Gesellschaftliche Risikokontrolle

Risikooptimierung kontra Risikobegrenzung

Timm Grams, Fulda

Der folgende sehr persönlich gehaltene Exkurs handelt vom Thema „Risikoakzeptanz“ im Anschluss an [1, Abschnitt 12.6]. Er enthält längere Auszüge aus dem Aufsatz [2]. Herausgestellt werden zwei grundlegende Denkstile der staatlichen Risikokontrolle: Risikooptimierung *und* Risikobegrenzung. *Es gibt Bestrebungen, der Philosophie der Risikobegrenzung Allgemeingültigkeit zuzumessen und sie zur Grundlage einer allumfassenden Risikokultur zu machen [3]. Die Fragwürdigkeit dieses Ansatzes wird hier herausgestellt. Im Zuge der Deregulierung und Reduzierung von Kontrollhierarchien spielt demgegenüber die Risikooptimierung eine zunehmende Rolle. Beispiel dafür ist das neue Konzept der EU [4].*

Inhalt

Einführung: Drei Bedeutungen des Begriffs Sicherheit ... 1

Elementare Risikobewältigung durch Klassifizierung ... 2

Der Denkstil der *Risikooptimierung* ... 3

Die Philosophie der *Risikobegrenzung* ... 4

Das subjektive Risiko ... 5

Risikokulturen: Vertrauen und Misstrauen in die Technik ... 7

Allumfassende Sicherheitskultur: eine Schimäre? ... 9

Risikooptimierung - ein praktikabler Ansatz der staatlichen Risikokontrolle ... 10

Das neue Konzept der Europäischen Gemeinschaft ... 12

Risikooptimierung in der Normung ... 12

Literatur + Links ... 13

Einführung: Drei Bedeutungen des Begriffs Sicherheit

Kontroversen haben meist viel stärkere Ursachen als in den Begriffen und ihrer Verwendung zum Ausdruck kommt. Unterschiede in der Begriffsverwendung sind Symptome, nicht Ursachen. Und die Ursachen interessieren mich, also das was hinter den Begriffen und ihren Bedeutungen verborgen ist. Mit geht es hier insbesondere um die Kernbegriffe der Sicherheitstechnik. Sie treten in verschiedenen Bedeutungen auf. Für den Begriff der „Sicherheit“ lassen sich wenigstens drei Bedeutungvarianten identifizieren.

Durch rationale und intersubjektiv nachprüfbare *Analyse* lassen sich die *Denkstile*, die hinter den unterschiedlichen Begriffen stecken, ans Tageslicht bringen. Dadurch wird ein Konsens über die Grenzen der Sicherheits- und Risikokulturen hinweg nicht automatisch erreicht. Aber eins kann man erreichen: Die Landschaft, in der wir uns bewegen, wird besser sichtbar, der Nebel verzieht sich, und wir können den eigenen Weg ausmachen. Und damit ist das Maximum dessen erreicht, was meines Erachtens erreichbar ist. Ich suche also nicht unbedingt nach dem Konsens, sondern bin auch schon mit dem *rationalen Dissens* zufrieden. Die folgenden Bedeutungsvarianten der (technischen) Sicherheit sollen näher betrachtet werden.

Sicherheit$_1$: Ein Produkt gilt als sicher, wenn es die Sicherheitsspezifikation erfüllt, wenn es also beispielsweise im Fehlerfall einen *als sicher spezifizierten Zustand* annimmt [5, Teil 1 und Teil 4]. Nehmen wir zum Beispiel einen Stromkreis, dessen

Leitungen so dimensioniert sind, dass alle Ströme kleiner als sechzehn Ampère dem sicheren Zustand zuzurechnen sind. Das ist eine Klassenbildung im mathematischen Sinn. Bei Kurzschluss möge eine Sicherung dafür sorgen, dass dieser Zustand nicht für unzuträglich lange Zeit verlassen wird. Der Begriff Sicherheit$_1$ hat grundsätzlich qualitativen Charakter und er entwickelt seine Bedeutung im Rahmen eines Klassifikationssystems.

Sicherheit$_2$: Die Sicherheit$_2$ wird wie die technische Zuverlässigkeit mittels Kenngrößen - also grundsätzlich quantitativ - beschrieben, nur dass hier nicht die funktionale Korrektheit (Erfüllung der funktionalen Spezifikation) sondern die *sicherheitsbezogene Korrektheit* (Erfüllung der Sicherheitsspezifikation) durch Wahrscheinlichkeitsaussagen bewertet wird [5, Teil 2 und Teil 4]. Beispiel für eine Aussage zur Sicherheit$_2$: Die mittlere Zeit bis zu einer Verletzung der Sicherheitsspezifikation - wenn beispielsweise beide Bremskreise eines Zweikreisbremssystems gleichzeitig versagen - beträgt 10^6 Jahre. Solche Zahlen bilden die Grundlage der technischen Risikoanalyse.

Sicherheit$_3$: Dieser Sicherheitsbegriff basiert auf einer Risikoanalyse der Gesamtanlage. Es gehen also sämtliche Komponenten, die Umwelt und die Betriebsbedingungen sowie die möglichen Schäden in die Analyse ein. Für dieses Risiko wird dann ermittelt, ob es unterhalb eines gewissen Grenzrisikos liegt oder nicht. Im ersten Fall ist die Anlage sicher, im zweiten nicht [6, Teil 2]. Als Beispiel zur Sicherheit$_3$ nehmen wir für das Verkehrsmittel Bahn einmal ein Grenzrisiko von hundert Toten pro Jahr an, bezogen auf das Gebiet der Bundesrepublik Deutschland. Gemessen am Verkehrsaufkommen und an den vielen tausend Toten im Straßenverkehr ist das ein zwar trauriges aber anscheinend doch akzeptables Risiko. Unfälle wie der von Eschede am 3. Juni 1998, wo 101 Tote zu beklagen waren, kommen selten vor, so dass trotz solcher Unfälle diese Grenze im Mittel wohl nicht überschritten wird. Die Bahn könnte nach dieser Festsetzung als sicheres Verkehrsmittel gelten.

Elementare Risikobewältigung durch Klassifizierung

Risikobewusstsein kam erst ziemlich spät in die Welt. Es ist eine Hervorbringung der Moderne. Aber auch ohne Risikobewusstsein sind wir den Risiken des Lebens nicht schutzlos ausgeliefert. Angeborene oder früh erlernte Mechanismen leiten uns, das Richtige, das weniger Gefährliche zu tun. Eine grundsätzliche Fähigkeit ist die Unterscheidung in Gut und Böse, in Vorteilhaftes und Schädliches. Wir tragen die *Neigung zur Klassifizierung* und zur Kategorienbildung in uns. So schützt uns die Natur vor Risiken.

Eine Theorie der Welt muss mit dem Trennen anfangen, nicht mit dem Messen und Abwägen, sagt beispielsweise die Anthropologin Mary Douglas (1986). Was den Sicherheitsbegriff in der ersten Bedeutungsvarianten angeht, basiert er auf dem grundlegen Mechanismus der Klassifizierung.

In Richtlinien, Normen und in Firmenunterlagen sind Klassifizierungsschemata festgelegt, beispielsweise das System der *Anforderungsklassen:* Im Rahmen eines organisierten sozialen Prozesses wird bestimmt, welchem Risikobereich eine neu zu entwickelnde Einrichtung zuzuordnen ist. Aus dieser Klassenzuordnung ergeben sich dann die zu ergreifenden technischen und organisatorischen Maßnahmen. Diese sicherheitstechnischen Festlegungen sind Bestandteil der *Sicherheitsspezifikation*.

Bei Unfallanalysen stößt man immer wieder darauf, dass im Zuge der Klassifizierung etwas schief gelaufen ist. Gut dokumentiert ist das beim Challenger-Unglück (28. Januar 1986) und beim missglückten Jungfernflug der Ariane 5 (4. Juni 1996).

Im Fall Challenger war es ein Paar Dichtungsringe, das *als wirksame Redundanz klassifiziert* war. Diese Einstufung wurde wohl irgendwann zurückgenommen, sie blieb aber in den Köpfen der beteiligten Ingenieure und Manager wirksam. Das führte neben anderem zu der verhängnisvollen Startfreigabe. Die Analyse des Unglücks zeigte, dass die Redundanz tatsächlich nicht wirksam war und das Versagen beider Dichtungsringe zur Katastrophe führte.

Im Tagungsband des 7. Elektrotechnik-Kolloquiums [7] habe ich die elementare Risikobewältigung durch Klassifizierung ausführlicher dargestellt.

Der Denkstil der *Risikooptimierung*

Der Sicherheitsbegriff in der zweiten Bedeutung hängt eng mit dem zweiten Grundmuster zusammen, nach dem wir die Welt ordnen: Vergegenwärtigung der Zukunft mit Hilfe von Wahrscheinlichkeitsaussagen.

Die Daseinsbewältigung durch Klassenbildung ist elementar und unverzichtbar. Aber sie ist dem Wesen nach statisch und konservativ. In der Renaissance entsteht mit dem aufblühenden Handel und dem damit einhergehenden gesellschaftlichen Wandel der Wunsch, die Zukunft zu kontrollieren.

In einer 1662 erschienenen wegweisenden Veröffentlichung des Pariser Port-Royal-Klosters findet sich der Satz: Die Angst vor einem Schaden sollte nicht nur proportional zur Größe des Schadens, sondern auch zur Wahrscheinlichkeit des Ereignisses sein [8]. Damit ist der moderne Risikobegriff in der Welt: *Risiko* quantifiziert die Angst vor einem möglichen Schaden und ist definiert als *Schadenserwartungswert*.

Im einfachsten Fall, wenn es nur um ein mögliches Ereignis mit dem Schaden x geht, das mit der Wahrscheinlichkeit p eintreten kann, ist das Risiko R gegeben durch die Formel $R = p \cdot x$. Anstelle mit Wahrscheinlichkeiten wird in der Technik auch mit Häufigkeiten gerechnet. Dadurch wird klar gemacht, dass sich die Eintrittswahrscheinlichkeit im Allgemeinen auf einen festen Zeitraum bezieht.

Der Begriff des Risikos hat damit zu tun, dass wir selbst Entscheidungen treffen können. Erst die Möglichkeit, Schäden zu vermeiden, hat uns Risiken eingebracht. Mit der Erfindung des Regenschirms kam das Risiko nass zu werden in die Welt (TIME, 28. July 2003).

Mit der Einführung des Risikobegriffs entsteht ein neuer Denkstil. Man kann ihn als *Risikooptimierung* bezeichnen: Wir können Entscheidungsalternativen gegeneinander abwägen und diejenige wählen, die mit dem geringsten Risiko verbunden ist.

Beispiel Kraftfahrzeugbremse [5, Teil 3]: Bei einem Einkreisbremssystem eines Automobils wird jeder Ausfall als sicherheitsbezogen *klassifiziert*. Aus Statistiken möge bekannt sein, dass der Bremskreis innerhalb der gesamten Betriebsdauer mit der Wahrscheinlichkeit $p = 10^{-2}$ ausfällt. Mit einem solchen sicherheitsbezogenen Ausfall sei der Schaden x verbunden. Das auf die Betriebsdauer bezogene Risiko eines Bremsversagens wäre bei einem Einkreisbremssystem dann gleich $R = p \cdot x = 10^{-2} \cdot x$. Bei einem Zweikreisbremssystem liegt ein sicherheitsbezogener Ausfall nur vor, wenn beide Bremskreise ausfallen. Die Wahrscheinlichkeit eines solchen sicherheitsbezogenen Ausfalls möge gleich $2 \cdot 10^{-8}$ sein. Das Risiko ist nun gleich $2 \cdot 10^{-8} \cdot x$. Es ist um den Faktor $2 \cdot 10^{-6}$ niedriger als bei der Einkreisbremse.

Tabelle 1 Gegenüberstellung der Sichtweisen auf das Risiko

Klassifizierung	*Risikobewertung*
Statisch	Dynamisch
Konservativ	Progressiv
Deterministisch	Probabilistisch
Ergebnis eines sozialen Prozesses	Analyseergebnis
Ermessensabhängig	Objektiv
Erfahrungsspeicher	Vergegenwärtigung der Zukunft
Qualitativ	Quantitativ

Die sicherheitsbezogenen Ausfallwahrscheinlichkeiten sind Kenngrößen der Sicherheit$_2$. Und allein diese Kenngrößen sind im eben durchgeführten Risikovergleich maßgebend. Die nur schwer erfassbare Schadenshöhe x spielt erst dann eine Rolle, wenn man die Risikoreduktion mit anderen Zielgrößen, beispielsweise dem finanziellen Aufwand, vergleichen muss.

Tabelle 1 zeigt eine Gegenüberstellung der beiden Grundmuster, nach denen wir die Welt ordnen: Klassifizierung und Risikobewertung. Sicherheit$_1$ stellt eine prägnante und anschauliche Abgrenzung im Zuge der elementaren Klassifizierung dar. In dieser Bedeutung gehört er zur linken Seite der Tabelle 1. Die Kenngrößen der Sicherheit$_2$ gehen in die Risikobewertung von technischen Einrichtungen ein. Sicherheit in der zweiten Bedeutung gehört zum Denkstil der *Risikooptimierung* und wird der rechten Seite zugeordnet. Um Sicherheit$_3$ geht es erst im folgenden Abschnitt.

Die Philosophie der *Risikobegrenzung*

Zu den Aufgaben des Staates gehört der Schutz der Öffentlichkeit vor Gefahren. Er setzt den rechtlichen Rahmen und legt die Schutzziele fest. Im Zuge des Aufbaus der Kernenergiewirtschaft wurde ein Ansatz diskutiert, den Chauncey Starr in seinem einflussreichen Aufsatz von 1969 vertreten hat [9]. Er fragt, welchen Preis unsere Gesellschaft bereit ist, für die Sicherheit zu bezahlen. Er stellt die Risiken, die freiwillig von den Menschen übernommen werden, denjenigen gegenüber, die ihnen aufgezwungen werden.

Das Konzept von Starr zieht als Maßzahl das objektive Risiko heran. Die subjektive Komponente wird dadurch berücksichtigt, dass die akzeptierten Risiken je nach Standpunkt variieren. Er stellt fest, dass wir uns ungern das antun lassen, was wir ohne zu Zögern uns selbst zumuten. Diese Variation des akzeptierten Risikos wird für Starr durch den Faktor 1000 abgedeckt.

Er kommt daraufhin zum Schluss, dass die Gesellschaft sehr wohl eine Antwort auf die Frage „Wie sicher ist sicher genug?“ finden kann.

Nach diesem Konzept kann sich die Gesellschaft für eine bestimmte Technik auf einen Wert für das *Grenzrisiko* - das ist das größte gerade noch akzeptable Risiko - verständigen. Damit wird entscheidbar, ob eine Anlage sicher ist oder nicht: Ergibt

die Risikoanalyse, dass das Grenzrisiko nicht überschritten wird, ist *Sicherheit* gegeben, andernfalls *Gefahr*. Mit Sicherheit ist Sicherheit_3 gemeint.

Wir wollen den Denkstil, der hinter Starrs Konzept steht, als *Risikobegrenzung* bezeichnen. Er tritt an die Stelle des Denkstils der Risikooptimierung.

Selbstverständlich setzt eine Risikoanalyse eine Klassifizierung von Schäden und Ereignissen voraus. Aber über den Begriff des Grenzrisikos wird eine Klassifizierung - die Unterscheidung nach Sicherheit und Gefahr - auf höherer Ebene angestrebt. Wir haben es also mit einer Folge von Betrachtungsweisen zu tun: Klassifizierung → Quantifizierung → Klassifizierung. Es ist sofort einsehbar, dass mit der zweiten Klassifizierungsstufe die Optimierung wieder aus dem Blickfeld gerät. So fängt man sich auf hoher Ebene die Unbeweglichkeit der Klassifizierung wieder ein.

Das wird in der DIN VDE 31 000/2 auch gar nicht verhehlt [6, Teil 2]. Sie macht gewissermaßen eine Rolle rückwärts: „Da sich das Grenzrisiko nur qualitativ beschreiben lässt, müssen sicherheitstechnische Festlegungen ... getroffen werden“. Dabei „beschränkt man sich im allgemeinen auf spezielle Angaben und setzt voraus, dass die generellen sicherheitstechnischen Grundsätze eingehalten werden“. Man landet bei der ursprünglichen Klassifizierung, also auf der linken Seite der Tabelle 1, und damit beim Sicherheitsbegriff in der ersten Bedeutungsvariante. Nichts ist gewonnen.

Dem Konzept der Risikobegrenzung stehen weitere Hinderungsgründe entgegen. Dazu gehören:

1. Die Subjektivität der Risikobewertung (siehe den folgenden Abschnitt) wird durch Starrs Risikogrenze nicht adäquat berücksichtigt. Das Konzept von Starr, das auch heute noch von Ingenieuren vertreten wird und das auch der Norm DIN VDE 31000/2 zu Grunde liegt, bleibt weit hinter dem zurück, was Daniel Bernoulli vor über zweihundert Jahren dazu gesagt hat. Und seither ist dem einiges hinzugefügt worden [10], [11].
2. Unterschiede in der Risikobewertung werden durch Gruppenbildung und das Entstehen von sich voneinander abgrenzenden *Risikokulturen* noch verstärkt (siehe den folgenden Abschnitt). Für die eine Gruppe ist das Risiko tragbar, solange nicht das Gegenteil bewiesen ist, und für die andere kann es nie genug Sicherheit geben.

Die Fiktion hat aber dennoch ihre Auswirkungen: Sie ist geeignet, die Weiterentwicklung von Normen mit ihren (qualitativen) sicherheitstechnischen Festlegungen im Zuge der Risikooptimierung und des technischen Fortschritts zu behindern. Nach der Philosophie der Risikobegrenzung kann man sich Fortschreibungen mit dem Argument sparen, dass man ja bereits unterhalb des im Konsens festgelegten Grenzrisikos liege. Noch nicht einmal eine Zugkatastrophe wie die von Eschede wäre dann ein Grund, nach den Ursachen zu forschen und die Technik zu verbessern. Aber spätestens im Ernstfall ist es mit dem Grenzrisiko-Denken aus, wie man sieht. Und mit dem Grenzrisiko-Denken fällt der Sicherheitsbegriff in der dritten Bedeutung.

Das subjektive Risiko

Der Fahrer schätzt das Risiko beim Überholen anders ein als sein Beifahrer. Hersteller und Betreiber eines Kernkraftwerks oder einer Mobilfunkanlage werden mit den Bürgerinitiativen nicht über die Risikobewertung einig. Unterschiede in der

Risikowahrnehmung trennen die Parteien. Und diese Unterschiede haben Gründe. Untersuchungen haben ergeben, dass die *Risikoakzeptanz* mit den Faktoren

- Bekanntheit einer Gefahr,
- Freiwilligkeit im Eingehen eines Risikos und
- Beeinflussbarkeit des Risikos

wächst [1, Abschnitt 12.6].

Niklas Luhmann unterscheidet ín diesem Zusammenhang zwischen dem Entscheider einerseits und dem ausschließlich Betroffenen anderseits. Und er spricht nur im Fall des Entscheiders von *Risiko:* Ein Risiko übernimmt jemand, der selbst entscheiden kann. Dem ausschließlich Betroffenen dagegen droht *Gefahr* [12].

Risiko, berechnet als mathematischer Erwartungswert objektiver Schäden, kann personenabhängigen und situationsabhängige Aspekte nicht erfassen. Daniel Bernoulli löste dieses Problem um 1783, indem er eine subjektive Bewertungsfunktion einführte. Sei s eine solche subjektive Bewertungsfunktion für die Schwere (severity) von Schäden: $s = s(x)$. Das *subjektive Risiko* ist definiert als Erwartungswert des subjektiven Schadens, also $R = p \cdot s(x)$. Für $s(x) = x$ ergibt sich die Formel des vorigen Abschnitts für das *objektive Risiko*.

Die Forschung zur Risikowahrnehmung hat eine Reihe von Vorstellungsmustern identifizieren können, die in der Bevölkerung zur Bewertung von Risiken benutzt werden. Der Beitrag von Ortwin Renn zum 7. Fuldaer ET-Kolloquium geht der Frage nach, welche Typen von Situationen und Objekten den verschiedenen Risikomustern zuzuordnen sind. Im Folgenden habe ich Ausschnitte aus seiner Darstellung verwendet [7].

Risiko als unmittelbare Bedrohung: Wenn wir uns im Bereich der Wahrnehmung von seltenen Zufallsereignissen befinden, spielt die Wahrscheinlichkeit eine geringe Rolle: die Zufälligkeit des Ereignisses ist der eigentliche Risikofaktor. Beispiele für Risikoquellen, die in diese Kategorie fallen, sind große technische Anlagen, wie etwa Kernkraftwerke, Flüssiggaslager, chemische Produktionsstätten und andere menschlich geschaffene Gefahrenpotentiale, die im Ernstfall katastrophale Auswirkungen auf Mensch und Umwelt haben können. Die Vorstellung, das Ereignis könne zu jedem beliebigen Zeitpunkt die betroffene Bevölkerung treffen, erzeugt das Gefühl von Bedrohtheit und Machtlosigkeit.

Risiko als Schicksalsschlag: Natürliche Katastrophen werden meist als unabwendbare Ereignisse angesehen, die zwar verheerende Auswirkungen nach sich ziehen, die aber ... dem menschlichen Zugriff entzogen sind. Sie sind in der Terminologie Niklas Luhmanns Gefahren, denen man ausgesetzt ist. Natürliche Belastungen und Risiken werden als vorgegebene, quasi unabdingbare Schicksalsschläge betrachtet, während technische Risiken als Konsequenzen von Entscheidungen und Handlungen angesehen werden. Diese Handlungen werden nach anderen Maßstäben bewertet und legitimiert... Im Gegensatz zur Situation der technischen Bedrohung ist die Zufälligkeit des Ereignisses nicht der Angst auslösende Faktor.

Risiko als Herausforderung der eigenen Kräfte: Wenn Reinhold Messner ohne Atemgerät die höchsten Berge der Welt bezwingt, obwohl das Risiko, dabei zu Schaden zu kommen, beachtlich ist, wenn Autofahrer wesentlich schneller fahren, als es die Polizei erlaubt, wenn Menschen sich mit Plastikflügeln in den Abgrund stürzen ... gehen Menschen Risiken ein, um ihre eigenen Kräfte herauszufordern und den Triumph eines gewonnenen Kampfes gegen Naturkräfte oder andere Risikofaktoren

auszukosten. Nach Felix von Cube sind all das Handlungen im Gefolge des Sicherheitstriebs und dienen der „Umwandlung von Unsicherheit in Sicherheit“ [1, Abschnitt 12.2].

Risiko als Glücksspiel: Häufig werden mit Glücksspielen versteckte Verteilungsideologien (etwa todsicheres Wettsystem, magische Glückszahlen oder ausgleichende Gerechtigkeit) verbunden. So glauben etwa 47 % aller Amerikaner, dass es besondere Glücksnummern gibt, die bestimmten Mitspielern eine bessere Gewinnchance vermitteln. Wird das Zufallsprinzip jedoch anerkannt, dann ist das wahrgenommene Konzept der stochastischen Verteilung von Auszahlungen dem technischen Risikokonzept, also dem Konzept des objektiven Risikos, am nächsten.

Risiko als Frühindikator für Gefahren: Mit der zunehmenden Berichterstattung über Umweltverschmutzung und deren Langzeitwirkungen auf Gesundheit, Leben und Natur haben wissenschaftliche Risikoberechnungen die Funktion von Frühwarnindikatoren erhalten. Nach diesem Risikoverständnis helfen wissenschaftliche Studien schleichende Gefahren frühzeitig zu entdecken und Kausalbeziehungen zwischen Aktivitäten oder Ereignissen und deren latente Wirkungen aufzudecken. Beispiele für dies Verwendung dieses Risikobegriffs findet man bei der kognitiven Bewältigung von geringen Strahlendosen, Lebensmittelzusätzen, chemischen Pflanzenschutzmitteln oder genetischen Manipulationen von Pflanzen und Tieren. Die Wahrnehmung dieser Risiken ist eng mit dem Bedürfnis verknüpft, für scheinbar unerklärliche Folgen (z.B. Robbensterben, Krebserkrankungen von Kindern, Waldsterben, etc.) Ursachen ausfindig zu machen.

Risikokulturen: Vertrauen und Misstrauen in die Technik

Eine herausragende Rolle für die Risikowahrnehmung und die damit zusammenhängende Ausprägung der subjektiven Bewertungsfunktion *s* spielen die Wertvorstellungen und sozialen Beziehungen von gesellschaftlichen Gruppierungen.

Als *Eigenwert* wird in der Soziologie ein Satz von kohärenten Wertvorstellung innerhalb einer Gruppe oder einer Organisation bezeichnet. Diese Wertvorstellungen sind Gleichgewichtszustände, die gruppenstabilisierend und kulturbildend wirken. Wertvorstellungen zusammen mit den damit verbundenen sozialen Beziehungen und Interaktionsmustern werden in der pluralistischen Kultursoziologie von Thompson, Ellis und Wildavsky *Way of Life* genannt [13].

Eigenwerte konstituieren und stabilisieren sich im Rahmen von zyklisch geschlossenen Kausalfolgen. Hier ist ein Beispiel für eine solche Kausalfolge: *Misstrauen* in die Technik lässt einen nach möglichst vielen Ursachen für deren Nichtfunktionieren suchen. Folglich werden auch menschliche Faktoren dem technischen System zugeordnet. Das ist schon deswegen nicht abwegig, weil technische Systeme durch schlechtes Design Bedienfehler durchaus provozieren können. Und in der Folge wird man durch diese umfassende *Zurechnung* (hier erkennt man wieder die zentrale Rolle der Klassifizierung) auch vermehrt Beispiele von Nichtfunktionieren der Technik finden. Das wiederum verstärkt das Misstrauen in die Technik. So wird der Kreis geschlossen. Und er ist stabil.

Andererseits wird - bei einem anderen Way of Life - ein grundsätzliches *Vertrauen* in die Technik nicht erschüttert, so lange sich Fehler den Personen - und nicht der Technik - zurechnen lassen, beispielsweise dem betrunkenen Kapitän der Exxon Valdez beim Tankerunglück vor Alaska im Jahr 1989. So lässt sich die Technik selbst als funktionierend darstellen. Die folgende Zeitungsmeldung vom 14.2.1995 über

Unfälle in der Zivilluftfahrt ist ebenfalls Ausdruck dieser Haltung: „Als Unsicherheitsfaktor Nummer eins erwies sich auch 1994 wieder der Mensch: Nicht weniger als 31 der 47 Unfälle sind auf menschliches Versagen zurückzuführen und immerhin 16 auf das Wetter“.

Die anthropologische Kultursoziologie hat auf der Basis der Grid-Group-Typologie von Mary Douglas vier institutionalisierte Kulturen (Ways of Life) identifiziert [14]. *Grid* beschreibt in dieser Typologie den Grad, in dem das Leben eines Individuums durch äußere Vorschriften bestimmt ist; und *Group* besagt, inwieweit das Leben eines Individuums durch die Gruppenmitgliedschaft absorbiert und getragen wird. Den vier Kulturen lassen sich spezifische Technik- und Risikoeinstellungen zuordnen (Tabelle 2).

Das gesellschaftliche Zentrum ist dort, wo Macht und Einfluss konzentriert sind. Die beiden Kulturen des gesellschaftlichen Zentrums sind der *Marktindividualismus* (low grid/low group) und die Kultur der *Hierarchien* (high grid/high group). Hierarchische Institutionen findet man bei den Kirchen, in Industrieunternehmen und im Bereich von Politik und öffentlicher Verwaltung - in den Bürokratien großer Organisationen also. Dazu kontrastiert der Individualismus des Marktes, also das fortwährend auf private Profitmaximierung abgestellte Verhalten.

Tabelle 2 Kulturelle Ausprägungen des Umgangs mit der Angst (helle Felder: Technikvertrauen, dunkle: Misstrauen gegenüber der Technik)

Grid-Group-Koordinaten	*Low Group*	*High Group*
High Grid	FATALISMUS Abwesenheit einer Risikobewertung	HIERARCHIE Philosophie der *Risikobegrenzung*
Low Grid	INDIVIDUALISMUS Maxime der *Risikooptimierung*	EGALITARISMUS Dogma des *Nullrisikos*

Marktindividualistische Kulturen sind in ihren technisch-ökologischen Funktionserwartungen uneingeschränkt optimistisch. Darüber hinaus werden technische Innovationen als Risiken im Luhmannschen Sinne, also mit Blick auf eigene Entscheidungen wahrgenommen. Das sind die Bedingungen für Technikvertrauen und für den Denkstil der Risikooptimierung.

In den hierarchischen Organisationen wird das Vertrauen in Technik durch Expertenkonsens ermöglicht. Die auch hier dominierende Risikoperspektive und deren Chancenorientierung fördert dabei Vertrauen in Experten. Wegen besonderer Sicherheitsbedürfnisse tendieren die Organisationen zu „Technikvertrauen unter Vorbehalt“ und zum Denkstil der Risikobegrenzung. Dieser Denkstil kommt auch den in Großorganisationen vorherrschenden Bestrebungen entgegen, Dinge möglichst dauerhaft und verlässlich zu regeln.

Die *fatalistischen* und die *egalitaristischen* Kulturen sind am gesellschaftlichen Rand angesiedelt (high grid/low group bzw. low grid/high group). Das ist abseits von Macht und Einfluss. Wer von Technikfolgen und vom Wandel des Arbeitsmarkts betroffen und nur schlecht organisationsfähig ist, wird fatalistische Verhaltensweisen zeigen. Egalitarismus ist bei Protestbewegungen und Sekten zu finden, wie beispielsweise bei den Amish. Hier steht die Gleichheit der Mitglieder der Gruppe obenan. Machtkonzentration wird abgelehnt.

Von den Protestbewegungen und den Bürgerinitiativen, die sich durch den Verzicht auf zentrale Führerschaft und durch sektenartige Abgrenzungsmechanismen auszeichnen, wird Technik als bedrohlich wahrgenommen; sie stellt in erster Linie Gefahr dar. Das fördert das Technikmisstrauen dieser Bewegungen.

Angstkommunikation alarmiert die Gesellschaft und sorgt gleichzeitig für den Gruppenzusammenhalt. Der Umgang mit dem Risiko ist kompromisslos nach der Devise „Sicherheit gibt es nie genug“. Einzig das *Nullrisiko* ist akzeptabel.

Wer von Technikfolgen betroffen ist, wer mit Dequalifikationswellen, ökologisch bedingten Gesundheitsbelastungen und Störfällen fertig werden muss, der wird eher zu fatalistischem Verhalten und zu Misstrauen neigen; Risiko ist ihm kaum einer Betrachtung wert.

Mary Douglas und Aaron Wildavsky [14] drücken die Tatsache, dass das gesellschaftliche Zentrum der Technik vertraut und der gesellschaftliche Rand ihr misstraut, so aus: „The Center is Complacent - The Border is Alarmed“.

Frau Dr. Hella Gläser vom Sicherheitstechnischen Dienst der Stadt Fulda hat in einem Diskussionsbeitrag anlässlich des 7. Fuldaer Elektrotechnik-Kolloquiums zum Thema „Risiko - Unser Umgang mit der Angst“ den Konflikt zwischen dem gesellschaftlichen Zentrum und dem Rand - hier eine Protestbewegung gegen den Mobilfunk - zur Sprache gebracht [7]: „Wie kommt man weg von der Forderung der Bürger nach dem Nullrisiko? Indem man dem Menschen mehr Handlungsmöglichkeiten gibt? ... Die Leute wollen das Nullrisiko. Wir haben versucht, die Antenne weit weg zu legen. Aber sie ist weiterhin vorhanden, und damit die Angst. Beteiligung bringt die Angst nicht weg.“

Darauf Prof. Dr. Klaus P. Japp, Soziologe an der Universität Bielefeld: „Das wundert mich nicht. Die Leute protestieren nicht wegen des Informationsdefizits. Auch bei Beteiligung bleiben sie nur Betroffene und werden nicht zu Entscheidern. Beteiligung ohne das Recht zu entscheiden bringt nichts.“

Auch wer nicht allen Details der hier ausgebreiteten pluralistischen Kulturtheorie folgen mag, wird ihrem zentralen Anliegen einige Sympathie entgegenbringen können: Diese Kulturtheorie stellt heraus, dass es so etwas wie *die* Kultur einer Nation gar nicht gibt. Die Unterschiede der politischen Einstellungen und Wertvorstellungen variieren innerhalb eines Landes oft stärker als zwischen verschiedenen Ländern.

Länder werden demnach durch miteinander konkurrierende politische Kulturen gestaltet. Und genau dieser Pluralismus, die Fluktuation und der Austausch zwischen den Kulturen sind unabdingbar für die Stabilität des Ganzen [11, S. 96 u. S. 215 ff.]. Daraus lässt sich folgern, dass sowohl das Vertrauen in die Technik sowie das Misstrauen gegenüber der Technik ihren Beitrag zur Stabilität der Gesellschaft leisten. Auf die richtige Balance kommt es an.

Allumfassende Sicherheitskultur: eine Schimäre?

Albert Kuhlmann greift in seinem Buch „Risikokultur“ den Faden von Chauncey Starr auf und spinnt ihn fort [3]. Er stellt die Philosophie der Risikobegrenzung in das Zentrum seiner Überlegungen zur Etablierung einer *allumfassenden Sicherheitskultur*. Das Vertrauen der Allgemeinheit in die Technik ist sein Ziel. Die Leute müssten nur „davon überzeugt werden, dass wir eindeutige Zulässigkeitsgrenzen für technische Risiken wollen, die von moralisch-ethischen Grundwerten getragen werden“. Für ihn sind es Fachkommissionen, die die Zulässigkeit von Risiken zu bestimmen haben. Risikokataster sollen dafür sorgen, dass die Risiken gleichmäßig auf das Volk verteilt werden.

Das Vorhaben der Entwicklung einer allgemeinen Sicherheitskultur überfordert das Instrumentarium des Ingenieurs. Es fängt schon damit an, dass wir uns schon nicht

über das *Ziel* für einer Sicherheitskultur einigen können. Der Gleichheitsgrundsatz (das *Equity Based Criterion* der britischen Health and Safety Executive, HSE) und das Prinzip vom größten Gesamtnutzen (*Benthams Prinzip* des „größten Glücks der größten Zahl“) lassen sich nicht auf einen Nenner bringen: Nach dem Gleichheitsgrundsatz ist das Individualrisiko, nach dem Gesamtnutzenkriterium das Kollektivrisiko zu minimieren. Der Ingenieur kann mit seinem Instrumentarium solche Konflikte nicht lösen.

Dazu kommt, dass das *Grenzrisiko-Denken* ungeeignet für die Begründung einer Sicherheitskultur ist. Dieses Denken verleugnet den erreichten Stand der Problembewältigung durch den Menschen, es ignoriert Erkenntnisse aus Psychologie, Soziologie und Kulturtheorie. Wichtiger noch ist, dass das Grenzrisikodenken die *Gefahr der Risikomaximierung* mit sich bringt. Dazu der Syndikus bei der Deutschen Bahn, Klaus-Dieter Wittenberg: „Zu hohe Sicherheitsauflagen können wegen der damit verbundenen Kosten dazu führen, dass der Betrieb von Eisenbahnen nach wirtschaftlichen Maßstäben eingestellt werden müsste, weil mit ihnen konkurrierende Systeme wegen geringerer Sicherheitsauflagen billiger produzieren können und damit am Markt überlegener sind. Es wird auch die Meinung vertreten, dass Risikogrenzwerte erarbeitet werden müssten und der Staat diese Grenzwerte festsetzen müsse“ [15]. Das risikoreichste Verkehrsmittel – vermutlich das Auto - wird so zum Maßstab gemacht!

Die „allumfassende Risikokultur“ trägt kaum verhüllte autoritäre Züge. Zwar werden immer wieder irgendwelche „moralisch-ethischen Grundwerte“ beschworen. Diese werden nirgendwo expliziert.

Eine allumfassende Risikokultur auf der Basis der Philosophie des Grenzrisikos steht im Widerspruch zum Pluralismus, der für die Demokratie so wichtig ist. Dem Verlangen nach *einer* Sicherheitskultur steht die Existenz mehrerer sehr stabiler Risikokulturen entgegen, wie im letzten Abschnitt gezeigt worden ist.

Risikooptimierung - ein praktikabler Ansatz der staatlichen Risikokontrolle

Der Staat ist nun eine dieser Großorganisation mit hierarchisch organisierten Bürokratien, von denen im vorigen Abschnitt die Rede war. Wie löst die Gesellschaft das Problem der Risikokontrolle, das im Abschnitt 6 zwar aufgeworfen aber nicht gelöst worden ist?

Angesichts der Konflikte zwischen den Risikokulturen wird es nicht gelingen, für irgendeine Technik mit hohem Gefährdungspotential ein für alle akzeptables Grenzrisiko zu definieren. Denn von welcher subjektiven Schadensfunktion s wäre auszugehen? Welche Kultur soll maßgebend sein?

Die kulturell geprägte subjektive Schadensfunktion s in der Risikoformel $R = p \cdot s(x)$ entzieht sich einer allgemeingültigen Festlegung. Nur eins kann man von ihr voraussetzen, nämlich, dass sie monoton wächst. Und natürlich liefert diese Funktion für nichtnegative x nichtnegative Werte $s(x)$. Insgesamt lässt sich daraus folgern, dass das Risiko mit dem absoluten Schaden wächst: je größer der Schaden x desto größer das Risiko R. Dasselbe gilt für die Schadenseintrittswahrscheinlichkeiten: je größer die Wahrscheinlichkeit p, desto größer das Risiko.

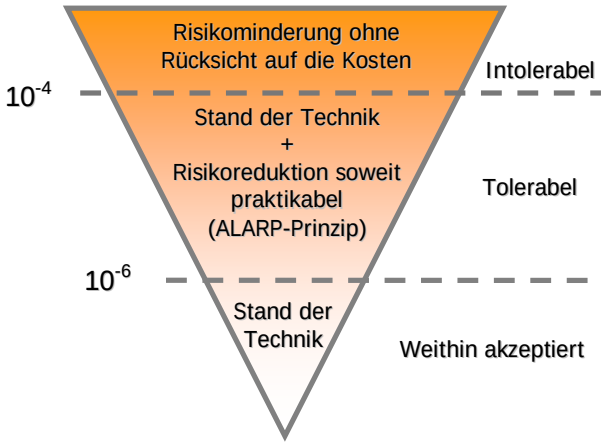

Bild 1 Orientierungsrahmen der tolerierbaren Risiken. Zahlenangaben: individuelles jährliches Todesfallrisiko

Also: auch wenn die Schadensfunktion *s* nicht bekannt ist und allgemeinverbindliche absolute Risikowerte nicht angegeben werden können, kann man Risiken verschiedener Techniken sehr wohl miteinander vergleichen und entscheiden, welche der Techniken das geringste Risiko bietet. Risikooptimierung auf rein technischer Grundlage ist demnach möglich.

Nach dieser Vorbemerkung ist erkennbar, wie die Aufgaben zwischen Legislative und Technik am besten aufzuteilen sind: Die Legislative legt den *gesetzlichen Rahmen* fest, so dass der Bereich Technik mit seinen Institutionen (Hersteller, Betreiber, Überwachungs- und Prüfstellen) dazu gebracht wird, die mit der Technik verbundenen Risiken zu minimieren.

Die Hauptlast der gesellschaftlichen Risikokontrolle wird so in den Markt hineinverlagert, also dahin, wo die Kultur des Individualismus und der Denkstil der Risikooptimierung vorherrschen.

Aber bevor vom Gesetzgeber dieser Optimierungsprozess in Kraft gesetzt werden kann, ist in einem politischen Entscheidungsprozess erst einmal herauszufinden, ob die gesamte Gesellschaft überhaupt bereit ist, für die Vorteile, die eine neue Technik für die soziale Wohlfahrt bietet, auch die Risiken in Kauf zu nehmen, die damit verbunden sind.

Die Regierung Großbritanniens hat die Administration der Arbeitssicherheit in der Health & Safety Executive (HSE) konzentriert. Diese Organisation hat die Leitlinien, denen sie bei ihren Entscheidungen unter Risiko folgt, einer öffentlichen Diskussion zugänglich gemacht [16]. Deshalb werden diese Leitlinien hier zur Erläuterung des Prozesses herangezogen.

Der in den Leitlinien abgesteckte Rahmen der *tolerierbaren Risiken* ist nicht starr, und er beschränkt sich auch nicht auf die Berücksichtigung nur einer einzigen Kennzahl für das Risiko. Risikogrenzwerte (wie für die das individuelle jährliche Todesfallrisiko in Bild 1) dienen der ersten Orientierung. Aber die im Rahmen der Gesetzgebung zu treffenden Entscheidungen hängen darüber hinaus vom politischen Prozess, von den konkreten Verhandlungen mit den Betroffenen und von der Praktikabilität der möglichen Lösungen ab. Und im Laufe dieses Prozesses werden Präferenzen und Wertvorstellungen auf sehr unterschiedliche Art und Weise kommuniziert, und keineswegs nur in der Terminologie des objektiven Risikos.

Das Dreieck des Bildes 1 soll Techniken repräsentieren, deren Risiken von unten nach oben zunehmen. Eingetragen in die drei durch die Risikogrenzen beschränkten Felder sind die erforderlichen Maßnahmen. Ganz unten reicht es, sich an den *Stand der Technik* (state of the art) zu halten. Techniken mit Risiken im oberen Bereich sind ausgeschlossen. An einer Risikoreduktion führt kein Weg vorbei. Im mittleren Bereich müssen die Hersteller die möglichst weitgehende Risikoreduktion nachweisen in dem Sinne, dass eine weitere Risikoreduktion nur mit unverhältnismäßig hohem Aufwand

möglich wäre (utility based gross disproportion criterion). Dieses Prinzip trägt den Namen ALARP (As Low As Reasonably Practicable).

Das neue Konzept der Europäischen Gemeinschaft

Auch die Europäische Gemeinschaft folgt bei der technischen Harmonisierung seit 1985 dem Denkstil der Risikooptimierung. Das *neue Konzept* (new approach) beschränkt sich auf die Festlegung und Durchsetzung der *allgemeinen wesentlichen Anforderungen* und schafft so den Rahmen für die Risikooptimierung durch die technischen Institutionen. Im früher verfolgten Ansatz wurde demgegenüber versucht, hoch technische Rechtsvorschriften für einzelne Produktkategorien zu beschließen. Der neue Ansatz geht einher mit der Reduktion des direkten Einflusses der Kontrollhierarchien und mit einer Stärkung des Marktindividualismus - kurz: Deregulierung (Tabelle 2).

Im Tagungsband des 7. Elektrotechnik-Kolloquiums [6] habe ich das neue Konzept der EG etwas ausführlicher dargestellt.

Risikooptimierung in der Normung

Der Normung kommt die Rolle zu, den Stand der Technik und die Leitlinien der Risikooptimierung zu kommunizieren. Als Beispiel nehme ich die Europanorm zur Funktionalen Sicherheit, die vor als IEC-Norm 61508 bekannt geworden ist, und die in Deutschland als VDE 0801 veröffentlicht wird [17].

Gegenstand der Norm sind elektrisch/elektronische/programmierbar elektronische Sicherheitssysteme in technischen Anlagen. Zentraler Bestandteile dieser Norm sind 1. ein sicherheitsbezogenes Lebenszyklusmodell, an dem sich der Aufbau der gesamten Norm orientiert, und 2. ein System von sicherheitsbezogenen Anforderungsstufen (Safety Integrity Levels, SIL).

Das Lebenszyklusmodell wurde bereits im Supplement „Ursachen für das Versagen von Automatisierungssystemen“ vorgestellt. Hier will ich kurz erläutern, warum es Anforderungsstufen bzw. -klassen überhaupt gibt und was man damit anfangen kann.

Anforderungsstufen kommen ins Spiel, wenn es darum geht, den einzelnen sicherheitsrelevanten Automatisierungssystemen der Anlage sicherheitsbezogene Zuverlässigkeitsforderungen zuzuweisen. Dem geht eine Phase vorweg, in der das Gesamtsystem einer Gefährdungs- und Risikoanalyse unterzogen wird. Im Rahmen der dabei anfallenden Entscheidungsprozesse ist grundsätzlich das ALARP-Prinzip zu befolgen.

Letztlich werden den einzelnen Sicherheitssystemen maximal zulässige sicherheitsbezogene Ausfallraten zugewiesen. Diese Ausfallraten beziehen sich zunächst ausschließlich auf Hardware-Ausfälle, für die man ja auf Statistiken zurückgreifen kann. Das System der Safety Integrity Levels (SIL) hat zum Ziel, die Kontrolle eingebauter Fehler (Programmier-, Entwurfs- und Fertigungsfehler), die sich statistisch kaum erfassen lassen, an die Kontrolle von Ausfällen zu koppeln, sie sozusagen im Huckepack-Verfahren mitzunehmen. Und das geht so: Die SIL teilen die kontinuierliche Skala der Ausfallraten in vier Stufen auf. Das hat den Vorteil, dass man jeder der Sicherheitsstufen Qualitäts- und Sicherheitsmaßnahmen zur Kontrolle der eingebauten Fehler zuordnen kann.

Die SIL koppeln die qualitativen Sicherheitsfestlegungen an die quantitativen Sicherheitsforderungen. Für Sicherheit in der ersten und der zweiten

Bedeutungsvariante (Sicherheit$_1$ und Sicherheit$_2$) ergibt sich so eine gemeinsame Skala. Die Risikooptimierung findet nun nicht mehr auf einer kontinuierlichen, sondern auf der diskretisierten Skala der SIL statt, Tabelle 3. Ein Vergleich mit den in [1, Abschnitt 6.1] eingeführten Anforderungsklassen zeigt, dass die sicherheitsbezogene Anforderungsstufe SIL 3 die Anforderungsklassen AK5 und AK6 in etwa abdeckt. Das ist der Risikobereich II, also der Bereich des höheren Risikos.

Tabelle 3 Sicherheitsbezogene Anforderungsstufen (SIL)

SIL	**Quantitative Anforderungen**	**Qualitative Anforderungen - Auswahl**	
	Intervalle der **Ausfallwahrscheinlichkeiten** (Anforderungbetrieb) bzw. der auf das Jahr bezogenen **Ausfallraten** (kontinuierlicher Betrieb)	**Fehlererkennung: Ausfälle**	**Fehlervermeidung und Fehlererkennung: eingebaute Fehler und Programmierfehler** Betrachtete Programmiersprachen: ADA, MODULA 2, Pascal, FORTRAN 77, C, Assembler, BASIC. Wenn eine Programmiersprache mit dem Zusatz pur nicht empfohlen ist, kann ein geeigneter Subset der Sprache doch noch akzeptabel sein.
1	$[10^{-2}, 10^{-1})$	Sicherheitsbezogene Fehler müssen durch Prüfung erkannt werden können.	Verwendung von Programmierrichtlinien.
2	$[10^{-3}, 10^{-2})$	Falls Fehler nicht durch automatische Diagnose entdeckt werden, muss das System auch bei einem einfachen Fehler sicherheitsbezogen korrekt arbeiten. Sicherheitsbezogene Fehler müssen durch Prüfung erkennbar sein.	Keine dynamischen Objekte, keine unbedingten Sprünge, Grenzwerttest, Äquivalenzklassentest. Nicht empfohlen: BASIC pur. Dazu die Forderungen aus SIL 1.
3	$[10^{-4}, 10^{-3})$	Das System muss bei Anwesenheit eines einfachen Fehlers sicherheitsbezogen korrekt arbeiten. Das Hinzutreten eines zweiten Fehlers muss hinreichend unwahrscheinlich sein, so dass die Ausfallwahrscheinlichkeit bzw. -rate unter dem angegebenen Wert bleibt. Komponenten ohne automatische Diagnose müssem auch bei Anwesenheit von zwei Fehlern sicherheitsbezogen korrekt arbeiten. Alle sicherheitsbezogenen Fehler müssen durch Prüfung erkannnt werden können.	Keine dynamischen Variablen, keine Pointer, keine Interrupts. Nicht empfohlen: C pur, BASIC. Dazu die Forderungen aus SIL 2.
4	$[10^{-5}, 10^{-4})$	Das System muss bei Anwesenheit eines Fehlers sicherheitsbezogen korrekt arbeiten, selbst wenn während der Fehlerentdeckung und Reparatur ein weiterer Fehler hinzukommt. Alle Fehler sollen vorrangig durch automatische Diagnose entdeckt werden können. Alle restlichen Fehler müssen durch Prüfung erkannt werden können. Sicherheitsbezogene Zuverlässigkeitsanalysen müssen auf Worst-Case-Annahmen beruhen.	Statische Prüfungen + formale Korrektheitsbeweise. Dazu die Forderungen aus SIL 3.

Literatur + Links

[1] Grams, T.: Grundlagen des Qualitäts- und Risikomanagements. Zuverlässigkeit, Sicherheit, Bedienbarkeit. **Vieweg** Praxiswissen, Braunschweig, Wiesbaden 2001

[2] Grams, T.: Risikooptimierung kontra Risikobegrenzung. Analyse eines alten und andauernden Richtungsstreits. Automatisierungstechische Praxis atp 8/2003

[3] Kuhlmann, A.: Sicherheitskultur. TÜV-Verlag, Köln 2000

[4] Europäische Kommission: Leitfaden für die Umsetzung der nach dem neuen Konzept und dem Gesamtkonzept verfaßten Richtlinien. Europäische Gemeinschaft, 2000

[5] VDI/VDE-Richtlinie 3542 (Okt. 2000): Sicherheitstechnische Begriffe für Automatisierungssysteme.
Blatt 1: Qualitative Begriffe.
Blatt 2: Quantitative Begriffe und Definitionen.
Blatt 3: Anwendungshinweise und Beispiele.
Blatt 4: Zuverlässigkeit und Sicherheit komplexer Systeme (Begriffe)

[6] DIN VDE 31 000, Teil 2 (Dezember 1987): Allgemeine Leitsätze für das sicherheitsgerechte Gestalten technischer Erzeugnisse. Begriffe der Sicherheitstechnik. Grundbegriffe.

[7] Grams, T. (Hrsg.): Risiko - Unser Umgang mit der Angst. Tagungsband zum 7. Fuldaer Elektrotechnik-Kolloquium 2002
Tagungsband
Schaukasten des Fachbereich ET der FH Fulda mit weiterem Begleitmaterial und Ausschnitten aus der Diskussion

[8] Bernstein, P. L.: Against the Gods. The remarkable story of risk. Wiley, New York 1996

[9] Starr, C.: Social Benefit versus Technological Risk. What is our Society willing to pay for safety? Science 165 (September 1969) 19, S. 1232-1238. Deutsche Übersetzung in Gotthard Bechmann (Hrsg.): Risiko und Gesellschaft. Grundlagen und Ergebnisse der interdisziplinären Risikoforschung. Westdeutscher Verlag, Opladen 1993, S. 3-24

[10] Kahneman, D.; Tversky, A.: Prospect Theory: An Analysis of Decision under Risk. Econometrica, 47 (March, 1979) 2, 263-291

[11] Neumann, J. v.; Morgenstern, O.: Theory of Games and Economic Behavior. Princeton University Press, Chichester 1944

[12] Luhmann, N.: Soziologie des Risikos. De Gruyter , Berlin, New York 1991

[13] Thompson, M.; Ellis, R.; Wildavsky, A.: Cultural Theory. Westview Press, Boulder, San Francisco, Oxford 1990

[14] Douglas, M.; Wildavsky, A.: Risk and Culture. University of California Press, Berkeley, Los Angeles 1982

[15] Der Syndikus bei der Deutschen Bahn, Klaus-Dieter Wittenberg, spricht in seinem Beitrag „Sicherheits- und Betreiberverantwortung im Eisenbahnbetrieb“ (SIGNAL+DRAHT (94) 12/2002, S. 37-42)

[16] HSE (2001): Reducing risks, protecting people. HSE’s decision-making process (HSE WebSite www.hse.gov.uk)

[17] IEC 61508: Functional Safety (deutsch: VDE 0801: Funktionale Sicherheit).
Part 1: General requirements (1998)
Part 2: Requirements for E/E/PE safety-related systems (2000)
Part 3: Software requirements (1998)
Part 4: Definitions and abbreviations (1998)
Part 5: Examples of methods for the determination of safety integrity levels (1998)
Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3 (2000)
Part 7: Overview of techniques and measures (2000)

Zur Seite „Zuverlässigkeit und Sicherheit - Begriffsbestimmungen“
Zurück zur Seite „Zuverlässigkeit und Sicherheit - Q&R-Management“
