

Gerhard Banse, Ernst-Otto Reher

Einleitung

Der Arbeitskreis „Allgemeine Technologie“ der Leibniz-Sozietät der Wissenschaften¹ führte am 16. November 2012 sein V. Symposium zur Thematik „Technik – Sicherheit – Techniksicherheit“ durch.²

Die Komplexität des Gegenstandes „Sicherheit“ wird in der nachfolgenden Abbildung 1 verdeutlicht. Um zu einem gesellschaftlichen Handlungsalgorithmus in Fragen der Sicherheit zu gelangen, sind vielfältige Sichten und Handlungen aus Wissenschaft, Wirtschaft, Kultur, Öffentlichkeit und Politik möglich bzw. erforderlich. Erst durch eine breit angelegte Betrachtung können Entscheidungsträger wirksam werden, das betrifft sowohl die Ebene der Artefakte mit ihren Produkten, als auch die menschliche Gesellschaft mit ihrer Umwelt, ihrem Lebensraum von Mensch, Tier und Pflanzen. Das „in die Welt setzen“ von Artefakten und Erzeugnissen von Produktions- und Dienstleistungstechnologien bedarf mehr denn je in unserer Zeit einer kritischen Sicherheitsbetrachtung. Eine Vielzahl von Maßnahmen, in Abbildung 1 nur auszugsweise dargestellt, wurde bisher entwickelt und konnten zum Einsatz gebracht werden (z.B. Technologiefolgenabschätzung, Begleitforschung).

Das Symposium behandelte Aspekte der Technologie- und Erzeugnissicherheit mit den Komplexen „Maschinen-, Apparate- und Anlagensicherheit“, „Erzeugnis- und Produktsicherheit“, „Sicherheit von Dienstleistungstechnologien“ und „Verbrauchersicherheit“.

Sicherheit ist ein zentrales Konzept in Gesellschaft, Wissenschaft und Technik. Geprägt wird dieses Konzept von unterschiedlichen Begriffsauffassungen, Kommunikationsstrategien und kulturellen Aspekten. In dem eintägigen Symposium haben Wissenschaftler aus verschiedenen Disziplinen ihre

1 Vgl. zum Arbeitskreis <http://www.leibniz-sozietat.de/> → Sozietät → Arbeitskreise → Arbeitskreis Allgemeine Technologie.

2 Die vier vorangegangenen Symposien zur Allgemeinen Technologie sind in den Bänden 50, 75, 99 und 112 der Sitzungsberichte der Leibniz-Sozietät dokumentiert (vgl. Banse/Reher 2002, 2004, 2008, 2011).

Forschungsergebnisse zum Thema (Technik-)Sicherheit mit dem Ziel diskutiert, gemeinsame Forschungsansätze vor allem zu Techniksicherheit, aber auch zu Sicherheitskommunikation und Sicherheitskulturen zu entwickeln.³

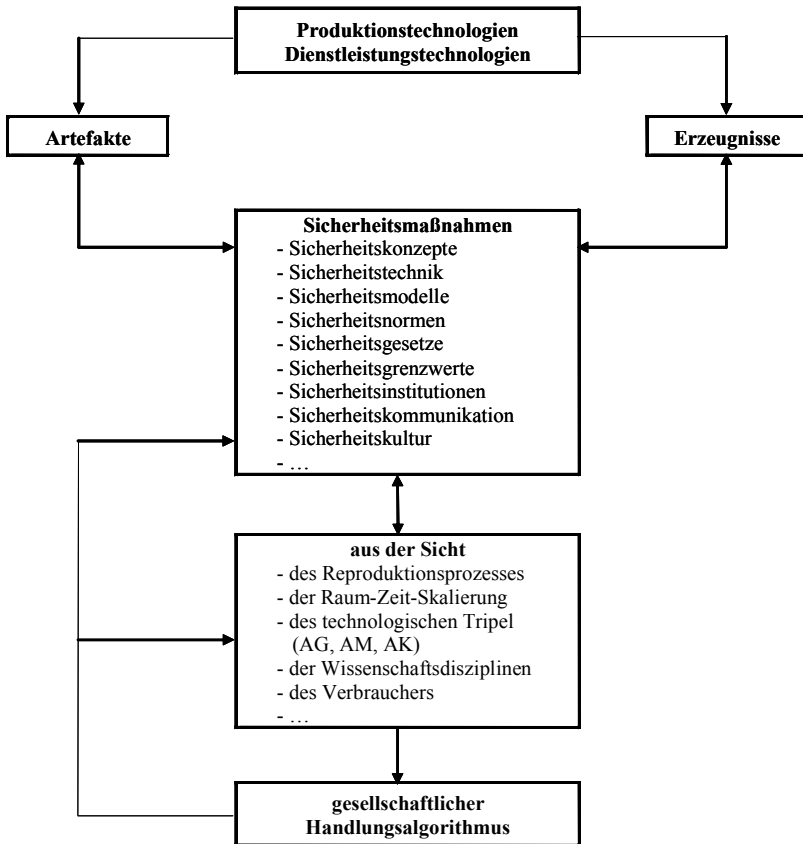


Abbildung 1: Sicherheitsmaßnahmen
Eigene Darstellung

Die Sicherheit technischer Handlungsvollzüge und technischer Hervorbringungen als weitgehender Ausschluss oder als bewusstes Handling von Risiken nimmt in den handlungsleitenden Wertvorstellungen technischer

3 Vgl. zu Techniksicherheit generell z.B. Banse 2013; Banse et al. 2009; Meyna/Peters 1985/86; Perrow 1987; Poy et al. 1994; Schneider 1991; Winzer et al. 2009.

Welterzeugung einen herausragenden Platz ein (vgl. näher dazu Banse 2009, 2011; Belyová/Banse 2011).

Als „Wissenschaften vom Machen“ sind zunächst die Technikwissenschaften herausgefordert, Sicherheit „zu erzeugen“, d.h. technische Sachsysteme und Technik-Mensch-Interaktionen so zu entwerfen und zu gestalten, dass von ihnen (ideal) keine bzw. (real) nur geringe Gefährdungen für „Schutzgüter“ ausgehen (nicht nur aktuell, sondern auch langfristig). Doch sind heute auch die Geistes- und Sozialwissenschaften aufgefordert, sich mit technikbezogener Sicherheit zu befassen, da technische Sachsysteme und Technik-Mensch-Interaktionen in einen sozialen und kulturellen Kontext eingebettet sind. Damit wächst die Relevanz der interkulturellen Forschung unter dem Einfluss der zunehmenden Globalisierung von Technikentwicklung und -anwendung (vgl. z.B. Gronau/Eversheim 2008; Hermeking 2010; Rösch 2008).

Lucia Belyová und *Gerhard Banse* gehen in ihrem Beitrag „Sicherheit und Sicherheitskultur“ davon aus, dass „Sicherheit“ einerseits ein zentraler Gegenstand wissenschaftlicher Forschung, andererseits ein schillernder Begriff ist, mit zahlreichen unterschiedlichen Bedeutungen belegt. Die Sicherheit in Mensch-Technik-Interaktionen lässt sich erhöhen

- durch „Investitionen“ in die technischen Sachsysteme bei deren konstruktiver Auslegung und produktionstechnischer Herstellung (etwa durch Verbesserungen hinsichtlich Zuverlässigkeit und Handhabbarkeit, der Schadensvorbeugung und der Gefährdungsabwehr);
- durch „Investitionen“ in die „Nutzer“ technischer Sachsysteme (etwa durch die Ausprägung von Kompetenz und spezifischer Persönlichkeitseigenschaften);
- durch „Investitionen“ in das (rechtliche, soziale, kulturelle, ...) „Umfeld“ der Technikherstellung, vor allem aber der Techniknutzung.

Dieses „Umfeld“ wird weitgehend (jedoch nicht vollständig!) durch das geprägt, was man seit etwa drei Jahrzehnten als „Sicherheitskultur“ bezeichnet. Damit wird eine Einsicht thematisiert, die spätestens mit der Reaktorkatastrophe von Chernobyl im Jahre 1986 gewonnen wurde: neben technischen und unmittelbar an den Nutzer adressierte Maßnahmen sind sozio-kulturelle Aspekte von entscheidender Bedeutung für die Sicherheit von bzw. in Technik-Mensch-Interaktionen. Darauf wird im Beitrag eingegangen. Das Konzept

„Sicherheitskultur“ wird genutzt, um kulturbedingte Verhaltensmerkmale zu beschreiben, die für die Gewährleistung der technikbezogenen Sicherheit („Techniksicherheit“) im komplexen Zusammenspiel von Technik, Organisation, Mensch und Umwelt für von Bedeutung sind.

Sicherheitskultur(en) besitzen einerseits eine mehr „theoretische bzw. normative“ Ebene (vor allem in Form von Anweisungen, Regeln, Vorschriften, Statements, Codes usw.; „externe Ebene“), andererseits eine mehr „praktische bzw. faktische“ Ebene (als gelebte und praktizierte Sicherheitskultur; „interne Ebene“). Letztere erfasst die Einstellungen und das Verhalten (vor allem) von Techniknutzern sowie die Kommunikation zwischen ihnen. Sicherheitskulturen bieten für den einzelnen Nutzer einen Rahmen, der die Ordnung menschlicher Wahrnehmung und Wertung sicherheitsrelevanter Sachverhalte und Zusammenhänge einerseits erst ermöglicht, andererseits auch strukturiert. Zugleich gehen in („gelebte“) Sicherheitskultur(en) unreflektierte Denkgewohnheiten und Handlungsprogramme sowie implizite Werthaltungen der Akteure ein. Für Sicherheitskulturen ist bedeutsam, dass nicht alle relevanten Akteure innerhalb einer Sprachgemeinschaft (etwa Konstrukteure und Nutzer) die gleichen unreflektierten und impliziten Werthaltungen besitzen bzw. entsprechend handeln. Das kann schwerwiegende Folgen haben (z.B. sprachliche Missverständnisse oder Übersetzungsfehler als Auslöser von Irrtümern mit Unfallfolgen). Bei Techniktransfer in andere Länder und damit andere Kulturen kommt hinzu, dass einerseits unterschiedliche Sicherheitskulturen (die der Ursprungs- und die der Zielregion) relevant werden, andererseits weitergehende „höherstufige“ sprachliche Verständigungsprozesse erforderlich sind.

Eine Operationalisierung (und damit auch Vergleichbarkeit) von Sicherheitskulturen ist derzeit (noch) schlecht durchführbar, da (inter- wie intrakulturelle) Indikatoren bislang kaum entwickelt wurden. Im Beitrag wird jedoch ein eigener Vorschlag vorgestellt.

An diese Überlegungen, die zugleich den Eröffnungs- bzw. Einleitungsvortrag des Symposiums bildeten, schließen drei inhaltliche Komplexe an: *erstens* Sicherheit im Zusammenhang mit der Kerntechnologie (Beiträge von Wolfgang Fratzscher, Norbert Mertzsch und Dieter Seeliger), *zweitens* Sicherheit und Materialtechnologie (Beiträge von Ernst-Otto Reher, Christian Kohlert und Dietrich Balzer) sowie *drittens* sozial- und geisteswissenschaftlichen Fragestellungen im Zusammenhang mit Sicherheit (Beiträge von Mukayil Kilic/Klaus Fuchs-Kittowski, Annelly Rothkegel sowie Martin Endress/Benjamin Rampp).

Wolfgang Fratzscher schließt mit seinem Beitrag „Über die Sicherheitskultur bei Kernkraftwerken“ unmittelbar an den Einführungsbeitrag an. Einleitend wird ein kurzer Blick auf die Herausbildung des Begriffes Sicherheit geworfen. Dann wird versucht, die wesentlichen Beiträge der Kerntechnik zur Entwicklung einer Sicherheitskultur aufzuzeigen. Dazu dient zunächst eine Sicht auf das Genehmigungsverfahren in Deutschland mit der Gesellschaft für Reaktorsicherheit, das sich herausgebildet hat aufgrund der speziellen Sicherheitsaspekte bei kernenergetischen Anlagen. Es ist dies das Auftreten der radioaktiven Strahlung, die durch Abschirmung und gas- und druckdichte Barrieren zurückgehalten werden soll. Es sind dies weiter die Maßnahmen zur Eindämmung der Auswirkungen menschlichen Fehlverhaltens und die Orientierung der Sicherheitsmaßnahmen am Lebenszyklus der Anlagen einschließlich der möglichen Unfälle bis hin zu Katastrophen und der endgültigen Beseitigung der Anlagen. Weiter wird angenommen werden, dass die Kerntechnik maßgebend zur Herausbildung der Technikfolgenabschätzung (TA) beigetragen hat. Diese hat, wie auch die Versuche, die Sicherheitsphilosophie der Kerntechnik auf andere Industriebereiche zu übertragen, nicht den erwarteten Erfolg gebracht. Das beweist, dass das Sicherheitsniveau in der Kerntechnik in manchen Dimensionen höher ist als in anderen Bereichen der Volkswirtschaft. Das schließt aber nicht aus, das außer der Sicherheit alle anderen Bewertungskriterien für die Einschätzung der Kerntechnik nicht mehr maßgebend sind. Abschließend wird eine Struktur der Gesamtheit der Sicherheitsdimensionen auf der Grundlage technologischer Überlegungen entworfen, deren Erfüllung für eine Einschätzung des Niveaus der Sicherheitskultur zugrunde gelegt werden kann.

Norbert Mertzsch behandelt „Sicherheitsaspekte beim Rückbau des KKW Rheinsberg“. Das Thema „Sicherheit“ hat bei der Stilllegung und dem Rückbau des Kernkraftwerkes Rheinsberg absolute Priorität. Dabei rücken entsprechend des Rückbaufortschritts jeweils unterschiedliche Sicherheitsaspekte in den Focus. Bei allen Maßnahmen zur Stilllegung des Kernkraftwerkes Rheinsberg besitzen Strahlenbetrachtungen für das Personal, die Bevölkerung und die Umgebung die entscheidende Bedeutung. Im Rahmen der Arbeitsplanung wurden und werden Maßnahmen zur Gewährleistung des Strahlenschutzes detailliert festgelegt. Durch technische Maßnahmen wird im Kernkraftwerk Rheinsberg sichergestellt, dass die im Rahmen der Stilllegungsgenehmigung festgelegten Grenzwerte für die Abgabe von Radionukliden über die Abluft und das Abwasser während der Stilllegungsarbeiten jederzeit sicher unterschritten werden. Dem physischen Schutz von Kern-

brennstoff wurde in der Nachbetriebsphase höchste Aufmerksamkeit gewidmet. Nach dem Abtransport des Kernbrennstoffs konnten die diesbezüglichen Maßnahmen deutlich reduziert werden, da sich das Gefährdungspotenzial drastisch verringerte. Für die weiteren Stilllegungs- und Rückbauarbeiten ist das Schutzziel „Rückhaltung radioaktiver Stoffe“ stets zu gewährleisten.

Ein weiterer wichtiger Sicherheitsaspekt ist die Arbeitssicherheit, denn Demontage- und Abbrucharbeiten gehören zu den Tätigkeiten mit erheblichem Gefährdungspotenzial. Das Gefährdungspotenzial besteht vor allem

- im Umgang mit schweren Lasten;
- durch die räumliche Enge;
- in der Gewährleistung der Statik der Anlagen und Gebäude;
- in der Beseitigung von Gefahrstoffen, wie Asbest;
- durch das Auftreten von Stäuben, radioaktiven Aerosolen, ionisierender Strahlung und Kontaminationen.

Dieser Beitrag kann für weitere KKW-Rückbauvorhaben als Beispiel angesehen und die gewonnenen Erfahrungen von Rheinsberg können sicherlich übernommen werden.

Dieter Seeliger wendet sich „Fukushima – bisherige Lehren aus der Katastrophe über die Sicherheit von Kernkraftwerken“ zu. Am 11. März 2011 erschütterte das bisher schwerste Erd- und Seebeben im Pazifik östlich von Japan die Region und löste mehrere Tsunami-Wellen aus, die weite Küstenbereiche im Nordosten der Hauptinsel Honshu überschwemmten und weiträumig totale Zerstörungen an Wohnsiedlungen, Infrastruktur, Industrieanlagen und landwirtschaftlich genutzten Flächen hinterließen. Als schwerster Verlust infolge dieser Naturkatastrophe sind tausende Menschenleben zu beklagen, viele werden noch immer vermisst. In der Kernkraftanlage Fukushima Dai-ichi mit sechs Reaktorblöcken setzten Erdbeben und Seewasser-Überflutung infolge des Tsunami die Reaktorkühlsysteme außer Betrieb, was nachfolgend zu schwersten Zerstörungen an vier Reaktoren und großflächiger Freisetzung von Radioaktivität führte, in deren Ergebnis dieser Reaktorunfall in die höchste Stufe der internationalen Skala eingeordnet wurde. Im Beitrag werden kurz die Abfolge der eingetretenen Zerstörungen und deren Auswirkungen sowie die Einleitung von sofortigen Gegenmaßnahmen und Ausarbeitung von Plänen zur mittel- und langfristigen Sicherung und Dekontaminierung seitens des Kraftwerksbetreibers TEPCO und der japanischen Atomaufsichtsbehörden erläutert.

Parallel zu den Aktivitäten vor Ort starteten internationale Gremien, insbesondere auf Initiative und unter Führung der Internationalen Atombehörde

IAEA der UNO in Wien, zahlreiche Projekte – Expertenmissionen, Konferenzen, Workshops etc. – mit dem Ziel, die Ursachen der Katastrophe und den aktuellen Stand ihrer Überwindung zu erfassen bzw. offen zu legen, notwendige Schlussfolgerungen hinsichtlich der Sicherheit des weiteren Betriebs der weltweit laufenden 430 Kernkraftwerke und Empfehlungen für erhöhte Sicherheitsvorschriften bei der Auslegung von Neuanlagen auszuarbeiten und diese über Beschlüsse der Regierungen in die verbindliche Rechtspraxis der Mitgliedsländer einfließen zu lassen. Hervorgehoben wird in diesem Zusammenhang auch die Durchführung von Stresstests an den KKW in der EU auf Vorschlag und Initiative der westeuropäischen kerntechnischen Genehmigungs- und Aufsichtsbehörde WENRA (Western European Nuclear Regulators' Association).

Wie ist der heutige Stand des Reaktorunfalls von Fukushima und sind die Perspektiven der Überwindung seiner Folgen zu bewerten? Wie groß sind mittel- und langfristige Schäden bei Menschen und Tieren infolge der erhöhten Strahlenbelastung zu erwarten? Handelt es sich bei diesem Unfall um das Eintreten eines angeblich „unvermeidlichen Restrisikos“ der komplexen Kernenergie-Technik? Zu diesen und weiteren Fragen versucht der Beitrag – über ein Jahr nach der Katastrophe – vorläufige Antworten zu finden.

Mit diesem Beitrag wird eine Reihe von offenen Fragen beantwortet, die bisher in dieser deutlichen Darstellung in der Öffentlichkeit nicht behandelt wurden. Die eingeleitete Energiewende in Deutschland bekommt so sicherlich weitere Befürworter.

Ernst-Otto Reher behandelt die „Überwachung und Qualitätssicherung fluider strukturierter Erzeugnisse aus Produktionsanlagen, dargestellt am Beispiel der Kunststofftechnologie“. Er kommt zu folgenden generalisierten Aussagen:

1. Produktionsanlagen der Materialtechnologien haben heutzutage eine Produktionskapazität, die Labormessverfahren zur Qualitätssicherung nur in seltenen Fällen zulassen. Zu groß ist der Ausschuss, der in der Prüfzeit im Labor die Anlage verlässt, z.B. 100 t/h Kunststoffe. Es kommen immer mehr online-Messverfahren im Echtzeitbetrieb zum Einsatz, um die Ausschussquote zu verhindern oder wesentlich zu minimieren.
2. Für strukturierte Fluide (Polymerschmelzen und -lösungen, Lebensmittel, Kosmetika, Pharmaka, Bio- und Nanoprodukte, Keramikschlicker, Farben und Lacke, Betonsuspensionen, Beschichtungsmassen u.v.m.) sind die rheologischen Eigenschaften signifikant für Struktur-Eigenschafts-Beziehungen, die die Verarbeitbarkeit dieser Fluide und ihre Anwendung

in der Praxis bestimmen. Auch weitere zusätzliche Messverfahren kommen zum Einsatz, z.B. IR-Spektroskopie.

3. Bei Nichteinhaltung vorgegebener rheologischer Eigenschaften der Polymerschmelzen bei der Synthese sind die Verarbeiter und Anwender der Polymerschmelzen (Granulat) nicht in der Lage, ihre Erzeugnisse in Qualität und Quantität mit ihren Verarbeitungsanlagen herzustellen. Das geforderte „Verarbeitungsfenster“ der Anlagen wird durch die rheologischen (strukturellen) Eigenschaften der Polymerschmelzen begrenzt. Die Polymerhersteller müssen die geforderten rheologischen Eigenschaften der Verarbeiter und Anwender garantieren. Ähnlich verhält es sich mit anderen strukturierten fluiden Erzeugnissen.
4. Die rheologischen Prozessgrenzen der Verarbeitungsanlagen im Arbeitsdiagramm können durch mathematische Prozessmodelle der Verarbeitungs-ausrüstung mit den rheologischen Materialfunktionen vorausberechnet werden. Für sie werden Intervalle zur Verarbeitbarkeit und Produktanwendung angegeben, die der Polymerhersteller garantieren muss. Die Durchsatzsteigerungen sind mit zusätzlichen Kosten verbunden, eine Kostenanalyse ermöglicht eine Technologieentscheidung.
5. Die Entwicklung der Mess- und Steuerverfahren einschließlich der dazu gehörigen Technik wird im Team von Materialwissenschaftlern (Naturwissenschaftlern) und Technikwissenschaftlern für die online-Verfahren betrieben. Sozial- und Geisteswissenschaftler erarbeiten Grenzwerte sowie Normen und sind bei den Gesetzesvorbereitungen involviert (siehe Abbildung 1).
6. Am Beispiel der Kunststofftechnologie werden verschiedene entwickelte Struktur-Eigenschafts-Beziehungen dargestellt, die für die online-Rheometrie im Echtzeitbetrieb entwickelt und angewendet wurden. Die Anwendung der Verfahren und der entwickelten technischen Lösungen konnten auch für andere, oben aufgezählte strukturierte Fluide erweitert und angewendet werden. Somit entstand ein Instrumentarium an Soft- und Hardware zur Überwachung und Qualitätssicherung fluiden Erzeugnisse in der Stoffwirtschaft.

Der Ausgangspunkt im Beitrag von *Christian Kohlert* „Sicherheit gegen Produktfälschung“ ist die Feststellung, dass Produktfälschungen und Plagiate schon lange keine „Kavaliersdelikte“ mehr sind, sondern den Volkswirtschaften sowie den im guten Glauben befindlichen Nutzern erhebliche Schäden zufügen. So werden Forschungsaufwendungen, wie z.B. in der Pharmaindustrie, nicht über das entstandene Produkt finanzierbar gemacht,

und die Endproduktutzer müssen möglicherweise ohne den angestrebten Nutzeffekt auskommen (bis hin zu persönlichen Schäden durch fehlende oder minderwertige Wirkstoffe). Einer Studie der OECD aus dem Jahre 2009 zufolge belaufen sich die Schäden dieser Produktpiraterie weltweit auf 184 Mrd. Euro und betragen damit schon über 50 Prozent mehr als 2007. Schätzungen gehen davon aus, dass dadurch alleine in Deutschland jährlich rund 50.000 Stellen verloren gehen. Selbstverständlich sind bestimmte Produktgruppen, wie hochwertige Konsumgüter der Bekleidungsindustrie, Kosmetika und Pharmazeutika, vorrangig betroffen, aber ausgespart vor diesem Problem ist fast keine Branche mehr.

Bei Plagiaten geht es in der Regel darum, unter hochwertigen Markennamen minderwertige Produkte zu verkaufen. Durch Kopieren der notwendigen Maschinen und Anlagen, durch Nutzung minderwertiger Rohstoffe sowie durch Umgehung qualitätssichernder Maßnahmen werden enorme Gewinnspannen erzielt. Da die Produkte selbst oft schwer prüfbar sind, wird in letzter Zeit verstärkt die Verpackung als Prüfkriterium für die Echtheit genutzt. Im Beitrag werden verschiedene Varianten der Gewährleistung der Fälschungssicherheit bzw. des Nachweises von Fälschungen über aktuelle optische, magnetische und andere Verfahren vorgestellt und bewertet:

- Buchstaben-Zahlen-Kombinationen mit Validierung über IT;
- Hologramme;
- Mikro- und Nanopartikel;
- molekulare Markierungssysteme (DNA);
- Funk-Chips (RFID);
- Hardwareschutz (Dongle).

Allen gemeinsam ist die menschliche Intelligenz – welche den Fälschern allerdings ebenfalls nicht abzusprechen ist. Zu berücksichtigen ist aber, dass ein Fälscher 100% seiner Leistung zum Fälschen einsetzt, dagegen ein Produktentwickler höchstens 1% zur Fälschungssicherheit. Absolut nicht zu fälschen ist nur der Zufall! Im Beitrag wird deshalb auch ein auf Zufall basierendes Sicherheitssystem für Verpackungen vorgestellt.

Dietrich Balzer widmet sich dem Thema „Die gegenwärtige und zukünftige Rolle der Automatisierungs- und Kommunikationstechnik in der Sicherheitswirtschaft“. Der Wirtschaftszweig „Sicherheit“ wird in der Wirtschaftsstatistik noch nicht ausgewiesen. National und international hat sich aber schon eine Sicherheitswirtschaft etabliert, wie wissenschaftliche Untersuchungen und Studien belegen. Auf Grund der spezifischen Eigenschaften der Automatisierungs- und Kommunikationstechnik spielt diese Technik in der

Sicherheitswirtschaft eine zentrale Rolle, die auf die Einheit von Informationsgewinnung, Informationsverarbeitung und Informationsnutzung zurückzuführen ist. Innerhalb der Sicherheitswirtschaft wird die Automatisierungs- und Kommunikationstechnik vor allem in folgenden Marktsegmenten eingesetzt:

- Sicherheitstechnik (Biometrie, Videotechnik, Sensorik, Leittechnik, Zutrittskontrolle);
- IT-Sicherheit (Netzsicherheit, Verschlüsselung, Virtual Private Network, Public Key Infrastructure, Smart Card);
- Sicherheitsdienstleistungen (Objekt- und Wachschatz, Risk Management, Trust Center, Sicherheits-Audits, Sicherheits-Engineering, Consulting).

Die Automatisierungs- und Kommunikationstechnik als sicherheitsorientierte Wissenschaftsdisziplin stellt für alle diese Marktsegmente Methoden und Produkte zur Verfügung, die auf die Kompensation nicht-ausregelbarer Störgrößen orientieren. Dabei geht es vor allem um Lösungen der Prozessüberwachung sowie der vorbeugenden und elementaren Prozesssicherung. Die damit im Zusammenhang stehenden Probleme werden an Hand von Beispielen aus der Verfahrens- und der Fertigungsindustrie erläutert.

Die Darlegungen von *Mukayil Kilic* und *Klaus Fuchs-Kittowski* zu „Sicherheitsrisiken und Vermeidungsverhalten im Fall der modernisierten und neuen Informationsquellen bei der Lenkung und Remotefunktionen von Fahrzeugen“ auf dem Symposium können aus Datenschutz- und Geheimhaltungsgründen (leider) nicht abgedruckt werden. Es wurde deshalb nur die Zusammenfassung aufgenommen.

Gegenstand des Beitrages von *Annely Rothkegel* ist die „Sicherheitskommunikation“. Der Beitrag zielt auf unterschiedliche Konzepte des Schlüsselbegriffs Sicherheit, die in der Kommunikation über Technik und Technikgebrauch entwickelt und vermittelt werden. In fachlinguistischer Sicht sind es die Kontexte, die die sich stets verändernden Bedeutungen von Schlüsselbegriffen prägen. Dabei wirken Faktoren aus den jeweiligen Domänen und daraus abgeleiteten Szenarien sowie Merkmale der (Fach-)Gemeinschaften zusammen. Unterschieden werden Diskurs- und Praxisgemeinschaften. In Diskursgemeinschaften werden Sicherheitskonzepte entwickelt und diskutiert, u.a. im Sinne von Maßnahmen der Abwehr, des Schutzes oder der Resilienz. Praxisgemeinschaften sind dadurch gekennzeichnet, dass Alltagskontexte des Technikgebrauchs einbezogen sind. Damit erscheint der Horizont der Sicherheitsmodellierung weit ausgedehnt, die Kommunikation darüber aber eher eingeschränkt (z.B. Sicherheitshinweise in Produktinformationen, Wer-

bung). Neben klassifikatorischen Definitionen sind es vor allem implizite Modelle von Sicherheit (Situationen mit/ohne Gefahren), die die Kommunikation im Mix von Fach- und Alltagswissen prägen. Beide zusammen lassen sich wiederum in unterschiedliche Sicherheitskulturen einordnen. In einem übergeordneten Rahmen werden auf diese Weise technische Systeme mit gesellschaftlichen Systemen verbunden. Diskutiert werden die begrifflichen Grundlagen und linguistische Möglichkeiten der Analyse, die exemplarisch demonstriert werden.

Die Texte werden abgeschlossen mit Darlegungen von *Martin Endress* und *Benjamin Rampp* zu „Vertrauen in der Sicherheitsgesellschaft“. Der Beitrag beschäftigt sich mit der Bedeutung unterschiedlicher Typen der Sicherheitsproduktion für verschiedene Modi des Vertrauens und dabei insbesondere den paradoxen Effekten der Herstellung von Sicherheit. Dazu wird, im Sinne eines Verständnisses gegenwärtiger gesellschaftlicher Konstellationen als „Sicherheitsgesellschaft“, zunächst der Wandel des Sicherheitsverständnisses und in diesem Zusammenhang insbesondere das Phänomen des Risikos (und der Nebenfolgen) in spätmodernen Gesellschaftskonstellationen analysiert. Auf dieser Basis werden zwei Idealtypen der Sicherheitsproduktion und Regierung identifiziert und unterschieden: ein exkludierend-disziplinierender Typus sowie ein liberal-inkludierender Typus. Um deren Effekte auf Vertrauenskulturen zu analysieren, werden drei unterschiedliche Modi des Vertrauens differenziert: reflexives Vertrauen, habituelles Vertrauen und fungierendes (Grund-)Vertrauen. In Bezug auf diese Modi wird dann diskutiert, welche Verschränkungen von Vertrauensmodi und Typen der Sicherheitsproduktion bestehen, d.h. welche (Neben)Folgen die unterschiedlichen Typen der Sicherheitsherstellung jeweils für Vertrauenskonstellationen haben.

Die Herausgeber bedanken sich bei all jenen, die sowohl zum Erfolg des 5. Symposiums zur Allgemeinen Technologie als auch zur Drucklegung dieses „Protokollbandes“ beigetragen haben. Insbesondere zu nennen sind die Rosa-Luxemburg-Stiftung, die die Durchführung des Symposiums unterstützte, die Autoren, die den Forderungen der Herausgeber hinsichtlich Manuskriptgestaltung weitgehend nachkamen, und die Senatsverwaltung für Wirtschaft, Technologie und Forschung von Berlin, die die Drucklegung ermöglichte.

Literatur

- Banse, G. (2009): Techniksicherheit und Sicherheitskulturen. In: Winzer, P.; Schnieder, E.; Bach, F.-W. (Hg.): Sicherheitsforschung – Chancen und Perspektiven. München (acatech), S. 195-215
- Banse, G. (2011): „Normale Katastrophen“. In: Maring, M. (Hg.): Fallstudien zur Ethik in Wissenschaft, Wirtschaft, Technik und Gesellschaft. Karlsruhe, S. 160-166
- Banse, G. (2013): Sicherheit. In: Grunwald, A. (Hg.): Handbuch Technikethik. Stuttgart/Weimar (im Druck)
- Banse, G.; Reher, E.-O. (Hg.) (2002): Allgemeine Technologie – Vergangenheit, Gegenwart, Zukunft. Berlin (Sitzungsberichte der Leibniz-Sozietät, Bd. 50, H. 7)
- Banse, G.; Reher, E.-O. (Hg.) (2004): Fortschritte bei der Herausbildung der Allgemeinen Technologie. Berlin (Sitzungsberichte der Leibniz-Sozietät, Bd. 75)
- Banse, G.; Reher, E.-O. (Hg.) (2008): Allgemeine Technologie – verallgemeinertes Fachwissen und konkretisiertes Orientierungswissen zur Technologie. Berlin (Sitzungsberichte der Leibniz-Sozietät der Wissenschaften, Bd. 99)
- Banse, G.; Reher, E.-O. (Hg.) (2011): Ambivalenzen von Technologien. Berlin (Sitzungsberichte der Leibniz-Sozietät der Wissenschaften, Bd. 112)
- Banse, G.; Rothkegel, A.; Renn, O. (2009): Interdisziplinäre Sicherheits- und Risikoforschung. In: Winzer, P.; Schnieder, E.; Bach, F.-W. (Hg.): Sicherheitsforschung – Chancen und Perspektiven. München (acatech), S. 155-170
- Belyová, L.; Banse, G. (2011): Safe Innovations, Innovative Safety. In: Loudín, J.; Hochgerner, J. (eds.): Social and Cultural Dimensions of Innovation in Knowledge Societies. Prague, pp. 67-80
- Gronau, N.; Eversheim, W. (Hg.): Umgang mit Wissen im interkulturellen Vergleich. Beiträge aus Forschung und Unternehmenspraxis. München (acatech)
- Hermeking, M. (2010): Technik und Kultur. Schnittstellen für die Interkulturelle Kommunikation. In: Banse, G.; Grunwald, A. (Hg.): Technik und Kultur. Bedingungen- und Beeinflussungsverhältnisse. Karlsruhe, S. 163-178
- Meyna, A.; Peters, O. H. (1985/86): Handbuch der Sicherheitstechnik. 2 Bde. München/Wien
- Perrow, Ch. (1987): Normale Katastrophen. Die unvermeidlichen Risiken der Großtechnik. Frankfurt am Main
- Poy, A.; Weißbach, H.-J.; Florian, M. (1994): Arbeitssicherheit und Funktionssicherheit vernetzter Systeme. Opladen
- Rösch, O. (Hg.) (2008): Technik und Kultur. Berlin
- Schneider, J. (Hg.) (1991): Risiko und Sicherheit technischer Systeme. Auf der Suche nach neuen Ansätzen. Basel u.a.
- Winzer, P.; Schnieder, E.; Bach, F.-W. (Hg.) (2009): Sicherheitsforschung – Chancen und Perspektiven. München (acatech)