigt werden:

- Für jede Baueinheit muss der „sichere Zustand” bzw. das „sichere Funktionsverhalten” eindeutig definiert und in der jeweiligen Spezifikation festgelegt werden. Dies setzt unter Umständen voraus, dass exakte Funktions- und Anforderungsanalysen für Bedienungstätigkeiten unter Berücksichtigung ihrer Machbarkeit durchgeführt werden.

- Die technische Gestaltung soll so erfolgen, dass bei einem Mehrfach-Versagen Wechselwirkungen im Versagensmechanismus, die zur Möglichkeit des Funktionsverlusts eines Teilsystems oder des Gesamtsystems führen, ausgeschlossen sind.

- Grenzwerte von Versagenswahrscheinlichkeiten, die für die jeweiligen Baueinheiten zu fordern sind, müssen so festgelegt werden, dass die Erfüllung der Sicherheitsanforderungen an das Gesamtsystem nicht in Frage gestellt wird.

Für das Zeitverhalten der Ausfallraten, die sicherheitskritische Versagensfälle betreffen, gelten die Forderungen an die Brauchbarkeitsdauer, die in der Spezifikation der jeweiligen Baueinheit festzulegen sind.

2.2.1.2 Anforderung an die Vorgehensweise zum sicherheitsgerechten Gestalten

Für alle sicherheitstechnischen Tätigkeiten – einschließlich der entsprechenden Nachweisführung – gilt im Hinblick auf die absehbare Gefährdung (siehe hierzu Tabelle 1) nachstehende Reihenfolge von methodisch geeigneten Maßnahmen:

- Ausschluss von sicherheitskritischen Versagensfällen (Versagensausschluss aufgrund natürlicher oder technischer Integrität),
- Ausschluss der Folgen sicherheitskritischer Versagensfälle (Versagensfolgenausschluss),
- Begrenzung der Wahrscheinlichkeit sicherheitskritischer Versagensfälle bzw. Fehler durch Anwendung der Zuverlässigkeitstechnik.

Diese Reihenfolge bezieht sich auf den sicherheitstechnischen Arbeitsablauf und stellt keine Rangfolge für eine sicherheitstechnische Wertigkeit der genannten Maßnahmen dar.

Das methodische Vorgehen, das durch vorstehend festgelegte Reihenfolge bestimmt ist, setzt voraus, dass sich alle Baueinheiten des Systems bei Beginn jedes Nutzungsabschnitts nachweislich in fehlerlosem und störungsfreiem Zustand befinden und Fehler, die sich sowohl während des Herstellungsablaufs, der Bedienung als auch bei Instandhaltungsmaßnahmen ergeben können, durch geeignete Vorkehrungen vermieden werden.

2.2.1.3 Sicherheitsmethodische Arbeitsschritte beim Projektmanagement

Im Projektmanagement muss das sicherheitsmethodische Konzept angewendet werden; dabei sind die folgenden Arbeitsschritte immer durchzuführen:

- Übertragung des methodisch erarbeiteten „Sicherheitstechnischen Anforderungskatalogs“ in Projekt- bzw. Systemspezifikationen, die den gesamten „Produkt-Lebenszyklus” umfassen;
- sicherheitsbezogene Anforderungen an die Gestaltung des Systems und seiner Baueinheiten, was eine Mitwirkung verschiedener sicherheitstechnisch relevanter Disziplinen erfordert;
- Planerische Festlegung der Umsetzungsschritte im Sinne eines Human Factor Engineering;
- Festlegung der Sicherheitsanforderungen, die der Nachweisführung unterliegen (öffentliche Sicherheit);
- Festlegung der Sicherheitsanforderungen, die zur Erlangung der Betriebsgenehmigung erforderlich sind;
- Zusammenstellung der sicherheitskritischen Versagensformen und Erstellung des Plans zum Sicherheits-Controlling (Ziel: „Lessons Learned” zur Erfahrungsrückführung).

2.2.2 Bausteine des sicherheitsmethodischen Konzepts

Die Grundsätze sicherheitsgerechten Gestaltens sind in systematischer Weise so aufeinander abzustimmen, dass damit eine interdisziplinäre Vorgehensweise festgelegt ist, die einheitlich sowohl für das betreffende Projekt und der damit geschaffenen neuartigen und zur Anwendung gebrachten herkömmlichen Technologie als auch für die Beurteilung durch die zuständige Aufsicht anwendbar ist. Eine weitere, allgemeine Anwendungsmöglichkeit bietet sich für Schadensuntersuchungen an technischen Einrichtungen an.

Damit wird eine für das gesamte Vorhaben eines Projekts gültige Arbeits- und Bewertungsmethodik geschaffen, die für die Zulassungsfähigkeit unerlässlichen sicherheitstechnischen Gestaltungskriterien in ein quantitativ bewertbares Verhältnis zu denjenigen Gestaltungskriterien bringt, die für die wirtschaftliche

Nutzanwendung und damit für die technische Zuverlässigkeit von Bedeutung sind.

Versagensbedingte Störungen haben ihre Ursache meist im Einzelteil oder in niedrig integrierten Baueinheiten; die sicherheitskritischen Auswirkungen werden jedoch oft erst anhand des funktionellen Zusammenwirkens erkennbar, das sich aus der technischen Gestaltung des Gesamtsystems ergibt. Der erforderliche Durchgriff ist hier nur mit einem geeigneten Informationsmanagement zu schaffen.

So ist z.B. ein grundlegender Mangel die Vieldeutigkeit von fachspezifisch unterschiedlich definierten Sachbegriffen. Weil zum Schaffen neuer Technologien stets eine Integration von Erkenntnissen aus mehreren Fachdisziplinen notwendig ist, sollten deshalb auch solche Begriffe systematisch vermieden werden, die in den Regeln der Technik nicht eindeutig und in allgemein anwendbarer Form definiert werden, weil sie entweder fachspezifisch unterschiedlich interpretierbar (wie z.B. der Begriff „fail safe") oder nur für bewusst begrenzte Anwendungsbereiche bestimmt sind (wie z.B. der Begriff „Signaltechnische Sicherheit" in DIN VDE 0831). Dies gilt ganz besonders dann, wenn der allgemeine Sprachgebrauch hierzu bereits eindeutige Begriffe aufweist (wie z.B. den Begriff „Sicherheit"). Allerdings sollten Begriffe wie „sicher" bzw. „Sicherheits-" in Bezeichnungen von Baueinheiten grundsätzlich nicht verwendet werden, auch dann nicht, wenn für diese Baueinheit bereits ein Sicherheitsnachweis vorliegen sollte.

Konkret wird hier Instandhaltung für alle Maßnahmen zur Bewahrung und Wiederherstellung des Sollzustandes baulicher Anlagen verwendet, soweit es sich nicht um eine Änderung handelt. Damit sind solche Begriffe wie Wartung, Inspektion und Instandsetzung mit umfasst, obwohl man inhaltlich zwischen Instandhaltung und Instandsetzung durchaus unterscheiden kann; denn Instandhaltung umfasst nach dem allgemeinen Sprachgebrauch Wartungs- und Modernisierungsarbeiten, die nach allgemeiner Verkehrsauffassung zur Erhaltung des Sollzustandes erforderlich sind, während unter Instandsetzung Maßnahmen zu verstehen sind, die notwendig sind, um den Sollzustand einer baulichen Anlage wieder herzustellen, nachdem sie diesen, aufgrund unvorhersehbarer Ereignisse, z.B. Brand, oder mangels ordnungsgemäßer Instandhaltungsarbeiten bereits verloren hat. Die Instandhaltung muss ordnungsgemäß sein. Das betrifft nicht nur die Häufigkeit und Zielrichtigkeit der Maßnahmen (z.B. der Wartung), sondern

betrifft insbesondere auch die Art der Durchführung. Sind dafür besondere Sachkunde oder spezifische technische Gerätschaften erforderlich, so kann die Instandhaltung unter Umständen nur dann ordnungsgemäß sein, wenn die Arbeiten von einem Handwerker, einem Sachverständigen oder einem Fachbetrieb durchgeführt werden.

Ein zweckdienliches Informationsmanagement ist unabdingbare Voraussetzung für die interdisziplinären Vorgehensweisen eines sicherheitsmethodisch ganzheitlichen Konzepts.

2.2.3 Human Factors Engineering

Die Diskussion um den Entwurf und die Konstruktion neuer technischer Anlagen dreht sich fast ausschließlich um technische Probleme, während Perspektiven des Human Factors Engineering (HFE) dabei, wenn überhaupt, eine nur untergeordnete Rolle spielen. Sicher muss in den ersten Phasen einer technischen Konzeption den grundlegenden technischen Designkriterien eine Priorität eingeräumt werden. Dies wird schon aus Gründen der damit angesprochenen Kostendimensionen nahe gelegt.

Sämtliche Systeme und besonders die komplexen Anlagen werden aber ausnahmslos aus technischen und menschlichen Komponenten bestehen, also sozio-technische Systeme sein. HFE-Prinzipien für den Entwurf sozio-technischer 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.

Es sind hier unterschiedliche Bereiche angesprochen, die interdisziplinär zu bearbeiten sind:

(1) Entwurf eines HFE-Gesamtplans

Der Plan soll verdeutlichen, wie und zu welchen Phasen des gesamten Entwurfs- und Konstruktionsprozesses zukünftiger Anlagen HFE-Gesichtspunkten systematisch Rechnung getragen werden soll.

(2) Auswertung von Betriebserfahrungen

Als erster Schritt ist es sinnvoll, aus HFE-Gesichtspunkten eine Auswertung der in bereits installierten, vergleichbaren Systemen identifizierten Erfahrungen vorzunehmen, um dort aufgetretene Probleme zu vermeiden und positive Erfahrungen in den künftigen Entwürfen zum Zuge kommen zu lassen.

(3) Funktionale Anforderungsanalyse und Aufgabenzuordnung

Ziel ist, die Anforderungen des Systems in seinen verschiedenen Funktionsbereichen zu analysieren, die Leistungsanforderungen zu identifizieren und die Grenzen und Möglichkeiten des Designs für Optionen der Aufgabenteilung von Mensch und Maschine auszuloten. Dem aus HFE-Erfahrungen wichtigen Prinzip des „aktiven Operateurs" wäre dabei besondere Beachtung zu schenken. Hierher gehören ebenfalls Fragen nach möglicherweise neuen Anforderungen an das Bedienungsteam und daraus sich ergebende Anforderungen an Qualifikationsmix und funktionale Neuzuordnungen der Aufgaben im Team sowie die Entwicklung entsprechender Kriterien für die Gestaltung der Arbeitsplätze. Ferner gehört hierher die Planung der Teilung von Aufgaben zwischen Mensch und Maschine, einschließlich der Planung für Automatisierungsmaßnahmen.

(4) Zentralisierung/Dezentralisierung von Überwachungs- und Leitständen.

Eng verbunden mit dem Problem funktionaler Anforderungsanalyse ist die Frage, inwieweit dezentrale Überwachungs- und Leitstände eingerichtet werden, deren Personal wiederum entsprechende Voraussetzungen der Qualifizierung erfordert.

(5) Organisationsaspekte

Die wechselseitige Zuordnung und die Interaktionsbedingungen von unterschiedlichen erforderlichen Personalkategorien sollten ebenso wie die dynamischen Veränderungen der Aufgabenzuständigkeit bei Normalbetrieb, Stör- und Unfällen analysiert werden. Ferner stellt sich die Frage, wie z.B. die europäischen Richtlinien zum Arbeits- und Umweltschutz eine Berücksichtigung der Arbeitswissenschaften erfordern und für die Arbeitsorganisation der Anlagen relevant sind.

(6) Ermittlung des Qualifikationsbedarfs

Je nach Funktionsteilung wären Qualifikationsbedarfspläne zu entwickeln und Vorschläge für ihre Umsetzung auszuarbeiten.

(7) Entscheidungsunterstützungssysteme (EUS)

Computer-gestützte EUS könnten genutzt werden zur Prüfung der Aufgabenerfüllung des Personals und zur Identifikation angemessener Prozeduren im Bedarfsfalle. In diesem Zusammenhang wäre zu untersuchen, inwieweit Veränderungen der Interaktionsformen des Personals durch die Nutzung computer-gestützter EUS bedingt werden.

(8) Gestaltung von Steuereinrichtungen (z.B. Warten, Leitstände)

Hierher gehören u.a. Fragen nach der Rolle analoger und digitaler Signalsysteme, ihrer Redundanz, der Nutzung adaptiver Displays, Transparenz der Meldungen und Rückkoppelungsschleifen für die Wirkungen von Handlungen der Operateure. Ebenso wäre zu untersuchen, wie dem Teamcharakter der Arbeit konsequent Rechnung getragen werden kann.

(9) Partizipative Ergonomie

Formen und Möglichkeiten der Einbeziehung erfahrener Operateure in den Designprozess sind zu untersuchen. Im Interesse einer iterativen Optimierungsstrategie sind Möglichkeiten und Folgen der Umsetzung des Prinzips „Zuerst der Simulator, dann die Anlage" zu analysieren. Desgleichen sind Möglichkeiten des Einsatzes von „Rapid Prototyping" zu untersuchen.

Hierbei bezeichnet der Begriff „schneller Prototypenbau" (bzw. englisch „Rapid Prototyping") die schnelle Herstellung von Musterbauteilen ausgehend von Konstruktionsdaten. Rapid Prototyping-Verfahren sind somit Fertigungsverfahren, die das Ziel haben, vorhandene CAD-Daten möglichst ohne manuelle Umwege direkt und schnell in Werkstücke umzusetzen. Die unter dem Begriff des „Rapid Prototyping" seit den achtziger Jahren des letzten Jahrhunderts bekannt gewordenen Verfahren sind in der Regel Urformverfahren, die das Werkstück schichtweise aus formlosem oder formneutralem Material unter Nutzung physikalischer und/oder chemischer Effekte aufbauen.

(10) Anlageninterne Stör- und Notfallmaßnahmen

Umsetzung von HFE-Prinzipien beim Entwickeln technisch korrekter, umfassender, expliziter und leicht zu handhabender Prozeduren bei Störungen, Stör- und Notfällen.

(11) Verhinderung von Fehlbedienungen

- Durch Gebote und Verbote sowie entsprechende Schulung;
- durch eingebaute Verriegelungseinrichtungen, die sich nach einer Fehlbedienung selbsttätig in einen sicheren Zustand bzw. sicheren Funktionsablauf schalten.

Insgesamt lassen sich drei Modelle der Einbeziehung von HFE-Experten in den Entwurfs- und Konstruktionsprozess komplexer sozio-technischer Einrichtungen unterscheiden, die je nach anstehendem Bedarf unterschiedlich zu nutzen sind:

(a) Integriertes Modell:

Hier ist der HFE-Fachmann (Arbeitswissenschaftler, Psychologe, Mediziner) von Anfang an im Entwurfsteam integriert, um geplante Arbeitsplätze und die Funktionen der dort tätigen Mitarbeiter hinsichtlich Sicherheit und Zuverlässigkeit, des Arbeitsschutzes, der Gesundheit und menschengerechter Gestaltung mit zu entwerfen.

(b) Intermittierendes Beteiligungsmodell:

Hier wird der HFE-Experte in kritischen Entwurfsphasen hinzugezogen, um etwa einen Prototyp zu bewerten. Dies gibt die Möglichkeit, erfahrene Operateure (Piloten, Wartenpersonal u. dergl.) einzubeziehen.

(c) Post hoc-Beteiligungsmodell:

Nur in seltenen Fällen werden sämtliche Designfehler vor der Inbetriebnahme des Systems entdeckt werden. Dann ist es notwendig, technische oder organisatorische Barrieren zu installieren, die eine dysfunktionale Nutzung des Systems oder gefährliche Systemzustände vermeiden. Unter allen Umständen ist jedoch zu vermeiden, dass eine post hoc Beteiligung von HFE-Experten zur standardmäßigen Beteiligung im Sinne eines Reparaturbetriebs gewählt wird.

Wenn ein Ereignis nicht innerhalb des Systems beherrscht werden kann und die Systemgrenzen überschritten werden, muss eine Maßnahme zur Behandlung der Nahtstelle greifen. Auch hierzu müssen die Erkenntnisse des HFE eingesetzt werden, um unbedingt auch die HFE-Bestandteile in die Notfallmanagement-planungen einzubinden.

2.2.4 Bewertung der Versagensvorsorge aus interdisziplinärer Sicht

Bewährte, systemtechnisch ausgerichtete Konzepte erlauben es, technische Erzeugnisse, komplexe Anlagen ebenso wie einfache Geräte, auf ihr potenzielles Versagensverhalten hin zu untersuchen. Dabei ist stets davon auszugehen, dass ein Versagen von technischen Erzeugnissen ebenso wenig ausgeschlossen werden kann, wie davon ausgegangen werden darf, dass der Mensch, der diese Technik handhabt, unfehlbar wäre. Die Ergebnisse derartiger Versagens-analysen, die zum Standardwerkzeug eines jeden Projekt- und Entwicklungs-ingenieurs zählen, lassen systematisch die bedeutsamen Versagensmöglich-keiten von Baueinheiten bereits im Entwurfs- bzw. Planungsstadium erkennen. Dies wiederum bildet die Voraussetzung für Präventivmassnahmen, mit denen unerwünschtes bzw. unzulässiges Versagen vermieden werden soll.

Zum Verständnis der weiteren Ausführungen sollen an dieser Stelle zunächst die beiden Begriffe „deterministische Vorgehensweise" und „probabilistische Vor-gehensweise" erläutert werden:

- Deterministische Vorgehensweise:

  Die deterministische Vorgehensweise entspricht in den Ingenieurwissen-schaften dem historisch gewachsenen, monokausalen Handlungsschema. Sie basiert auf eindeutigen Wenn-dann-Beziehungen sowie auf der Sachlage, dass ein bestimmtes Ereignis zu einem vorbestimmten Zeitpunkt eintritt. Sie bildet auch in der heutigen Technik immer noch die klassische Vorgehens-weise bei Konzipierung, Gestaltung und Prüfung technischer Einrichtungen.

  Auch für die Sicherheitstechnik wurde diese Vorgehensweise adaptiert, wenn es darum ging (oder geht), Maßnahmen zu konzipieren als Vorkehrung gegen sicherheitskritisches Versagen. Hierbei stellt das „Wenn" das sicherheitskriti-sche Versagen dar und das „Dann" die sicherheitstechnische Vorkehrung. Beide stellen in der klassischen Technik eine logisch ein-deutige (in vorwärts gerichteter Logik) oder auch ein-ein-deutige (in vor- und rückwärts gerichte-

ter Logik) Verknüpfung dar und beziehen sich auf monokausale Wirkstrukturen.

Die deterministische Vorgehensweise im Ingenieurwesen steht im Einklang mit den ebenfalls klassischen Denk- und Entscheidungsstrukturen im Rechtswesen.

- Probabilistische Vorgehensweise:

  Die probabilistische Vorgehensweise stützt sich auf wahrscheinlichkeitstheoretische oder statistische Grundlagen. Im Gegensatz zur deterministischen Vorgehensweise basiert die probabilistische Vorgehensweise nicht auf Gewissheit, sondern auf der Möglichkeit, dass ein bestimmtes Ereignis – mit einer bestimmten Wahrscheinlichkeit – eintritt. Der Zeitpunkt des Ereigniseintritts ist nicht vorbestimmt und auch nicht vorher bestimmbar.

  Moderne Technik (wie Anlagentechnik, Bautechnik, Energieversorgungstechnik, Informations- und Kommunikationstechnik, Kraftfahrzeugtechnik, Luft- und Raumfahrtechnik) beinhaltet unterdessen hoch vernetzte Funktionen, computer-gestützte Einrichtungen und kommt zunehmend auch in aggressiven Umfeldbereichen (wie Weltraum, Hoch- und Tiefsee, Wüste, Dschungel) zum Einsatz. Dies führt zwangsläufig zu komplexen und hoch integrierten Strukturen, die sicherheitstechnisch nicht mehr allein in deterministischer Vorgehensweise beherrschbar sind, sondern durch probabilistische Vorgehensweisen (wie beispielsweise durch die Zuverlässigkeitstechnik) ergänzt (bzw. vervollständigt) werden müssen.

  Bei Konzipierung, Gestaltung und Prüfung derart komplexer technischer Einrichtungen hat sich die Anwendung der Zuverlässigkeitstechnik seit Jahrzehnten bewährt. Ohne Anwendung der Zuverlässigkeit wären die Errungenschaften der heutigen weltumfassenden Verkehrsluftfahrt, der wissenschaftlichen bzw. kommerziellen Raumfahrt sowie der heutigen Automobiltechnik nicht möglich gewesen.

  In der Luft- und (bemannten) Raumfahrt hat sich die Anwendung der Zuverlässigkeitstechnik auch bei der sicherheitstechnischen Konzipierung und Gestaltung von hoch integrierten komplexen technischen Einrichtungen längst bewährt. Dennoch schreitet die Adaptierung in anderen technischen Anwendungsbereichen aufgrund etablierter Traditionen nur sehr zögerlich voran.

Das Versagensverhalten technischer Erzeugnisse kann nur dann weitgehend von der Systematik her vollständig erfasst werden und für ingenieurmäßig gezielte Präventivmaßnahmen nutzbar gemacht werden, wenn auch dessen stochastischen Erscheinungsformen in probabilistischer Betrachtungsweise Rechnung getragen wird. Dabei ist außerdem zu berücksichtigen, dass das Versagensverhalten von noch durchschaubaren, vorwiegend mit „unverlierbaren" Eigenschaftsmerkmalen („passiven" Sicherheitsmerkmalen) ausgestatteten Systemen (wie z.B. Tragwerke, Stütz- und Halteeinrichtungen, mechanische Verriegelungen, Brandschutzdämmungen) auch bei ausschließlich deterministischer Betrachtungsweise in der Regel voll erfasst werden kann, während es bei komplexen, vorwiegend mit „verlierbaren" Eigenschaftsmerkmalen („aktiven" Sicherheitsmerkmalen) ausgestatteten Systemen (wie z.B. Energieversorgungen, Antriebe, Regelungseinrichtungen, Kühleinrichtungen, Löscheinrichtungen) im Wesentlichen durch seine stochastischen Erscheinungsformen gekennzeichnet ist.

Sollen Ingenieure unter diesen Gegebenheiten auch mit probabilistischen Ansätzen zweckbestimmt arbeiten, müssen auf jeden Fall Wahrscheinlichkeitsgrenzwerte zur Verfügung stehen. Seit der Veröffentlichung der Sicherheitsnorm DIN VDE 31000-2 „Allgemeine Leitsätze für das sicherheitsgerechte Gestalten technischer Erzeugnisse – Begriffe der Sicherheitstechnik – Grundbegriffe" von 12/87 gilt die Risikobetrachtung als probabilistische Betrachtung stochastischer Versagensformen von technischen Erzeugnissen als allgemein anerkannter Stand der Technik.

Das Betrachten von Grenzwerten für ein Risiko setzt voraus, dass sie auch von der allgemeinen Öffentlichkeit akzeptiert werden (siehe Abschnitt 3). Jeder so betrachtete Grenzwert muss sich an der Akzeptanz durch die unvoreingenommene „Öffentlichkeit" orientieren (öffentliche Sicherheit). Versuche, die in die Richtung zielen, den Grad der Akzeptanz durch demoskopische Umfragen ermitteln zu wollen, sind zum Scheitern verurteilt. Sie werden bestenfalls die in der Öffentlichkeit stets vorhandene Polarisierung zwischen Bewunderung der Technik und einer meist auf Unkenntnis, aber auch – wegen des unvermeidbaren Auftretens nachweislicher Fehler von Mensch und Maschine – auf berechtigten Zweifeln beruhenden Skepsis gegenüber der Technik offenkundig machen. Dabei ist die Gefahr nicht auszuschließen, dass diese Polarisierung politisch missgedeutet wird, wenn die Ergebnisse solcher Umfragen der Öffentlichkeit vorgestellt werden.

Ein anderer, auch schon beschrittener Weg sollte dagegen zielstrebig weiterverfolgt werden. Es gilt den Grad der öffentlichen Akzeptanz an den stochastischen Eigenschafts-Merkmalen von durch die Öffentlichkeit bereits akzeptierten Technologien, wie sie sich in Schifffahrt, Bautechnik, Bahnverkehr, Luftfahrt, Straßenverkehr, Energietechnik, Chemietechnik, verfahrenstechnischen Anlagen oder auch in Kraftwerken herkömmlicher Technologie darstellen, zu messen. Dies kann auch an natürlichen Risiken geschehen, die z.B. durch die menschliche Lebenserwartung gekennzeichnet sind. Allerdings setzt das Gelingen dieses Vorhabens voraus, dass betroffene Institutionen ihre Datenbanken für den allgemeinen Gebrauch zugänglich machen.

Mit einem Festschreiben derartiger Grenzwerte wäre allerdings noch keine endgültige Lösung erreicht. So ist es letztendlich unerlässlich, dass das erforderliche Maß an Sicherheit in das technische System integriert wird. Konsequenterweise ist der aufsichtführenden Institution gegenüber nachzuweisen, inwieweit dies tatsächlich gelungen ist. Instrumente, mit denen dieser Nachweis wirklich effizient erbracht werden kann, sind zurzeit allerdings nur zum Teil verfügbar und müssten noch weiter entwickelt werden.

Hieraus ergibt sich in Verbindung mit dem dazu notwendigen probabilistischen Konzept ein quantitatives Problem. Die Zahlenwerte (Daten), mit denen Sicherheit zu berechnen ist, müssen sehr klein sein, da sicherheitskritische Ereignisse nur sehr selten möglich werden dürfen. Will man solche Zahlenwerte mit stochastischen Methoden nachweisen, kommt man schnell an Grenzen, die wegen des erforderlichen Aufwands nicht überschritten werden können. Deshalb sei in diesem Zusammenhang auf die bewährten datenbank-basierten Konzepte verwiesen, wie sie beispielsweise in den (einst) international gebräuchlichen U.S.-amerikanischen Normen MIL-HDBK-217F, Notice 2, Reliability Prediction of Electronic Equipment und NPRD-95, Nonelectronic Parts Reliability Data dargelegt sind.

Die probabilistische Betrachtung stochastischer Versagensformen als Ergänzung des deterministischen Konzepts der klassischen Sicherheitstechnik wurde entwickelt, um auch komplexe Systeme, die vorwiegend durch ihre Vielzahl „verlierbarer" Eigenschaftsmerkmale gekennzeichnet sind, sicherheitstechnisch sinnvoll beherrschbar zu machen. Es wird immer wieder versucht, das klassische, sicherheitstechnisch umfassend bewährte, deterministische Konzept durch

ein probabilistisches Konzept vollständig zu ersetzen. Dieser Versuch scheitert häufig am Mangel geeigneter, verlässlicher Daten.

In diesem Grenzbereich zwischen deterministischen und probabilistischen Konzepten ist eine in der Sache begründete Unkenntnis nicht ganz auszuschließen. So beruhen deterministische Sicherheitsmassnahmen auf der Überlegung, dass technische Erzeugnisse bei Auftreten eines sicherheitskritischen Versagens umgehend in einen sicheren Zustand zu überführen sind, der häufig in einer Funktionshemmung (z.B. im bewusst herbeigeführten Abschalten einer Anlage) besteht, also in einem kommandierten Versagen (diese Begriffsbestimmung erfolgt in Anlehnung an DIN 25424, 3.8, c)). Bei komplexen technischen Systemen jedoch mit ihren vielen Teilelementen führt das sicherheitgesteuerte „Abschalten" einzelner Teilsysteme zu Zuverlässigkeitsproblemen, die nach Abschluss einer technischen Entwicklung bzw. Fertigstellung einer Anlage kaum mehr zu lösen sind.

Dieses Verhalten führte zur Erkenntnis, dass Sicherheits- und Zuverlässigkeitstechnik in untrennbarer Logik miteinander verbunden bleiben müssen. Beide Teilgebiete behandeln Versagensformen, die stochastischer Natur sind; deshalb kann das Versagensverhalten nur mit stochastischer Methodik vollständig erfasst werden. Aus diesem Grund sind auch die vorgeschlagenen deterministischen Unterstützungsmaßnahmen in ihren Auswirkungen auf die Zuverlässigkeit ebenfalls stochastisch zu erfassen.

2.2.5 Kriterien für ein interdisziplinär ganzheitliches Sicherheitskonzept

Bei der Herleitung von Kriterien für ein interdisziplinär nutzbares Konzept (anlässlich eines technologischen Innovationsvorhabens) wurde bewusst vermieden, wieder nur ein Sicherheitskonzept zu schaffen, das ausschließlich für ein bestimmtes Anwendungsgebiet zutrifft. So sind die erarbeiteten Kriterien allgemeingültig und lassen sich demzufolge auf jedes Anwendungsgebiet und jede Technologie gleichermaßen anwenden. Dies gilt auch für Grundlagen des nachstehend vorgestellten interdisziplinär anwendbaren sicherheitsmethodischen Konzepts (siehe Abschnitt 2.3), in dem diese Einzelkriterien in ihrer logischen Verknüpfung erfasst sind. Deren allgemeine Gültigkeit bietet für die Anwendung folgende Vorteile:

- Institutionen, die im Gesamtprozess die konkrete staatliche Verantwortung für öffentlich-technische Sicherheit wahrnehmen und Prüfungen, Genehmigungen, Konformitätserklärungen und Tolerierungen durchführen und die Kontrolle und Aufsicht übernehmen, können nach den gleichen Kriterien desselben Konzeptes arbeiten. Sie nutzen also dieselben Elemente unter dem Blickwinkel der staatlichen Verantwortung, sei sie direkt ausgeübt, im öffentlichen Beleihungsverfahren angewendet oder strukturbedingt durch anerkannte (akkreditierte) Private erfolgt.

- Bei einheitlicher Einführung des Sicherheitskonzeptes wird eine anwendungsunabhängige und klare Kommunikation zwischen den verschiedenen beteiligten Fachgebieten ermöglicht – einer der wesentlichen Grundsätze des ganzheitlichen und fachgebietsübergreifenden Konzepts aus der Systemtechnik, verallgemeinert für alle Technikfelder.

- Vorbedingung für ein zweckbestimmtes sicherheitsorientiertes Konzept ist es allerdings, dass
  - während Planung, Entwicklung und Herstellung hinreichend geeignete Maßnahmen (Erzeugen von Sicherheit, Sicherheitsmanagement, Qualitätsmanagement, sicherheitstechnische Nachweisführung) und
  - im Verlauf der Betriebsphase sowie der Entsorgung und dem Rückbau Maßnahmen (Sicherheits-Management, sicherheitstechnische Nachweisführung)

  ergriffen werden, die angemessen sind und mit denen das gefertigte Erzeugnis tatsächlich die sicherheitsgerechte technische Auslegung aufweist.

- Ebenso wie jede andere interdisziplinäre Arbeitsweise erfordert das sicherheitsorientierte Konzept zweckdienliche, organisatorische Voraussetzungen, um eine wirksame Anwendung zu ermöglichen. Dabei sind folgende Gesichtspunkte zu berücksichtigen:
  - Nur eine zentrale, für das betrachtete System insgesamt verantwortliche und mit hinreichenden Befugnissen ausgestattete Steuerungsstelle ist sachlich in der Lage, bei den sicherheitstechnischen Tätigkeiten auch systemübergreifende Kriterien angemessen zu berücksichtigen. Voraussetzung ist allerdings, dass für alle Bestandteile des betrachteten Systems selbst Sicherheit nachgewiesen werden kann.

- Da dieses sicherheitsorientierte Konzept wirtschaftliche Nutzbarkeit ebenso gewährleistet wie eine sicherheitsgerechte technische Auslegung, kann im Hinblick auf diese umfassende Zielsetzung die Gesamtverantwortung nur bei dem Entwicklungsingenieur liegen, der mit den sicherheitstechnischen Merkmalen umfassend vertraut ist, weil er sie selbst in das betrachtete System hineinentwickelt hat (typisches Beispiel für eine Matrixorganisation).
- Der gutachtlich tätige Ingenieur hat ausschließlich die sicherheitstechnische Angemessenheit dieser technischen Auslegung zu beurteilen. Hierzu bedarf es je nach Komplexität und Umfang des Konzeptes der entsprechenden kaskadenartigen Einschaltung der Begutachtung (Prinzip, Dimensionierung, Ausführung). Das Prinzip muss die Begrenztheit der Konsequenz, die Überschaubarkeit, die Kontrollierbarkeit der Auswirkungen negativer Art und die Reversibilität berücksichtigen.
- Die Beachtung anwendbarer „Regeln der Technik" bzw. gesetzlich bedingter Vorschriften ist für sich allein eine zwar gebotene, wenngleich nicht notwendigerweise hinreichende Voraussetzung für einen in sich schlüssigen Sicherheitsnachweis.
- Darüber hinaus muss selbstverständlich der Stand der Technik sowie gegebenenfalls der Stand von Wissenschaft und Technik beachtet werden (näheres hierzu siehe Abschnitt 3.5).

Dem Entwurf, der Bemessung und Konstruktion von technischen Anlagen werden im Hinblick auf die Beschaffenheit und Gebrauchsfähigkeit bestimmte Qualitäten der Werkstoffe, Komponenten, Systeme, Anlagen, Produkte und der Ausführung zugrunde gelegt.

Es ist wichtig, die Planungsvorgaben selbst, ihre rechnerischen und experimentellen Nachweise und Konstruktionspläne daraufhin zu prüfen, ob das Produkt mit diesen Vorgaben sowie mit den vorgesehenen Prüf- und Freigabemaßnahmen bei der Ausführung den Anforderungen entsprechend ausgeführt werden kann (Prüfung und Freigabe der Planungsvorgaben).

Damit die Ausführung nicht unzulässig von den zugrunde gelegten Vorgaben abweicht (z.B. aufgrund der Veränderlichkeit der Werkstoff- und Bauteileigenschaften, aufgrund der Unsicherheiten bei Einbau und Errichtung oder aufgrund von Fehlern und Irrtümern bei den verschiedenen Herstellungsschritten), sind

geeignete Prüf- und Nachweismaßnahmen bei allen wesentlichen Phasen der Ausführung vorzusehen (Verfolgung und Prüfung der Ausführung).

Ist zu erwarten, dass Qualitäten sich während der Nutzungsdauer ungünstig verändern, so können wiederkehrende Prüfungen sowie besondere Erhaltungsmaßnahmen erforderlich sein (Abschlussprüfung und Nachweisführung vor Inbetriebnahme).

- Anforderungen an die Organisation der Nachweisführung

  Nur durch entsprechende Koordination der vorgesehenen Prüfungen ist zu erreichen, dass sich Prüfmaßnahmen sinnvoll ergänzen, unbeabsichtigte Lücken in der Nachweisführung vermieden und die notwendigen Informationen weitergegeben werden.

  Für die Beurteilung von Prüfmaßnahmen ist neben ihrer unmittelbaren Aufgabe, ungünstige Abweichungen aufzuzeigen, auch ihre mittelbare Wirkung, nämlich ihr positiver oder negativer Einfluss auf Leistung und Qualität von Bedeutung.

  Die Verantwortlichkeiten für alle Prüfmaßnahmen, insbesondere für die Durchsetzung von Maßnahmen bei unzureichenden Prüfergebnissen, bedürfen einer verständlichen und eindeutigen Regelung.

  Alle wesentlichen Prüfergebnisse sind aufzuzeichnen.

  Das Erstellen eines Prüfplanes ist dann erforderlich, wenn viele Auftragnehmer und Unterauftragnehmer am Bauvorhaben beteiligt sind und wenn Fehlentscheidungen und Lücken in der Nachweisführung beträchtliche Folgen nach sich ziehen können.

- Elemente der Nachweisführung

  Im Hinblick auf Art und Umfang der Nachweisführung kann unterschieden werden zwischen

  – Herstellerprüfungen, die entweder ausschließlich betriebsintern oder betriebsextern geregelt sind,
  – Fremdprüfungen durch einen unabhängigen Dritten, die entweder unabhängig von der Herstellerprüfung erfolgen oder sich ausschließlich auf die Überprüfung einer ordnungsgemäßen Herstellerprüfung beziehen,

- Abnahmeprüfungen von Seiten des Auftraggebers/Kunden, die der Beurteilung und dem Nachweis der Qualität einer Ware oder einer Leistung bei Übergang von Verantwortung oder Eigentum dienen.

Herstellerprüfungen werden grundsätzlich büro- oder betriebsintern durchgeführt und können, je nach Bedeutung der Nachweisführung, in Form einer Selbstprüfung oder durch Personen, die nicht unmittelbar am Herstellungsvorgang beteiligt sind, erfolgen.

Die büro- oder betriebsintern geregelten Herstellerprüfungen oder auch besondere Maßnahmen zur Herstellungssteuerung, liegen in alleiniger Zuständigkeit des Herstellers.

Die Planung von Prüfungen umfasst die eindeutige Festlegung von Regeln für die Beurteilung der Qualität oder einer Leistung sowie Maßnahmen bei negativen Prüfergebnissen.

Die Bedeutung der einzelnen Elemente der Nachweisführung ist unterschiedlich, je nachdem, ob es sich um Prüfungen der Planungsvorgaben, der baulichen Ausführung oder um Prüfungen vor Inbetriebnahme handelt.

- Abstufung von Prüfungen

Die Abstufung der Prüfmaßnahmen zur sicherheitstechnischen Nachweisführung hängt ab von:

- der Intensität der Prüfung (Häufigkeit und Umfang von Prüfungen),

- den Beurteilungskriterien und Maßnahmen bei negativen Prüfergebnissen,

- dem Grad der Unabhängigkeit der Prüfung des betroffenen Vorgangs,

- dem Einsatz mehrfacher unabhängiger Prüfungen, wobei je nach Erfordernis der Qualitätssicherung folgende Abstufung möglich ist:
  - nur Herstellerprüfungen,
  - betriebsextern geregelte Herstellerprüfungen zusammen mit Fremdprüfungen oder Abnahmeprüfungen,
  - betriebsextern geregelte Herstellerprüfungen zusammen mit Fremdprüfungen sowie Abnahmeprüfungen oder einer zweiten unabhängigen Fremdprüfung.

Aus diesen Zusammenhängen kann die Festlegung von Qualitätssicherungsstufen und ihre Zuordnung zu den Gefährdungsklassen (siehe Tabelle 1) abgeleitet werden. Einzelne Teilsysteme oder Bauteile können unterschiedlich ausgeprägten Qualitätssicherungsstufen unterliegen.

- Prüfung und Freigabe der Planungsvorgaben
  - Prüfung von Entwurf, Bemessung und konstruktiver Durchbildung

    Es gilt zu prüfen, ob alle maßgebenden Gefährdungen erkannt und geeignete Maßnahmen zu ihrer Abwendung vorgesehen sind. Dies betrifft insbesondere die zweckmäßige Wahl des Systems, der Werkstoffe und der Herstellungsart, der Verfahren und Hilfsmittel der Bauausführung sowie die Auslegung des Systems oder der Anlage (Funktionsprüfung, Zugänglichkeit). Unter anderem ist auch zu überprüfen, ob alle wesentlichen organisatorischen Voraussetzungen, z.B. spezielle handwerkliche und betriebliche Qualifikation, erfüllt werden können, ob alle für die Ausführung erforderlichen Prüfungen vorgesehen sind, ob alle Nutzungsbedingungen und erforderlichen Erhaltungsmaßnahmen festgelegt sind.

    Die Überprüfung der Auslegung kann auf verschiedene Arten mit unterschiedlichem Aufwand erfolgen, z.B. durch Versuche, Berechnungen oder Analogiebetrachtungen. Unter anderem wird nachzuprüfen sein, ob die Berechnung die maßgeblichen Anforderungen und die tatsächlichen Einflüsse, Randbedingungen und Nutzungsbedingungen erfasst, ob Nachweise für alle wesentlichen Bauteile geführt werden, ob geeignete Rechenmodelle verwendet werden, ob die Berechnung in sich widerspruchsfrei ist, und ob alle Einwirkungen korrekt von dem System ertragen werden. Weiter ist zu prüfen, ob Veränderungen von Bauteilen unzulässige Funktionsstörungen verursachen.

    Hinsichtlich der Art der Überprüfung kann man unterscheiden zwischen
    - vollständiger Nachrechnung durch unabhängige Dritte,
    - Modellversuchen,
    - Prototypenprüfungen,
  - Prüfung und Freigabe der Ausführungsunterlagen

    Es gilt zu prüfen, dass die Ausführungsunterlagen alle erforderlichen Angaben für die Ausführung enthalten, so z.B. Toleranzgrenzen oder Anweisungen hinsichtlich des Fertigungsablaufs. Dabei ist es unter anderem von Bedeutung, ob Bemessungsergebnisse richtig übertragen wurden, ob die

Anweisungen bzw. Zeichnungen vorgegebenen Anforderungen entsprechen, ob andere Randbedingungen berücksichtigt sind.

Da alle Informationen und Vorgaben seitens der Planung weitgehend anhand der Ausführungspläne für die Fertigung, Montage bzw. Integration übermittelt werden, kommt ihrer Prüfung auf Eindeutigkeit und Vollständigkeit besondere Bedeutung zu.

- Prüfungen der baulichen Ausführung (Abnahmeprüfung)
  - Serienherstellung – Einzelherstellung

    Hinsichtlich der Art und der Bedeutung von Prüfungen ist zu unterscheiden zwischen
    - Serienherstellung mit dem Ziel gleich bleibender Qualität,
    - Einzelherstellung mit dem Ziel, den Planungsvorgaben zu entsprechen.

    Bei der Einzelherstellung haben vorbeugende Maßnahmen Vorrang.

    Bei der Ausführung komplexer technischer Systeme oder großer technischer Anlagen handelt es sich im Allgemeinen um Einzelherstellung, wobei nur einzelne Bauteile oder Werkstoffe der Serienherstellung unterliegen. Somit sind Qualitätssicherungssysteme, z.B. nach DIN 55 350, „Begriffe zu Qualitätsmanagement und Statistik", die sich an der Serienherstellung orientieren, nicht unmittelbar auf alle Phasen der Bauausführung übertragbar.
  - Beurteilungsverfahren und -kriterien

    Bei der vollständigen Prüfung wird jede Produktionseinheit geprüft. Eine Einheit wird als „gut" angenommen oder als „schlecht" zurückgewiesen. Erfolgt die Beurteilung nach quantitativen Kriterien, so entsprechen diese im Allgemeinen vorgegebenen Toleranzen.
  - Wiederkehrende Prüfung

    Zeitlich gestaffelt sind wiederkehrende Prüfungen durchzuführen, um sich auch während seiner gesamten Nutzungsdauer zu vergewissern, dass ein technisches Produkt mit der gültigen Konfiguration übereinstimmt, gemäß der es geplant, entwickelt, gebaut, in Betrieb genommen wurde und betrieben wird.

2.2.6 Passive und aktive Sicherheitsmaßnahmen

Folgende Grundeinteilung kann vorgenommen werden:

Eine Komponente, ein Anlagenteil oder eine gesamte Anlage werden zur Erfüllung unterschiedlicher Funktionen entwickelt. Hierbei wird zwischen aktiven und passiven Funktionen unterschieden.

- Passive Funktionen beinhalten grundsätzlich „unverlierbare bzw. inhärente Eigenschaften". Diese Funktionen können im Normalfall bzw. -betrieb nicht „verloren" gehen. Es wird kein Aktuator betätigt. Passive Funktionen können zum Beispiel Halte-, Stütz- und Verriegelungsaufgaben darstellen. Als konkretes Beispiel kann die Decke eines Stockwerkes oder die statischen Eigenschaften eines ganzen Bauwerkes genannt werden. Um diese Funktionen zu erhalten, sind eine Berücksichtigung der Eigenschaften der Hardware und die Anforderungen an die Bauteile notwendig. Prüfungen, Pflege und Wartung gehören ebenso dazu.
- Aktive Funktionen hingegen können grundsätzlich „verloren" gehen. Sie sind gekennzeichnet durch die Nutzung eines aktiv wirkenden Bauteils. Als Beispiele können eine Beleuchtungseinrichtung oder ein Regler genannt werden. Bei einem Verlust dieser Funktionen sind Sicherungen notwendig, die entsprechend dem möglichen Ausfallverhalten geeignet implementiert sein müssen.
- Wo immer möglich, ist den passiven Sicherheitsmaßnahmen Vorrang einzuräumen. Im Anwendungsfall müssen aktive Sicherheitsmaßnahmen für die jeweilige Gefährdungsklasse (siehe Tabelle 1) eine nachweislich mindestens gleichwertige Wirkung erbringen.

2.2.7 Beherrschung von Versagensmechanismen

Versagt ein Bauteil, das eine passive Funktion unterstützt, ist in erster Näherung der Mangel in der Konstruktion oder in der baulichen Ausführung zu suchen. Bei einem Versagen einer aktiven Funktion können die wesentlichen Bauteile in Ordnung sein. Hierbei können einzelne Eigenschaftsmerkmale eines Gerätes versagt haben, weil dieses schadhaft geworden ist, oder aber die Steuerung oder das Zusammenspiel von Funktionselementen kann versagt haben – beispielsweise aufgrund eines Anweisungs- bzw. Bedienfehlers.

Versagensmechanismen kann man in Kategorien einteilen. Insgesamt lassen sich sieben verschiedene Versagensarten kategorisieren, die man in drei Bereiche einteilen kann:

- Versagen beim Aufbau einer Funktion:
  - Einem System fehlt die vorgesehene Funktion.
  - Die vorgesehene Funktion kommt nur teilweise zustande.
  - Die Funktion kommt zum falschen Zeitpunkt zustande.
- Versagen bei schon vorhandener Funktion:
  - Es entsteht ein Totalversagen der vorhandenen Funktion.
  - Es entsteht eine Degradierung eines Funktionselementes; dieses Element kann seine Funktion nur noch teilweise erfüllen.
- Versagen bei Beendigung einer Funktion:
  - Die Funktion wird unqualifiziert beendet.
  - Die Funktion wird zur falschen Zeit beendet.

Zum Erzeugen von Technischer Sicherheit muss das Versagen von Funktionen gewichtet werden. Um die Wahrscheinlichkeit des Eintritts eines möglichen Versagens auf ein akzeptables Maß zu reduzieren, können verschiedene Vorgehensweisen eingeschlagen werden:

- Eine Funktion fällt aus und der technische Zustand des Systems, der Anlage bleibt trotzdem sicher. Es wird die bestimmungsgemäße Funktion zwar aufgegeben, jedoch entstehen keine Schäden. Man nennt diesen „Rückfall"-Zustand „Fail Safe". Hierbei wird trotz Ausfall einer Systemkomponente in Richtung sicherer Zustand abgeschaltet, wobei dafür Sorge getroffen wurde, dass der im Rückfall zu erreichende Endzustand sicher ist. Es tritt keine Schädigung an Personen und Sachen ein, aber die Funktion ist nicht mehr – auch nicht mit Einschränkungen – vorhanden. Das System „steht" sozusagen.

  Als Beispiel für die „Fail Safe"-Vorgehensweise sei hier das Auslösen einer Zwangsbremsung bei einem Eisenbahnzug genannt.
- Falls eine Funktion eines Systems oder einer Anlage jedoch trotz eines Versagens eines Bauteils, das die Funktion unterstützt, aufrecht erhalten werden soll oder zumindest eingeschränkt erhalten bleiben muss, nennt man diesen Zustand „Fail Operational". Hierbei werden Einschränkungen durch Notprogramme (automatisch oder durch den Menschen aufgerufen) realisiert,

die besonders wichtige Funktionen aufrechterhalten. Ein katastrophales Verhalten kann bei Nutzung und Abarbeitung dieser Strategie kaum eintreten. Ein systematisches Vorgehen zu Festlegung von geeigneten Strategien ist hier besonders wichtig.

Hier seien als Beispiel für die „Fail Operational”-Vorgehensweise die technischen und organisatorischen Vorsorgekonzepte beim fliegenden Flugzeug genannt.

- Wenn weder „Fail Safe”- noch „Fail Operational”-Strategien angewendet werden können, dann bietet sich die Anwendung der „Zuverlässigkeitstechnik” zur Reduzierung des Risikos an – allerdings nur für die Gefährdungsklasse 1 (siehe Tabelle 1). Unter diesem Begriff wird die Anwendung von Wahrscheinlichkeitsbetrachtungen verstanden, die durch Nutzung von Erfahrungswerten, Expertisen, theoretischen Untersuchungen, Versagensbetrachtungen und anderen Verfahren die Möglichkeit eines Ausfalles untersuchen. Bei genügend geringer Wahrscheinlichkeit eines Schadens kann dann das System oder die Anlage auch in Betrieb gehen.

  Um auch hier ein Beispiel zu nennen, sei auf das sicherheitstechnische Zuverlässigkeitskonzept verwiesen, wie es bei Lageregelungssystemen für Senkrechtstarter oder beim Landerechner der Mondlandefähre zur Anwendung kommt.

2.2.8 Erzeugen von Sicherheit nach dem Phasenkonzept

Zur Erreichung geeigneter Sicherheitszustände bedarf es unterschiedlicher Festlegungen und Schritte in den verschiedenen Phasen des Lebenszyklus eines Systems, einer Anlage oder eines Produkts durch die eingebundenen Personen (siehe Abschnitt 2.1.2).

Konstrukteure und Entwickler der Hard- und Software, Lieferanten, Betreiber, Personal zur Montage, Bedienung, Wartung, Reparatur und Entsorgung sowie die zuständigen aufsichtführenden Institutionen (Behörden) müssen daher geeignete und realistische Maßnahmen und Wege entwickeln und diskutieren, die das Versagen der Funktionen oder eine Veränderung der Eigenschaften weitestgehend verhindern können. Die Erarbeitung von internationalen Lösungen ist anstrebenswert, da eine Vielzahl von Produkten nicht nur national entwickelt und genutzt wird. Die weltweite Akzeptanz von guten Sicherheitslösungen, die sich durchaus unterscheiden können, ist hilfreich.

Für die Entwicklung von sicherheitsrelevanten Systemen und Funktionen ist eine Erarbeitung von geeigneten und angepassten Prozessen sinnvoll, um die verschiedenen Anforderungen an die Sicherheitseigenschaften zu erreichen. Solche Prozesse können folgende Themen enthalten, die an die Funktion und Aufgabe der Systeme angepasst sein können bzw. müssen:

- Systemdefinition
- Gefahrenanalyse
- Risikobetrachtung
- Ableitung von Sicherheitsanforderungen
- Realisierungsphase
- Dokumentation
- Managementaufgaben
- Querschnittsprozesse
- Unterstützungsprozesse
- Lieferantenbeziehungen

Durch die schnelle Weiterentwicklung und Innovation der Technologien müssen parallele Arbeiten erfolgen, die die Notwendigkeit von Erweiterungen, Spezialisierungen und Änderungen von vorhandenen Regulierungen und Standards prüfen und umsetzen. Durch die Innovationen werden Technikfelder beschritten, die in der Vergangenheit vielfach nicht in den bisherigen Konzepten berücksichtigt werden konnten. Gerade die Nutzung von Elektronik zur Realisierung von innovativen Funktionen braucht solche neuen Randbedingungen, die aus der Vergangenheit nicht immer übernommen werden können. Die Nutzung von Funktionen hängt entscheidend von der Rechtssicherheit für den Hersteller ab, die u.a. vom Stand der Technik beschrieben wird.

Für komplexe Systeme und Anlagen oder wenn die öffentlich-technische Sicherheit betroffen ist, ist ein so genannter „Safety Case” (Sicherheitsbericht) zu fordern. Er sollte darüber hinaus für alle Fälle eine wählbare Option sein, aber in den oben angeführten Bereichen Teil der praktizierten Sicherheitskultur sein müssen. Ausgehend von den Vorgehensweisen in der Luft- und Raumfahrttechnik, der chemischen Verfahrenstechnik oder vergleichbar komplexen Anlagen der Energiewirtschaft muss gefordert werden, dass ein sachlich angemessenes Sicherheitsmanagement ausgearbeitet, vorgelegt und angewendet wird und vom ersten Augenblick an – also schon bei den Ideen und ersten Überlegungen

zum Design – die Dokumentation zu einem „Sicherheitstechnischen Anforderungskatalog“ beginnt. Die Fortschreibung muss kontinuierlich erfolgen und alle Änderungen und Modifikationen sind in Revisionsfassungen zu dokumentieren. Für alle Technikfelder gilt, dass eine Systembeschreibung Bestandteil des Safety Case ist. Weiter sind enthalten das Sicherheitsmanagement bzw. der Sicherheitsplan, eine Risikoabschätzung, ein Notfallplan sowie die Anweisung zur Dokumentation. Je nach konkretem Fall können bei sehr arbeitsteiligen Fertigungen weitere – komponenten- und phasenbezogene – Teile hinzukommen, z.B. so genannte Fertigungs- und Prüffolgepläne. Der Safety Case startet mit der Produktidee und wächst über die Zeit und den Phasen des Lebenszyklus.

Für die Phasen des Lebenszyklus eines Systems (einer Anlage oder eines Produkts) gelten prinzipiell ähnliche Anforderungen. Auch während der Nutzung, Wartung, Reparatur, Stilllegung und Entsorgung werden geeignete Verfahren, Prozesse, Anweisungen erarbeitet, die Sicherheit erzeugen und erhalten. Eine sorgfältige Erarbeitung solcher Verfahren gewährleistet auch in diesem Bereich optimale Ergebnisse und hohe Sicherheitsstandards. Die Einhaltung der erarbeiteten Methoden und Prozesse durch Betreiber und Nutzer ist jedoch Voraussetzung für langfristig gewährleistete hohe Sicherheit. Auch hier ist durch geeignete Kommunikation um Verständnis und Sensibilität zu werben. Der Mensch steht hier an einer Schlüsselposition des Prozesses zum Erzeugen von Sicherheit.

Technische Sicherheit gehört zu denjenigen Eigenschaften eines Systems, einer Anlage oder eines Produkts, die nicht nur mittels eines geregelten Prozesses gezielt zu erzeugen sind, sondern stets auch der Nachweisführung bedürfen – gleichgültig, ob durch Prüfungen in eigener Verantwortung (des Herstellers: 1st party), durch mögliche Auftraggeber/Kunden (2nd party) oder durch unabhängige Dritte (3rd party). Eine wichtige Rolle für die Aussagekraft von Prüfungen spielt die Art der hierbei beteiligten Parteien.

Bei Betrachtung der Lebensphasen im Abschnitt 4 „Überprüfbarkeit der Sicherheit“ wird deshalb dargestellt, welche Rolle Prüfungen spielen. Kritisch zu beurteilen ist dabei, ob die Überprüfungen sich allein durch die Marktteilnehmer regeln lassen bzw. inwieweit Prüfungen durch unabhängige Dritte durchgeführt werden müssen, weil der Markt kein hinreichend geeignetes Regulativ bietet. Bei den unabhängigen Dritten ist zu prüfen, inwieweit die Kontrollfunktion privatisiert werden kann (z.B. in Form von privatwirtschaftlichen Audit-Systemen)

bzw. welche Verantwortung besser durch den Staat selbst zu tragen ist. Dabei ist in Betracht zu ziehen, dass die Verantwortung umso nachdrücklicher vom Staat wahrgenommen werden muss, je höher die Gefährdungsklasse gemäß Tabelle 1 ist. Bei dieser Betrachtung ist zu bedenken, dass reine Gewährleistungsverantwortung beim Staat (siehe hierzu Abschnitt 4.3.3) nur bei Gefährdungsklasse 1 erlaubt sein sollte.

2.3 Folgerungen aus einem sicherheitsmethodischen Konzept

Aus ethisch/moralischen Gründen sowie den rechtlichen Vorgaben resultiert die Verpflichtung, technische Einrichtungen sicherheitsgerecht zu gestalten. Die dabei im Wesentlichen auch heute noch praktizierte Arbeitsweise stützt sich auf einen Erfahrungsschatz, der sich im Lauf der allgemeinen technischen Entwicklung zu einem nicht unbeträchtlichen Umfang herausgebildet hat – allerdings vornehmlich unter dem Zwang aufgetretener Schadensereignisse.

Ingenieure, die technische Einrichtungen konzipieren, entwickeln und bauen, haben im Rahmen ihrer Gesamtverantwortung auch der Pflicht nachzukommen, diese technischen Einrichtungen sicherheitsgerecht zu gestalten. Dennoch liegt das verbleibende Sicherheitsrisiko, das beim Umgang mit technischen Einrichtungen niemals vollständig auszuschließen ist, sachlich bedingt stets beim Betreiber bzw. Nutzer. Aus dieser Situation, die durch eine sachbedingte Polarisierung gekennzeichnet ist, resultiert zwangsläufig die Problemstellung: „Was und wie viel ist sicher genug?" Um diese Problemstellung auch bei Anwendung neuer Technologien einer ganzheitlichen Lösung zugänglich machen zu können, sind technische Gestaltung und erforderliche Nachweisführung methodisch so vorzunehmen, dass dem schadenvorbeugenden, risikomindernden Charakter sicherheitstechnischer Vorkehrungsmaßnahmen durch eine entsprechend ausgerichtete, vorwiegend analytisch-präventive Vorgehensweise Rechnung getragen wird.

Vorbedingung für wirkungsvolle sicherheitstechnische Tätigkeiten ist eine ingenieurmäßig korrekt vorgenommene konstruktive Durchbildung, die Gewähr dafür bietet, dass die technische Einrichtung kein Schadensereignis erwarten lässt, wenn sie wie vorgesehen bei tatsächlich gegebenen Umwelteinflüssen betrieben bzw. genutzt wird. In diesem Zusammenhang sind insbesondere in der Luft- und Raumfahrttechnik gebräuchliche Gestaltungsprinzipien zu nennen. Lebens-

dauerkonzepte auf Schadensfreiheit, die redundante, die ausfallsichere und auch die schadenstolerante Gestaltung haben, haben trotz ihrer nicht immer eindeutigen Wortbedeutung und ihrer teilweise sich überlappenden Wirkungsweisen wesentlich zur konstruktiven Durchbildung im Hinblick auf Sicherheit nicht nur im Flugzeugbau beigetragen. Eine weitere Vorbedingung ist die bauliche Ausführung der technischen Einrichtung in fehlerfreiem Zustand. „Versagenssichere Gestaltung" bedeutet „fail-safe-design", d.h. den bewussten Umgang mit Gestaltungsprinzipien, die die Technische Sicherheit zum integralen Bestandteil von Produktbeschaffenheit und -verhalten machen.

Fehler, Störungen und Versagensfälle in technischen Einrichtungen können nicht grundsätzlich ausgeschlossen werden – sei es, weil sie zeitlich zufällig auftreten, weil unvorhersehbare Einwirkungen nicht angemessen beherrschbar sind (z.B. Blitzschlag), sei es, weil unbeabsichtigte Fehlbedienungen nicht bedingungslos vermieden werden können. Eine sicherheitsgerechte technische Gestaltung muss also neben der korrekten konstruktiven Durchbildung auch Vorkehrungen umfassen, mit denen derartigen Fehlern wirksam begegnet werden kann, wie beispielsweise durch sicherheitstechnische Verriegelungseinrichtungen, mit denen sich jede Art von Fehlbedienung verlässlich unterbinden lässt. Diese Fehlermöglichkeiten, die bei neuen Technologien keineswegs als bekannt vorausgesetzt werden können, müssen systematisch analysiert werden, damit Ursache und Wirkung der Fehlermöglichkeiten so weit wie möglich determiniert werden können.

Die Komplexität technologisch neuartiger Systeme macht es erforderlich, auch das stochastische Versagensverhalten analytisch zu erfassen, um die Wirksamkeit sicherheitsorientierter Vorkehrungen prüfen und nachweisen zu können. Hierfür stehen die bewährten Methoden der Zuverlässigkeitstechnik zur Verfügung. Es entspricht durchaus dem heute gegebenen „Stand von Wissenschaft und Technik" (§ 7 II Nr. 3 des Atomgesetzes), wenn der Nachweis einer sicherheitsmäßig angemessenen und ausreichenden Zuverlässigkeit dann bevorzugt wird, wenn der dabei mögliche Aufwand zu statistisch abgesicherten Ergebnissen führen kann und eine anderweitige sicherheitsorientierte Nachweisführung kein in sich schlüssiges Ergebnis erwarten lässt. Auch solche Erkenntnisse der Zuverlässigkeitstechnik, die sich nicht ausschließlich auf deren numerische Verfahren beziehen, können sinnvoll in die Sicherheitstechnik einbezogen werden, um diejenigen Randbedingungen zu ermitteln, unter denen redundante Einrichtungen sicherheitstechnisch erforderlich sind.

Traditionell wurde der Status der Sicherheitstechnik durch Lernen aus Erfahrung geprägt (siehe Abschnitt 4.2: „Erfahrungsrückfluss” oder „Feed back-Kontrolle”). Dies bedeutet, dass sich die sicherheitstechnische Erfahrung zwar vergleichsweise leicht auf Produkte und technische Einrichtungen übertragen lässt, die mit früheren und gegenwärtigen Produkten und Einrichtungen technologisch vergleichbar sind. Als problematisch erweist es sich jedoch stets, wenn „Sicherheit durch Erfahrung aus der Vergangenheit” auf technologisch weiterentwickelte oder gänzlich neuartige Produkte und Einrichtungen übertragen werden soll. Hier werden vorausschauende Ansätze der Risikoabschätzung erforderlich, die mit probabilistischen Methoden die möglichen Versagensarten identifizieren und entsprechende Vorkehrungen im Design implementieren („Feed forward-Kontrolle”). Häufig wird eine Kombination beider Vorgehensweisen erforderlich sein. Dies wird im Folgenden noch vertieft beschrieben.

2.3.1 Übertragung des Technischen Sicherheitsstandards auf technologisch vergleichbare Produkte

Beschränken sich Entwicklung und Herstellung eines Produkts bzw. einer anderen technischen Einrichtung auf den bestehenden Stand der Technik, d.h. das betreffende Produkt beinhaltet weder gravierende technologische Neuerungen noch stellt es insgesamt eine technologische Innovation dar, so reichen die vorhandenen rechtlichen und technischen Regelungen aus, um Sicherheit für dieses Produkt verbürgen zu können. Entweder

- enthalten die einschlägig gültigen Rechtsverordnungen eine allgemeine Verweisung auf die Technischen Regelwerke bzw. eine unbestimmte Verweisung auf den Stand der Technik oder
- die Bau- und Durchführungsverordnungen schließen eine direkte Verweisung auf die einschlägig anwendbaren Technischen Regelwerke schon ein.
- In der Technik werden die hierbei genutzten Möglichkeiten durch zwei Schwerpunkte beschrieben:
  - einerseits: Sicherheit durch Vollnormung (wie in Elektro- und Bautechnik)
  - andererseits: versagensanalytisch basierte Sicherheitstechnik (wie in der Luft- und Raumfahrttechnik),

  Mischformen aus beiden Schwerpunkten kommen zunehmend ebenfalls zur Anwendung.

- Auch unterschiedliche Zuordnungen der Sicherheitsverantwortung sind in der Rechtsanwendung üblich:
  - Hersteller, Eigentümer (Halter), Betreiber, staatliche Stelle.
- Das Änderungspotenzial beschränkt sich in erster Linie auf die Technischen Regelwerke bzw. sachbedingt auf den Stand der Technik.

2.3.2 Übertragung des Technischen Sicherheitsstandards auf technologisch weiterentwickelte Produkte

Bei technologisch weiterentwickelten Produkten gestaltet sich die Sicherheitstechnik wie folgt:

- Rechtsgrundlagen sind auch hier eindeutig zuordenbar.

- Ebenso sind Aufsichtsbehörde bzw. aufsichtführende Institution für den betreffenden Anwendungsfall festgelegt.

- Die Anwendung des so genannten Stands der Technik gestaltet sich hier in gewissem Umfang problematisch:
  - Rechtsverordnungen (mit Verweisung auf den Stand der Technik) bleiben gültig,
  - Sicherheitstechnische Anwendbarkeit der Normen ist jedoch fraglich, und erfordert in jedem Einzelfall eine Klärung durch versagensanalytisch basierte Sicherheitstechnik, die stets möglich ist.
  - Es besteht kein rechtlicher Zwang zur Klärung der sicherheitstechnischen Anwendbarkeit der Normen.
  - Es besteht die Problematik stets vorhandener Meinungsvielfalt bei der Aufsichtführung.

- Unterschiedliche Zuordnung der Sicherheitsverantwortung in der Rechtsanwendung:
  - Hersteller, Eigentümer, Halter, Betreiber, staatliche Stelle.

2.3.3 Übertragung des Technischen Sicherheitsstandards auf technologisch neuartige Produkte

Bei technologischen Innovationsvorhaben muss auch im Zusammenhang mit der Sicherheitstechnik Neuland beschritten werden (wie z.B. bei der Entwicklung der Magnetbahn-Technologie), weil der gegebene Stand der Technik nicht die neue, bisher unbekannte Technologie abzudecken vermag. Hier ist der Einsatz vorausschauender probabilistischer Methoden der Risikoabschätzung erforderlich:

- Rechtsgrundlagen sind nicht ohne weiteres zuordenbar:
  - Es kommt zu Verlegenheitslösungen wie z.B. das Gesetz über den Bau und den Betrieb von Versuchsanlagen zur Erprobung von Techniken für den spurgeführten Verkehr (Versuchsanlagengesetz), ohne das eine Versuchsanlage zur Erprobung dieser neuartigen Technologie rechtlich gar nicht erlaubt gewesen wäre.
  - Aufsichtsbehörden bzw. aufsichtführende Institutionen gibt es (noch) nicht; sie sind für den einzelnen Anwendungsfall gesondert festzulegen; im Falle der Magnetbahn war das niedersächsische Wirtschafts- und Verkehrsministerium zuständig.

- Anwendung des Stands der Technik ist hier nicht möglich:
  - Es gibt weder erschöpfende Rechtsverordnungen (alleinige Verweisung auf den Stand der Technik ist hier sicherheitstechnisch fragwürdig) noch
  - eine Normung, woraus sich ein Zwang zu versagensanalytisch basierter Sicherheitstechnik ergibt.
  - Die Problematik besteht darin, dass gegebenenfalls hilfsweise eingeschaltete Gutachter eine Meinungsvielfalt entstehen lassen, da es keine Regeln für ein geordnetes, interdisziplinär abgestimmtes Vorgehenskonzept gibt (siehe auch Abschnitt 6.3.2).

- Zuordnung der Sicherheitsverantwortung verbleibt hier fast ausschließlich beim Entwickler bzw. Hersteller, da die Rechtsordnung in der Regel keine anderen Stellen vorsieht, die eine solche Sicherheitsverantwortung übernehmen oder auch nur teilen würden.

3 Grenzen der Sicherheit

Die Grenzen der Sicherheit sind fließend. Sie werden einerseits durch die Randbedingungen der Entwicklungs-, Fertigungs- und Nutzungsprozesse sowie die Kosten bestimmt und andererseits ergeben sie sich aus dem fortschreitenden Stand von Wissenschaft und Technik. Die Ziehung von Grenzen ist notwendig. Sie bedeutet Gewinn. Als ethische Aufgabe ist der sinnvolle Verzicht weder Schwäche noch Defizit und Mangel. Gleichzeitig sind Tendenzen zum extremen Verlagern der Grenzen zu beobachten. Daraus ergeben sich folgende Bedrohungsszenarien:

- Gefährdung der Ernährungsgrundlage („Reinheit" der Nahrungs- und Futtermittel sowie des Trinkwassers),
- Gezielte Störungen verursacht durch kriminelle Energien (Sabotage, Attentate, Terrorakte),
- Kriegseinwirkungen und höhere Gewalt sowie Naturgewalten,
- Gefährdung durch Arzneimittel (abschreckende Warnung vor unerwarteten Nebenwirkungen) sowie durch Bedarfsgegenstände, Haushaltschemikalien, Kosmetika,
- Gefahren neuer Technologien, wie z.B. Schädlingsbekämpfung, Nutzung der Gentechnik, Kernenergietechnik.

Dem ist aus ethischer Sicht (siehe Abschnitt 1.6) hinzuzufügen, dass die Menschheit nicht nur für den Erhalt der eigenen Lebensgrundlage und die der nachfolgender Generationen in der Verantwortung steht, sondern sie ist Bewahrer und Schutzpatron von Leben jeglicher Art (Tierschutz, Erhalt der Artenvielfalt, Schutz der Biosphäre). Dagegen wird und muss eine Bevölkerung am Existenzminimum ausschließlich um ihre Selbsterhaltung kämpfen. Ein verfeinertes Empfinden für die Auswirkung von Technik darf daher als Charakteristikum einer saturierten Gesellschaft gelten. Das bedeutet, dass die Ansichten über Schaden und Nutzen der Technik und ihrer Sicherheits-Standards inhomogen sind.

Wenn die Grenzen der Sicherheit im Umkehrschluss als Ausmaß der Bedrohung individueller Freiheit zu verstehen sind, so kann nur eine rationale Abwägung

von Individualschutz gegen Gemeinschaftsschutz in einem demokratischen Prozess eine Grenze der Sicherheit festsetzen. Es muss dabei immer deutlich gemacht werden, dass es sich hierbei um eine Güterabwägung zwischen dem beabsichtigten und dem unbestreitbar geschaffenen Nutzen und einem im Rahmen des verbleibenden Risikos denkbaren Schaden handelt. Nutznießer ist auf jeden Fall die Solidargemeinschaft, die insgesamt einen Gewinn erzielt.

In jedem Fall gelten für die Festlegung eines Sicherheitskonzepts folgende Grundgedanken:

- Absolute Sicherheit im Sinne eines Null-Risikos kann vom Gesetz- und Verordnungsgeber nicht gefordert werden (Risikoverbot), weil es prinzipiell nicht möglich ist.
- Allerdings sollten unter diesem Gesichtspunkt alle Möglichkeiten genutzt werden, damit bei unterschiedlichen technischen Produkten, Prozessen, Anlagen und Systemen das Verhältnis zwischen dem Risiko eines denkbaren Schadens und dem geschaffenen Nutzen für die zu schützenden Rechtsgüter (Risikoäquivalenz) ausgewogen ist.
- Der Maßstab für die größten noch vertretbaren Schäden wird nicht nur durch das Schutzbedürfnis der betrachteten Rechtsgüter bestimmt, sondern auch durch die Absicht, gesellschaftliche Bedürfnisse zu befriedigen (Nutzen), wobei es im allgemeinen einer Abwägung im gesellschaftlichen Konsens bedarf (Risikosteuerung).

3.1 Gesellschaftlich akzeptierte und staatlich definierte Grenzen

In einem Rechtsstaat darf der Bürger zuverlässig erwarten, dass Entscheidungen, die Leben und Gesundheit betreffen, öffentlich legitimiert werden. Das geht nicht ohne Kommunikation. Dabei kann es nicht das Ziel sein, die jeweils andere Seite davon zu überzeugen, dass ein Grenzrisiko tragbar oder unzumutbar ist. Vielmehr soll der Bürger in die Lage versetzt werden, den Anspruch auf Mitsprache umzusetzen, um eine quasi „Risikomündigkeit” einzulösen. Es ist die Fähigkeit angesprochen, auf der Basis der Kenntnis der faktisch nachweisbaren Konsequenzen von schadenauslösenden Ereignissen oder Aktivitäten, der verbleibenden Unsicherheiten und anderer risikorelevanter Faktoren eine persönliche Beurteilung vornehmen zu können. Die Fähigkeit soll bzw. wird den Wertvorstellungen für die Gestaltung des eigenen Lebens sowie den persön-

lichen Kriterien zur Beurteilung der Akzeptabilität dieser Risiken für die Gesellschaft insgesamt entsprechen.

Bei Anerkennung der Mitsprache des Bürgers ist es Aufgabe der politischen Institutionen, die dazu notwendige Kommunikationsbasis aufzubauen und zu pflegen. Im Rahmen einer Risikokommunikation sind alle Formen der Kommunikation von der einfachen Dokumentation von Ergebnissen, über gezielte Informationsangebote bis hin zum Dialog und der Beteiligung an der Entscheidungsfindung angezeigt.

Die Festlegung von Grenzen und eine Risikobewertung stoßen in einer Gesellschaft, in der Wertepluralismus herrscht und politische Handlungen stets unter hohem Rechtfertigungsdruck stehen, oft auf Skepsis oder Misstrauen. Aussagen über Risiken sind daher auf Plausibilität und Vertrauen in so genannten Regulierungsgremien angewiesen. Je mehr Individuen und Gruppen die Möglichkeit haben, aktiv an der Risikobetrachtung mitzuwirken, desto größer ist die Chance, dass sie Vertrauen in die politischen Institutionen entwickeln und auch selbst Verantwortungen übernehmen.

Dabei kann und darf eine Beteiligung allerdings kein Ersatz für effektives Risikomanagement sein; die Beteiligung dient allein der Entscheidungshilfe. Vor allem die Verantwortung der legalen Entscheidungsträger sollte dadurch nicht verschleiert oder aufgeweicht werden. Beteiligung ist zu verstehen als

- gegenseitige Information (als unabdingbare Voraussetzung zur richtigen Entscheidungsfindung),
- frühzeitige Mitwirkung von Betroffenen und der maßgeblichen gesellschaftlichen Gruppen (gegebenenfalls unter Einräumung eines – rechtfertigbaren – Vetorechts) und
- Mitentscheidung.

Das Postulat „praktischer Vernunft" als Maßstab der Entscheidungsträger bedingt, dass zwar nach dem Stand von Wissenschaft und Technik „praktisch" ausgeschlossen werden kann, dass ein Schadensereignis eintritt. Im Gegensatz zur „theoretischen Vernunft" jedoch strebt „praktische Vernunft" nicht die bloße Erkenntnis von Ideen an, sondern gibt gleichzeitig erfüllbare Handlungsorientierungen, die auf der Erkenntnis beruhen, dass stets ein restliches Risiko verbleibt.

Hierin wird angesichts der theoretisch unendlich vielen Möglichkeiten der Schadensvorsorge ein Korrektiv in Form von „sachlichen" und „vernünftigen" Maßstäben und Grenzen gesehen. Inhaltlich wird gerade nicht der absolute Schadensausschluss gefordert, sondern es genügt, dass nach dem Erkenntnisstand der Ingenieure und Naturwissenschaftler, unter Einbezug menschlichen Ermessens, der Schadensfall als praktisch ausgeschlossen erscheint. Übertragen in das Technische Sicherheitsrecht, stellt beispielsweise die Forderung nach Sicherungssystemen mit verringerter Versagenswahrscheinlichkeit eine derartige Handlungsorientierung dar. Dazu gehören auch alle konstruktiven Vorkehrungen gegen – insbesondere zeitgleiches – Mehrfachversagen.

Was Ingenieure und Naturwissenschaftler oft für nicht nachvollziehbar halten, ist aus Sicht verschiedener gesellschaftlicher Gruppierungen gleichwohl rational. Die Rationalität gesellschaftlicher Entscheidungen in einem hochkomplexen System sind schwerwiegende Herausforderungen, weil alle Demokratien ihre Legitimität durch enge Korrespondenz mit der öffentlichen Meinung sichern. Wo bei speziellen Sachverhalten z.B. der Wille zur Sachrationalität fehlt, weil gesellschaftspolitische Erfordernisse im Vordergrund stehen, werden die Instrumente der Sachrationalität entweder gar nicht oder nicht entsprechend der ihnen innewohnenden Möglichkeiten benutzt.

Im Allgemeinen lässt sich das Grenzrisiko nicht quantitativ erfassen. Es wird in der Regel indirekt durch sicherheitstechnische Festlegung beschrieben. Diese Konkretisierung oder Festlegung des Grenzrisikos setzt voraus, dass die mit bestimmten technischen Produkten, Prozessen, Anlagen und Systemen verbundenen Schadenseintrittswahrscheinlichkeit und Schadensumfänge ausreichend bekannt und qualitativ beschreibbar sind. Die Beschreibung und Bewertung von technischen Risiken gehört daher gleichfalls zu den Aufgaben der Regulierungsgremien bzw. des Staates, der die Beiträge der betroffenen Kreise wertend einbezieht (siehe Abschnitt 3.5.4).

3.2 Unerreichbarkeit absoluter Sicherheit

Eine absolute Sicherheit kann es aus mehreren Gründen nicht geben, weil

- technische Prozesse niemals mit 100%-iger Zuverlässigkeit, d.h. ohne jegliche Störung, ablaufen und auch die betroffenen technischen Einrichtungen

deshalb nicht a priori gegen jegliches Versagen gefeit sein können (Sicherungseinrichtungen wie „fail safe“ und „fail operational“),

- Werkstoffeigenschaften nicht 100%-ig erfassbar und deshalb auch nicht absolut verlässlich sein können
  (in der Technik wird dieser Erkenntnis z.B. durch „worst case“-Betrachtungen und so genannte Sicherheitsfaktoren Rechnung getragen),
- der Stand des Wissens niemals vollständig und erschöpfend fassbar ist,
- die ökonomische Machbarkeit den Bemühungen um maximale Sicherheit Grenzen setzt,
- das menschliches Handeln immer der Möglichkeit des Irrtums und der Fehlhandlung unterliegt.

Unkenntnisse und die Unvollkommenheit der Technischen Sicherheit lassen sich allerdings einschränken. Die Wirkungen sicherheitsgerichteter Maßnahmen können aber gegenüber der absoluten Sicherheit nur als asymptotische Annäherung beschrieben werden. Ein Schadenseintritt kann nur dann mit absoluter Sicherheit ausgeschlossen werden, wenn er naturgesetzlich unmöglich wäre. Somit gilt, dass jedem technischen Sicherheitssystem grundsätzlich dessen Versagensmöglichkeit immanent ist. Absolute Sicherheit kann von keiner technischen Einrichtung verwirklicht werden. Es bleibt immer ein restliches Risiko, das allerdings geringer sein muss als ein bestimmtes Grenzrisiko. Deshalb führt eine Forderung nach absoluter Sicherheit oder fehlerfreien Lösungen komplexer Technik-Systeme in die falsche Zielrichtung.

Unter der klassischen Fragestellung zur Sicherheitstechnik: „Wie sicher ist sicher genug?” verbergen sich Zielkonflikte zwischen Technischer Sicherheit und Praktikabilität einerseits und finanzieller Machbarkeit sowie gesellschaftlichen Sicherheitsvorstellungen andererseits. Eine allein auf ein Maximum hin orientierte Technische Sicherheit kann für den Benutzer im Zweifelsfall sogar schädlich sein. Ein überhöhtes Maß an Technischer Sicherheit führt bisweilen zu einer Einbuße an praktischer Handhabbarkeit. So birgt gesteigerte Komplexität von Sicherheitssystemen sogar die Gefahr der Risikoerhöhung in sich.

Aus sicherheitstechnischer sowie aus umweltpolitischer, wirtschaftlicher und rechtlicher Sicht gilt es demzufolge, optimierte, also relative Sicherheit zu erzeugen. Dabei sind die verbleibenden Grenzrisiken von Anlagen, Produkten und Betriebsweisen zu ermitteln und mit den Risiken der bewährten Sicherheitstechnik, alternativer Produkte und sonstiger zivilisatorischer Umweltbelastungen

sowie mit den natürlichen Lebensrisiken zu vergleichen und durch Kommunikationsmanagement einer weit reichenden Akzeptanz zuzuführen.

Erst solche vergleichenden Risiko-Abschätzungen lassen erkennen, welcher naturwissenschaftliche, technische und rechtliche Stellenwert der optimalen Sicherheit einer Anlage, einem Produkt oder einer Betriebsweise zukommt. Der Schutz des Menschen und seiner Umwelt durch die Technische Sicherheit kann und muss sehr wohl optimiert werden, wird aber stets relativ bleiben.

3.3 Risiko-Verständnis

Der Begriff „Risiko" wird unterschiedlich verstanden und verwendet; er ist ein vielfach gebrauchtes Wort unserer Tage. Deshalb erfolgt hier eine Klarstellung und Definition im Rahmen dieser Denkschrift zur Technischen Sicherheit:

Risiko ist sowohl die quantitative als auch die qualitative Charakterisierung eines Schadens hinsichtlich der Möglichkeit seines Eintreffens und der Tragweite der Schadenswirkung.

Nach W. Bons (Zeitschrift „Kunst und Technik" des Deutschen Museums, München, Vol. 4, S. 18, 1999) erklärt sich, „dass die Risiken eine typische moderne Form des Umgangs mit Unsicherheiten sind". Ein Blick auf die Entstehungsgeschichte des Risiko-Konzeptes zeigt, dass es im Kontext des Fernhandels italienischer Städte im Mittelalter entstand. Der Fernhandel war eine ebenso planvolle wie unsichere Angelegenheit. Diese Unsicherheiten wurden nicht als Gefahren benannt, also als Bedrohung gesehen, gegen die man nichts machen konnte, sondern als Risiken bezeichnet (italienisch: rischiare = wagen). Der Kaufmann unterwarf sich nicht den Unsicherheiten, sondern forderte sie kalkulierend heraus und spekulierte auf Erfolg. Aber die Unsicherheiten, die er einging, begriff er nicht länger als schicksalhafte Bedrohung sondern als berechenbare Wagnisse, also als Probleme, die sich nur dann negativ bemerkbar machten, wenn er falsch kalkulierte und keine Vorsichtsmaßnahmen traf.

Die komplementären Begriffe Risiko – Chance bezeichnen das Wagnis, dass eine Handlung, eine Aktivität, ein Ereignis zu einem Schaden – Nutzen, Verlust – Gewinn, Nachteil – Vorteil führt. Der Begriff des Risikos ist im Zusammenhang mit dem Gesetz über die friedliche Nutzung der Kernenergie und gegen ihre Gefahren (Atomgesetz) ausführlicher diskutiert worden, wobei das Atom-

gesetz unter Bezugnahme auf den Stand von Wissenschaft und Technik von einer Trennung zwischen abzuwehrenden Gefahren und den Schadenswahrscheinlichkeiten ausgeht. Maßgeblichen Einfluss auf die Einteilung in den kategorialen Rahmen von Gefahrenabwehr, Risikovorsorge und Grenzrisiko haben die Eintrittswahrscheinlichkeit und die Höhe eines bestimmten Schadens und eine darauf aufbauende Wertung. Jenseits von Gefahrenabwehr und Risikovorsorge beginnt der Bereich des so genannten „Grenzrisikos", welches als „sozialadäquate Last" von allen Bürgern zu tragen ist. Implizit ergibt sich das Grenzrisiko aus der Summe der technischen Regelwerke und dem verantwortlichen Handeln gemäß dieser Regelwerke unter Nutzung des kumulierten Wissens.

Die Verantwortbarkeit von Grenzen der Sicherheit besteht darin, die Bereitschaft der Betroffenen, mit Risiken nach technischer, ökonomischer, ökologischer und ethischer Reflexion angemessen umzugehen, sie abzuschätzen und zu bewerten und erst im Gesamtergebnis zu akzeptieren oder abzulehnen. Sicherheit, hier präzisiert als Technische Sicherheit und definiert durch ein Grenzrisiko, muss in einer Reihe von Wechselwirkungen von der Zielsetzung über die Verwirklichung und Nützlichkeit bis zur Kontrolle gesehen und in der Risikowahrnehmung beachtet werden.

Naturwissenschaftlich fundierte Risikoanalysen sind hilfreiche und notwendige Instrumente einer rationalen Vorgehensweise. Nur mit ihrer Hilfe lassen sich Risiken verstehen und Optionen mit geringsten Erwartungswerten von Schaden auswählen. Die Bürger nehmen das Risiko aber weniger naturwissenschaftlich als vielmehr gefühlsmäßig wahr. Wenn man auf ihr Empfinden hören will, müsste man rein rational die naturwissenschaftlich folgerichtige Risikoanalyse für solche Empfindungen öffnen; damit dürfte die Risikoanalyse allerdings nicht mehr als naturwissenschaftlich folgerichtig bezeichnet werden. So verbleibt die Analyse zwar im fachlichen Umfeld. Die Öffentlichkeit ist jedoch in die Risikokommunikation einzubeziehen, mit der die Ergebnisse der Analyse den interessierten Kreisen der Gesellschaft nahe gebracht werden können.

3.4 Sachzusammenhang zwischen Risiko, Sicherheitstechnik und Technischer Sicherheit

Das – in der Regel rein zufällige und multikausal verknüpfte – globale Geschehen in unserer Welt ist weder mit mathematischer Genauigkeit vorhersehbar noch vorher bestimmbar. Die Komplexität dieses natürlichen Geschehens bietet

dem Menschen, wenn überhaupt, nur sehr geringe Möglichkeit zur Einflussnahme. Zwar sind lokal begrenzte Eingriffe in die Natur in sehr eingeschränktem Maße möglich; die daraus resultierenden Folgen lassen sich oft gar nicht oder nur ungenügend abschätzen. Der Mensch bleibt dem natürlichen Geschehen weitgehend ausgesetzt, wodurch für ihn ein naturbedingtes Lebensrisiko besteht. Natürliche Risiken erscheinen schicksalhaft.

Der Mensch hat gelernt, sich technische Einrichtungen zu schaffen, die sich vom prähistorischen Faustkeil bis zum neuzeitlichen Industriekomplex, vom schlichten Feuerplatz bis zur modernen Energieversorgung erstrecken. Im Gegensatz zu den natürlichen Risiken kann der Mensch die Risiken, die mit technischen Einrichtungen verbunden sind, die er sich zur eigenen Daseinsvorsorge selbst geschaffen hat, sehr wohl und sogar weitgehend beherrschen. Zur Beherrschung dieser technischen Risiken steht dem Menschen das gesamte Methodeninstrumentarium der Sicherheitstechnik zur Verfügung. Bei fachkompetenter und sachgerechter Anwendung lässt sich ein außerordentlich hohes Maß an Technischer Sicherheit erzielen. Eine technische Einrichtung gilt als „technisch sicher“, wenn das Risiko, das mit dem Vorhandensein und der Nutzung dieser technischen Einrichtung verbunden ist, sich nachweislich so beherrschen lässt, dass ein bestimmtes Grenzrisiko nicht unterschritten wird (siehe Abschnitt 3). Unter dem Begriff Technische Sicherheit werden die Eigenschaftsmerkmale einer technischen Einrichtung verstanden, für die nachgewiesen ist, dass sie technisch sicher ist.

Dieser Sachzusammenhang lässt sich wie folgt zusammenfassen:

- Natürliche Risiken sind nur eingeschränkt beherrschbar; technische Risiken hingegen lassen sich ebenso beherrschen wie die Technik selbst.
- Die Sicherheitstechnik ist das Methodeninstrumentarium zur Beherrschung von technischen Risiken.
- Technische Sicherheit wird durch Anwendung der Sicherheitstechnik erzeugt und nachgewiesen.

3.5 Sicherheitstechnische Machbarkeit

Technische Sicherheit wird erzeugt und gepflegt. Der Staat muss administrativ auf die Möglichkeit von Schäden und auf technische Risiken reagieren, um eine Schädigung seiner Bürger abzuwenden. Dazu dient das Technische Sicherheits-

recht, das in seiner Gesamtheit auf die Eigenarten der Technik durch die Ausprägung folgender Attribute reagiert:

- Der zwangsläufige Zeitabstand zwischen der Fertigentwicklung einer neuen Technologie und den ihr erst im Nachgang zugeordneten rechtlichen Regelung hat zu anwendungsbezogenen gesetzlichen Regelungen geführt; das Technikrecht ist zersplittert und gilt jeweils nur für bestimmte technische Anwendungsbereiche (Technikfelder).
- Die Konkretisierung der aus gutem Grund unbestimmt formulierten Forderung nach Technischer Sicherheit wird vom Gesetzgeber auf die Rechtsanwenderebene der Fachwelt, der Behörden und Gerichte verlagert.
- Gesetzliche Forderungen nach Technischer Sicherheit werden durch unbestimmte Rechtsbegriffe wie „allgemein anerkannte Regeln der Technik", „Stand der Technik" oder „Stand von Wissenschaft und Technik" umschrieben, um sicherheitstechnische Beschaffenheits- und Verhaltensanforderungen zu formulieren.

Technische Produkte dürfen nur in den Verkehr gebracht werden, wenn die aus ihnen hergestellten technischen Anlagen bei ordnungsgemäßer Instandhaltung während einer zweckentsprechenden, angemessenen Dauer das Schutzziel aller einschlägigen Rechtsvorschriften erfüllen. Und sie müssen gebrauchstauglich sein. Technische Sicherheit basiert – neben dem einschlägigen Wissen der handelnden Menschen und denjenigen Organisationen, die unmittelbar mit dem Fachgebiet Sicherheit befasst sind – weitgehend auf den Technischen Regelwerken, Rechtsvorschriften und Belastungsgrenzen, die je nach Anwendungsbezug historisch bedingt unterschiedlich sind und häufig durch unterschiedliche Fachsprachen geprägt sind.

3.5.1 Allgemein anerkannte Regeln der Technik

Der Begriff „allgemein anerkannte Regeln der Technik" ist ein Rechtsbegriff, der seit längerem auch im Strafrecht verwandt wird. So wird beispielsweise nach § 323 StGB (Baugefährdung) derjenige bestraft, der bei der Planung, Leitung oder Ausführung eines Baues oder des Abbruchs eines Bauwerkes gegen die allgemein anerkannten Regeln der Technik verstößt und dadurch Leib oder Leben eines anderen gefährdet. Die allgemein anerkannten Regeln der Technik sind nicht nur dadurch erfüllt, dass eine Regel bei naturwissenschaftlicher Erkenntnis

als richtig dasteht, sondern sie muss auch allgemein anerkannt, also durchweg durch die betreffenden Ingenieure zur Anwendung gelangen und in der Praxis als richtig erkannt sein.

Das bedeutet demnach, dass es nicht darauf ankommt, ob die Wissenschaft eine Regel anerkennt und gelehrt habe, oder aber auch, ob diese in der einschlägigen Fachliteratur anerkannt werde, sondern die Überzeugung von der Notwendigkeit muss vielmehr auch die ausübende Baukunst sowie das Ingenieurwesen und das Baugewerbe, die System- (Anlagen-, Produkt-) und Prozessgestaltung, also die Praxis, besitzen. Diese Überzeugung muss sich derart gefestigt haben, dass im Sinne des Gesetzes von allgemeiner Anerkennung gesprochen werden kann.

Nach herrschender Auffassung besteht die faktische Vermutung, dass eine Norm den zum Zeitpunkt ihres Erscheinens gegebenen „Stand der Technik" wiedergibt. Sehr häufig wird es aber im Zeitpunkt des Erscheinens noch an der Anwendung in der Praxis fehlen, zumal, wenn es sich um die Durchsetzung neuer Technologien handelt. Bei sehr langwierigen Normungsverfahren komplexer Materien ist es im Übrigen nicht ausgeschlossen, dass die Norm schon im Zeitpunkt der Veröffentlichung nicht mehr der allgemeinen Anschauung entspricht, und die darin festgelegten Regeln deshalb nicht mehr dem Stand der Technik entsprechen. Allerdings besteht eine tatsächliche, jedoch jederzeit widerlegbare Vermutung, dass die einschlägigen Normen „Regeln der Technik" wiedergeben, die allgemein anerkannt sind.

„Allgemein anerkannte Regeln der Technik" sind von Fachleuten im Konsens erarbeitet worden. Sie können geschrieben oder ungeschrieben sein; sie sind jedoch in aller Regel kodifiziert. Eine Norm kann eine allgemein anerkannte Regel der Technik sein, sie muss es aber nicht. Nach herrschender Auffassung besteht lediglich eine faktische Vermutung, dass eine Norm im Zeitpunkt des Erscheinens, insbesondere, wenn sie im Verfahren nach DIN 820 „Normungsarbeit" zustande gekommen ist, eine allgemein anerkannte Regel der Technik ist. Das Technikrecht gestaltet seine Anforderungen mit unbestimmten Rechtsbegriffen, um technische Entwicklungen innerhalb des Rechtsrahmens effizient zu gestalten. Zur Konkretisierung stützt es sich deshalb auf die allgemein anerkannten Regeln der Technik, die auch unter dem Begriff „untergesetzliches Regelwerk" zusammengefasst werden. Entsprechende Rechtsetzungen formulieren beispielsweise die durchaus widerlegbare Fiktion, dass alle technischen

Regeln, die rechtlich allgemein eingeführt und bekannt gemacht sind, als allgemein anerkannte Regeln der Technik gelten.

3.5.2 Stand der Technik

Der Stand der Technik ist ein unbestimmter Rechtsbegriff und stellt die technischen Möglichkeiten zu einem bestimmten Zeitpunkt basierend auf gesicherten Erkenntnissen von Wissenschaft und Technik dar. Er findet sich in vielen Vorschriften und Verträgen und wird durch die Regelungen zur Rechtsförmlichkeit präzise definiert. Man bezeichnet damit Maßnahmen, die in ihrem Anforderungsgehalt zwischen den allgemein anerkannten Regeln der Technik und dem Stand von Wissenschaft und Technik liegen.

Stand der Technik ist der Entwicklungsstand fortschrittlicher Verfahren, Einrichtungen oder Betriebsweisen, der die praktische Eignung der Maßnahme im Hinblick auf die angestrebten Ziele (z.B. der Ziele des Arbeitsschutzes, des Umweltschutzes, der Sicherheit für Dritte, der Wirtschaftlichkeit: Also allgemein zur Erreichung eines hohen Niveaus bezogen auf die zu beachtenden Aspekte) insgesamt gesichert erscheinen lässt. Er ist aber noch nicht hinreichend und zeitlich ausreichend erprobt und meist nur Spezialisten bekannt, weshalb z.B. im Bauwesen üblicherweise die Einhaltung der allgemein anerkannten Regeln der Technik vertraglich gefordert wird.

3.5.3 Stand von Wissenschaft und Technik

Im Gegensatz zum „Stand der Technik“ bezeichnet der „Stand von Wissenschaft und Technik“ einen technischen Entwicklungsstand, bei dem Verfahren und Einrichtungen in Versuchs- und Pilotanlagen erprobt werden, jedoch eine Umsetzung in der Praxis noch aussteht (siehe Abbildung 2).

Die Verknüpfung von Rechtsbegriffen mit dem Begriff des „Standes von Wissenschaft und Technik” entlastet den Gesetzgeber von der sicherheitstechnischen Detailregelung, für die er weder von der Aufgabenzuweisung im Rahmen der Gewaltenteilung noch von der Sachkunde her befähigt ist. Mit der Bezugnahme auf den „Stand von Wissenschaft und Technik” (wie z.B. in § 7 Abs. 2 Nr. 3 Atomgesetz) verlangt der Gesetzgeber deshalb die Beachtung der wissenschaftlichen und technischen Entwicklung vor dem Hintergrund der rechtlichen Regelung: es muss diejenige Vorsorge zur Minimierung des technischen Risikos

getroffen werden, die nach den neuesten wissenschaftlichen Erkenntnissen für erforderlich gehalten wird.

Die Feststellung und Bewertung des „Standes von Wissenschaft und Technik" muss – im Bereich der Gefahrenbeurteilung wie im Bereich der Gefahrbeherrschung – unter Beachtung des naturwissenschaftlich-technischen Grundsatzes der „Ausgewogenheit" erfolgen: d.h. ein Risiko kann vernachlässigt werden, wenn es isoliert vorkommt, als solches nur gering zu bewerten ist, sich nicht mit gleichartigen anderen Risiken zu einem nennenswerten Risikobeitrag addiert, im Falle seiner Berücksichtigung aber notwendig andere, u.U. größere Risiken verursachen würde.

Der Stand von Wissenschaft und Technik kommt jedoch in weitem Umfang in Regelwerken zum Ausdruck, die von unterschiedlichen Gremien erstellt werden. Als Stand von Wissenschaft und Technik ist der augenblickliche Forschungs- und Entwicklungsstand innerhalb einer wissenschaftlichen Disziplin zu verstehen. Er muss sich auf schlüssige Beweise stützen, die der Überprüfbarkeit durch Dritte standhalten. Über ihn verständigen sich Fachleute zunächst im wissenschaftlichen Diskurs, um ihn dann einer fachlichen Öffentlichkeit zugänglich zu machen.

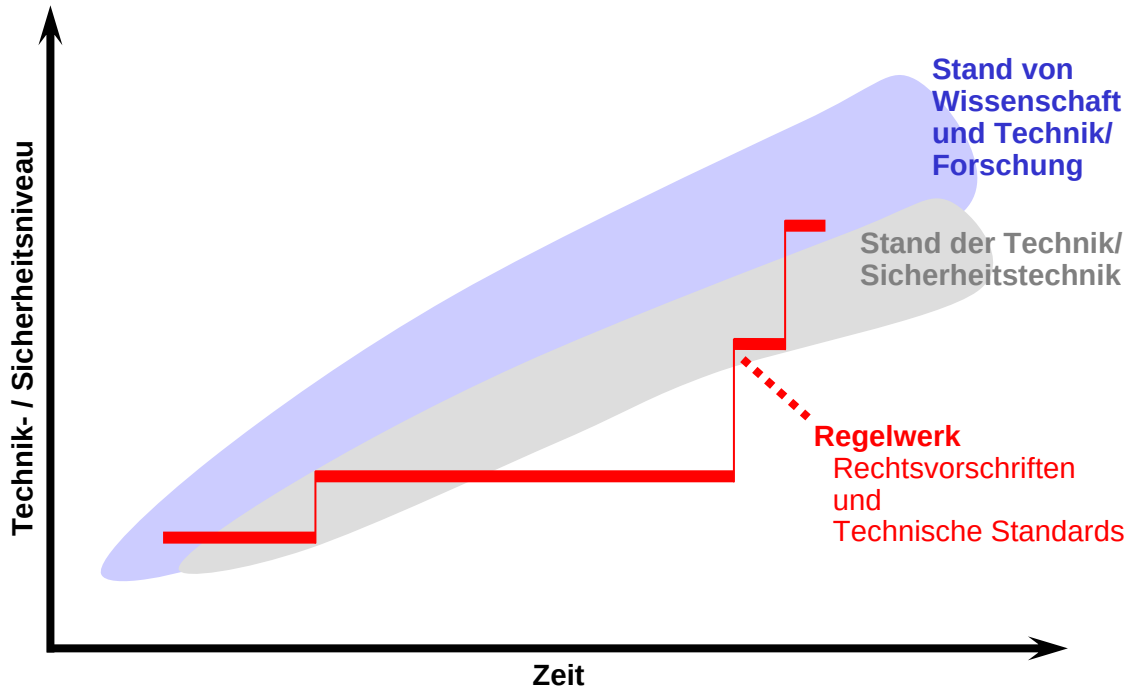


Abbildung 2: Stand der Technik – Regelwerk

3.5.4 Methodik zur Ermittlung von Grenzen der Sicherheit

Die Verlagerung von Grenzwerten für großtechnische Anlagen in untergesetzliche Regelwerke bringt verschiedene Probleme mit sich. Einmal stellt sich die Frage nach der Legitimation der Gremienarbeit, nach deren Besetzung sowie dem Verfahren für gewonnene Erkenntnisse. Weiter ist das gesamte Regelwerk auf Grund der Vielzahl solcher Gremien und Regelungen häufig unübersichtlich, weist Überlappungen und in manchen Fällen sogar Widersprüche auf, ist in Aufbau, Systematik und Wortlaut uneinheitlich und erschwert dem Rechtsanwender damit die Orientierung. Dies ist gerade in einem Bereich gefährlich, wo es um hohe Investitionen einerseits und beträchtliche Risiken für mögliche Drittbetroffene einschließlich der Klagelast andererseits geht.

Ein zusätzliches Problem erwächst aus der Vermischung objektiver Erkenntnisse der Forschung nach Wahrheit und ihrer Bewertung. Die vorstehend angesprochenen Gremien sind regelmäßig für den Erkenntnisprozess und daraus abzuleitende Konsequenzen kompetent und legitimiert, nicht aber für die gesellschaftspolitische Bewertung von Risiken (siehe Abschnitt 3.3).

Die sicherheitstechnische Machbarkeit in ihrer Schrittfolge und Abwicklung durchläuft mehr oder minder deutlich die Phasen des Produkt-Lebensyklus wie im Abschnitt 1.5 ausgeführt (siehe auch Abbildung 2). Dieses Phasenkonzept erleichtert nicht nur das technische Management, sondern sichert in besonderem Maße auch die notwendigen organisatorischen Maßnahmen und führt letztlich zum Risiko-Management.

Dem **Planungsprozess** werden im Produkt-Lebenszyklus die folgenden beiden Phasen zugeordnet:

- Konzeptionsphase
- Definitionsphase

Dem **Realisierungsprozess** werden diese beiden Phasen des Produkt-Lebenszyklus zugeordnet:

- Entwicklungs- und Konstruktionsphase
- Herstellungsphase

Der **Betriebsprozess** umfasst schließlich diese beiden Phasen:

- Betriebs- und Nutzungsphase
- Rückbau-, Entsorgungs- und Recyclingphase

Wenn zur Verschärfung von Grenzwerten in Sachen Sicherheit und Umweltschutz der Erlass neuer Gesetze und strengerer Verordnungen gefordert wird, wird in vielen Staaten der Welt der Beifall nicht ausbleiben. In der Realität werden schon wegen der Dauer der legislativen Verfahren und infolge von Übergangsfristen spürbare Verbesserungen höchstens mittel- bis langfristig erzielt. Gänzlich unbeachtet bleibt dabei der Effekt, dass jede zusätzliche Komplizierung der ohnehin schon unübersichtlichen Gesetzes- und Regelwerke das Risiko erhöht, dass die Rechtsanwendung infolge Überforderung und Nichtwissen beeinträchtigt wird. Zu bevorzugen wäre, die heute geltenden Gesetze und Verordnungen zu Sicherheit und Umweltschutz in wesentlich größerem Ausmaß durchschaubar zu machen; allein damit ließe sich der Standard an Sicherheit und Umweltschutz deutlich erhöhen, ohne dass ein neues Gesetz erlassen werden müsste.

Die Reduzierung der Komplexität technischer Einrichtungen, der Ungewissheiten und Risiken wird stetig in technischen, ökonomischen oder ökologischen Problemfällen angestrebt. Hierbei sind Kompromisse schon deshalb unausweichlich, weil die Mittel zur Realisation begrenzt und die verfügbaren Informationen unvollkommen sind. Ein Kompromiss kann seinem Wesen nach kein Optimum, sondern nur das unter gegebenen Umständen noch Machbare darstellen und deshalb keinen absoluten Wahrheitsgehalt beanspruchen.

Die Minimierung von Risiken muss sozialverträglich erfolgen; dabei ist ständig zwischen individuellem und gesellschaftlichem Nutzen abzuwägen. Hier sind Kompromisse unumgänglich, die jedoch ethisch begründbar sind. Man kann feststellen, dass die Bestimmung der Grenzen der Sicherheit im Rahmen der sicherheitstechnischen Machbarkeit auf Verantwortung, Akzeptanz, Kompromissen, dem Maßstab der praktischen Vernunft, der politischen Durchsetzbarkeit und letztendlich auf ethischen Normen beruht. Die Festlegung der Technischen Sicherheit benötigt Praktikabilität, Kostenbewusstsein und ist dem Fortschritt in Forschung und Entwicklung verpflichtet. Sie wird vom Stand des Wissens und von der gesellschaftlichen Akzeptanz bestimmt.

4 Überprüfbarkeit der Sicherheit

Sicherheit ist nur insoweit zu gewährleisten, wie sie auch überprüfbar ist. Es wird gezeigt, wodurch der Überprüfbarkeit Grenzen gesetzt werden, welche methodischen Ansätze zu ihrer Verbesserung bestehen und welche Instrumente sich für die verschiedenen Phasen im Lebenszyklus eines technischen Produkts oder Systems für die Überprüfung der Technischen Sicherheit bewährt haben.

4.1 Grenzen der Überprüfbarkeit

4.1.1 Erkenntnisstand

Der Erkenntnisstand wird in den verschiedenen Kategorien festgelegt, die im deutschen Rechtssystem Anwendung finden können. Technische Produkte dürfen nur verwendet werden, wenn die aus ihnen hergestellten technischen Einrichtungen (Systeme, Anlagen, Produkte) bei ordnungsgemäßer Instandhaltung während einer zweckentsprechenden, angemessenen Dauer das Schutzziel aller einschlägigen Rechtsvorschriften erfüllen. Diese Klassifizierung ist nach dem Grad der Verbindlichkeit strukturiert: in allgemein anerkannte Regeln der Technik, in Stand der Technik und in Stand von Wissenschaft und Technik (siehe Abschnitt 3.5):

- Die „Allgemein anerkannten Regeln der Technik" entstehen durch Konsens der Fachleute, sind in aller Regel kodifiziert und werden verbindlich angewendet. Eine Norm kann eine allgemein anerkannte Regel der Technik sein, sie muss es aber nicht.
- Der „Stand der Technik" berücksichtigt den dynamischen Zustand der Auswertung von Erfahrungen und Erkenntnissen. Er beschreibt technische Möglichkeiten zu einem bestimmten Zeitpunkt und definiert auch ihre wirtschaftlichen Randbedingungen.
- Der „Stand von Wissenschaft und Technik" ist ein Zustand, der nicht als Allgemeingut angesehen werden kann. Er stellt Ergebnisse aus Forschung und Entwicklung für die Anwendung zur Diskussion. Dem Anwender nutzt unter Umständen ein Stand von Wissenschaft und Technik zur Erfüllung der Anforderungen, um ein verbleibendes Risiko möglichst klein zu halten.

4.1.2 Verantwortung

4.1.2.1 Arten der Verantwortung

Technische Prozesse, insbesondere die Überprüfung ihrer Sicherheit, finden unter der Verantwortung von Menschen statt. Die Verantwortung für die Überprüfung der Sicherheit kann vom Einzelnen wahrgenommen werden, wenn sie für ihn überschaubar ist. Häufig treten aber in der Technik komplexere Formen von Verantwortung auf. Für die Wahrnehmung dieser Verantwortung haben Institutionen oder Korporationen gegenüber ihren Kunden, ihren Mitgliedern, Anteilseignern oder der Gesellschaft eine spezifische Aufgabe zu leisten.

Die Verantwortung des Einzelnen ergibt sich zum einen aus seiner Rollenverantwortung, als Pflicht zur optimalen Erfüllung der aufgetragenen Aufgaben. So ist jeder zuerst für das Ergebnis und die direkten Folgen des eigenen Handelns verantwortlich. Hierzu zählen auch die Ergebnisse und Folgen durch unterlassene Handlungen. Ein Spezialfall der Rollenverantwortung ist die Präventionsverantwortung, die einen Prüfingenieur beispielsweise verpflichtet, systematisch nach Schwachstellen einer Anlage zu suchen und so vorsorgend Unfälle und Störungen zu verhindern. Zum Zweiten trägt jeder außerhalb der ihm aufgetragenen Verpflichtung die ganz allgemeine Verpflichtung, die Grundrechte, wie etwa das Recht auf Leben, das Recht auf Privateigentum usw. zu achten und einzuhalten.

Institutionen können als juristische Personen selbst keine Verantwortung tragen; sie wird von handelnden Personen übernommen. Deshalb muss die Verantwortung den jeweils handelnden Personen übertragen werden, die diese Institutionen vertreten. Die Komplexität der Aufgaben erfordert daher eine klare Aufteilung der Gesamtverantwortung in Bereiche, deren Umfang an den Möglichkeiten der Einzelpersonen auszurichten ist.

4.1.2.2 Konflikt zwischen wirtschaftlichen Zwängen und technischer Notwendigkeit

Ein häufiger Konfliktfall besteht zwischen der Verantwortung der Institution für die eingesetzten Mittel und der allgemeinen Verantwortung für die Sicherheit. Ausgangspunkt ist die Überlegung, dass die Menge und Qualität von Waren und

Dienstleistungen offensichtlich besser durch die Regelungsmechanismen des Marktes gesteuert werden als durch staatliche Steuerung. Durch das inhärente Konkurrenzprinzip werden Optimierungsprozesse gefördert, ohne deren Umsetzung eine Verdrängung vom Markt erfolgt. Die regulierende Wirkung des Marktes sorgt bei üblichen Waren und Dienstleistungen für ein Gleichgewicht zwischen der Menge und Qualität eines Produktes und der Kundenzufriedenheit. Solange der Kunde in der Lage ist, die Qualität einzuschätzen, zu prüfen oder zu erfahren, kann er in den Markt eingreifen.

Bei einer Störung des Marktes durch externe Effekte (Umwelteinflüsse) oder ungleiche Wissensverteilung der Marktteilnehmer muss aber der Staat in den freien Markt eingreifen, indem er Sollvorgaben an die Beschaffenheit von Produkten festlegt. Dadurch werden (nicht immer) höhere Qualitäten festgeschrieben, als sie sich im freien Spiel des Marktes ergeben würden. Der Staat trifft damit Vorsorge im Interesse der Allgemeinheit. Er setzt für die Technische Sicherheit das Verfassungsgebot der körperlichen Unversehrtheit durch. Nebenbei wehrt er hohe Folgekosten für die öffentliche Hand ab, die im Fall der Nichtregulierung zu erwarten wären.

Für den Bereich der öffentlich-technischen Sicherheit lässt sich das Marktprinzip aus einer Reihe von Gründen nur eingeschränkt anwenden. Dazu sind die hier interessierenden Hauptfaktoren im Einzelnen von fachkundiger Seite zu prüfen, ehe ein technisches Produkt auf den Markt gebracht wird.

Im Bereich der Waren hat nur eine beschränkte Menge ausschließliche Sicherheitsfunktion (z.B. Feuerlöscher, Sicherheitsventile, Sicherheitsgurte). Deren Eigenschaften kann der Käufer nicht immer einschätzen. Bedeutsam ist, wie häufig und in welchen Situationen die betreffenden Produkte ihre Funktion beweisen müssen: im Routineeinsatz, im normalen Einsatz einschließlich üblicher Zwischenfälle, in Unfallsituationen oder im Katastrophenfall.

Die Qualität eines Feuerlöschers, der im Idealfall nie benutzt werden muss, kann vom Kunden nicht bewertet werden. Wenn sich aber die Qualität eines sicherheitsrelevanten Produkts nicht einschätzen lässt, geht der regulierende Einfluss auf den Markt verloren. Untaugliche Produkte drohen sich am Markt zu halten oder bei Preisvorteilen gar den Markt zu dominieren.

Wesentlich häufiger haben Waren neben ihrer Gebrauchseigenschaft auch eine Sicherheitsfunktion (z.B. Prozess-/Transportbehälter, Pipeline, Kfz-Bremse). In diesen Fällen wird das Verkaufsinteresse durch die Sicherheitsfunktion überlagert. Gehen Verkaufs- und öffentliches Sicherheitsinteresse in die gleiche Richtung, unterstützt der Markt die Durchsetzung sicherer Waren.

Wie die Erfahrung zeigt, versagt dieses Prinzip allerdings im Fall geteilter oder unklarer Verantwortlichkeiten. Negative Kundenerfahrungen schlagen dann nicht auf den Hersteller der Ware durch. Typischerweise treten Sicherheitsdefizite auch dann auf, wenn der wirtschaftliche Nutzen eines Produktes / einer Dienstleistung gegenüber Pflichten / Auflagen abnimmt. Gefahrguttransporte mit hochwertigen Waren sind sicher anders zu regulieren als Abfalltransporte.

4.1.2.3 Prioritäten für die Entscheidung von Verantwortungskonflikten

Es kann ein Optimum zwischen wirtschaftlichem Aufwand und erreichter Sicherheit geben, das allerdings unter dem moralischen Vorbehalt der ausreichenden Sicherheit stehen muss. Für die Entscheidung von Verantwortungs- und Rollenkonflikten ergeben sich nach H. Lenk und M. Maring folgende Prioritäten („Technik zwischen Können und Sollen – Wer verantwortet die Technik?", in TÜV Saarland Foundation [Hrsg.], Congress-Documentation Saarbrücken 2001: World Congress on Safety of Modern Technical Systems, [pp. 725-738], Köln: TÜV Verlag):

(1) „Moralische Rechte jedes betroffenen Individuums abwägen" (siehe Abschnitt 1.6).

(2) „Kompromiss suchen, der jeden gleich berücksichtigt", im Falle eines unlösbaren Konflikts „zwischen gleichwertigen Grundrechten".

(3) „Erst nach Abwägung der moralischen Rechte jeder Partei darf und sollte man für die Lösung votieren, die den geringsten Schaden für alle Parteien mit sich bringt.

(4) Erst nach Anwendung von (1) bis (3) Nutzen gegen Schaden abwägen.

(5) Bei praktisch unlösbaren Konflikten zwischen den beteiligten Parteien sollte man hinsichtlich Schädigungen und Nutzen für die verschiedenen Parteien faire Kompromisse suchen („faire Kompromisse" sind beispielsweise annähernd gleich verteilte oder gerechtfertigt proportionierte Lasten- bzw. Nutzenverteilung).

(6) Universalmoralische Verantwortung geht in der Regel vor Aufgaben- bzw. Rollenverantwortung.

(7) Das öffentliche Wohl, das Gemeinwohl soll allen anderen spezifischen und partikularen nichtmoralischen Interessen vorangehen.

(8) Auch in technischen Regelwerken sind Prioritätsprinzipien formuliert. Nach DIN VDE 31000-2 „Allgemeine Leitsätze für das sicherheitsgerechte Gestalten technischer Erzeugnisse – Begriffe der Sicherheitstechnik – Grundbegriffe" lässt sich beispielsweise folgende Regel aufstellen: „Bei der sicherheitsgerechten Gestaltung ist derjenigen Lösung der Vorzug zu geben, durch die das Schutzziel technisch sinnvoll und wirtschaftlich am besten erreicht wird. Im Zweifel sollte zunächst davon ausgegangen werden, dass sicherheitstechnische Erfordernisse Vorrang haben vor wirtschaftlichen Überlegungen." Andererseits hat sich insbesondere in der zivilen Luftfahrttechnik gezeigt, dass in der Regel auch solche sicherheitstechnischen Lösungen möglich sind, die nicht zwangsläufig im Zielkonflikt mit wirtschaftlichen Lösungen stehen müssen.

(9) Bei „Dringlichkeit" geht ökologische Verträglichkeit vor ökonomischer Nutzanwendung.

(10) Konkrete Humanität geht vor abstrakten Forderungen und universalen Prinzipien (konkret human- und sozialverträgliche Güterabwägung).

4.2 Lernen als kontinuierliche Aufgabe

Störungen oder Unfälle, auch Beinaheunfälle (einschließlich der Abweichungen vom bestimmungsgemäßen Betrieb), sind unbeabsichtigte, unerwartete Systemzustände. Da sie unerwartet sind, besteht auch keine Möglichkeit ihrer Prüfbarkeit. In vielen Ereignisanalysen konnte gezeigt werden, dass die Handlung des Operators zwar die Störung ausgelöst haben mag, allein zur „Erklärung" aber

nicht ausreicht. Raumzeitlich weit vor die auslösende Einzelhandlung gelagert sind häufig Design-, Konstruktions-, Wartungs- und Managementfehler, die ebenfalls als notwendige Voraussetzungen anzusehen sind. Diese Fehler müssen vermieden bzw. durch systematischen Erfahrungsrückfluss ausgeräumt werden. Grundsätzlich bieten sich für diese Zielsetzung drei Strategien an:

4.2.1 Feed forward-Kontrolle von Sicherheit und Zuverlässigkeit

Probabilistische Ansätze der Risikoabschätzung, die auch Personalhandlungen im Sinne einer Human Reliability Analysis (HRA) berücksichtigen, werden in diversen Industriezweigen (u.a. Kernindustrie, zivile Luftfahrt und Bautechnik seit langem gezielt angewendet. Allerdings lassen diese Verfahren zu wünschen übrig. Zwar sind die notwendigen statistischen Daten über Ausfälle technischer Komponenten vergleichsweise gut. Dies gilt aber nicht für die zugrunde gelegten statistischen Informationen und die Qualität der gewählten Modellvorstellungen zu menschlichem Handeln. Man muss berücksichtigen, dass diese Verfahren lediglich Teilaussagen zulassen und damit gewisse Schwächen aufweisen. Es fehlen die statistisch gesicherten Datenbasen, daher arbeiten diese Verfahren weitgehend mit Experteneinschätzungen („informed guesses"). Aber das muss die Möglichkeiten probabilistischer Verfahren nicht schmälern. Diese Methoden sind zur Hypothesengewinnung und zur Sensitivierung des Bewusstseins für Human Factors-Aspekte (HF) beim Entwurf und der Konstruktion der Anlagen nützlich und sollten weiter entwickelt werden. Für eine belastbare Sicherheitsaussage reichen sie allein angewandt jedoch nicht aus.

4.2.2 Feed back-Kontrolle von Sicherheit und Zuverlässigkeit

Menschen lernen aus Erfahrung, hauptsächlich aus Fehlern; Organisationen lernen aus Ereignissen einschließlich Beinahe-Ereignissen, die systematisch analysiert werden müssen. Unmittelbar bezogen auf die systematische Ursachenanalyse muss ein ereignisbezogenes Berichtswesen eingesetzt werden. Die wenigsten Industrien hohen Gefährdungspotenzials haben ein effizientes Berichtssystem über Stör- und Unfälle. Dort, wo Aufsichtbehörden ein solches System vorschreiben und anhand von Kriterien der Berichtspflicht durchsetzen, wird dies oft als lästig empfunden. Noch seltener werden Ereignisberichte unterhalb einer vorgegebenen Berichtsschwelle erfasst, dokumentiert und analy-

siert, obwohl gerade diese ein besonders instruktives Lernen ermöglichen dürften. Es sollte überlegt werden, wie derartige Berichtssysteme unter- und oberhalb der Berichtspflicht zu konzipieren und zu implementieren sind, um das geboten erscheinende Maximum an Erkenntnisgewinn zu ermöglichen. Dazu bedarf es einer Neuausrichtung der Fehlerkultur in Deutschland, die letztlich darin gipfelt, den erstmalig auftretenden Fehler zu kommunizieren und nur seine Wiederholung zu ahnden.

4.2.3 System organisationalen Lernens

Der Lernprozess muss im Sinne eines organisationalen Lernens institutionalisiert sein. Beide Formen der Kontrolle von Sicherheit („feed forward" und „feed back") können – in einen systematischen Zusammenhang gebracht – einander befruchten. Ein solcher Zusammenhang muss durch den Aufbau von Analyse- und Berichtsdatenbanken hergestellt werden. Dabei sind zu berücksichtigen:

- einheitliche Kategoriensysteme
- periodische Analysen über mehrere Ereignisse
- die Ableitung entsprechender Präventionskonzepte sowie
- eine zeitnahe sichergestellte Rückkoppelung von Ergebnissen an Betroffene

4.2.4 Ermittlung des Standes der Technik als Lernschema

Die Ermittlung des Standes der Technik ist oft Voraussetzung für gesetzeskonformes Handeln. Auf Grund dieser herausragenden Bedeutung wurden verschiedene Versuche unternommen, diesen (Lern-) Prozess zur Ermittlung der Anforderungen zu systematisieren. Er beginnt mit der Festlegung, wofür, wozu und durch wen der Stand der Technik ermittelt werden soll. Darunter ist im Einzelfall folgendes zu verstehen:

- Wofür (für welches Objekt):
  Es kann sich um einen bestimmten Anlagentyp, eine konkrete Anlage, eine Teilanlage oder ein sicherheitstechnisch bedeutsames Anlagenteil handeln.

- Wozu (für welchen Zweck/aus welcher Veranlassung):
  Hier wird nach Anlass (Zusammenhang, Hintergrund) gefragt, z.B. die Durchführung eines Genehmigungsverfahrens für eine Neuanlage, eine Änderung (Erweiterung, Kapazitätserhöhung, Schadstoffreduzierung, …) oder eine Nachrüstung einer bestehenden Anlage.
- Durch wen (Person/Einrichtung):
  Hier ist anzugeben, um welche Art Betrieb es sich handelt (z. B. Klein- und mittelständisches Unternehmen oder Großbetrieb), welche innerbetrieblichen Organisationseinheiten und Externen beteiligt sind, insbesondere bei wem die Federführung angesiedelt ist.

Um zu beurteilen, ob eine Anlage dem Stand der Technik entspricht, können folgende Erkenntnisse herangezogen werden:

- Vergleichbare Verfahren, Einrichtungen und Betriebsweisen,
- Kombination oder Verknüpfung unterschiedlicher Sicherheitsmaßnahmen,
- Sicherheitsvorkehrungen in anderen Anlagenarten, die hinsichtlich ihrer Technologie und der eingesetzten Stoffe mit der betrachteten Anlage vergleichbar sind.

Die Wahrnehmung der Sicherheitspflicht sollte in drei Stufen erfolgen. Die Schritte verdeutlichen, dass bestimmte sicherheitstechnische Maßnahmen bei der Ermittlung des Standes der Technik herangezogen werden können, ohne dass daraus bereits eine Verpflichtung abzuleiten wäre. Die bestimmten Maßnahmen müssen nicht in der zu beurteilenden Anlage realisiert werden, da es nur auf die Entsprechung mit der Vergleichsgröße ankommt.

- Auf der ersten Stufe ist für eine bestimmte sicherheitstechnische Aufgabenstellung der Stand der Technik zu ermitteln (z.B. im Rahmen einer Pilot- oder Demonstrationsanlage), um als Vergleichsgröße für die konkret zu beurteilende Anlage zu dienen.
- Auf der zweiten Stufe erfolgt die wertende Betrachtung, ob die konkrete Anlage dem ermittelten Stand der Technik entspricht. Es wird überprüft, ob mit den vorgesehenen Maßnahmen an der konkreten Anlage die Schutzziele erreicht werden (Entsprechungsprüfung).

- Auf der dritten Stufe wird – ausgehend von den Ergebnissen der oben genannten Stufen – über das Genehmigungs- oder Aufsichtsverfahren entschieden (Rechtsfolge).

4.2.4.1 Bedingungen für den Ermittlungsprozess

Bei der Ermittlung des Standes der Technik ist zu berücksichtigen, was sich bei anderen vergleichbaren Anlagen im Betrieb oder Probebetrieb bewährt hat oder was der allgemeine technische Entwicklungsstand als praktisch geeignet erscheinen lässt. Trifft keine dieser drei Kriterien zu, ist ein Ermittlungsprozess einzuleiten. Dabei müssen folgende fünf Bedingungen erfüllt werden:

- Alle Schritte des Ermittlungsprozesses müssen durchlaufen werden, gegebenenfalls einzelne Schritte mehrfach (Iterationsschleifen),
- die beteiligten Personen müssen geeignet sein,
- die herangezogenen Erkenntnisquellen müssen die Thematik erschöpfend abdecken,
- die angewandten Methoden/Untersuchungen müssen geeignet und ausreichend sein,
- die Entscheidungen müssen dem rechtlichen Maßstab des Standes der Technik entsprechen.

Die Einhaltung des Standes der Technik ist eine Pflicht der Anlagen-Betreiber. Wird die Pflicht nicht erfüllt bzw. der Pflicht nicht nachgekommen, kann dies erhebliche Konsequenzen haben. Deshalb ist es erforderlich, den Ermittlungsprozess methodisch, nachvollziehbar zu gestalten und mit Sorgfalt durchzuführen.

In bestimmten Fällen ist es möglich, den Stand der Technik für eine Anlage auf der Basis technischer Regeln, Verwaltungsvorschriften oder Leitfäden festzustellen. Diese Fälle können gegeben sein, wenn Anlagengrenzen, vorhandene Stoffe und Betriebszweck der in einer technischen Regel usw. beschriebenen Anlage weitgehend entsprechen. Die herangezogenen Regeln, Leitfäden oder Verwaltungsvorschriften müssen aktuell und die notwendigen Sicherheitsmaßnahmen ausreichend beschrieben sein. Besondere anlagenbezogene oder umweltbedingte Gefahrenquellen sind auszuschließen.

Im Allgemeinen wird sich der Stand der Technik auf der Grundlage der Technischen Regeln und dem Ergebnis des Diskurses der Fachleute ergeben.

4.2.4.2 Schritte des Ermittlungsprozesses

Für die Ermittlung des Standes der Technik sollten folgende sieben Prozessschritte durchlaufen werden (gemäß der ersten Stufe in Abschnitt 4.2.4):

(1) Definition der Aufgabenstellung,
(2) Erfassen der sicherheitsrelevanten Unterlagen und Daten der Anlage/des Verfahrens,
(3) Ermitteln der sicherheitsrelevanten Bereiche (Verfahrensschritte und Anlagenteile),
(4) Analysieren der möglichen Gefahrenquellen,
(5) Bestimmen und auswählen der Erkenntnisquellen,
(6) Auswerten der gesammelten Erkenntnisquellen,
(7) Entscheidung finden,

wobei die Reihenfolge der Prozessschritte (2) bis (6) je nach Anwendungsfall variieren kann.

Die Prozessschritte sollten in Iterationsschleifen durchlaufen werden, bis eine ausreichende Gewissheit über den Stand der Technik vorliegt. Die Iterationsschleifen können einzelne oder mehrere Prozessschritte umfassen.

Die Ermittlung des Standes der Technik ist nur als ein Schritt beim Erarbeiten einer sicherheitstechnischen Betrachtung zu sehen. Hieran schließen sich noch an:

- Umsetzung des Standes der Technik bezogen auf die Aufgabenstellung
- Dokumentation dieser Umsetzung
- Untersuchung und Beschreibung der verbleibenden Risiken
- Notfallplanung

4.2.4.3 Entscheidungsfindung

In der Regel werden sich verschiedene Möglichkeiten ergeben, wie der Stand der Technik in einer konkreten Anlage umgesetzt werden kann. Die schließlich gewählte Gestaltungsmöglichkeit muss begründet und nachvollziehbar erklärt werden.

Per Definition müssen Verfahren, Einrichtungen und Betriebsweisen

- sich im Betrieb bewährt haben,
- mit Erfolg erprobt worden sein oder
- den Nachweis ihrer praktischen Eignung erbracht haben,

damit sie dem Stand der Technik entsprechen können. Weiter müssen die Verfahren, Einrichtungen und Betriebsweisen dem fortgeschrittenen Entwicklungsstand entsprechen. Dabei ist eine sorgfältige Abwägung von Wirksamkeit und Zuverlässigkeit einer Maßnahme in Bezug auf die konkrete Gefahrenquelle eine Grundvoraussetzung, um Fehler zu vermeiden, die die Wahrscheinlichkeit von Störfällen erhöhen können.

4.3 Controlling der Technischen Sicherheit im Produkt-Lebenszyklus

Aus dem Qualitätsmanagement ist bekannt, dass der Aufwand für die Beseitigung eines Fehlers umso größer ist, je später er im Planungs- bzw. Produktionsprozess entdeckt wird. Dies lässt sich sicher auch auf die sicherheitsrelevanten Fehler übertragen. Um kostenoptimal zu sein, muss man deshalb fordern, die sicherheitstechnische Betrachtung schon von der ersten Phase der Entwicklung an mitzuführen. Diese Beurteilungsfunktion kann in das Entwicklungsteam integriert werden oder aber jeweils beim Erreichen von Meilensteinen als externe Kontrolle, etwa durch eine zentrale Abteilung (Sicherheit / Qualität) und gegebenenfalls durch Dritte erfolgen.

Die erhobenen sicherheitstechnischen Informationen und getroffenen Entscheidungen sollten für Soll-Ist-Vergleiche im Sinne eines Controllings der Technischen Sicherheit in den folgenden Phasen des Produkt-Lebenszyklus ständig verfügbar gehalten werden. Es bietet sich an, diese Controllinginformationen für

den kontinuierlichen Aufbau des „Safety Case” in einer Hierarchie mit Sicherheitszielen zu strukturieren.

4.3.1 Phasenbezogene Verfolgung der Technischen Sicherheit

Für das gesamte Objekt (System, Anlage, Produkt) ist in interdisziplinärer Zusammenarbeit eine umfassende Gefahrenanalyse durchzuführen (siehe Abschnitte 2.1 und 2.2). Zu berücksichtigen sind dabei anlagenbezogene und umweltbedingte Gefahrenquellen, einschließlich naturbedingter Zustände, Ereignisse und Eingriffe Unbefugter.

Die Gefahren und deren Ursachen sollten unter Anwendung einer anerkannten, bewährten Prüfmethode analysiert werden. So lässt sich ein ausreichendes Maß an Gründlichkeit und Prüftiefe sicherstellen. Das zu untersuchende Objekt ist dazu in überschaubare Bereiche einzugrenzen.

Die Abbruchkriterien bei der Gefahrenanalyse sollten aufgezeigt werden. Abbruchkriterien können beispielsweise Prüftiefe, Ausschluss von bestimmten einzelnen Gefahrenquellen, Stoffmerkmale und Prozesskenngrößen betreffen.

Als Arbeitsgrundlage dienen die erfassten Unterlagen und Daten sowie Informationen aus Anlagen- und Ortsbegehungen. Deckt die Gefahrenanalyse eine oder mehrere Gefahrenquellen auf, so ist zu ermitteln, welche Maßnahmen nach dem Stand der Technik zu treffen sind. Davon unabhängig sind die möglichen Folgen dennoch denkbarer Störungen zu ermitteln, hinsichtlich ihres Risikos zu bewerten und Schutzmaßnahmen zu ergreifen.

4.3.2 Organisation der Nachweisführung

Bei der Organisation der Nachweisführung ist zu unterscheiden zwischen Eigen- und Fremdprüfungen. Die Fremdprüfungen können privatrechtlich organisiert sein oder von Staats wegen auf rechtlichen Grundlagen durchgeführt werden (staatliche bzw. vom Staat beliehene Stellen).

Nur durch Koordination einer mit hinreichenden Befugnissen ausgestatteten Stelle ist zu erreichen, dass Prüfmaßnahmen sich sinnvoll ergänzen, sowie unbeabsichtigte Lücken in der Nachweisführung vermieden und die notwendigen In-

formationen weitergegeben werden. Bedeutsam für die Beurteilung von Prüfmaßnahmen ist neben ihrer unmittelbaren Aufgabe, ungünstige Abweichungen aufzuzeigen, auch ihre mittelbare Wirkung, auf Leistung bzw. Qualität positiv oder negativ Einfluss zu nehmen.

4.3.2.1 Elemente der Nachweisführung

Im Hinblick auf Art und Umfang der Nachweisführung kann unterschieden werden zwischen

- Herstellerprüfungen, die entweder ausschließlich betriebsintern oder betriebsextern geregelt sind,
- Fremdprüfungen durch einen unabhängigen Dritten, die entweder unabhängig von der Herstellerprüfung erfolgen oder sich ausschließlich auf die Überprüfung einer ordnungsgemäßen Herstellerprüfung beziehen.
- Abnahmeprüfungen von Seiten des (abnehmenden) Auftraggebers, die der Beurteilung und dem Nachweis der Qualität einer Ware oder einer Leistung bei Übergang von Verantwortung oder Eigentum dienen.

Herstellerprüfungen werden grundsätzlich büro- oder betriebsintern durchgeführt. Sie können – je nach Bedeutung der Nachweisführung – in Form einer Selbstprüfung oder durch Personen erfolgen, die nicht unmittelbar am Herstellungsvorgang beteiligt sind.

Die büro- oder betriebsintern geregelten Herstellerprüfungen liegen – wie auch besondere Maßnahmen zur Herstellungssteuerung – in alleiniger Zuständigkeit des Herstellers.

Die Planung der Nachweisführung beinhaltet die eindeutige Festlegung von Regeln für die Beurteilung sowie korrektiven bzw. präventiven Maßnahmen bei negativen Prüfergebnissen. Die Bedeutung der einzelnen Elemente der Nachweisführung erfordert eine Dokumentation.

4.3.2.2 Abstufung der Nachweisführung

Die Wirksamkeit von Prüfmaßnahmen wird durch folgende Faktoren bedingt:

- dem Grad der Unabhängigkeit der Prüfung vom betroffenen Vorgang
- der Qualifikation des Prüfpersonals
- der Intensität der Kontrolle (Häufigkeit und Umfang von Prüfungen)
- den Beurteilungskriterien und Maßnahmen bei negativen Prüfergebnissen
- dem Einsatz mehrfacher unabhängiger Prüfungen

Mit Blick auf diese Zusammenhänge lassen sich Qualitätssicherungsstufen und ihre Zuordnung zu den Gefährdungsklassen festlegen. Einzelne Leistungen können unterschiedlichen Qualitätssicherungsstufen unterliegen.

4.3.3 Modulkonzept der Europäischen Union

Es besteht ein starker Druck, bisher vom Staat wahrgenommene Prüf- und Überwachungsfunktionen zu privatisieren. Dies wird oft mit Potenzialen zur Effizienzsteigerung oder der gestiegenen Eigenverantwortung der Hersteller begründet. Ein weiterer Grund liegt im europäischen Integrationsprozess: Die EU-Mitgliedsstaaten sind davon ausgegangen, dass durch ein privatwirtschaftliches Zulassungsregime der Abbau von Handelsbarrieren im Binnenmarkt schneller gelingt. Insbesondere Anfang der 90-er Jahre haben diese Tendenzen zur Risikoverlagerung (in Verbindung mit einer Abwälzung der Verantwortung) auf die private Wirtschaft zu einer wahren Explosion von formalen Qualitätsmanagementsystemen und den zugehörigen Auditierungen geführt. Aufwand und Nutzen von Qualitätsmanagementsystemen und ihren Audits sind daher zu einem zentralen Diskussionspunkt bei der Überprüfung der Technischen Sicherheit geworden.

Das Neue Konzept [1] und das Gesamtkonzept der Europäischen Union für die Konformitätsbewertung [2] – inklusive der anschließenden Modulbeschlüsse [3] –

---

1 Entschließung des Rates 90/C10/010 vom 07.05.85 über eine neue Konzeption [New Approach] auf dem Gebiet der technischen Harmonisierung und der Normung, *Amtsblatt der Europäischen Gemeinschaft Nr. C 136 vom 04.06.85, Seiten 0001 – 0009*

2 Entschließung des Rates 90/C10/01 vom 21.12.89 zu einem Gesamtkonzept [Global Approach] für die Konformitätsbewertung, *Amtsblatt der Europäischen Gemeinschaft Nr. C 010 vom 16.01.90, Seiten 0001 – 0002*

3 Beschluss des Rates 90/683/EWG vom 13.12.90 über die in den technischen Harmonisierungsrichtlinien zu verwendenden Module für die verschiedenen Phasen der Konformitätsbewertungsverfahren, *Amtsblatt der Europäischen Gemeinschaft Nr. L 380 vom 31.12.90, Seite 001*, und Beschluss des Rates 93/465/EWG vom 22.07.93 über die in den technischen Harmonisierungsrichtlinien zu verwendenden Module für die verschiedenen Phasen der Konformitätsbewertungsverfahren und die Regeln für die Anbringung und Verwendung der CE-Konformitätskennzeichnung, *Amtsblatt der Europäischen Gemeinschaft Nr. L 220 vom 30.08.93 Seiten 0023 – 0039*

stellen das Paradebeispiel für die Privatisierung und die Abstufung von Kontrollverfahren im Technischen Sicherheitsrecht dar. Durch das Gesamtkonzept und die Modulbeschlüsse der EU werden Kontrollverfahren zur Verwendung in den Gesetzesvorhaben der EU für den freien Warenverkehr beschrieben. Die Module stellen ein abgestuftes System dar, das von der Herstellerselbsterklärung (Modul A) bis zur Einzelabnahme des Produkts durch einen unabhängigen Dritten (Modul G) und die umfassende Qualitätssicherung (Modul H) reicht. Die EU-Richtlinien und das abgeleitete nationale Recht enthalten eine Auswahl der Module, die das Risiko des regulierten Produkts berücksichtigen. Um sein Produkt für den EU-Binnenmarkt zu qualifizieren, kann der Hersteller einen dieser Module auswählen, der seinen Produktionsbedürfnissen am besten entspricht, sofern eine produktspezifische Richtlinie ihn nicht anderweitig festlegt.

Mit der Schaffung des EU-Binnenmarktes werden die bisherigen Grenzen innerstaatlicher Sicherheitsstrukturen an die Grenzen Europas verlagert. Bei weltweiten Aktivitäten müssen die unterschiedlichen Sicherheitsstrukturen miteinander abgeglichen werden (Kompatibilitätsklauseln bzw. Abgleich).

Hatte sich die Bundesrepublik Deutschland bisher noch deutlich an der Risikominderung aktiv beteiligt, indem staatliche – oder staatlich beliehene – Stellen in hoheitlicher Funktion sicherheitstechnische Nachweisführungen durchführten bzw. daran mitwirkten (Durchführungsverantwortung des Staates), so sehen die einschlägigen Richtlinien der Europäischen Union (EU) vor, dass auch diese hoheitlichen Nachweisführungen dem freien Markt überlassen bleiben und vom Staat nur noch überwacht werden können (reine Gewährleistungsverantwortung des Staates). Konnte bisher die sicherheitstechnische Fachkompetenz bei den hoheitlich wirkenden Stellen gebündelt bleiben, so muss diese sicherheitstechnische Fachkompetenz jetzt auf dem freien Markt beschafft werden. Mit der VDI-Denkschrift wird ein sicherheitsmethodisches Konzept angekündigt, das es unabhängig vom technologischen Anwendungsbereich ermöglicht, Technische Sicherheit systematisch für Systeme, Anlagen, Prozesse und technische Produkte zu erzeugen, nachzuweisen und zu bewahren. Dabei wird die risikosteuernde Funktion des Staates zu beachten, also der notwendige Beitrag zur Durchführungsverantwortung bzw. der mögliche Anteil an der Gewährleistungsverantwortung festzulegen sein.

4.3.4 Kontrollrichtlinie der Europäischen Union

Die Europäische Gemeinschaft hat es sich zum Ziel gesetzt, auf ihrem Gebiet den freien Markt durch den freien Verkehr von Waren, Kapital, Dienstleistungen und Personen zu fördern. Einerseits hat sie für das Inverkehrbringen von Produkten mit sicherheits- und gesundheitsrelevanten Eigenschaften Beschaffenheitsanforderungen festgelegt – und insoweit in den Markt eingegriffen. Andererseits hat sie aber den Markt für Dienstleistungen in Verbindung mit dem Nachweis der Konformität geöffnet. Die Prüfung, Zertifizierung und Überwachung einschließlich der Akkreditierung von Stellen für diese Aufgaben stehen grundsätzlich – vorbehaltlich einzelstaatlicher Einschränkung – jedermann offen und unterliegen damit dem Wettbewerb.

Zur Durchsetzung der Ziele der Europäischen Union wurden Instrumente in Form unabhängiger Konformitätsnachweise geschaffen. Mit ihrem „Neuen Konzept" ersetzt die Europäische Union zunehmend bisher zuständige Behörden und amtlich anerkannte Sachverständige durch „Benannte Stellen" mit Prüf- und Zertifizierungsrechten und -pflichten. Dieses „Neue Konzept" geht davon aus, dass die Dienstleistungen dieser „Benannten Stellen" dem freien Markt unterliegen (Liberalisierung).

4.3.5 Planungsprozess

Der Planungsprozess umfasst die Konzeptions- und die Definitionsphase (siehe Abschnitt 3.5.4). Während dieser beiden Phasen werden die folgenden Ziele und Zwecke verfolgt.

4.3.5.1 Ziel und Zweck

Ziele sind dadurch charakterisiert, dass sie nach Inhalt, Zeit und Ausmaß eindeutig qualifiziert und quantifiziert sind. In einem Zielvereinbarungsprozess werden Einzelziele für die verantwortlichen Mitarbeiter stufengerecht abgeleitet und entwickelt. Je nach Verantwortlichkeitsbereichen der Mitarbeiter können dies Deckungsbeitragsziele, Kosten- oder Leistungsziele sein. Durch ihre Kombination lassen sich konsistente Zielsysteme entwickeln, die sowohl für die Verantwortlichkeiten als auch für die Entscheidungsfindung geeignet sind. Die Führung durch Zielvereinbarung ist der Zielsetzung deutlich überlegen, weil die Mitarbeiter in den Zielableitungsprozess eingebunden sind.

Der sicherheitstechnische Anteil an der Konzeptionsphase ist die Sammlung und Auswertung verfügbarer sicherheitsrelevanter Informationen. Aus externen Anforderungen durch Absatzmärkte/Gesellschaft/Recht, der technologischen Entwicklung, den Zuliefer- und Rohstoffmärkten sowie den internen Möglichkeiten des Unternehmens wie Personalbestand und -qualifikation, bestehendes Produktprogramm und den Fertigungsmitteln wird das Programm bestimmt, in dem grundsätzlich die Entwicklung neuer Produkte (wie auch von Systemen und Anlagen) sicherheitstechnisch möglich ist.

Im Resultat des Produkt-Lebenszyklus muss sich eine vereinbarte Qualitätsanforderung wiederfinden. Sie besteht aus der Gesamtheit der betrachteten Einzelanforderungen an die Beschaffenheit des Produktes. Das wichtigste Merkmal für qualitätbestimmende Anforderungen ist, dass diese messbar in Prüfpläne aufgenommen und mit Toleranzen versehen werden (siehe Abschnitt 3.5.3).

Der Schwerpunkt der **Konzeptionsphase** liegt für den Themenkreis Sicherheit bei folgenden Tätigkeiten:

- Organisation der sicherheitstechnisch relevanten Arbeiten unter Berücksichtigung des Stands von Wissenschaft und Technik,
- Festlegung der Verantwortlichkeiten und Zuständigkeiten für den Themenkreis Sicherheit,
- Zusammentragen aller sicherheitstechnisch relevanten technischen Anforderungen, z.B. aus technischen Normen, einschlägigen Rechtsvorschriften und sonstigen Regelwerken,
- Auswertung der „Lessons Learned” aus vorhergehenden Ereignissen,
- Bestimmung der Gefährdungspotenziale,
- Definition des übergeordneten „Sicherheitstechnischen Anforderungskatalogs“ für das Gesamtsystem bzw. die gesamte Anlage,
- Darstellung der Sicherheitsanforderungen,
- Definition einer Grobstruktur für die Erledigung der sicherheitstechnischen Aufgabenstellung,
- Nachweisführung, dass dieser übergeordnete „Sicherheitstechnische Anforderungskatalog“ in sich schlüssig ist, den einschlägigen Vorschriften ent-

spricht und die in diesem Katalog festgelegten „Sicherheitstechnischen Anforderungen“ stets auch überprüfbar und nachweisbar sind.

In der **Definitionsphase** sind für den Themenkreis Sicherheit grundsätzlich die gleichen Tätigkeiten wie in der Konzeptionsphase vorzusehen – jedoch vielfach in konkreterer Form sowie erweitert um die rückverfolgbare Archivierung:

- Überprüfung der Organisation der sicherheitstechnisch relevanten Arbeiten und gegebenenfalls deren Anpassung an die gegebenenfalls veränderten Gegebenheiten der Definitionsphase,
- Bestätigung oder Neufestlegung der Verantwortlichkeiten und Zuständigkeiten für den Themenkreis Sicherheit, sofern sich für die Definitionsphase insgesamt Änderungen bei Verantwortlichkeiten und Zuständigkeiten ergeben haben,
- Fortsetzung des Zusammentragens aller sicherheitstechnisch relevanten technischen Anforderungen, z.B. aus technischen Normen, einschlägigen Rechtsvorschriften und sonstigen Regelwerken,
- Fortsetzung der „Lessons Learned” und Auswertung für jede hier zu definierende Baueinheit,
- Gefahrenanalyse, Ermittlung der Grenzrisiken und von Risikoäquivalenten,
- Festlegung und Freigabe des „Sicherheitstechnischen Anforderungskatalogs“ und der zugehörigen sicherheitstechnischen Grenzwerte,
- Definition der nachgeordneten „Sicherheitstechnischen Anforderungskataloge“ für jede hier zu definierende Baueinheit in logischer Weiterführung des übergeordneten „Sicherheitstechnischen Anforderungskatalogs“ für das Gesamtsystem bzw. die gesamte Anlage,
- Anwendung des sicherheitsmethodischen Konzepts für jede hier zu definierende Baueinheit,
- Rückverfolgbare Archivierung der erstellten Dokumentation,
- Nachweisführung, dass die hier definierten „Sicherheitstechnischen Anforderungskataloge“ für die nachgeordneten Baueinheiten in sich schlüssig sind, mit dem übergeordneten „Sicherheitstechnischen Anforderungskatalog“ nicht in Widerspruch stehen und den einschlägigen Vorschriften entsprechen. Die in diesen Katalogen festgelegten Sicherheitsanforderungen müssen ebenfalls nachweislich überprüfbar sein.

4.3.5.2 Werkstoffe, Stichprobenverfahren

Um die Homogenität der zu verwendenden Werkstoffe zu bewerten, muss der Hersteller aus einer in sich homogenen Gesamtheit (z.B. aus einem Fertigungslos) eine statistisch zufällige Auswahl treffen, d.h. eine Stichprobe ziehen. Sie muss aus einer repräsentativen Anzahl von Proben aus einem Los von in Frage kommenden Referenzwerkstoffen stammen. Dieses Bewertungsverfahren ist in Übereinstimmung mit anerkannten, einheitlichen Stichprobenplänen, d.h. nach DIN ISO 2859-1 „Annahmestichprobenprüfung anhand der Anzahl fehlerhafter Einheiten oder Fehler (Attributprüfung) – Nach der annehmbaren Qualitätsgrenzlage (AQL) geordnete Stichprobenpläne für die Prüfung einer Serie von Losen" durchzuführen und zu dokumentieren.

Bei der Herstellung von Einzelstücken (Unikaten) muss sich die Eignung des Werkstoffs aus einer analogen Vorgehensweise mit spezifischer Prüfmethodik ergeben.

4.3.5.3 Prüfbarkeit der Anforderungen

Es ist sicherzustellen, dass nur geeignete Produkte und Leistungen beschafft werden, die die Anforderungen auch erfüllen können. Dazu sind alle Unterauftragnehmer und Lieferanten zu überprüfen, inwieweit sie die erforderliche Qualitätsfähigkeit besitzen; in den Beschaffungsunterlagen müssen alle maßgeblichen Daten vollständig enthalten und nachprüfbar sein. Die Rückverfolgbarkeit soll die Möglichkeit eröffnen, Werdegang, Verwendung oder den Ort einer Baueinheit anhand ihrer ebenfalls aufgezeichneten Kennzeichnungen verfolgen zu können. Die Rückverfolgbarkeit bezieht sich besonders auf

- die Herkunft von Werkstoffen und Bauteilen
- die Verarbeitungsgeschichte des Produkts
- die Verteilung und den Verbleib des Produkts nach seiner Auslieferung

4.3.5.4 Berücksichtigung des Konfliktpotenzials Wirtschaftlichkeit / Technische Sicherheit

Das gewinnorientierte Marktprinzip für den Bereich der öffentlich-technischen Sicherheit stellt kein hinreichend geeignetes Sicherheitsinstrument dar und kann

hier aus einer Reihe von Gründen insoweit nur eingeschränkt Anwendung finden. Dazu sind die interessierenden Hauptfaktoren im Einzelnen zu prüfen und zu berücksichtigen:

- Das Produkt „Sicherheit"

  Neben anderen Faktoren, die auf die Technische Sicherheit Einfluss nehmen, wie Ausbildung/Fachkunde, allgemeine Sicherheitskultur/Beachtungsgrad von Regelungen wird hier die Sicherheit Waren und Dienstleistungen zugeordnet.

- Der Anwender

  Bei der Wertung der angebotenen Produkte und Dienstleistungen entscheidet der Anwender primär nur für sich, wobei Interessen des Allgemeinwohls üblicherweise nicht in Betracht gezogen werden. Deshalb kann dieser Fall nicht als belastbare Größe in Sicherheitserwägungen Platz finden.

  Die Berücksichtigung des Interesses Dritter und der Allgemeinheit muss deshalb erzwungen oder durch positive Anreize erreicht werden.

- Das öffentliche Interesse

  Zum Schutz der Allgemeinheit und der Umwelt greift der Staat in den Markt ein. Er trifft damit Vorsorge für das Gemeinwohl, die öffentliche Sicherheit und Ordnung.

  Zur ihrer Durchsetzung werden Anforderungen an Beschaffenheit und Betrieb sowie ein gestaffeltes Kontrollsystem mit Instrumenten unabhängiger Konformitätsnachweise gestellt.

- Hoheitlich-staatliche Aufsicht (Marktaufsicht)

  Im Fall eines liberalisierten Prüf- und Zertifizierungsmarktes in Europa – unter Umständen der gewollten Zukunft der Mehrheit der in der Europäischen Union beteiligten Staaten –, bei dem zum Teil nicht davon ausgegangen werden kann, dass Waren und Dienstleistungen mit sicherheitstechnischer Funktion im öffentlichen Interesse bereitgestellt werden, ist das Instrument der Marktaufsicht ein unverzichtbares Element zur Durchsetzung des öffentlichen Sicherheitsinteresses. Die Einrichtung einer Marktaufsicht ist ein notwendiges, aber noch nicht hinreichendes Instrument für den Bereich der Technischen Sicherheit. Sicherheit ist sowohl ein Einzel- als auch

ein Kollektivbedürfnis. Es lässt sich nicht durchgängig von den Marktkräften befriedigen. Dieses gilt besonders für in die Zukunft gerichtete Kollektivbedürfnisse. Aus diesem Grunde muss die Bundesrepublik Deutschland hoheitlich regulierend in den Markt eingreifen, also einer Änderung der gegebenenfalls gewollten Zukunft der Mehrheit von europäischen Staaten widersprechen.

4.3.5.5 Verantwortlichkeiten

Die Verantwortlichkeiten für alle Nachweis- oder Prüfmaßnahmen, insbesondere für die Durchsetzung von Maßnahmen bei unzureichenden Nachweis- oder Prüfergebnissen, müssen verständlich und eindeutig geregelt sein. Alle wesentlichen Nachweis- oder Prüfergebnisse sind aufzuzeichnen. Wenn mehrere Auftragnehmer und Unterauftragnehmer am Herstell- bzw. Produktionsprozess beteiligt sind und wenn Fehlentscheidungen und Lücken in der Nachweisführung beträchtliche Folgen verursachen können, ist ein Nachweis- oder Prüfplan erforderlich.

4.3.6 Realisierungsprozess

Der Realisierungsprozess besteht aus der Entwicklungs- und Konstruktions- sowie der Herstellungsphase. Das grundsätzliche Ziel des Realisierungsprozesses deckt sich im Wesentlichen mit dem des Planungsprozesses (siehe Abschnitt 3.5.4). Allerdings kann in der Herstellungsphase nur unter ganz bestimmten Randbedingungen noch mit dem Instrument der Zielvereinbarung gearbeitet werden, das der Zielsetzung wird häufiger anzuwenden sein.

4.3.6.1 Ziel und Zweck

Die Schwerpunkte der **Entwicklungs- und Konstruktionsphase** (siehe Abschnitt 3.5.4) liegen für den Themenkreis Sicherheit bei folgenden Tätigkeiten:

- Überprüfung der Organisation der sicherheitstechnisch relevanten Arbeiten und gegebenenfalls deren Anpassung an die gegebenenfalls veränderten Gegebenheiten der Entwicklungs- und Konstruktionsphase,
- Einrichten des Qualitäts- und Sicherheitsmanagements mit Neufestlegung der Verantwortlichkeiten und Zuständigkeiten für den Themenkreis Sicherheit,

sofern sich für die Entwicklungs- und Konstruktionsphase insgesamt Änderungen bei Verantwortlichkeiten und Zuständigkeiten ergeben haben,

- Fortsetzung des Zusammentragens aller sicherheitstechnisch relevanten technischen Anforderungen, z.B. aus technischen Normen, einschlägigen Rechtsvorschriften und sonstigen Regelwerken,
- Ermittlung von Eintrittswahrscheinlichkeiten und Schadensumfängen je Versagensart,
- Fortsetzung der „Lessons Learned" und Auswertung für jede hier zu entwickelnde bzw. zu konstruierende Baueinheit,
- Einbindung der zuständigen aufsichtführenden Institutionen (Behörden, Träger öffentlicher Belange, benannte Stellen, Sachverständige o.ä.) beim Erzeugen und Überprüfen von Sicherheit, soweit rechtlich und sachlich erforderlich,
- Anwendung der „Sicherheitstechnischen Anforderungen" und deren Umsetzung für jede hier zu entwickelnde bzw. zu konstruierende Baueinheit, indem das sicherheitsmethodische Konzept für jede hier zu entwickelnde bzw. zu konstruierende Baueinheit angewendet wird,
- Nachweisführung, dass die hier angewandten und umgesetzten „Sicherheitstechnischen Anforderungen"
  - für die nachgeordneten Baueinheiten wirksam sind,
  - mit dem übergeordneten „Sicherheitstechnischen Anforderungskatalog" nicht in Widerspruch stehen,
  - den einschlägigen Vorschriften entsprechen sowie
  - die im Einzelnen festgelegten „Sicherheitstechnischen Anforderungen" erfüllen,
- Optimierung der sicherheitstechnischen Anwendungen,
- Überprüfung und Nachweis der festgelegten Sicherheitsanforderungen für die hier betroffenen Einzelkonzepte im Zuge der Qualifikation (Typprüfung o.ä.),
- Vorlage eines Sicherheitsberichtes (als förmlichen Abschluss der sicherheitstechnischen Nachweisführung) – gegebenenfalls als Baustein des Safety Case (siehe Abschnitt 2.2.8).

Für den Schwerpunkt der **Herstellungsphase** (siehe Abschnitt 3.5.4) ergeben sich für den Themenkreis Sicherheit folgende Tätigkeiten, die zum Teil eine weitere Detaillierung der Tätigkeiten aus der Entwicklungs- und Konstruktions-

phase darstellen, zum größeren Teil jedoch spezifisch für den Herstellungsprozess sind:

- Überprüfung der Organisation der sicherheitstechnisch relevanten Arbeiten und deren Anpassung an die gegebenenfalls veränderten Gegebenheiten der Herstellungsphase – soweit erforderlich,
- Neufestlegung der Verantwortlichkeiten und Zuständigkeiten im Rahmen des Qualitätsmanagements für den Themenkreis Sicherheit – sofern sich für die Herstellungsphase insgesamt Änderungen bei Verantwortlichkeiten und Zuständigkeiten ergeben haben,
- Einschaltung der zuständigen Qualitätssicherungsorganisation (in Eigen- oder Fremdprüfung) in den Herstellungsprozess mit Schwerpunktsetzung auf die sicherheitstechnischen Vorgaben und Merkmale,
- Sicherstellung, dass die angewandten Fertigungsprozesse nicht nur wirtschaftlich, sondern stets auch reproduzierbar sind – und zwar mit Schwerpunkt Sicherheit,
- Einbindung der zuständigen aufsichtführenden Institutionen (Behörden, Träger öffentlicher Belange, benannte Stellen, Sachverständige o.ä.) bei Überprüfung von Sicherheit, soweit rechtlich und sachlich erforderlich,
- Fertigungstechnische Umsetzung des einschlägigen Stands der Technik bzw. Anwendung der allgemein anerkannten Regeln der Technik und in jedem Fall unter Verwendung aller sicherheitstechnisch relevanten technischen Anforderungen, z.B. aus technischen Normen, Fertigungs- und Qualitätssicherungsvorschriften,
- Nachweisführung, dass die hier angewandten und umgesetzten „Sicherheitstechnischen Anforderungen“ für die nachgeordneten Baueinheiten wirksam sind, mit dem übergeordneten „Sicherheitstechnischen Anforderungskatalog“ nicht in Widerspruch stehen, den einschlägigen Vorschriften entsprechen und dass die im Einzelnen festgelegten „Sicherheitstechnischen Anforderungen“ erfüllt und im Zuge der technischen Abnahme (Abnahmeprüfung o.ä.) überprüft, nachgewiesen und rückverfolgbar dokumentiert werden.
- Bei der Abnahmeprüfung ist die Konformität der hergestellten Produkte (oder des Systems, der Anlage) mit den in den vorangehenden Phasen erarbeiteten und festgelegten „Sicherheitstechnischen Anforderungen“ nachzuweisen.

4.3.6.2 Gefahrenanalyse

Die Gefahren und deren Ursachen sollten unter Anwendung einer bewährten Untersuchungsmethode analysiert werden. So lässt sich ein ausreichendes Maß an Gründlichkeit und Prüftiefe sicherstellen. Die zu untersuchende Baueinheit ist dazu gegebenenfalls in überschaubare Bereiche abzugrenzen.

Für die gesamte Baueinheit ist eine umfassende Gefahrenanalyse durchzuführen. Zu berücksichtigen sind dabei anlagenbezogene und umweltbedingte Gefahrenquellen, einschließlich naturbedingter Zustände und Ereignisse sowie Eingriffe Unbefugter.

Als Arbeitsgrundlage dienen die erfassten Unterlagen und Daten sowie Informationen aus Anlagen- und gegebenenfalls Ortsbegehungen.

Deckt die Gefahrenanalyse eine oder mehrere Gefahrenquellen auf, so ist zu ermitteln, welche Maßnahmen nach dem Stand der Technik zu treffen sind. Davon unabhängig sind die möglichen Folgen dennoch denkbarer Störungen zu ermitteln, hinsichtlich ihres Risikos eines Schadenseintritts und seiner Auswirkung zu bewerten und – unter Beachtung der normativen Vorgaben für das Grenzrisiko – Schutzmaßnahmen zu ergreifen.

4.3.6.3 Prüfbarkeit der Anforderungen

Verifizierung der Vorgaben aus den vorangegangenen Phasen:

- Hinsichtlich der Art und der Bedeutung von Prüfungen ist zu unterscheiden zwischen Serienherstellung mit dem Ziel gleich bleibender Qualität und Einzelherstellung mit dem Ziel, den Planungsvorgaben zu entsprechen.
- Festgestellte Abweichungen sind durch korrektive Maßnahmen beherrschbar. Im Hinblick auf die Beherrschung des Fertigungsprozesses ist bei der Serienfertigung auf Reproduzierbarkeit des Fertigungsprozesses zu achten (Bauabweichung); bei der Einzelherstellung haben präventive Maßnahmen Vorrang.

4.3.6.4 Prüfung und Freigabe der Planungsunterlagen

- Prüfung von Entwurf, Bemessung und konstruktiver Durchbildung

  Es gilt zu prüfen, ob alle maßgebenden Gefährdungen erkannt und geeignete Maßnahmen zu ihrer Abwendung vorgesehen sind. Dies betrifft insbesondere die zweckmäßige Wahl des Systems, der Stoffe und Bauarten, der Verfahren und Hilfsmittel der Ausführung sowie die Auslegung (Zugänglichkeit). Unter anderem gilt es ferner zu überprüfen, ob

  - alle wesentlichen organisatorischen Voraussetzungen, z.B. spezielle handwerkliche und betriebliche Qualifikation, erfüllt werden können,
  - alle für die Ausführung erforderlichen Prüfungen vorgesehen sind,
  - alle Nutzungsbedingungen und gegebenenfalls erforderlichen Erhaltungsmaßnahmen vor Inbetriebnahme festgelegt sind.

- Die Überprüfung der Planungsunterlagen kann auf verschiedene Arten mit unterschiedlichem Aufwand erfolgen. Unter anderem wird nachzuprüfen sein, ob

  - die Berechnung die maßgeblichen Anforderungen und die tatsächlichen Einflüsse, Randbedingungen und Nutzungsbedingungen erfasst werden,
  - Nachweise für alle wesentlichen Bauteile geführt werden,
  - geeignete Rechenmodelle verwendet werden,
  - die Berechnung in sich widerspruchsfrei ist,
  - alle Annahmen korrekt über das System verfolgt werden,
  - durch Veränderung von Bauteilen oder des Systems keine Schäden verursacht werden.

  Hinsichtlich der Art der Überprüfung kann man unterscheiden zwischen

  - vollständiger Vergleichsrechnung, die unabhängig von der vorliegenden Berechnung erfolgt, wobei maßgebliche Bemessungsergebnisse verglichen werden,
  - teilweiser Prüfrechnung, bei der nur wesentliche Teile der Berechnung durch Nachrechnung oder Vergleichsrechnung detailliert überprüft werden,
  - Prüfung der Herstellungs- bzw. Produktionsunterlagen (Bauunterlagen).

- Die Herstellungs- bzw. Produktionsunterlagen müssen alle erforderlichen Angaben für die Ausführung enthalten, so z.B. Toleranzgrenzen oder Veränderungen sowie Anweisungen hinsichtlich des Produktionsablaufs. Dabei ist unter anderem von Bedeutung, ob Bemessungsergebnisse richtig übertragen wurden, ob die Zeichnungen gegebenen Anforderungen entsprechen, ob andere Randbedingungen berücksichtigt sind und ob die Pläne eindeutig und unmissverständlich sind.

4.3.6.5 Rückverfolgbarkeit der Dokumentation

Der Hersteller muss über ein Qualitätsmanagementsystem verfügen, das in der Regel folgende Sachverhalte umfasst:

- Dokumentation und rückverfolgbare Archivierung der Ausführungsunterlagen,
- Regelungen zur Gewährleistung der geeigneten Auswahl (z.B. Probenmatrix, Partikelgröße, Konzentrationsbereich) von in Frage kommenden Referenzwerkstoffen,
- Vorbereitungsverfahren,
- Bewertung und Quantifizierung des erforderlichen Homogenitätsgrades des Werkstoffs,
- Bewertung der Stabilität des Werkstoffs, einschließlich laufender Bewertung der Stabilität – sofern erforderlich,
- Verfahren zur Durchführung der Charakterisierung der geforderten Eigenschaften,
- Praktische Realisierung der Rückführbarkeit auf nationale oder internationale Normale der gesetzlichen Maßeinheiten,
- Zuweisung der Merkmalswerte, einschließlich Vorbereitung der Zertifikate oder Erklärungen in Übereinstimmung mit ISO Guide 31 „Referenzwerkstoffe" – wenn angebracht,
- Bereitstellung geeigneter Produktionseinrichtungen,
- Regelungen für geeignete Möglichkeiten zur Identifizierung, Etikettierung und Verpackung, Abpack- und Zustellverfahren sowie Kundenservice.

Dem Dokumentations- und Archivierungssystem muss entnommen werden können, welche Tätigkeiten vom Hersteller und welche durch Kooperationspartner

ausgeführt werden. Es muss außerdem die vom Hersteller eingesetzten Regelungen und Verfahren beinhalten.

4.3.6.6 Genehmigungsverfahren

Die Herstellung bestimmter sicherheitstechnisch wichtiger Produkte kann bereits einer behördlichen Genehmigungspflicht oder Zulassungspflicht unterliegen. Die entsprechenden Auflagen (Freigabeverfahren) müssen in das Qualitätsmanagementsystem aufgenommen und beachtet werden.

Das Sicherheitsmanagement muss als Bestandteil des Qualitätsmanagementsystems betrachtet werden. Genehmigungen bedingen häufig auch die Berücksichtigung des Schutzes gegen unbefugten Zugriff („security“).

Das Qualitätsmanagementsystem selbst unterliegt einem regelmäßigen Zertifizierungsprozess durch Dritte, die so genannten akkreditierten Zertifizierer.

4.3.6.7 Werkstoffverwendung

- Qualitätssicherungssystem (Eigen- und Fremdüberwachung mit Dokumentation zur Rückverfolgung):
  - Mehrere Faktoren können dazu führen, dass die Ausführung unzulässig von den zugrunde gelegten Vorgaben abweicht. Zu diesen Faktoren zählen z.B. veränderte Werkstoff- und Bauteileigenschaften, Unsicherheiten bei Einbau und Errichtung oder Fehler und Irrtümer bei den verschiedenen Herstellungsschritten. Dagegen sind Kontrollmaßnahmen bei allen wesentlichen Phasen der Ausführung vorzusehen (vorbeugende Überwachung der Bauausführung).
  - Besteht die Gefahr, dass sich Eigenschaften während der Nutzungsdauer unzulässig bzw. erwartungswidrig verändern, so können besondere Erhaltungsmaßnahmen erforderlich sein (begleitende Überwachung vor Inbetriebnahme).

- Kompatibilität der Komponenten

  Der Hersteller muss in regelmäßigen Abständen und in nach einem zuvor festgelegten Plan und Verfahren interne Audits seiner Tätigkeiten durch-

führen. Damit weist er nach, dass seine Tätigkeitsabläufe weiterhin mit den Anforderungen des Qualitätsmanagementsystems übereinstimmen.

Das Programm zur internen Auditierung muss alle Elemente des im Qualitätsmanagement-Handbuch dargelegten Qualitätsmanagementsystems ansprechen, einschließlich der technischen und Produktionstätigkeiten, die zur Zuweisung der Merkmalswerte auf einen Referenzwerkstoff (Materialverträglichkeit, „fit/form/function“) führen. Es liegt in der Verantwortung des Qualitätsmanagement-Beauftragten, Audits entsprechend dem aufgestellten Programm und auf Anforderung der Leitung zu planen und zu organisieren. Derartige Audits müssen von geschultem und qualifiziertem Personal durchgeführt werden. Das Personal muss – wo immer es die Mittel zulassen – unabhängig von der zu auditierenden Tätigkeit sein.

Das Personal darf nicht seine eigenen Tätigkeiten auditieren – es sei denn, dies ist erforderlich und nachgewiesen effektiv durchgeführt.

4.3.6.8 Marktaufsicht / hoheitliche Aufsicht

Das Instrument der Marktaufsicht ist ein unverzichtbares Element hoheitlichen Handelns zur Durchsetzung öffentlich-rechtlicher Sicherheitsbelange. Mit seinen rechtlichen Möglichkeiten kann der Staat in den Markt eingreifen und Fehlentwicklungen beseitigen. Der Staat tut dies auf vielfältige Weise, indem er selbst geeignetes Aufsichtspersonal vorhält oder sich so genannter beliehener Unternehmer bedient.

Die Transparenz (rückverfolgbar) für das Handeln der (staatlichen) Marktaufsicht muss vom Hersteller geschaffen werden.

4.3.7 Betriebsprozess

Der Betriebsprozess beinhaltet die Betriebs- und Nutzungsphase, in die sich nach Abschluss der Nutzung in der Regel auch die Rückbau-, Entsorgungs-, Recyclingphase integrieren lässt (siehe Abschnitt 3.5.4).

4.3.7.1 Ziel und Zweck

Als Instrument der Zielerreichung steht hier die Zielsetzung im Vordergrund, mit der der wirtschaftliche, zuverlässige und sichere Betrieb erreicht werden soll.

In der **Betriebs- und Nutzungsphase** (siehe Abschnitt 3.5.4) ist zu unter scheiden zwischen Produkten (Anlagen, Waren und Dienstleistungen), die genehmigungsfrei sind, und solchen, die vor Inbetriebnahme einer Genehmigung bedürfen. In beiden Fällen sind aber folgende Gesichtspunkte zu berücksichtigen:

- Sicherheitsmanagement
- sicherheitstechnische Überwachung
- Sicherheit bei etwaigen Nachrüstungen

Für die **Rückbau-, Entsorgungs-, Recyclingphase** (siehe Abschnitt 3.5.4) gelten im Prinzip die gleichen Verfahren, wie sie bei den vorangegangenen Phasen beschrieben wurden, aber wegen der oft fehlenden Regeln der Technik mit erhöhtem Prüf- und Aufsichtsaufwand . Erschwerend kommt hinzu, dass es sich bei der Rückbau-, Entsorgungs-, Recyclingphase nicht um serienmäßige Verfahren handelt, weshalb das betreffende Personal diese Aufgabe mit besonderer Aufmerksamkeit und Verantwortung lösen muss. Vor allem hat das leitende Personal ein angemessenes und geeignetes Qualitätsmanagementsystem zu schaffen, das den besonderen Verfahrensschritten bei der Rückbau-, Entsorgungs-, Recyclingphase gerecht wird.

Der Schwerpunkt der Rückbau-, Entsorgungs-, Recyclingphase liegt für den Themenkreis Sicherheit bei folgenden Tätigkeiten:

- Organisation der sicherheitstechnisch relevanten Arbeiten,
- Festlegung der Verantwortlichkeiten und Zuständigkeiten für den Themenkreis Sicherheit,
- Auswertung der „Lessons Learned” aus vorhergehenden Ereignissen zur Bestimmung präventiver Maßnahmen,
- Bestandschutz aus den früheren Grenzwerten,

- Definition des übergeordneten „Sicherheitstechnischen Anforderungskatalogs“ für die gesamte Rückbau-, Entsorgungs-, Recyclingphase,
- Nachweisführung, dass diese übergeordneten „Sicherheitstechnischen Anforderungen“ in sich schlüssig sind, den einschlägigen Vorschriften entsprechen und dass die in diesem Katalog festgelegten „Sicherheitstechnischen Anforderungen“ stets auch überprüfbar und nachweisbar sind.

4.3.7.2 Genehmigung

Umweltbelastende oder sicherheitstechnisch wichtige Industrieanlagen und Gewerbebetriebe benötigen eine Genehmigung nach den entsprechenden Gesetzen. Das Genehmigungsverfahren soll sicherstellen, dass

- Die Mitarbeiter, gegebenenfalls die Nachbarschaft und auch die Allgemeinheit vor schädlichen Umwelteinwirkungen und sonstigen Gefahren geschützt werden,
- die notwendige Vorsorge gegen schädliche Umwelteinwirkungen und sonstige Gefahren sowie erhebliche Nachteile oder Belästigungen getroffen wird,
- Abfälle vermieden oder verwertet und – soweit nicht vermeidbar oder verwertbar – ordnungsgemäß beseitigt werden,
- Energie sparsam und effizient verwendet wird.

Im Genehmigungsverfahren wird außerdem geprüft, ob andere öffentlich-rechtliche Vorschriften (z.B. Naturschutzrecht, Wasserrecht, Bauordnungsrecht) gewahrt und die erforderlichen Maßnahmen zum Arbeitsschutz getroffen sind.

Eine Genehmigung kann zahlreiche andere behördliche Entscheidungen einschließen (Konzentrationswirkung).

Die behördlichen Verfahren, z.B. Baugenehmigungen, Erlaubnisse für überwachungsbedürftige Anlagen nach dem Geräte- und Produktsicherheitsgesetz, Eignungsfeststellungen für Anlagen zum Lagern, Abfüllen, Umschlagen, Herstellen, Behandeln oder Verwenden wassergefährdender Stoffe werden gebündelt.

4.3.7.3 Zustandskontrollen

Alle betrieblichen Verfahrensabläufe müssen systematisch in regelmäßigen Abständen überprüft werden. So lassen sich potenzielle Quellen von Nichtkonformitäten sowie alle Möglichkeiten zur Verbesserung, entweder technischer Art oder innerhalb des Qualitätsmanagementsystems, identifizieren. Maßnahmepläne müssen ausgearbeitet, umgesetzt und überwacht werden, um die Wahrscheinlichkeit des Auftretens von Nichtkonformitäten zu vermindern und die Vorteile aus den Verbesserungen wahrzunehmen. Die Ergebnisse der vorbeugenden Maßnahmen müssen zu Zwecken der Managementbewertung vorgelegt werden.

4.3.7.4 Nutzungsvorschriften

Nutzungsanweisungen dienen der Qualitätserhaltung während des Betriebs; sie sind schriftlich und detailliert in den Qualitätsvereinbarungen auszuarbeiten und vom Hersteller dem Nutzer zu übergeben. Nutzungsanweisungen sind Bestandteil der Qualitätsplanung auf Grundlage des Qualitätsmanagementsystems. Hierbei sind das Geräte- und Produktsicherheitsgesetz und entsprechende gesetzliche Regelungen zu beachten.

4.3.7.5 Instandhaltung

Produkte müssen zur Erfüllung der Anforderungen an technische Anlagen nur in dem Umfang beitragen, als Letztere auch ordnungsgemäß instand gehalten werden.

Nach der Norm DIN 31051 „Instandhaltung, Begriffe und Maßnahmen”, 01/85, sind unter Instandhaltung alle Maßnahmen zur Bewahrung und Wiederherstellung des Sollzustandes technischer Systeme und Anlagen zu verstehen, soweit sie nicht verändert werden. Damit sind Begriffe wie Wartung, Inspektion und Instandsetzung mit umfasst.

4.3.7.6 Nachrüstung

Für komplexe Systeme und Industriegüter mit langer Nutzungsdauer (wie beispielsweise Verkehrsflugzeuge, Schienennetze für den spurgeführten Verkehr,

chemische Großanlagen, Kraftwerke usw.) wird häufig eine Verlängerung der Brauchbarkeitsdauer angestrebt. Je nach Umfang der erforderlichen Nachrüstung sind Teilmaßnahmen aus den verschiedenen Lebenszyklusphasen erneut durchzuführen, damit bei Wiederaufnahme der Nutzung ein gleicher Betriebs- und Sicherheitsstand gewährleistet bleibt wie vor der Nachrüstung.

Für bestimmte Bereiche ist die Nachrüstung nach dem Stand der Technik bzw. von Wissenschaft und Technik rechtlich vorgeschrieben.

4.3.8 Qualitätsmanagement in der Sicherheitstechnik

4.3.8.1 Rolle und Nutzen von Qualitätsmanagementsystemen

Die systematische Bewertung und Umsetzung von technischen Anforderungen ist die Grundlage jedes Qualitätsmanagementsystems, wie z.B. nach DIN EN ISO 9000 „Qualitätsmanagementsysteme". Diese Anforderungen beziehen sich auf alle Phasen. Da sie bereits im Planungsprozess aufgenommen werden, ist dieser Sachverhalt für das Qualitätsmanagement ein entscheidender Schritt, weil die von Fehlern induzierten Kosten mit jedem Folgeschritt anwachsen.

Zu einer erfüllbaren Qualitätsanforderung gehört eine durchdachte Qualitätsplanung, die aus folgenden Hauptelementen besteht:

- Planung der Identifizierung, Klassifizierung und Gewichten der Qualitätsmerkmale des Produkts, Festlegen der Ziele und der Qualitätsanforderungen,
- Planung der Führungs- und Ausführungstätigkeiten wie Vorbereiten der Anwendung des Qualitätsmanagementsystems mit Ablauf- und Zeitplänen,
- Erstellen von Qualitätsmanagement-Plänen und Einrichtung eines Prozesses zur ständigen Qualitätsverbesserung.

Bei konsequenter Anwendung des Qualitätsmanagementsystems wird das Erreichen der geforderten Qualität des Produktes erwartet. Diese Erwartung muss sich auf eine hohe Zuverlässigkeit des angewandten Systems verlassen können. Als äußeres Zeichen dieser Erwartungshaltung gilt die festgestellte Konformität des Produktes mit den Anforderungen und den entsprechenden Dokumenten.

Für Laboratorien beispielsweise, die Stoffkenndaten ermitteln, existiert ein auditierbares Managementsystem in Form der GLP-Standards (Gute Labor-Praxis)

der „Organisation for Economic Co-operation and Development” (OECD). Dies ist durch eine Richtlinie für die Staaten der Europäischen Gemeinschaft verbindlich eingeführt worden.

4.3.8.2 Qualitätsmanagementsystem und qualifiziertes Personal

In festgelegten Zeitabständen muss der Produktlieferant das Qualitätsmanagementsystem auditieren. Dabei sind die Zeitabstände so zu wählen, dass die Eignung und Wirksamkeit bei der Erfüllung der Anforderungen und der festgelegten Qualitätspolitik und ihrer Ziele sichergestellt werden kann. Zum Zweck der Rückverfolgbarkeit sind Aufzeichnungen hierüber notwendig und im erforderlichen Umfang rückverfolgbar zu archivieren.

Der Hersteller muss ein Qualitätsmanagementsystem – in der Regel gemäß DIN EN ISO 9000 „Qualitätsmanagementsysteme” – aufbauen, umsetzen und aufrechterhalten, das für seinen Tätigkeitsbereich einschließlich Art, Umfang und Größenordnung der Produktion angemessen ist. Der Hersteller muss seine Qualitätsmanagement-Politik, Ziele und Verpflichtungen definieren und dokumentieren.

Das Qualitätsmanagement muss sich weiterhin zur Herstellung von Referenzwerkstoffen verpflichten, die mit den in ISO Guide 30 „Verwendete Begriffe und Bezeichnungen beim Nachweis mit Referenzwerkstoffen” angeführten Definitionen in Übereinstimmung stehen und deren Merkmalswerte unter Nutzung zugelassener statistischer Verfahren bewertet werden. Das Qualitätsmanagement muss sich zudem verpflichten, die im ISO Guide 31 „Referenzwerkstoffe” enthaltenen Angaben bezüglich Werkstoffzertifikate und Bereitstellung dazugehöriger Informationen für die Nutzer einzuhalten. Das Qualitätsmanagement muss ferner die beabsichtigte Verwendung des gelieferten Werkstoffbereichs spezifizieren und die Organisation des Herstellers verpflichten zu gewährleisten, dass die Kunden umfassend informiert werden.

Der **Hersteller** muss

- über leitendes Personal verfügen, das durch technisches Personal unterstützt wird; dieses wiederum muss über Befugnisse und Mittel zur Aufgabenerfüllung verfügen. Das technische Personal muss zudem Abweichungen vom

Qualitätsmanagementsystem bzw. von den Verfahren zur Herstellung des Referenzwerkstoffs identifizieren und Prozesse zur Verhinderung oder Minimierung derartiger Abweichungen auslösen können,

- über Regelungen verfügen, die gewährleisten, dass sein Management und Personal frei ist von jeglichem kommerziellen, finanziellen oder anderem internen und externen Druck, der die Qualität ihrer Arbeit nachteilig beeinflussen könnte,

- über Regelungen und Verfahren verfügen, die gewährleisten, dass vertrauliche Informationen und die Eigentumsrechte seiner Kunden geschützt sind,

- über Regelungen und Verfahren verfügen, die jegliche Beteiligung an Tätigkeiten vermeiden, die das Vertrauen in seine Kompetenz, Unparteilichkeit, Urteilsvermögen oder betriebliche Integrität verringern,

- mit Hilfe von Organigrammen die Organisation und Managementstruktur des Herstellers, seine Stellung innerhalb einer Trägerorganisation und die Beziehungen zwischen Management, technischen Verfahren, unterstützenden Dienstleistungen, Kooperationspartnern und dem Qualitätsmanagementsystem definieren,

- Verantwortlichkeiten, Befugnisse und Beziehungen zwischen dem gesamten Personal beschreiben, das die Arbeit, die die Qualität der Herstellung der Referenzwerkstoffe beeinflusst, leitet, ausführt oder überprüft,

- über eine technische Leitung verfügen, die die gesamte Verantwortung für die technischen Vorgänge und für die Bereitstellung der erforderlichen Mittel hat, um die geforderte Qualität der Produktionsvorgänge zu gewährleisten,

- über ein Archivierungssystem zur rückverfolgbaren Dokumentation verfügen
  - zur Lenkung von Dokumenten (spezifizierte Anforderungen, Freigabe- und Änderungswesen),
  - zur Lenkung von Aufzeichnungen (Nachweisführung, Prüfprotokolle),
  - für die internen Audits (geplant, ad hoc),

- zur Lenkung fehlerhafter Produkte (Bauabweichungswesen),
- über Korrekturmaßnahmen,
- über Vorbeugungsmaßnahmen.

Die Zuständigkeiten und Verantwortlichkeiten für alle Nachweisführungen, insbesondere für die Durchsetzung von Maßnahmen bei unzureichenden Prüfergebnissen, sollten verständlich und eindeutig geregelt sein. Wenn viele Auftragnehmer und Unterauftragnehmer am Bauvorhaben beteiligt sind und wenn Fehlentscheidungen und Kontrolllücken beträchtliche Folgen verursachen können, ist ein Prüfplan zur integrierten Nachweisführung sinnvoll. All diese Einzelmaßnahmen müssen auch das gemeinsame Ziel eines Integrierten Sicherheitsmanagements verfolgen.

Der **Betreiber** muss zumindest die Nutzungsauflagen des Herstellers erfüllen, wozu vor allen Dingen die sicherheitstechnischen Auflagen gehören. Zu diesem Zweck muss er ein dafür geeignetes Qualitätsmanagementsystem aufbauen, umsetzen und aufrechterhalten, das für seinen Tätigkeitsbereich einschließlich Art, Umfang und Größenordnung des Betriebs angemessen ist. Hersteller und Betreiber müssen Ziele und Verpflichtungen definieren und gegebenenfalls dokumentieren. So kann die Qualität aller Aspekte der Produktion, der Werkstoffeigenschaften (z.B. Festigkeit, Homogenität und sonstige Werkstoffeigenschaften), der Charakterisierung (z.B. Gerätekalibrierung und Validierung von Messmethoden), der Zuweisung von Merkmalswerten (z.B. Einsatz geeigneter statistischer Verfahren) und Verfahren zu Werkstoffhandhabung, -lagerung und -transport gewährleistet und aufrechterhalten werden.

Der Betreiber muss über ausreichendes Personal verfügen, welches die erforderliche Ausbildung, Schulung, technische Kenntnisse und Erfahrungen für die zugewiesenen Aufgaben besitzt. Der Betreiber muss gewährleisten, dass das Bedienungspersonal, im Zweifelsfall zusätzlich geschult wird, um eine kompetente Durchführung der Messungen, Bedienung der Geräte und andere, die Qualität beeinflussenden Tätigkeiten abzusichern. Wenn möglich sollte das Erreichen der Kompetenz durch Schulungen nach objektiven Maßstäben bewertet werden.

Wenn Managementsysteme vorgeschrieben sind, müssen sie den Vorgaben entsprechen. Es kann möglich sein, dass das Qualitätsmanagementsystem andere wie Sicherheits- oder Sicherungsmanagementsysteme integriert.

5 Gesellschaftliche Betrachtungen

5.1 Vorbeugung gegen sicherheitskritisches Versagen

5.1.1 Nationale und internationale Entwicklungen

Zielgrößen für die öffentlich-technische Sicherheit werden im nationalen Rahmen in Regeln festgehalten, die vom Grundgesetz über Gesetze und Verordnungen bis hin zu Normen und Verhaltensregeln reichen. Die international gesellschaftsabhängige Ausformung impliziert Unterschiede der Strukturen in verschiedenen Staaten und Regionen. Das zunehmende Zusammenwirken in Wirtschaftsräumen, die Staats- und Regionalgrenzen überschreiten, macht eine Anpassung und Öffnung bisher überwiegend nationalstaatlicher Regelungen notwendig. Die Skala der zu treffenden Maßnahmen reicht dabei von der gegenseitigen Anerkennung regional weiter unterschiedlicher Strukturen bis hin zu weltweit einheitlichen, harmonisierten Strukturen und Regelungen zur Gefahreneindämmung für bestimmte Sektoren. So unterliegen die Formen und Inhalte von Nachweisen in der Prüf- und Sicherheitstechnik einem Wandel, dessen Auswirkungen einzuschätzen sind.

Mit dem Übergang nationaler Kompetenzen auf supranationale Einrichtungen ist auch in Technik und Wirtschaft eine Veränderung nationaler Gepflogenheiten gewachsener und oft bewährter Traditionen verbunden. Diese Änderungen sind auf nachteilige Auswirkungen für die Sicherheit zu überprüfen, gegebenenfalls ist eine Gegensteuerung zu veranlassen.

Folgerung hieraus ist: Bei den europäischen und letztlich globalen Erfordernissen zur Weiterentwicklung der öffentlich-technischen Sicherheit sind nicht nur das hergebrachte deutsche System, sondern auch andere Systeme vergleichend zu analysieren und zu bewerten. Zur Bestimmung eines geeigneten Systems zur Gewährleistung öffentlich-technischer Sicherheit müssen der jeweilige rechtliche Hintergrund, der Stand der Technik und die Erfordernisse der Wirtschaft berücksichtigt werden. Einzubeziehen in die zukunftorientierte Problemanalyse sind auch die Tätigkeiten unabhängiger Dritter (3rd party) vor dem Hintergrund der ganzen Spannweite von mit staatlichen Prüfaufgaben beliehenen Organisa-

tionen, bis hin zu am Markt agierenden Dienstleitern (Problemfeld: Durchführungs- und Gewährleistungsverantwortung des Staates).

Um Ansätze für konsensfähige Lösungen für unbestreitbar sichere Systeme zu entwickeln, sollte zunächst das technische Risiko betrachtet und analysiert werden. In jedem Fall muss sich die Technik an die Spitze der Diskussion über konsensuale Lösungen und Organisationsformen der Sicherheitslandschaft stellen.

5.1.2 Sicherheit und Legislative

Die Gewährleistung der Technischen Sicherheit ist in ihrer Bedeutung nicht anders zu werten, als die Verantwortung für die innere und äußere Sicherheit. Es gehört zu den Kernaufgaben des Staates, hierfür die geeigneten Rahmenbedingungen zu schaffen. Für die Beantwortung der Frage, welches Risiko (im Sinne: Risiko – Chance) zulässig und welches unzulässig ist, sind Staat und Öffentlichkeit gefordert. Der Staat tut dies durch entsprechende Gesetze wie z.B. Atomgesetz, Chemikaliengesetz, Gesetz zur Beförderung gefährlicher Güter, Sprengstoffgesetz. Verordnungen konkretisieren die erforderliche Vorsorge; die in Bezug zu nehmenden Normen und Regeln komplettieren dieses Regelungssystem.

Unmittelbare staatliche Aktivitäten innerhalb des Regelungssystems werden verdrängt durch zunehmend angewandte Marktaufsichtsverfahren; hier muss zukünftig eine Rollenverteilung zwischen Staat und Privaten risikoabhängig ausbalanciert werden.

5.1.3 Sicherheit und Deregulierung

In sicherheitsrelevanten Bereichen darf sich der Staat nicht nur auf die Regelsetzung und die Strafandrohung beschränken, er muss vielmehr mit der Vorgabe der Normen und Strukturen im erforderlichen Maß durch aktives Handeln gleichzeitig deren Erfüllung und Einhaltung sicherstellen. Es ist politischer Wille, bisher staatliche Aufgaben vermehrt in die Hände privater Einrichtungen bzw. der Wirtschaft zu geben. Um die erforderliche Balance zu halten, bedarf es einer adäquaten Ausrichtung der staatlichen Aufgaben in den sich ändernden Prüf- und Genehmigungssystemen.

Die Strukturen innerhalb der Sicherheitstechnik müssen zwischen Staat und Wirtschaft ausbalanciert werden, wie aber auch die Balance zwischen Vorsorge, Prävention (Gefahrenabwehr) und Repression (Strafen auf Schadensereignisse) zu halten ist. Diese Staffelung des erforderlichen Anforderungsprofils am Gefährdungs- bzw. Schadenspotenzial bezieht sich nicht nur auf die technischen Anforderungen, sondern auch auf die Maßnahmen auf den Feldern Genehmigung und Überwachung. Die Einbindung aller interessierten Kreise und ihre aktive Mitwirkung (Hersteller und Betreiber sowie Staat und unabhängige Dritte) muss systematisch organisiert werden. Das bedeutet, dass sich der Staat selbst ausgewogen in die Genehmigungs- und Aufsichtspflicht einbringen muss. Auch er muss sein Wirken in den Gesamtzusammenhang der Mechanismen stellen, die gewährleisten, dass die höchsten noch vertretbaren Risiken nicht überschritten werden.

5.1.4 Sicherheit und Wirtschaft

Wirtschaftlich von großer Bedeutung ist die möglichst einheitliche und großen Wirtschaftsräumen zugeordnete Aufstellung von Normen und Regeln. Hier kann es beim Ausgleich unterschiedlicher Zielvorstellungen aus den beteiligten Gesellschaften zu Anpassungen kommen, welche die ursprünglich nationale Ausformung von Normen und Regeln nicht mehr ausreichend widerspiegelt. Umso sorgfältiger müssen die Regeln gestaltet werden, um im Gesamtsystem öffentlich-technischer Sicherheit keine Einbußen zu erleiden.

Im anglo-amerikanischen Wirtschaftsraum erfahren organisatorische Aspekte (Verhaltensanforderungen im Betrieb und detaillierte Tätigkeitsvorschriften) stärkere Betonung, als dies in Deutschland der Fall ist, wo mehr auf produktbezogene Sicherheit (Beschaffenheitsanforderungen bzgl. Bauweisen und Ausrüstung) gesetzt wurde. Ein gewichteter Ausgleich dieser Positionen in umfassenden Systemen könnte Vorteile bringen, die einfache Adaption von einem Mehr an Organisation und einem Weniger an baulichen Anforderungen wäre nachteilig. In jedem Fall muss künftig über institutionalisierte Nahtstellenbetrachtungen von Beschaffenheits- und Verhaltensanforderungen das gewollte Maß an öffentlich-technischer Sicherheit verifiziert werden. Dies umso mehr, da im Rahmen der Europäisierung des sicherheitstechnischen Rechts die Beschaffenheitsanforderungen an technische Produkte zunehmend auf europäischer Ebene festgelegt werden, und zwar mit dem Ziel, den freien Warenverkehr zu gewährleisten.

5.1.5 Sicherheit und Zuständigkeitsverteilungen

Erforderlich ist neben der ausgewogenen Einbindung von Hersteller- und Betreiberinteressen die Mitwirkung von Fachbehörden und unabhängigen Sachverständigen. Risiken eines Schadenseintritts und dessen -auswirkungen sowie Unterschiede in den Strukturen für Produkte einerseits und Anlagen andererseits müssen beachtet werden. Die Verhaltensregeln gewinnen damit im europäischen Bereich und im amerikanischen Verständnis deutlich sichtbar große Bedeutung vor dem Hintergrund, dass die Normen für Bauteile und Produkte Kompromisse darstellen können, bei denen bisherige deutsche Zielvorstellungen nicht gänzlich eingebracht werden konnten.

In dem Maße wie das stringente Durchsetzen des Vorsorgegebotes des Grundgesetzes nicht mehr von staatlichen oder direkt im Auftrag des Staates handelnden Einrichtungen wahrgenommen wird, ergibt sich die Notwendigkeit von Staats wegen zur Wahrung von Neutralität und Objektivität sowie Kontinuität mit der Konsequenz (Rechtseinheitlichkeit, Rechtssicherheit), unabhängige Einrichtungen mit Aufgaben der Koordinierung und Gewährleistung des Erfahrungsaustausches privater Einrichtungen zu betrauen.

5.1.6 Sicherheit als vorrangiges Qualitätsmerkmal

Die heute in einigen Anwendungsbereichen praktizierten Qualitätsmanagementmaßnahmen reichen allein nicht aus, um sicherheitskritische Qualitätsmängel und potenzielle Versagensursachen rechtzeitig aufdecken und abstellen zu können. Dennoch scheint nicht hinreichend bewusst zu sein, dass ein System nur dann als sicher gewertet werden darf, wenn Gewissheit besteht, dass die sicherheitstechnischen Qualitätsmerkmale in der vorgegebenen Ausprägung tatsächlich gegeben sind. Hier ist unter Ingenieuren und Naturwissenschaftlern noch das notwendige Bewusstsein zu schaffen: Qualitätsmanagement ist das Konzept, das die technischen Sicherheitsmerkmale hinreichend genau beschreibt und den Verantwortlichen somit erst die Möglichkeit zum erforderlichen Eingreifen und Nachbessern gibt.

5.1.7 Qualitätsmanagement als Konzept für das Sicherheitsmanagement

Sicherheit will wie jedes andere Qualitätsmerkmal geplant, verfolgt und nachgewiesen werden. In diesem Zusammenhang kann allerdings auf Bewährtes zurückgegriffen werden – nämlich auf die DIN EN ISO 9000 „Qualitätsmanagementsysteme". In den Qualitätsmanagement-Anforderungen dieser Norm sind die Erfordernisse für ein verlässliches Sicherheitssystem beschrieben, welches für ein Erfolg versprechendes Qualitätsmanagement – oder im Zusammenhang mit der Technischen Sicherheit – für ein verlässliches Sicherheitsmanagement notwendig ist. Ein nach den Vorgaben dieser Norm zertifiziertes Unternehmensmanagement gilt als qualitätsfähig. Ein auf die Vorgaben dieser Norm ausgerichtetes Sicherheitsmanagement darf somit als sicherheitsfähig gelten. Im Bereich der europäischen Luftfahrtunternehmen wurde die DIN EN ISO 9000 „Qualitätsmanagementsysteme" eingeführt. Die Frage ist, inwieweit diese Norm auch in den anderen Anwendungsbereichen, die einen Bezug zur öffentlichen Sicherheit haben, eingeführt ist und praktiziert wird.

Im Bereich der Bautechnik wurde dieses System analog in den Bauordnungen der Bundesländer verankert und ist bei allen sicherheitstechnisch bedeutsamen Bauprodukten anzuwenden (vgl. Musterbauordnung, §§ 20 ff., und die Prüf-, Überwachungs- und Zertifizierungs-Verordnungen der Bundesländer). In anderen Technikbereichen werden Sicherheits- oder Qualitätsmanagementsysteme gefordert (von der Störfallverordnung betroffene Anlagen, Herstellung von Gefahrgutverpackungen) wobei die Wahl des Qualitätsmanagementsystems allerdings dem Verantwortlichen überlassen bleibt, solange das System wirksam ist.

Im Rahmen des Sicherheitsmanagements, mit dem für komplexe Systeme Sicherheitsmethodik und -technik umgesetzt werden, müssen offene Fragen zu allen organisatorischen, methodischen und sicherheitstechnischen Problemen – aber auch Verbesserungsvorschläge zu spezifizierten Festlegungen – an eine zentrale Ansprechstelle gerichtet werden können.

5.1.8 Konfigurationssteuerung und Änderungsverfahren

Auch eine Rahmenspezifikation Sicherheit muss – wie jede andere Spezifikation auch – einem förmlichen Freigabe- und Änderungsverfahren unterliegen, und

zwar auf der Grundlage einer ordnungsgemäßen Konfigurationssteuerung, deren Grundsätze und Abläufe sich in einer Richtlinie zur Konfigurationssteuerung festgelegen lassen.

5.1.9 Der Mensch als Kriterium für das Sicherheitsmanagement

Technisch komplexe Systeme zählen in der Regel zu den Mensch-Maschine-Systemen, in denen das eingesetzte Personal mit maßgeblichen Betriebsfunktionen betraut ist. Zu diesen Funktionen gehören vor allem auch sicherheitstechnische Funktionen. Bei derartigen Mensch-Maschine-Systemen ist der betrieblichen Einbindung des Personals besondere Aufmerksamkeit zu widmen.

Auch hier ist unter Ingenieuren und Naturwissenschaftlern noch das erforderliche Bewusstsein zu schaffen:

Personal, das um die sicherheitstechnischen Sachzusammenhänge weiß, das uneingeschränkten Zugriff auf die sicherheitstechnisch erforderlichen Einrichtungen hat, das ständig über den jeweiligen Betriebszustand und das sicherheitstechnische Umfeld umfassend informiert ist und das stets aufs Neue für seine „betriebliche Funktion" bewertet wird, kann nicht zu einem schwachen Glied in der betrieblichen bzw. sicherheitstechnischen Funktionskette werden.

Mit seinen naturgemäßen Fähigkeiten und Unzulänglichkeiten stellt der Mensch in diesem Zusammenhang mit den Mensch-Maschine-Systemen ein wesentliches Kriterium für das Sicherheitsmanagement dar.

5.2 Kommunikation Technischer Sicherheit mit der Öffentlichkeit

Bei schwierigen Themen, insbesondere solchen, die in der Bevölkerung auch Ängste erzeugen könnten, wird die Wissenschaft bemüht, um aufzuklären. Dies gilt für die Medizin, die Umwelt, die Städteplanung, den Arbeitsmarkt, die Steuerpolitik, die Energieversorgung ebenso wie die Sicherheit technischer Einrichtungen. Oft rutschen die damit befassten Vertreter der Wissenschaft unversehens in eine Rolle, die unterschiedlichen Interessenspositionen und Lobbys legitimieren zu sollen. Das Ideal wissenschaftlicher Widerspruchsfreiheit, der Konsens der Wissenschaft, geht infolge des so ausgelösten Streits unter Wissen-

schaftlern verloren. In der Öffentlichkeit entsteht das Bild wissenschaftlicher Hilflosigkeit. Dieser Konflikt liegt meist in der Komplexität vieler heute anstehender Probleme begründet. „Beweise" haben dann notgedrungen hypothetischen Charakter. Je nach gewählter Hypothese und je nach gesetzten Randbedingungen kommt man zu unterschiedlichen Schlussfolgerungen.

Durch Mehrdeutigkeit und Unverständlichkeit der benutzten Begriffe wird die Öffentlichkeit mehr verunsichert als aufgeklärt. Als Beispiel sei hier der Begriff „Sicherheit" angesprochen. Korrekterweise müsste der fachkundige Wissenschaftler darauf hinweisen, dass es 100%-ige Sicherheit niemals und nirgends geben kann. Zahlenangaben zur Auftretenswahrscheinlichkeit von 10^{-7} (1 : 10 Millionen) hinterlassen beim Laien eine gewisse Verständnislosigkeit. Der Begriff „Häufigkeit", mit dem hier ja „Seltenheit" gemeint ist, hat für den fachkundigen Ingenieur andere Bedeutungsinhalte als für die Bevölkerung im Allgemeinen. Bei ihr schwingen qualitativ ganz andere Bedeutungsgehalte mit – etwa Gefahr, Katastrophenpotenzial des Schadensfalles, vermutete Schrecklichkeit des Schadens, persönliche Betroffenheit, Auswirkungen auf die eigenen Kinder, hilfloses Ausgesetztsein und Mangel an Kontrollierbarkeit. Die zwei verschiedenen Diskursebenen bleiben dabei unverbunden. Da die Bringschuld zu verständlicher Risikokommunikation bei der Wissenschaft liegt, muss sie zumindest fünf wichtige psychologische Faktoren der Gefahrenwahrnehmung kennen und ihnen Rechnung tragen:

(1) *Freiwilligkeit:*

Gefahren, denen man sich freiwillig aussetzt, werden eher unterschätzt. Dies gilt für das Rauchen ebenso wie das Autofahren.

(2) *Kontrollierbarkeit:*

Gefahren, die durch die eigenen Fähigkeiten kontrollierbar erscheinen, werden eher unterschätzt. Ein Beispiel ist die Tätigkeit des Dachdeckers.

(3) *Katastrophenpotenzial:*

Gefahren mit hohem Katastrophenpotenzial werden eher überschätzt, etwa die Möglichkeit vieler Toter bei einem Flugzeugabsturz.

(4) Betroffenheit:

Gefahren, von denen man selbst betroffen ist, werden eher überschätzt, z.B. mögliche Nebenwirkungen bei der Einnahme von Medikamenten.

(5) Bekanntheit / Gewohnheit:

Gefahren, die bekannt sind, werden eher unterschätzt. Das Rauchen mag hier als Beispiel dienen.

Risikokommunikation bedarf der konstruktiven Handhabung sowie einer sachorientierten Auseinandersetzung bei der Bewertung der Risiken. Risikokommunikation, die das Vertrauen zu den Adressaten zerstört, kommt häufig vom Herunterspielen von Risiken, von Vertuschung anfälliger Störungen oder Unfällen, Handeln im Widerspruch zu Aussagen. Ähnlich negativ wirken verspätetes Reagieren auf öffentliche Beschuldigung statt proaktive Information oder die Bekanntgabe un- oder missverständlicher Informationen.

Risikokommunikation muss daher neue Wege suchen. Als angemessene Strategien der Risikokommunikation bieten sich an:

- Bestimmte Formen der Darstellung *kleiner Wahrscheinlichkeiten*: Die Bedeutung und das Zustandekommen von numerisch wieder gegebenen Wahrscheinlichkeiten muss jeweils erläutert werden – einschließlich der Randbedingungen.

- *Risikovergleiche*, d.h. etwa der Vergleich des Risikos einer Müllverbrennungsanlage mit einem Bahnunfall: Nur wenn die Dimensionen wie Kontrollierbarkeit, Freiwilligkeit oder Katastrophenpotenzial vergleichbar sind, haben Risikovergleiche eine Chance verstanden zu werden.

- *Risikokompensation*: hier werden erwartete Risiken gegen erwarteten Nutzen miteinander verglichen (Bau einer Chemiefabrik und ihre Auswirkungen auf den lokalen Arbeitsmarkt).

- *Vertrauen und Glaubwürdigkeit:* verständliche und widerspruchsfreie Informationsaufbereitung, respektvolle Behandlung der Adressaten von Risikokommunikation, keine Unterschlagung von Informationen.

Da Risikokommunikation in unserer Gesellschaft immer wichtiger wird, müssen insgesamt Risikokonzepte vorgelegt werden, die sich nicht nur an einer Begrenzung der Eintrittswahrscheinlichkeiten von Stör- und Unfällen orientieren. Diese sind im herkömmlichen ingenieurwissenschaftlichen Sprachgebrauch für Laien grundsätzlich schwer verständlich. Vielmehr geht es darum, auf die *Minderung des Schadensumfangs* abzuheben und die psychologischen Erkenntnisse der Gefahrenwahrnehmung und erfolgreicher Kommunikationsbedingungen zu berücksichtigen.

Kommunikation zwischen Interessengruppen konträrer Zielsetzung ist ohne schiedsrichterliche Instanz aussichtslos, sofern Kompromissfähigkeit innerhalb der Gruppen als Schwäche bei der Durchsetzung der eigenen Interessen diskreditiert wird. Es handelt sich dann nicht mehr um einen Abwägungsprozess zwischen Risiken und Chancen für die Gemeinschaft – wie immer definiert –, wenn das Wohlergehen des Individuums „das Maß aller Dinge" ist. Interessenvertreter von Gruppen haben immerhin ein eindeutiges Mandat. Wenn sie unter dem Signum ihrer Gruppe auftreten, ist ihre Aufgabe im öffentlichen Diskurs allgemein zu erkennen.

Schwieriger zu definieren ist die Position der Administration. Ihr wird nach allgemeinem Verständnis die Mittlerrolle zwischen dem anerkannten Stand von Wissenschaft und Technik und dem Sicherheitsbedürfnis der Öffentlichkeit zugesprochen. In der Praxis befinden sich jedoch politikberatende Einrichtungen manchmal in einem – gegebenenfalls nur „gefühlten" Abhängigkeitsverhältnis zu einer übergeordneten politischen Instanz. Es ist dann nicht notwendigerweise ihre Aufgabe, sich nur der wissenschaftlichen Objektivität zu verpflichten. Sie sind gewissermaßen voreingenommen, und ihre Aufgabe besteht in der nahezu unbeirrbaren Verfolgung bestimmter Schutzziele (öffentliche Sicherheit, Gesundheitsschutz, Umweltschutz). Der Erfolgszwang, unter dem sie stehen bzw. glauben zu stehen, führt im ungünstigen Fall zu einem Aufeinandertreffen gegenläufiger Maximalforderungen, über die in einem abgehobenen politischen Raum nach dem Opportunitätsprinzip entschieden wird. Der eigentlich wünschenswerte Ausgleich der Interessen, der auf einer interdisziplinären Expertenebene zu einer faktischen Ausarbeitung für politische Optionen führen müsste, wird insofern verpasst.

Deshalb ist die Tendenz zu begrüßen, dieses Problem der repräsentativen Demokratie zu überwinden, wo immer es möglich ist. Es gilt zunächst, die

Öffentlichkeit im Vorfeld sicherheitsrelevanter Entscheidung mit den Fakten und Ungewissheiten vertraut zu machen. Sie muss in die Lage versetzt werden, die Tragweite der Optionen in allen Facetten zu erkennen, damit sich jeder Interessierte vor seinem persönlichen Hintergrund entscheiden kann. Dabei sollte man sich von der Vorstellung lösen, es handle sich um eine Holschuld des Einzelnen, und die Möglichkeit der Beteiligung bestünde immer. Die „schweigende Mehrheit" ist durch ein nicht zu übersehendes Angebot zu animieren, aktiv am Konsens der Informierten mitzuwirken.

Im Prinzip haben wir diese Möglichkeit. Die öffentlich-rechtlichen Medien könnten die Rolle einer Bildungseinrichtung übernehmen und das Forum für Risikokommunikation sein. Die heutige, teils verflachte Talkshow ließe sich ablösen durch eine eingängige Wissensvermittlung in einem Diskurs, deren Teilnehmer der Diskussionskultur verpflichtet sind (gegebenenfalls unter Nutzung allgemein zugänglicher Informations- und Kommunikationstechniken). Wenn es gelänge, diese Form der Auseinandersetzung um die Folgen wissenschaftlich-technischer Innovationen als Routine zu etablieren, würde auch der Druck auf die Experten zunehmen, der Öffentlichkeit ihren Sachverstand zur Verfügung zu stellen und sich an der Resonanz der Auditorien messen zu lassen.

Risikokommunikation im demokratisch verstandenen Diskurs ist ein mühsames Unterfangen und dazu noch mit ungewissem Ausgang. Dennoch ist dies die einzige seriöse Möglichkeit der Problemlösung.

6 Empfehlungen

Auch wenn in der breiten Öffentlichkeit zurzeit möglicherweise ein anderer Eindruck vorherrscht, stellen wir Ingenieure immer wieder fest, dass die Entwicklung der Technischen Sicherheit stets mit der technischen Gesamtentwicklung Schritt gehalten hat.

Allerdings ist ebenfalls festzustellen, dass sich das interdisziplinäre Zusammenwirken, mit dem in der Technik der zunehmenden Spezialisierung begegnet wird, nur in rudimentären Ansätzen in der Sicherheitstechnik wieder findet.

Während sich in der allgemeinen Technik seit Jahrzehnten generalistische Konzepte und systemtechnische Managementverfahren längst bewährt haben, mit deren Hilfe sich arbeitsteilige Spezialisierungen interdisziplinär wieder zusammenführen lassen, scheinen Sicherheitstechnik, Sicherheitsrecht und die einschlägige Normung noch heute davon unberührt geblieben zu sein.

Es besteht akuter Handlungsbedarf, in der Sicherheitstechnik in gleicher Weise generalistische Konzepte und systemtechnische Managementverfahren einzuführen, wie sie in der allgemeinen Technik seit Jahrzehnten gang und gäbe sind.

Als generalistisches Konzept mag für die Sicherheitstechnik das in dieser Denkschrift angesprochene **sicherheitsmethodische Konzept** dienen; als geeignetes **systemtechnisches Managementverfahren** lässt sich DIN EN ISO 9000 „Qualitätsmanagementsysteme” heranziehen. Der Verein Deutscher Ingenieure bietet die interdisziplinäre Arbeitsplattform, die hier vorgestellten Grundzüge im erforderlichen Umfang auszuarbeiten und weiter zu pflegen.

In den vorangegangenen Abschnitten ist dargelegt, wie Technische Sicherheit geplant, erzeugt und dauerhaft erhalten wird. Ebenfalls wurde beschrieben, wie sich die unterschiedlichen Einwirkungen auf einen Produktionsprozess auswirken – seien sie technischen oder menschlichen Ursprungs. Die für ein Produkt verantwortlichen Personen müssen bei jedem Planungs- und Produktionsschritt das erreichte Maß an Sicherheit kennen, denn jeder Folgeschritt baut auf dem vorangegangenen Schritt auf (daher: Fortschritt); nicht erkannte Fehler würden sonst weiter getragen. Aber auch hier zeigt sich, dass nur das gesehen und beachtet wird, was man weiß.

Die Gesellschaft, die Lehre und Forschung bezahlt sowie Technik fördert, hat ein Recht auf Informationen. Es besteht deshalb eine Bringpflicht zur Information über die Zusammenhänge Technischer Sicherheit durch die Natur- und Ingenieurwissenschaften. Im Folgenden sind die maßgeblichen Bereiche angesprochen.

6.1 Forschungslandschaft

Die Forschungslandschaft gliedert sich in vier Bereiche, und zwar in

- Hochschulen (Universitäten, Fachhochschulen sowie Musik- und Kunsthochschulen, ganz überwiegend unter rechtlicher und finanzieller Verantwortung der Länder),

- Forschungs- (Förder-) Organisationen (Deutsche Forschungsgemeinschaft, Helmholtz-Gemeinschaft, Max-Planck-Gesellschaft, Fraunhofer-Gesellschaft und Wissenschaftsgemeinschaft Gottfried Wilhelm Leibnitz),

- Forschungszentren der Industrie – einschließlich der in den kleinen und mittelständischen Unternehmen (KMU),

- Forschungsinstitute des Bundes und der Länder.

Die Forschung in der Bundesrepublik Deutschland verfügt damit über ein hohes Potenzial, was sich auch anhand des Anteils der Bruttoinlandsausgaben für Forschung und Entwicklung von 2,55 % (für das Jahr 2003) am Bruttoinlandsprodukt erkennen lässt. Von 1998 bis 2003 ist wieder starke Zunahme erfolgt, so dass in 2003 insgesamt 54,3 Milliarden € zur Verfügung standen. Der Anteil der Wirtschaft beläuft sich dabei auf rund zwei Drittel. Der Anteil der Forschung, der der Sicherheitsforschung zugerechnet werden kann, ist dabei nicht durchgängig identifizierbar. Geht man von Schwerpunktausrichtungen der Wirtschaftsforschung für Produkte aus sowie von geringen Anteilen der anderen Arten für die Sicherheitsforschung, kann nur auf einen zu geringen Anteil der Forschung für Sicherheitsprobleme geschlossen werden.

Unterstellt man, dass von Produkten aus Deutschland – quasi als Markenzeichen – neben Qualität auch Sicherheit erwartet wird, und damit eine Markterwartung

zum Ausdruck kommt, muss sich die Forschung verstärkt auch Sicherheitsfragen widmen.

- Zunächst kann eine Evaluierung der Sicherheitsforschung klären helfen, ob die Qualität das benötigte Niveau aufweist.

- Davon ausgehend muss eine Reorientierung einsetzen. So beklagt der Dechema/GVC-Forschungsausschuss „Sicherheitstechnik in Chemieanlagen" z.B.
  - die fehlende Forschungsförderung für Themen der Sicherheitstechnik durch die öffentliche Hand,
  - die Entwicklung, dass in der Vergangenheit primär sicherheitstechnisch orientierte Lehrstühle und Institute heute zunehmend auf andere Forschungsbereiche ausgerichtet werden,
  - die mit dem Rückgang universitärer Forschungskapazitäten auf dem Gebiet der Sicherheitstechnik einhergehenden Einschränkungen bei den Ausbildungsinhalten und -möglichkeiten,
  - das Fehlen eines hinreichenden sicherheitstechnischen Basiswissens bei Hochschulabgängern, das erst zusätzlich durch externe oder firmeninterne Fachseminare vermittelt werden muss,
  - eine in Verfahrenstechnik und Technischer Chemie deutlich gesunkene Zahl der Studierenden, was gleichermaßen die Weitergabe der sicherheitstechnischen Erkenntnisse einschränkt, und
  - den zunehmend begrenzteren Handlungsspielraum der deutschen Industrie für Forschung und Entwicklung auch in der Sicherheitstechnik, u.a. als eine Folge des globalen Wettbewerbs, der zum Teil durch nicht einheitliche internationale Rahmenbedingungen verschärft wird.

Dies gilt auch allgemein und unterstreicht die hier getroffene Empfehlung nach Reorientierung der Sicherheitsforschung.

Die Komplexität, die wirtschaftliche Verflechtung und die notwendige Detailtiefe sowie die neuen Felder der dynamisch verlaufenden Innovationen erfordern die Einbindung der Forschung in Deutschland in internationale Netzwerke, insbesondere in die der Europäischen Union. Hier bilden sich ständig neue Einrichtungen, wie die Europäischen Technologieplattformen. Allein die Plattform

„Safety for Sustainable European Industry Growth" weist mehrere Focus-Gruppen zu Fragen des Risikos und des Human Factors Engineering auf.

Die internationale Einbindung der deutschen Sicherheitsforschung ist zu definieren und zu steuern; es sind dafür geeignete Strukturen zu benennen und zu schaffen.

Näher wird auf die Internationalisierung in Abschnitt 6.4 eingegangen.

6.2 Ausbildungs- und Lehrangebote der Hochschulen

Ein Lehrangebot auf dem benötigten hohen Niveau kann nur im Zusammenhang mit einer fundierten Forschung aufrecht erhalten werden, um der Wirtschaft ausreichend qualifizierte Ingenieure zur Verfügung stellen zu können. Sicherheitstechnik muss daher integraler Bestandteil der Ausbildung aller technischen Fachhochschulen, Technischen Hochschulen und Universitäten ebenso sein wie Gegenstand von Fort- und Weiterbildungsmaßnahmen privater Bildungsträger.

Die notwendigen Bildungsmaßnahmen für die Vermittlung sicherheitstechnischer Grundausbildung müssen von technischen Hochschulen und Universitäten im Rahmen ingenieurwissenschaftlicher Lehrpläne getragen werden. Unter die Angebote, die in der tertiären Ausbildung angeboten werden müssen, gehören vor allem:

- Technikfolgenabschätzung und Risikoanalyse
- Risikokommunikation
- Einflüsse menschlichen Verhaltens auf die Sicherheit (Human Factors)
- Interdisziplinäre Kooperationskompetenz
- Notfallplanung
- Rolle nationaler und internationaler Regelungsbemühungen
- Berufsethische Prinzipien der Ingenieurtätigkeit

Angesichts der Breite und der gesellschaftlichen Bedeutung des hierzu erforderlichen Lehrangebotes ist der gegenwärtig zu beobachtende Abbau von qualifizierten Lehrkapazitäten und die Umwidmung sicherheitstechnisch orientierter Lehrstühle auf andere Gebiete an technischen Hochschulen und Universitäten nicht adäquat. Im Interesse der künftigen Gewährleistung von Technischer

Sicherheit sind die für die Hochschulen verantwortlichen Kultusverwaltungen aufgefordert, diesem Abbau schnell Einhalt zu gebieten. Um der damit verbundenen Verknappung kompetenten Lehrpersonals entgegen zu wirken, müsste auf Seiten der Industrie erwogen werden, sicherheitstechnische Stiftungslehrstühle einzurichten.

Die langfristige Vorsorge für den sicherheitstechnischen Kompetenzerhalt und die Kompetenzanpassung an neue technische und gesellschaftliche Herausforderungen ist insbesondere von privaten Bildungsträgern der Industrie zu treffen. Es ist zu begrüßen, dass die Einrichtung von Bildungsakademien und Schulungseinrichtungen (z.B. Simulatorzentren zur periodischen Überprüfung und Fortentwicklung notwendiger Kompetenzen) bereits seit langem in einigen Industriezweigen vorangetrieben wird. Allerdings spielen sicherheitstechnische Fragestellungen in den Lehrprogrammen eine nur untergeordnete Rolle. Das muss dringend korrigiert werden. Dementsprechend ist die Industrie aufgefordert, langfristig das sicherheitstechnisch qualifizierte Personal auszubilden und zu beschäftigen, um zu gewährleisten, dass durch das natürliche Ausscheiden von Fachkräften und einen möglichen Mangel an Zuwachs jüngeren Fachpersonals keine Engpässe der sicherheitstechnischen Kompetenz entstehen. Dies setzt voraus, dass ein zukunftsorientiertes Wissens- bzw. Informationsmanagement über eine gründliche Dokumentation technischer Entscheidungen und entsprechende Maßnahmen der Weitervermittlung des angesammelten Wissens erfolgt (vergleiche hierzu Abschnitt 6.3.3).

6.3 Thematische Schwerpunkte

6.3.1 Öffentlichkeit

Die Akzeptanz der Technik in der Öffentlichkeit hängt weitgehend davon ab, wie ein möglichst umfassendes Verständnis über Bedingungen und Grenzen sicherer Technikentwicklung bei den Menschen erreicht wird, die von technischen Gegebenheiten betroffen sind. Im Sinne einer Bringschuld verpflichtet dies alle mit Sicherheitsfragen befassten Experten und Institutionen (Wissenschaftler, Forschungseinrichtungen, Ingenieure, Gerichte, Industrie und öffentlicher Wirkungskreis) dazu, die Öffentlichkeit durch verständliche Informations- und Kommunikationsstrategien von den Erfordernissen und Möglichkeiten sicherer Technik in Kenntnis zu setzen.

Ein besonderer Stellenwert in der sachgemäßen Information der Öffentlichkeit kommt Multiplikatoren und Meinungsträgern zu: Medienvertreter, leitendes Personal der Parteien, Lehrkräfte an Schulen und Hochschulen sowie anderen privaten und öffentlichen Bildungseinrichtungen, Vertreter aus Ingenieurvereinen und Industrieverbänden.

Um den Transfer sachgerechter Technikinformationen von den „Produzenten" der Technik an die „Endnutzer" zu ermöglichen, sollte die Bildung von Netzwerken für Technische Sicherheit mit themenspezifischen Anlaufstellen („Knoten") ins Auge gefasst werden. Diese Knoten wären mit fachspezifisch qualifizierten Experten zu besetzen, um den Informationsbedarf einer interessierten Öffentlichkeit zu decken oder die Vermittlung an entsprechende fachkompetente Stellen zu übernehmen.

6.3.2 Technikrat

Sicherheitstechnik muss ganzheitlich und deutlich systemischer behandelt werden. Grenzen von Technikfeldern müssen überwunden werden, genauso wie Ressortbereiche in Sicherheitsfragen durchlässig sein müssen. Die historisch entstandene Strukturierung der Sicherheitstechnik nach anwendungsorientierten Sach- und Fachgebieten führt heute zu unzähligen Gremien. Bei interdisziplinären Technologievorhaben verursachen deren fachspezifische Regelungen eine Vielzahl von nur schwer handhabbaren Nahtstellenproblemen.

Ein Sicherheitscodex „Technik" wäre als Vision eine idealtypische Lösung zur Effizienzsteigerung des Handelns in der Technik, und hier für die Gesamtheit der Wirtschaft einschließlich der sicherheitlichen Bewertung von entsprechenden Teilen des Technikhandelns. Die Zielgröße, nämlich langfristige Schaffung eines Sicherheitscodes „Technik", kann eine herausragende Aufgabe eines Technikrates werden, der analog zum Wissenschaftsrat zu schaffen wäre.

Dieser berät die Bundesregierung und die Regierungen der Länder. Ein herausragender Focus ist die Entwicklung der Hochschulen, der Wissenschaft und der Forschung. Er gibt Empfehlungen und Stellungnahmen zu zwei Kernbereichen, nämlich zu den wissenschaftlichen Institutionen sowie zu übergreifenden Fragen des Wissenschaftssystems. Ein Technikrat sollte selbstverständlich auch die Bundesregierung und gegebenenfalls die Regierungen der Länder, aber in jedem

Fall die Wirtschaft und die gesellschaftlichen Gruppierungen zu Fragestellungen des Umgangs mit der Technik informieren und beraten.

Der Technikrat könnte als eine seiner Arbeitssäulen die Zuständigkeit für den oben angeführten Sicherheitscode „Technik“ übernehmen und diesen mit entsprechenden Strukturen steuern und inhaltlich begleiten. Eine weitere Arbeitssäule kann dann die Sicherheitstechnik sein, die mit diesem Teil des Technikrates ein Optimum an zusammenfassender Betrachtung aller Elemente der Technik hätte. Weitere Arbeitssäulen – wie Ethik, Wissenschaft – sind vorstellbar und sollten im Benehmen mit der Wirtschaft definiert und aufgestellt werden. Sicher gehört in diesen Bereich weiterer Arbeitssäulen das Innovationspotenzial der Technik, wie auch die Umsetzung von Forschungsergebnissen in marktfähige Produkte im Technikbereich.

Träger des Technikrates wäre der Staat, vertreten durch die Bundes- und Länderregierungen, die auch hier die Interessen der Bürger wahrnehmen, sowie die Wirtschaft und weitere Nicht-Regierungs-Vertretungen wie Gewerkschaften und Umweltverbände. Weitere Details zu den Strukturen und der Arbeitsweise sind den Beratungen des VDI-Arbeitskreises „Technische Sicherheit” vorbehalten. Aus sachlichen Überlegungen heraus wäre das Sekretariat eines solchen Technikrates beim Verein Deutscher Ingenieure anzusiedeln.

6.3.3 Informationsmanagement

Vor dem Hintergrund, dass sich bei komplexeren Systemen die technischen Sicherheitskonzepte und die Nahtstellen Mensch-Technik nicht trivial beschreiben und einfach steuern lassen, ist die Dokumentation und Kommunikation der technischen und organisatorischen Teilkonzepte ein wichtiger Bestandteil des ganzheitlichen Sicherheitskonzeptes geworden. Die zur Dokumentation und Kommunikation nutzbringend anzuwendenden Instrumente stellt das Fachgebiet des Informations- oder Wissensmanagements zur Verfügung. Der Begriff Informationsmanagement wurde Mitte der achtziger Jahre in den Vereinigten Staaten von Amerika im Zusammenhang mit Überlegungen zum papierlosen Büro eingeführt. Heutzutage wird der Begriff Wissensmanagement synonym verwendet, obwohl streng genommen das Wissen, das sich in den Köpfen der Menschen befindet, nicht gemanagt werden kann. Was als Wissensmanagement bezeichnet wird, ist letztlich Informationsmanagement und dient dazu, die Randbedingungen für die Wissensarbeit zu schaffen. Aufgrund

der historischen Entwicklung setzte sich jedoch der Begriff „Wissensmanagement" durch. Die Disziplin Informations- oder Wissensmanagement hat ihre Wurzeln in der Informationstechnik mit dem Schwerpunkt der Dokumentation und dem elektronischen Austausch von Informationen. Ergänzt wurden die Instrumente zum Informationsmanagement stark durch Beiträge aus den Wirtschafts- und Sozialwissenschaften, aber auch Kybernetik und Verhaltens- und Kommunikationspsychologie lieferten Beiträge. Wohl nicht zufällig wurde in den letzten 20 Jahren das Sicherheits- und Gefahrenabwehrmanagement parallel zum Informations- und Wissensmanagement eingeführt. Damit können Instrumente des Informationsmanagements schrittweise ebenso für das Sicherheitsmanagement genutzt werden. Sicherheitstechnisch hochsensible Systeme wie die Verkehrsluftfahrt oder kerntechnische sowie chemische Anlagen wären ohne ein perfektes Management gar nicht auf dem hohen Sicherheitsniveau zu halten, wie das in einer Industriegesellschaft gefordert wird. Im Bereich der Technischen Sicherheit müssen die Instrumente des Informationsmanagements verstärkt in denjenigen Technik- und Wirtschaftsbereichen genutzt werden, bei denen aufgrund ihrer Struktur (z.B. kleine und mittelständische Unternehmen), der Vielfalt und Individualität bezüglich sicherheitsrelevanter Fragestellungen (z.B. bei verfahrenstechnischen Anlagen) moderne Instrumente des Informationsmanagements erst partiell eingesetzt werden.

Das Ziel des Informationsmanagements wird gelegentlich mit dem Slogan „Die richtige Information zur richtigen Zeit am richtigen Ort" plakativ zusammengefasst. Es fehlt letztlich noch der Gesichtspunkt der Effizienz. Der Aufwand für das Informationsmanagement muss nämlich der sicherheitsbezogenen Fragestellung angemessen sein – und zwar sowohl wegen des Risikos mit seinen beschriebenen Facetten als auch wegen der wirtschaftlichen Rahmenbedingungen, in denen sich ein Unternehmen, eine Prüforganisation oder eine Behörde bewegen kann oder muss.

Aus dem zitierten Slogan lassen sich vielfältige Fragen ableiten, die konkrete Herausforderungen an das Informationsmanagement betreffen:

- Sind für die Aufgabenstellung alle sicherheitsrelevanten Aspekte berücksichtigt? Heutzutage ist es nicht schwer, aus Bibliotheken oder dem Internet jede Information zusammenzutragen.

Allerdings tauchen weitere Fragen auf:

- Wie lassen sich die für meine Aufgabenstellung relevanten Informationen herausfiltern, und wie lassen sich diese aufgabenspezifisch verdichten?

- Sind alle – auch die Randgebiete betreffenden – Daten erfasst?

Die zunehmende Spezialisierung der Fachdisziplinen erfordert immer öfter, bei der Suche nach Sicherheitslösungen den Blick auf Nachbardisziplinen zu lenken, und letztlich bleibt die uralte Fragestellung:

- Sind die ermittelten Daten und Informationen richtig?

Für die Lösung derartiger Fragestellungen waren schon immer und werden auch in Zukunft die Fachexperten die Schlüssel zum Erfolg sein. Es herrscht weitgehender Konsens, dass geeignete IT-Plattformen, wie Intra- und Internet oder Datenbanken und Recherchesysteme zwar notwendige Voraussetzungen sind – wie früher Papier und Bleistift sowie das Schriftgut. Der Erfolg des Informationsmanagements hängt allerdings davon ab, dass der Mensch in den Mittelpunkt gestellt wird. Folgt man dieser Erkenntnis, lassen sich die aktuellen Arbeiten im Bereich des Informations- und Wissensmanagements so fokussieren, dass die Interaktionen zwischen beteiligten Personen unterstützt werden. Dann spielt es keine Rolle mehr, inwieweit es sich dabei um Experten oder beteiligte Personengruppen handelt, die zu offenen Expertennetzwerken oder geschlossenen „communities" gehören, ob sie innerhalb einer Firma oder Behörde kommunizieren oder übergreifend zwischen Institutionen oder Interessengruppen. Nationale Netzwerke stehen dabei neben europäischen und internationalen Netzwerken. Beispielsweise fördert die Europäische Union die Bildung europäischer Netzwerke vor allem mit dem Ziel, die Wirtschaft zu stärken, aber auch mit dem Ziel, das von der Gesellschaft erwartete Niveau an Sicherheit zu gewährleisten. Netzwerke, deren Fokus überwiegend sicherheitsbezogene Themen sind, tun sich allerdings schwer, da die Mittel zur Unterstützung von Netzwerken überwiegend in Projekte fließen, die einen unmittelbaren wirtschaftlichen Erfolg versprechen. Hier wird an die zuständigen Stellen in Unternehmen, in der Politik und in den Verwaltungen appelliert, die besondere Bedeutung der Technischen Sicherheit in einer zunehmend komplexeren Gesellschaft berücksichtigend, die notwendigen Mittel bereitzustellen, damit die richtige sicherheitsrelevante Information zur richtigen Zeit am richtigen Ort sein kann.

6.4 Notfallplanung

Die Notfallplanung für Großschadensereignisse muss ebenfalls internationaler ausgestaltet werden. Allein für Deutschland gilt schon, dass zahlreiche Produkte und Systeme, deren Eigensicherheit zwar ausreichend belegt und dokumentiert ist, in ihrer Nutzungsphase weitere Risiken entfalten. Derartige Gefahrenquellen können die eigenen Produkt- und Systemgrenzen deutlich überschreiten und einen größeren Umweltbereich, der nicht mit dem Produkt oder Betrieb kausal verknüpft ist, gefährden. In solchen Fällen muss die Sicherheitsphilosophie für die Produktbeherrschung auch die Notfallplanung für das potenziell betroffene Umfeld einbeziehen. Hierzu zählen neben den Werks- und Verbandseinrichtungen in der Regel Einrichtungen der staatlichen Exekutive (wie Bezirksregierungen, Landräte und Bürgermeister), aber auch direkt für den Katastrophenschutz zuständige Einrichtungen (wie Feuerwehr und Technisches Hilfswerk). Das gesamte Netz ist in Struktur und Verantwortung deutlicher zu definieren, wie die Nahtstelle zu den Planern und Betreibern von Produkten, Systemen und Anlagen zu institutionalisieren sind.

Grenzüberschreitende Auswirkungen sind nicht nur möglich, sondern zunehmend zu erwarten. Die für die Bundesrepublik Deutschland empfohlene deutlichere Strukturierung des Netzwerkes muss analog in eine Empfehlung zur internationalen Struktur von Hilfseinrichtungen übertragen werden.

6.5 Internationalisierung

Die Globalisierung der Märkte erfordert auch die Internationalisierung der Sicherheitstechnik bei den Produkt- und Systemherstellern. Immer häufiger müssen Waren und ihre Herstellung sicherheitstechnischen Prinzipien genügen, die ihren freien Austausch und ihren sicheren Gebrauch in allen Empfängerstaaten gewährleisten. Die Kräfte des Marktes allein reichen nicht aus, um die erforderlichen Sicherheitseigenschaften von Produkten und Systemen hinreichend zu gestalten, weil ihnen oft ökonomische Aspekte entgegenstehen. Deshalb ist eine Sicherheitsstruktur notwendig, die Mindeststandards der Technischen Sicherheit am Markt etabliert und sich dabei staatlicher Aufsicht und wirkungsvoller Sanktionen bedient.

Hierzu sind grenzüberschreitende Vereinbarungen auf staatlicher Ebene unverzichtbar.

7 Schlussbemerkung

Der Verein Deutscher Ingenieure sieht sich aufgrund seiner interdisziplinären Fachkompetenz aufgerufen, diesen Prozess der sicherheitstechnischen Erkenntnis einzuleiten und zu fördern. Das hier vorgelegte Papier bildet die Grundlage für das daraus herzuleitende interdisziplinäre sicherheitsmethodische Konzept.

Die Darstellung dieses sicherheitsmethodischen Konzepts soll einer breiteren Fachöffentlichkeit zeigen, wie Technische Sicherheit erzeugt wird und welche methodischen Ansätze dafür erforderlich sind. Die gezeigten Wege sind realistisch und bei konsequentem, ethisch reflektiertem Handeln der interdisziplinär beteiligten Fachleute machbar.

Wichtig ist eine Vertrauensbasis zwischen Gesellschaft und Technik, die nur im offenen, ehrlich geführten Diskurs miteinander erreicht werden kann. Die feststellbare Technikfeindlichkeit eines untechnischen Publikums muss durch laienverständliche Unterrichtung über Risiken im Umgang mit technischen Erzeugnissen abgebaut werden. Dies wiederum kann aber nur erfolgreich geschehen, wenn zunächst Begriffe und Methoden auf dem Felde der Sicherheitstechnik unter den Fachleuten interdisziplinär harmonisiert und gesichert darstellbar sind.

Ebenso wie die allgemeine Technik bedarf auch die Sicherheitstechnik generalistischer Konzepte für interdisziplinäres Vorgehen sowie geeigneter systemtechnischer Managementverfahren. Hierzu bedarf es noch großer Anstrengungen im Raum der Wissenschaft und der Wirtschaft.

Die Schritte, die die Kommission und der Rat der Europäischen Union (EU) mit Einführung des „Neuen Konzepts“ und des „Gesamtkonzepts“ unternommen haben, führen gewiss in die richtige Richtung.

Sie weisen aber insbesondere in den Industriebereichen, in denen der EG-Prüfung der betreffenden Produkte keine Systemprüfung durch eine staatliche Stelle nachgeschaltet ist, mit ihrer Schwerpunktsetzung auf freien Warenverkehr innerhalb der EU in bestimmten Sektoren deutliche Schwächen auf, was die Technische Sicherheit betrifft, und bleiben somit zum Teil weit hinter der Wirksamkeit des abgelösten, historisch und bedarfsgerecht gewachsenen Systems zurück.

Diese Schwächen, die den mit Sicherheitsfragen befassten Experten bereits bei der Einführung bekannt waren, sind vielfältig und die Europäische Kommission bessert zurzeit nach.

Neben den produktbezogenen Richtlinien gilt die „Richtlinie über die allgemeine Produktsicherheit“ 2001/95/EG vom 03.12.01 (veröffentlicht im Amtsblatt Nr. L 011 vom 15.01.02); diese regelt, dass alle Produkte, die innerhalb des Europäischen Wirtschaftsraums in Verkehr gebracht werden, sicher sein müssen. Wie dies sicherzustellen ist, bedarf weiterer Regelung – und zwar nicht nur im Bereich des Sicherheitsrechts, sondern vor allem auf dem Sachgebiet der Sicherheitstechnik selbst.

Alle betroffenen und interessierten Personen und Institutionen sind hiermit aufgerufen, sich an der weiteren Gestaltung eines interdisziplinär anwendbaren, sicherheitsmethodischen Konzepts und dessen Umsetzung zu beteiligen.

Mandat und VDI-Gremien

Das Präsidium und der Wissenschaftliche Beirat des VDI haben den interdisziplinär besetzten Ausschuss „Technische Sicherheit“ mit der Zielsetzung eingesetzt, den Sachstand zu den unterschiedlichen Vorgehensweisen und Konzepten zur Erreichung von technischer Sicherheit in allen Branchen und Ingenieurdisziplinen transparent darzustellen und mögliche Handlungsbedarfe aufzuzeigen. Mit dieser Denkschrift hat der Ausschuss seine Erkenntnisse mit Zustimmung der VDI-Gremien niedergelegt. Der VDI lädt die Fachöffentlichkeit ein, sich an der Diskussion dieser Erkenntnisse und der Deckung der aufgezeigten Handlungsbedarfe aktiv zu beteiligen.

In dem VDI-Ausschuss „Technische Sicherheit“ haben nachfolgend aufgeführte Personen kontinuierlich mitgewirkt:

Eschenfelder, Dieter, Dipl.-Ing., Düsseldorf
Gelfort, Eike, Dr. rer. nat., Köln
Graßmuck, Jochem, Dipl.-Ing., Berlin
Pilz, Wolf-Dieter, Dipl.-Ing., Gerolsbach (Vorsitzender)
Schulz-Forberg, Bernd, Prof. Dr., Berlin (stellvertretender Vorsitzender)
Schweinsberg, Ralf, Bonn
Wilpert, Bernhard, Prof. Dr. Dr. h. c., Berlin

Darüber hinaus haben zeitweise weitere Experten aus unterschiedlichen Branchen beratend mitgewirkt.

Hinweis zu den in dieser VDI-Denkschrift verwendeten Begriffsbestimmungen:

Die interdisziplinäre Zielrichtung dieser VDI-Denkschrift bringt es mit sich, dass die hierin verwendeten Begriffe in den verschiedenen technischen und nichttechnischen Fachdisziplinen und Anwendungsgebieten in gleicher Ausprägung zu verstehen sind. Allerdings erweisen sich die in den verschiedenen Technikfeldern gängigen Begriffsbestimmungen zur Sicherheitstechnik als zu unterschiedlich, als dass sie diesem Anspruch gerecht werden könnten. Der VDI-Arbeitskreis „Technische Sicherheit“ hat deshalb ein datenbank-gestütztes Glossar eingerichtet, in welches sich die zum Verständnis dieser Denkschrift erforderlichen Begriffsbestimmungen einpflegen lassen[4].

[4] Die betreffende Datenbank, die zur Zeit noch nicht abschließend bearbeitet ist, ist unter folgender Internet-Adresse einsehbar:

URL: www.tes.bam.de/vdi

Unter Beachtung von Groß- und Kleinschreibung gelten die folgenden Zugangsdaten:

Login: VDI
Passwort: Positionspapier

Verein Deutscher Ingenieure e.V.
VDI Technik und Wissenschaft
VDI-Ausschuss Technische Sicherheit
Postfach 10 11 39
40002 Düsseldorf

Telefon +49 (0) 211 62 14-2 96
Telefax +49 (0) 211 62 14-1 81
technik-und-wissenschaft@vdi.de

9.07/1.000