11. Technisierungsstrategien und der Human Factor

Stefan Strohschneider

Gegenstand dieses Beitrags ist die Diskussion der Interaktion von Technisierungsstrategien im Sicherheitsbereich und den direkt davon Betroffenen. Den Menschen also, die im Kontext verschiedener Dienstleistungsorganisationen das Produkt »Sicherheit« herstellen und deren Arbeit von konkreten technologischen Innovationen betroffen ist. Um die Nachvollziehbarkeit dieser Diskussion zu verbessern, erscheint eine begriffliche Vorbemerkung notwendig: Der deutsche Begriff »Sicherheit« kann im Englischen bekanntlich sowohl mit »safety« (Sicherheit vor unintentionalen Gefährdungen) als auch mit »security« (Sicherheit vor intentionalen Bedrohungen) übersetzt werden. Was die Erforschung des menschlichen Umgangs mit komplexen soziotechnischen Systemen betrifft, so sind mit dieser Unterscheidung zwei ziemlich distinkte Forschungstraditionen angesprochen. Wenn man die verfügbare Literatur sichtet, wird man feststellen, dass im Zusammenhang der hier angesprochenen Thematik die »safety-Forschung« mehr Aufmerksamkeit erfährt als die »security-Forschung«: Die Produzenten von »safety« sind in sehr viel umfangreicherem Ausmaß Gegenstand von Forschungsbemühungen als die Produzenten von »security«. Als zusammenfassende Bezeichnung dieses Forschungsfeldes hat sich in den vergangenen Jahren auch im Deutschen der Begriff »Human-Factors-Forschung« eingebürgert.[1]

Aus dieser Beobachtung ergibt sich die Gliederung des vorliegenden Beitrags. In einem ersten Abschnitt werden – besonders für den mit der Human-Factors-Forschung (»Human Factors« wird im Folgenden mit »HF« abgekürzt) weniger vertrauten Leser – basale Prämissen dieses Ansatzes vorgestellt. Anschließend werden einige der wesentlichen Konsequenzen von Technisierungsstrategien, die sich im Zusammenhang mit »safety« als bedeutsam herausgestellt haben, erläutert und schließlich auf

1 | Vgl. Petra Badke-Schaub/Gesine Hofinger/Kristina Lauche (Hg.): Human Factors: Psychologie sicheren Handelns in Hochrisikobranchen, Heidelberg: Springer Verlag 2008.

ihre Anwendbarkeit im Bereich der »security« diskutiert. Dies ist eine Analogieübertragung, die selbstverständlich spekulative Aspekte enthält, aber auf Grund der strukturellen Ähnlichkeiten beider Aufgabenbereiche gerechtfertigt erscheint.[2]

11.1 Safety, komplexe soziotechnische Systeme und die Rolle des Menschen

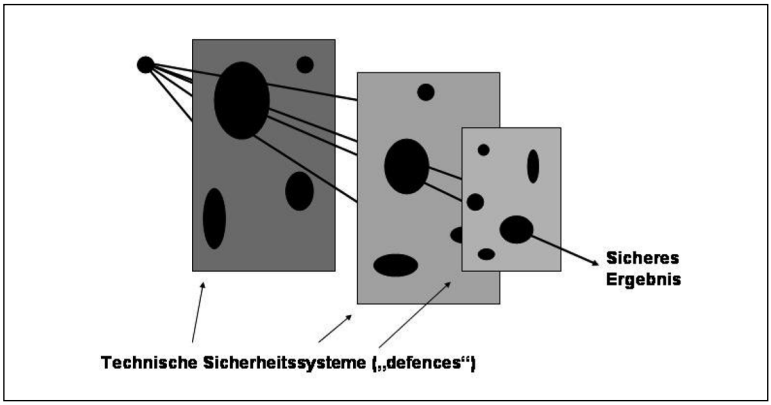
Die nachfolgend zu beschreibende Forschungslandschaft lässt Technisierungsstrategien zur Erhöhung von Sicherheit durchaus als zweischneidiges Schwert erscheinen. Diese Beurteilung lässt sich vermutlich besser nachvollziehen, wenn man zunächst einen kurzen Blick auf die Entwicklung der Untersuchung der Funktionsprinzipien der menschlichen Auseinandersetzung mit komplexen soziotechnischen Systemen im Kontext der HF-Forschung wirft.

Die frühe HF-Forschung der 70er und 80er Jahre des vorigen Jahrhunderts ging von der Prämisse aus, dass der Mensch ein prinzipiell fehleranfälliges Wesen sei und seine Neigung zu irrationalem und daher unberechenbarem Handeln – der »human error« – insbesondere in hochkomplexen Systemen ein kaum zu kalkulierendes Sicherheitsrisiko darstellt.[3] Ergo suchte man nach technischen Barrieren und Korrekturmöglichkeiten, um die gravierenden Fehler zu verhindern oder zumindest ihre Konsequenzen zu minimieren. Prägnant zusammengefasst ist diese Strategie im sog. »Schweizer Käsescheibenmodell« des englischen Fehlerforschers James Reason (s. Abb. 12): Menschen verfügen in praktisch jeder Situation über verschiedene Handlungsoptionen und haben damit im Prinzip unendlich viele Möglichkeiten, im Sinne der Sicherheit erwünschte oder auch unerwünschte Handlungsfolgen zu generieren. Um die Wahrscheinlichkeit von Handlungstrajektorien mit unerwünschten Folgen zu minimieren, baut man technische Schutzschilde ein. Diese Schutzschilde sollen nur solche Handlungen »durchlassen«, die zu einem erwünschten Ergebnis führen, die anderen aber blockieren. Dabei muss man natürlich darauf achten, dass es nicht trotzdem noch »Ausreißer« gibt. Sobald man diese erkennt, schiebt man eben, so die basale Logik, weitere Schutzschilde dazwischen.

2 | S. dazu auch Nicklas Dahlström/Sidney Dekker: »Security and safety synergy: Advancing security with Human Factors knowledge«, in: John G. Voeller (Hg.), Wiley Handbook of Science & Technology for Homeland Security, Chichester, GB: John Wiley & sons 2008.

3 | Rene Amalberti et al.: »Human factors in aviation: An introductory course« in: Klaus-Martin Goeters (Hg.), Aviation psychology: A science and a profession, Aldershot, GB: Ashgate 1998, S. 19-43.

Abbildung 12: Das »Schweizer Käsescheibenmodell« der Fehlervermeidungsstrategie durch technische Sicherheitssysteme. Adaptiert nach Reason.[4]



Da, wie gesagt, die Vielfalt menschlicher Handlungsoptionen praktisch unendlich ist, führt dieses Denken fast zwangsweise zu immer mehr Technik und zu immer mehr technischer Redundanz. Es verdient festgehalten zu werden, dass mit dieser Philosophie in einigen Bereichen (z.B. in der zivilen Luftfahrt) zumindest anfänglich großartige Erfolge erzielt werden konnten.[5] Gemäß der Prinzipien des operanten Konditionierens, unterstützt durch entsprechende wirtschaftliche Interessen, führt dies gewissermaßen zu einer Verselbständigung dieser Technisierungsstrategie. Das Ergebnis ist nicht überraschend: In einigen Bereichen (wie der zivilen Luftfahrt) hat der Sicherheitsgewinn durch zusätzliche Technik zumindest eine Asymptote erreicht, in anderen Bereichen geht mit zunehmender technischer Komplexität der Sicherheitslösungen die Sicherheit zurück. Das lässt sich belegen: Gemäß einer 2008 veröffentlichten Studie des Internationalen Verbandes von Schiffsversicherern hat der Verlust an Schiffen in den letzten zehn Jahren – eine Dekade, die geprägt war von der Einführung elektronischer Navigationshilfen wie der elektronischen Seekarte, einem automatischen Strandungswarnsystem oder der automatischen Schiffsidentifizierung – um 270 Prozent gegenüber der vorherigen Dekade zugenommen.[6] Diese Zunahme ist weitaus höher als der Anstieg des internationalen Seefrachtverkehrs und könnte u.a. auf die

4 | James Reason: Menschliches Versagen: Psychologische Risikofaktoren und moderne Technologien, Heidelberg: Spektrum Verlag 1994.

5 | S. dazu National Transportation Safety Board (Hg.): We are all safer: Lessons learned and lives saved, Washington, DC: Safety Report/SR-07/01, 5. Auflage 2007.

6 | Genaueres bei Andy Norris: »Laying the blame for bridge design«, in: Digital Ship, Oct. 2008, S. 34; s. dazu auch Bengt Schager: »Accidents due to human error are increasing in the maritime industry«, in: The Swedish Club Letter, 2-2008 (2008), S. 12-13; s.a. Radu Hanzu-Pazara et al.: »Reducing of maritime accidents

Kombination neuartiger technischer Sicherheitssysteme bei gleichzeitiger Personalreduktion zurückgeführt werden.

Die Schiffsversicherer gehen noch davon aus, dass dieser Anstieg in wesentlichen Teilen durch eine Zunahme des »human error« verursacht ist. In anderen, etwas sensibleren Branchen haben derartige Befunde zu einer Revision des Menschenbildes geführt: Man denkt nun darüber nach, ob die Interpretation des »human factor« als Sicherheitsrisiko vielleicht eine etwas einseitige Sichtweise darstellt, ob es nicht vielleicht zielführender ist, den »human factor« als ein Element eines komplexen soziotechnischen Systems zu betrachten, das die Möglichkeit hat, aktiv an der Aufrechterhaltung der Funktionsfähigkeit des Gesamtsystems mitzuwirken. Mittlerweile hat sich für die Eigenschaft eines Systems der Ausdruck »resilience« eingebürgert.[7] Resilience übersetzt man sich wohl am besten mit »Belastbarkeit«, »Elastizität« oder »Widerstandsfähigkeit«. Ein System ist resilient, wenn es in der Lage ist, seine wesentlichen Funktionen trotz unerwarteter Störungen, Ausfälle oder Katastrophen weiter zu erfüllen.[8]

Wie eine Reihe von Ereignissen – wiederum vor allem im Bereich der zivilen Luftfahrt dokumentiert – zeigt, könnte diese systemstabilisierende Eigenschaft insbesondere unter Sonder- und Extrembedingungen wichtig sein, die von der Technik alleine nicht bewältigt werden können. Eines der sehr breit rezipierten Ereignisse, das dazu beigetragen hat, den positiven Beitrag von Menschen zur Erhöhung der Widerstandsfähigkeit eines Systems in den Blick zu nehmen, war ein Flugunglück von Sioux City in den USA.[9] Eine DC 10 der United Airlines, Flug 232, wurde am 19. Juli 1989 mitten im Reiseflug von einem – nach bis dahin geltender Doktrin – unmöglichen Ereignis befallen: Dem gleichzeitigen Ausfall aller drei (redundanten) Hydrauliksysteme. Damit hatten die Piloten eigentlich keinerlei Möglichkeit mehr, das Flugzeug zu steuern: Ein Absturz erschien den Sachverständigen am Boden unvermeidbar. Dennoch gelang es der Besatzung mit Hilfe eines zufällig an Bord befindlichen Fluglehrers, die Maschine durch Regulierung des Schubs der beiden Tragflächentriebwerke notdürftig zu kontrollieren und schließlich auf dem Flughafen von Sioux

caused by human factors using simulators in training process«, in: Journal of Maritime Research 5 (2008), S. 3-18.

7 | Erik Hollnagel/Christopher Nemeth/Sidney Dekker (Hg.): Resilience engineering perspectives: Remaining sensitive to the possibility of failure, Aldershot, GB: Ashgate 2008.

8 | Bundesverwaltungsamt – Zentralstelle für Zivilschutz (Hg.): Stress im Katastrophenschutz: Zwischenbilanz und Forschungsbedarf. Ergebnisse eines Workshops, Bonn: Schriftenreihe WissenschaftsForum der Akademie für Krisenmanagement, Notfallplanung und Zivilschutz, Band 2, 2002.

9 | Eine gute Übersicht über die Ereignisse sowie weiterführende Literatur findet sich in der Wikipedia; s. http://en.wikipedia.org/wiki/United_Airlines_Flight_23 (zugegriffen am 24.2.2009).

City zu landen. Zwar ging das Flugzeug bei der Bruchlandung in Flammen auf, immerhin aber überlebten 185 der 296 Menschen an Bord.

Man kann dieses Ereignis als Anti-Käsescheiben-Argument interpretieren: Hier hat nicht der Mensch versagt und die Technik die Situation gerettet, sondern andersherum: Menschen haben ein bereits zusammengebrochenes technisches System retten können. Gekonntes und innovatives menschliches Handeln hat das Gesamtsystem resilient gemacht. Mit dieser Formulierung ist ein Wandel in der Forschungsausrichtung verbunden: Auf welche Weise kann der »Faktor Mensch« zur Widerstandsfähigkeit eines soziotechnischen Systems beitragen, oder andersherum gefragt: Inwieweit kann eine gedankenlos durchgeführte Technisierung diesen Beitrag behindern?

11.2 Technisierung und Widerstandsfähigkeit

Um anzudeuten, welche Aspekte bei der Behandlung dieser Fragestellung zu beachten sind, möchte ich im Folgenden fünf theoretische Konzepte diskutieren, die sich im Zusammenhang mit dem Thema »Mensch und Technik« im Rahmen einer safety-orientierten HF-Forschung als bedeutsam herausgestellt haben. Diese Auswahl ist nicht mit der Behauptung verbunden, sie stelle eine vollständige Abhandlung dar. Vielmehr ist sie durch die Annahme begründet, dass es sich hier um solche Konzepte handelt, die auch bei einer zunehmenden Technisierung von »security« relevant werden können. Gemeinsam ist ihnen, dass sie Bedingungen und Folgen des Einsatzes hochentwickelter Technologien beschreiben, die nicht unmittelbar evident sind, aber unter Umständen den eigentlich intendierten Sicherheitsgewinn zunichte machen können.

11.2.1 »Complacency«

Ein erster wichtiger Aspekt, der bei zunehmender Technisierung zu beachten ist, wird in der Literatur zu »human factors und system safety« als »complacency« bezeichnet – am besten wohl mit »vom Vertrauen in die Technik überzeugtes Zurücklehnen« zu übertragen. Complacency entsteht als Folge zunehmender Technisierung dann, wenn der menschliche Teil eines soziotechnischen Systems acht- und sorglos wird, gewissermaßen von der Haltung geprägt ist: »Ach, auf mich und meine Achtsamkeit kommt es ja nicht mehr so an, die Technik regelt das schon alleine!«

Complacency kann zwei möglicherweise kritische Konsequenzen haben. Die eine hat damit zu tun, dass das zufriedene Zurücklehnen bei den Handelnden zu einer Einschränkung des Situationsbildes führt. Die Aufnahme von Informationen wird eingeschränkt (man beschränkt sich z.B. auf die Beobachtung von Monitoren, andere visuelle Quellen oder andere Sinneskanäle bleiben ungenutzt), die Verarbeitung der Information zu einem integrierten Lagebild unterbleibt (»das System wird mich schon

alarmieren, wenn was los ist«), die fortwährende Entwicklung möglicher Zukunftsszenarien wird vernachlässigt.[10] Entsteht dann aber tatsächlich eine Situation, die rasches und kompetentes Handeln erforderlich macht, geht viel Zeit verloren, um diese Prozesse nachzuholen.

Derartigen Problemen wird in jüngerer Zeit viel Aufmerksamkeit gewidmet. Mangelnde »situation awareness« scheint bei der Entstehung vieler sicherheitskritischer Situationen eine wichtige Rolle zu spielen;[11] offenbar können technische Regelungssysteme die Anforderungen an die Entwicklung eines adäquaten Lagebildes komplizieren. Beispielsweise können viele Regelungssysteme in unterschiedlichen »modes« betrieben werden, die unterschiedliche Funktionalitäten bereitstellen. In kritischen Situationen scheint die »mode awareness« besonders leicht verloren zu gehen, was die Wahrscheinlichkeit für Fehlinterpretationen von Anzeigen und von Fehleingaben erhöht.[12] Allerdings sollte man sich davor hüten, in mangelndem Situationsbewusstsein einen individuellen Fehler zu sehen, und stattdessen die systemischen Ursachen für die Entwicklung eingeschränkter Lagebilder in den Blick nehmen.[13]

Eine zweite, indirekte Konsequenz von »complacency« hat mit den wirtschaftlichen Aspekten der Produktion von Sicherheit zu tun: Wenn die Technik sowieso alles alleine macht, kann man den Mitarbeitern ja zusätzlich andere Aufgaben zuordnen – das macht die Sicherheit billiger. Je mehr andere Aufgaben aber zu erledigen sind, desto größer wird die Versuchung, die Zeit und Aufmerksamkeit dafür von der Sicherheit »zu borgen« – um einen Ausdruck von Sidney Dekker zu verwenden.[14] Dieser Autor hat gezeigt, wie Menschen in hochtechnologisierten Systemen vom System dafür belohnt werden, Sicherheitsvorschriften zu missachten, um

10 | Raja Parasuraman/Robert Molloy/Indramani Singh: »Performance consequences of automation-induced complacency«, in: The International Journal of Aviation Psychology 3(1) (1993), S. 1-23.

11 | Vgl. Mica Endsley: »Toward a theory of situation awareness in dynamic systems«, in: Human Factors 37 (1995), S. 32-64; Frank Durso/Scott Gronlund: »Situation awareness«, in: Frank Durso (Hg.), Handbook of applied cognition, New York: Wiley 1999, S. 283-314.

12 | Vgl. dazu Nadine Sarter/David Woods: »How in the world did we ever get into that mode? Mode error and awareness in supervisory control«, in: Human Factors 37 (1995), S. 5-19; sowie Margareta Lützhöft: »Studying the effects of technological change: Bridge automation and human factors«, in: Ortung und Navigation 2 (2002), S. 107-113.

13 | Dieser sehr kritische Blick auf »situation awareness« wird z.B. am Zentrum für Mensch-Maschine-Systeme der TU Berlin propagiert, s. z.B. Stefanie Huber et al.: »Situation awareness and lighting on airport taxiways: Should situation awareness measurement be situation-specific?«, Valencia, SP: Beitrag zur European Association of Aviation Psychology Conference 2008.

14 | Sidney Dekker: 10 questions about human error: A new view of human errors and system safety, Hillsdale, NJ: Erlbaum 2005.

mehr Dinge pro Zeit erledigen zu können, vereinfachte Abkürzungen für komplizierte (aber sichere) Prozeduren zu entwickeln, ihre Aufmerksamkeit auf den Verwaltungskram zu richten. Die Entlastung von Mitarbeitern durch technische Überwachungs- und Regelungssysteme kann damit – über den Umweg der complacency – tatsächlich zur Reduktion von Sicherheit beitragen.

11.2.2 Systemverständnis

Die erfolgreiche Nutzung technischer Sicherheitssysteme setzt Systemverständnis voraus. Es genügt nicht nur die Kenntnis einzelner Komponenten, sondern die exakte Kenntnis der Produktion, Integration und Interaktion der relevanten Daten und ihrer Darstellung, z.B. in einem Lagebild, samt der Fähigkeit zur präzisen Vorhersage der Auswirkungen steuernder Eingriffe.[15] In manchen Bereichen gibt es Spezialisten, die das können. Die zunehmende Verfügbarkeit billiger Informationstechnik lässt es aber verlockend erscheinen, entsprechend komplexe Systeme aber auch dort zu installieren, wo man eine entsprechende Ausbildung der Nutzer für nicht finanzierbar hält. Oft reicht ihre Systemkenntnis dann gerade weit genug, um Routinesituationen bewältigen zu können; in Ausnahmesituationen bleibt ihnen lediglich das Handeln nach dem Prinzip von Versuch und Irrtum.[16]

Die Ausbildungsproblematik wird dadurch verschärft, dass in den meisten Fällen technologische Innovationen im Sicherheitsbereich »technology driven« sind und nicht »user driven«: Ein neues Sicherheitsprodukt, eine neue Sicherheitskonzeption ist nur in Ausnahmefällen eine Reaktion auf ein Bedürfnis des Marktes. In den meisten Fällen werden

15 | Als Beispiel denke man an das Feuermeldesystem in einem Hochhaus oder an teilredundante Systeme zur Positionsbestimmung schneller Verkehrsmittel (etwa einer Magnetschwebebahn); die Strandung des Kreuzfahrtschiffes »Royal Majesty« am 10.6.1995 war u.a. dadurch bedingt, dass die Besatzung nur mangelhafte Kenntnisse der internen Datenverarbeitungssequenzen des GPS-Systems hatte (s. Margareta Lützhöft/Sidney Dekker: »On your watch: Automation on the bridge«, in: The Journal of Navigation 55 [2002], S. 83-96.).

16 | Ich möchte hierzu eine illustrierende Anekdote schildern: Im Rahmen eines vom BMBF finanzierten Forschungsprojektes zur Informationsintegration auf Schiffsbrücken hatte ich Gelegenheit, bei Mitfahrten auf Frachtschiffen Feldforschung zu betreiben. Während einer Fahrt gerieten wir nachts in der Nordsee in einen schweren Sturm mit Orkanböen. Durch einen heftigen Seeschlag löste sich in einer Brückenkonsole ein schwerer Gegenstand und polterte hin und her. Der Kapitän – ein langjährig erfahrener Seemann – schraubte die Konsole auf und wir sahen im Licht einer Taschenlampe einen etwa computergroßen gelben Gegenstand, der lose war. »Tja, da weiß ich jetzt auch nicht, was das ist«, sprach der Kapitän, schraubte die Konsole wieder zu und begann, die ebenfalls herumfliegenden Schnittchen von der Seekarte zu kratzen.

vielversprechende Ideen junger Ingenieure in der Industrie und durch die Industrie entwickelt, ein wenig getestet und dann verkauft. Die Käufer wiederum, egal ob öffentlich oder privat, stehen unter dem Rechtfertigungsdruck, immer das neueste, ergo sicherste Produkt nutzen zu müssen, und die Nutzer – sie werden in der Regel erst gar nicht gefragt. Da die Neuentwicklung aber auch nicht auf ihre Bedürfnisse zurückgeht, sind sie nicht in jedem Fall intrinsisch motiviert, sich mit der »neuen Technik« auseinanderzusetzen.[17]

Nun könnte man natürlich Wissensdefizite zu einer individuellen Angelegenheit erklären, aber das ginge am Kern des Problems vorbei. Mangelndes Systemverständnis der Nutzer ist ein Systemproblem, kein individuelles. Die Sicherheitsindustrie investiert erhebliche Summen in die Entwicklung neuer Geräte, aber fast nichts in die Unterstützung der Ausbildung der Gerätenutzer. In den Fällen, in denen nicht der Auftraggeber entsprechende Schulungen anbietet, durchführt und kontrolliert (das ist z.B. in der Luftfahrt der Fall oder der Atomindustrie, manchmal auch in der Medizin, in der Seefahrt eher nicht), ist es nach wie vor nicht ungewöhnlich, dass der Techniker dem Nutzer ein mehrhundertseitiges Handbuch auf den Tisch legt mit der Bemerkung: »Wenn Sie irgendwelche Fragen haben – da steht alles drin.«[18]

Es verdient durchaus betont zu werden, dass in einigen mit der Produktion von »safety« oder »security« befassten Organisationen bzw. Branchen Forschungs- und Entwicklungsinstitute existieren, deren Arbeit zur Hoffnung Anlass gibt, dass die Nutzerperspektive in einen Entwicklungsprozess Eingang findet, die Regel allerdings ist das nicht.

11.2.3 Subjektives Kompetenzempfinden

Viele psychologische Handlungstheorien gehen davon aus, dass Menschen generell danach bestrebt sind, ihr »subjektives Kompetenzempfinden« möglichst hoch zu halten. Das subjektive Kompetenzempfinden kann man verstehen als zusammenfassende Abbildung des Ausmaßes, in dem es einem gelingt, seine persönlichen Bedürfnisse zu befriedigen. Zwei sehr wesentliche Quellen des subjektiven Kompetenzempfindens sind das Verständnis der Welt um einen herum und das Ausmaß, in dem

17 | S. dazu z.B. auch Steven Poltrock/Jonathan Grudin: »Organizational obstacles to interface design and development: Two participant-observer studies«, in: ACM Transactions on Computer-Human Interaction 1 (1994), S. 52-80; Jerry Busby/Ralph Hibberd: »Mutual misconceptions between designers and operators of hazardous systems«, in: Research in Engineering Design 13 (2002), S. 132-138.
18 | Ute Meck/Stefan Strohschneider/Ulrike Brüggemann: »Interaction design in ship building: An investigation in the integration of the user perspective in the design of ship bridges«, in: Journal of Maritime Studies (eingereicht).

man sie kontrollieren kann.[19] Systemverständnis und aktive Einflussmöglichkeiten sind damit wichtige Determinanten des subjektiven Kompetenzempfindens von Menschen, die mit der Produktion von Sicherheit beschäftigt sind. Im Bereich der »safety-Forschung« hat sich nun gezeigt, dass gedankenlos implementierte Technisierungsstrategien dazu führen können, dass genau diese beiden Säulen des Kompetenzempfindens geschwächt werden: Komplexe soziotechnische Systeme steuern sich weitgehend selbst, der aktiv handelnde Mensch wird aus der Kontrollschleife entfernt und auf anspruchslose und eingeschränkte Überwachungsaufgaben verwiesen. Unglücklicherweise ist jedoch genau das ein Typ von Tätigkeit, den wir als Menschen nicht wirklich gut beherrschen.[20]

Der damit verbundene Verlust an kritischer Aufmerksamkeit und die häufig zu beobachtende initiale Konfusionsphase in Sondersituationen wurden oben bereits erwähnt. Eine weitere Konsequenz von Automatisierung im Sicherheitsbereich erscheint ebenso diskussionswürdig: Wenn Systemverständnis und Kontrolle als Säulen des subjektiven Kompetenzempfindens nur in sehr eingeschränktem Maße zur Verfügung stehen, sind die Betroffenen im Interesse ihrer psychischen Gesundheit darauf angewiesen, sich nach anderen Quellen umzusehen. Hierfür kommt im Kontext beruflicher Tätigkeiten vor allem der soziale Bereich in Frage, die Suche nach dem Erleben von Gemeinschaft und gegenseitiger Bestätigung. Dies könnte mit ein Grund dafür sein, dass im Sicherheitsbereich tätige Teams zumindest von außen so häufig als »verschworene Gemeinschaften« erscheinen,[21] die sich gegenseitig ihrer Professionalität versichern, die einen ausgeprägten Korpsgeist aufweisen und deren Mitglieder

19 | S. dazu Albert Bandura: »Self-efficacy: Toward a unifying theory of behavioral change«, in: Psychological Review 84 (1977), S. 191-215; Dietrich Dörner: Bauplan für eine Seele, Reinbek bei Hamburg: Rowohlt 1999; Stefan Strohschneider: »Kompetenzdynamik und Kompetenzregulation beim Planen«, in: Stefan Strohschneider/Rüdiger von der Weth (Hg.), Ja, mach nur einen Plan: Pannen und Fehlschläge – Ursachen, Beispiele, Lösungen, Bern: Huber Verlag 2002, 2. Auflage, S. 35-51.

20 | Diese These wird mit Vehemenz z.B. von Natasha Merat (Natasha Merat: »Is drivers' situation awareness influenced by a fully automated driving scenario?« Paper auf de HFES 8, Soesterberg NL 2008) vertreten. Margareta Lützhöft (Studying the effects of technological change, 2002) zeigt, dass Operateure dazu neigen, Kontrollsysteme, die über verschiedene Modi verfügen, im primitivsten Modus »zu fahren«, um ihre Fähigkeiten, ihr handwerkliches Können beweisen zu können (vgl. zur sog. »mode awareness« Nadine Sarter/Woods, David: »How in the world did we ever get into that mode? Mode error and awareness in supervisory control«, in: Human Factors 37 (1995), S. 5-19.

21 | s. Rudi Heimann: »Polizeikultur und Veränderung – ein Blick hinter die Kulissen«, Vortrag auf der Jahrestagung »Kultur und sicheres Handeln« der Plattform Menschen in komplexen Arbeitswelten, Dornburg 2008 für die Polizei; weitere Beispiele für den Korpsgeist von Hochleistungsteams in: Peter Pawlowsky/Peter

gegenseitige Nähe suchen – sich aber eben u.U. auch stark nach außen abschotten, was bekanntlich bis zum Realitätsverlust führen kann.[22]

Menschen, die derartige Kontroll- oder Überwachungstätigkeiten alleine ausführen müssen, haben diese Möglichkeiten nur in begrenztem Umfang. Sie werden entweder soziale Kontakte aktiv und ggf. vorschriftswidrig herstellen oder sie flüchten sich in Tagträume und Phantasietätigkeit. Natürlich steht dies dem eigentlichen Sicherheitsauftrag diametral entgegen, ist aber wiederum nicht als Ausdruck individueller Schwäche zu interpretieren, sondern als Resultat eines nicht sorgfältig an das menschliche Bedürfnissystem angepassten technischen Designs.[23]

11.2.4 Bereichsübergreifende Kompetenzen

Mit dem »subjektiven Kompetenzempfinden« sind motivationale Grundlagen des Handelns angesprochen, die bei der Implementierung von Technik im Sicherheitsbereich beachtet werden müssen, um unerwünschte Nebenwirkungen zu vermeiden. Im Hinblick auf den speziellen Beitrag von Menschen zur Erhöhung der Elastizität und Widerstandsfähigkeit eines Systems sind in den letzten Jahren darüber hinaus einige allgemeine, bereichsübergreifend einsetzbare Kompetenzen (»generic competencies«) in den Fokus der Sicherheitsforschung geraten.[24] Jenseits der tätigkeitsspezifischen Kenntnisse und Fertigkeiten erfordert der konstruktive Umgang mit nicht routinemäßig zu lösenden Situationen Fähigkeiten im kommunikativen, organisatorischen und strategisch-problemlöserischen

---

Mistele (Hg.): Hochleistungsmanagement: Leistungspotenziale in Organisationen gezielt fördern. Wiesbaden: Gabler Verlag 2008.

22 | S. die grundlegende Arbeit von Irving Janis: Victims of groupthink: A psychological study of foreign-policy decisions and fiascoes, Atlanta, GA: Houghton Mifflin 1972; kritisch dazu Stefan Schulz-Hardt: Realitätsflucht in Entscheidungsprozessen: Vom Groupthink zum Entscheidungsautismus, Bern: Huber 1997.

23 | Mir sind keine Studien bekannt, die sich diesen Phänomenen gezielt gewidmet hätten. Allerdings gibt es eine Fülle anekdotischer Evidenz besonders aus solchen Arbeitsfeldern, in denen Menschen über längere Zeiträume hinweg weder soziale Kontakte pflegen noch aktive Kontrolle ausüben können. Als Mittel gegen das Tagträumen erlaubt man in manchen Organisationen mittlerweile Zeitungslektüre oder Hörbücher, in anderen installiert man »Totmannknöpfe« – die dann allerdings trickreich dysfunktional gemacht werden.

24 | S. dazu u.a. Edward Borodzicz: »The missing ingredient is the value of flexibility«, in: Simulation & Gaming 35 (2004), S. 414-426; Günter Horn/Stefan Strohschneider: »Kommunikation im Krisenstab«, in: Gesine Hofinger (Hg.), Kommunikation in kritischen Situationen, Frankfurt a.M.: Verlag für Polizeiwissenschaft 2005, S. 101-120; Roel van Winsen/Nicklas Dahlström/Sidney Dekker/James Nyce: »Rule and role-retreat: An empirical study of procedures and resilience«, in: Journal of Cognitive Engineering and Decision Making (eingereicht).

Bereich, die nicht auf erwartbare »taktische« Situationen beschränkt sind. Dazu zählen vor allem:[25]

- Eine diskursive Kommunikationsfähigkeit, d.h. die Fähigkeit, Ereignisse und kausale Zusammenhänge (verbal, visuell) darzustellen und zusammen mit anderen Beteiligten ein möglichst umfassendes »Bild« einer Situation zu erarbeiten;
- Die Fähigkeit, Entscheidungen auch unter Unsicherheit und Zeitdruck treffen zu können, ohne in jedem Fall auf die Existenz von Regeln oder die Anweisungen eines Vorgesetzten zurückgreifen zu müssen;
- Die Fähigkeit zum konstruktiven Umgang mit Informationsüberflutung auf der einen, unzuverlässiger oder fehlender Information auf der anderen Seite;
- »Problemlösefähigkeit«, die Fähigkeit zur Entwicklung neuartiger Handlungsalternativen.

Der Aufbau solcher Kompetenzen ist ein langwieriger Prozess, der die reflektierte Auseinandersetzung mit einer Vielzahl unterschiedlicher Anforderungen voraussetzt. Das Problem von Technisierungsstrategien besteht darin, dass mittlerweile in verschiedenen Branchen nachgewiesen werden konnte, dass Technisierung und Automatisierung genau diese Fähigkeiten verkümmern lassen.[26] Im Grunde genommen ist das gar nicht so überraschend: Jemand, der jahrelang alleine vor seinen Monitoren sitzt, verlernt das konstruktive Gespräch und hat dann im Notfall natürlich Schwierigkeiten, gemeinsam mit anderen aus bruchstückhaften und widersprüchlichen Informationen ein gemeinsames Lagebild diskursiv zu erzeugen. Menschen, die jahrelang immer nur auf bestimmte Anzeigen in vorgeschriebener Weise reagieren müssen, verlernen es, in Abwesenheit verlässlicher Anzeigen selbständig Entscheidungen zu treffen. Das ist eine – auch unter ethischen Gesichtspunkten – verheerende Auswir-

25 | S. dazu z.B. Cornelius Buerschaper/Gesine Hofinger/Rüdiger von der Weth: »Strategisches Denken aus dem Computer? Über den Nutzen eines Trainings allgemeiner Problemlösestrategien«, in: Ulrich Blötz (Hg.), Planspiele in der beruflichen Bildung: Auswahl, Konzepte, Lernarrangements, Erfahrungen, Bonn: Bundesinstitut für Berufsbildung 2005, Begleit-CD-ROM; Henry Wilson: »Emergency response preparedness: Small group training. Part 2 – training methods compared with learning styles«, in: Disaster Prevention and Management 9 (2000), S. 180-213.

26 | S. dazu Dietrich Manzey: »Systemgestaltung und Automatisierung«, in: Petra Badke-Schaub/Gesine Hofinger/Kristina Lauche (Hg.), Human Factors: Psychologie sicheren Handelns in Hochrisikobranchen, Heidelberg: Springer Verlag 2008, S. 307-324; sowie auch Sidney Dekker/Nicklas Dahlström/Roel van Winsen/James Nyce: »Crew resilience and simulator training in aviation«, in: Erik Hollnagel et al. (Hg.), Resilience Engineering Perspectives, Aldershot, UK: Ashgate 2008, S. 119-126.

kung gedankenloser Automatisierung, die nur schwer zu korrigieren ist. Gezielte Trainingsmaßnahmen sind hier sicherlich eine Möglichkeit, die aber durch entsprechende organisatorische Strukturen und die Anreicherung von Arbeitsprozessen ergänzt werden muss.[27]

11.2.5 Gemeinsame mentale Modelle

Die bisherigen Ausführungen konzentrierten sich auf individuelle Phänomene und Prozesse im Kontext der Technisierung der Sicherheitsproduktion. Damit soll jedoch nicht behauptet werden, dass die individuelle Ebene die einzig relevante wäre. In der HF-Forschung hat sich das Konzept der »gemeinsamen mentalen Modelle« als bedeutsamer Ansatz zum Verständnis der Schwierigkeiten und Probleme der Zusammenarbeit von Menschen in komplexen Situationen herauskristallisiert. Als »mentales Modell« bezeichnet man die kognitive Repräsentation eines außerweltlichen Funktionszusammenhanges,[28] mit dem »gemeinsamen« mentalen Modell bezeichnet man einen hohen Übereinstimmungsgrad zwischen den individuellen Modellen der Mitglieder eines Teams über Schlüsselbereiche der gemeinsam relevanten Realität.[29]

Die enorme Bedeutung gemeinsamer mentaler Modelle für die Bewältigung schwieriger Situationen durch Teams, Stäbe usw. ist mittlerweile überzeugend nachgewiesen.[30] Was die Auswirkungen von Technisierungsstrategien anbelangt, kommt man dabei zu bisweilen überraschenden Einsichten. So untersucht man beispielsweise unter dem Stichwort »multi-agency-cooperation« die Schwierigkeiten und Fallgruben, die bei der Zusammenarbeit verschiedener Dienste in kritischen Großlagen entstehen. Bei dieser Form der Zusammenarbeit erweisen sich vor allem zwei potenzielle »Bruchlinien« als bedeutsam: die Frage der Machtverteilung und das Problem des Aufbaus eines gemeinsamen Lageverständnisses,

27 | Vgl. Gesine Hofinger: »Teamtrainings für die Krisenbewältigung«, in: Cornelius Buerschaper/Susanne Starke (Hg.), Führung und Teamarbeit in kritischen Situationen, Frankfurt a.M.: Verlag für Polizeiwissenschaft 2008, S. 190-205; Stefan Strohschneider: »Human Factors Training«, in: Petra Badke-Schaub/Gesine Hofinger/Kristina Lauche (Hg.), Human Factors: Psychologie sicheren Handelns in Hochrisikobranchen, Heidelberg: Springer Verlag 2008, S. 289-306.

28 | Philip Johnson-Laird: »Mental models in cognitive science«, in: Cognitive Science 4 (1980), S. 71-115.

29 | S. dazu Richard Klimoski/Susan Mohammed: »Team mental model: Construct or metaphor?«, in: Journal of Management 20 (1994), S. 403-437; aber auch Reimer Bierhals: »Führung mit geteilten mentalen Modellen«, in: Cornelius Buerschaper/Susanne Starke (Hg.), Führung und Teamarbeit in kritischen Situationen, Frankfurt a.M.: Verlag für Polizeiwissenschaft 2008, S. 86-109.

30 | S. dazu zusammenfassend Douglas Paton/Duncan Jackson: »Developing disaster management capability: An assessment centre approach«, in: Disaster Prevention and Management 11 (2002), S. 115-122.

eine geteilten mentalen Modells. Technisierung spielt hinsichtlich beider Aspekte eine Rolle: Zusammenarbeit bei kritischen Großlagen erfordert von den beteiligten Diensten in der Regel den Aufbau von ad-hoc-Strukturen, die mit den geübten Abläufen nichts mehr gemeinsam haben. Darüber hinaus müssen einzelne Dienste u.U. dazu gebracht werden, im Sinne der Gesamtlösung ihre eigenen »goldenen Regeln« zu verletzen.[31]

Eine sehr kritische Analyse legt beispielsweise der englische Organisationssoziologe Richard McMaster vor, der die Organisationsstrukturen und Entscheidungsfindungsprozesse während der Flutkatastrophe in England 2007 untersucht hat.[32] Auf dem Papier sahen die Strukturen der interorganisationalen Zusammenarbeit zwischen Polizei, Feuerwehr, Militär, Umweltschutzorganisationen usw. einfach und klar aus. In der Realität entwickelten sich jedoch davon deutlich abweichende ad-hoc-Strukturen, die zwar flexibel an die Lage angepasst waren, aber erhebliche Kommunikationserfordernisse mit sich brachten. McMaster führt den Erfolg derartig flexibler Reaktionen darauf zurück, dass zwischen exponierten Protagonisten der beteiligten Dienste Vertrauen hergestellt werden kann, wenn die Lageeinschätzungen ausdiskutiert und Machtfragen ausbalanciert werden können. Der Aufbau von Vertrauen aber erfordert Kommunikation, am besten von Angesicht zu Angesicht. Laut seiner Studie war die erfolgreiche Bewältigung einiger kritischer Situationen während der Flut nur deshalb möglich, weil es *keine* gemeinsame Informationsplattform gab, weil die Stäbe gezwungen waren, miteinander zu reden, und sich auf diese Weise ein gemeinsames Lagebild entwickeln und Vertrauen entstehen konnte.

Man muss nicht so weit gehen wie McMaster, der mahnt, dass »technology may even be a barrier to shared understanding in multi-agency operations«.[33] Man sollte aber bedenken, dass erfolgreiche Interaktion im Sicherheitsbereich bestimmte diskursive Formen der Kommunikation erfordert, die durch technische Kommunikationslösungen nicht erschwert oder sogar unmöglich gemacht werden dürfen.

31 | S. dazu Rüdiger von der Weth: »Risikoabwägung und Prozesssteuerung in kritischen Situationen«, in: Stefan Strohschneider (Hg.), Entscheiden in kritischen Situationen, Frankfurt a.M.: Verlag für Polizeiwissenschaft, 2. Auflage 2007, S. 41-54, und seine Analyse der Bewältigung der Flutkatastrophe in Sachsen.

32 | Richard McMaster/Chris Baber: »Multi-agency operations: Cooperation during flooding«, Paper auf der Human Factors and ergonomics Society European Chapter Conference in Soesterberg, NL 2008.

33 | Richard McMaster, mündl. Mitteilung, 16.10.2008.

11.3 Schlussbemerkung

Die safety-orientierte HF-Forschung macht auf einige psychische und soziale Voraussetzungen aufmerksam, die bedacht werden sollten, wenn Technisierung die intendierten Effekte – nämlich ein Mehr an Sicherheit – haben soll. Dies sollte jedoch keineswegs als Argument gegen jegliche Technisierung verstanden werden. Beispielsweise sind technische Neuentwicklungen unter Nutzerperspektive dann relativ unproblematisch, wenn sie das menschliche Wahrnehmungsvermögen verbessern, ohne die sozialen, kognitiven oder motivationalen Voraussetzungen des Handelns gravierend zu verändern.[34, 35] Dies gilt insbesondere in den Bereichen der »security«, wo man mit absichtlichen Schädigungsversuchen rechnet.

Alle über die Einführung schlichter Wahrnehmungsapparate hinausgehenden Innovationen müssen jedoch damit rechnen, dass sie zwar bestimmte Probleme lösen, aber mit Sicherheit auch neue schaffen. Deren Gravidität muss jedoch in jedem Einzelfall überprüft werden – häufig ist das erst nach längerer Nutzungsphase möglich. Es gilt damit auch im Bereich der »security« Abstand zu nehmen von der naiven Annahme, mehr Technik bedeute automatisch mehr Sicherheit. Technische Innovationen werden dann problematisch, wenn sie eingespielte und zuverlässig funktionierende Prozesse verändern und wenn die spezifisch menschlichen Stärken – flexible Reaktion auf unvorhergesehene Ereignisse, Abpuffern von Systemausfällen – beeinträchtigt werden. Es geht dabei nicht nur um das vordergründige Problem der Akzeptanz von Technik durch die Nutzer. Es geht um das tiefer greifende Problem, inwieweit eine technologische Innovation im Sicherheitsbereich die kritischen Fähigkeiten des Sicherheit schaffenden Personals langfristig verkümmern lässt.

34 | Ein Beispiel für eine solche Innovation ist das Fernglas. Die Entwicklung fortgeschrittener Sensorik könnte ein weiteres Beispiel sein: Es ist besser, wenn der Bergmann durch einen guten Sensor vor zu hoher Methangaskonzentration gewarnt wird, als wenn dafür ein Kanarienvogel sterben muss, und es ist besser, einen Kanarienvogel zu opfern, als darauf zu warten, bis man die Wirkungen des tödlichen Gases selber spürt.

35 | Hier wird aus der Perspektive des Nutzers argumentiert. Damit wird keinesfalls geleugnet, dass auch für den Nutzer unproblematische Wahrnehmungsapparate auf der gesellschaftlichen Ebene weitreichende ethische Implikationen haben können.

Literatur

Amalberti, Rene et al.: »Human factors in aviation: An introductory course«, in: Klaus-Martin Goeters (Hg.), Aviation psychology: A science and a profession, Aldershot, GB: Ashgate 1998, S. 19-43.

Badke-Schaub, Petra/Hofinger, Gesine/Lauche, Kristina (Hg.): Human Factors: Psychologie sicheren Handelns in Hochrisikobranchen, Heidelberg: Springer Verlag 2008.

Bandura, Albert: »Self-efficacy: Toward a unifying theory of behavioral change«, in: Psychological Review 84 (1977), S. 191-215.

Bierhals, Reimer: »Führung mit geteilten mentalen Modellen«, in: Cornelius Buerschaper/Susanne Starke (Hg.), Führung und Teamarbeit in kritischen Situationen, Frankfurt a.M.: Verlag für Polizeiwissenschaft 2008, S. 86-109.

Borodzicz, Edward: »The missing ingredient is the value of flexibility«, in: Simulation & Gaming 35 (2004), S. 414-426.

Buerschaper, Cornelius/Hofinger, Gesine/von der Weth, Rüdiger: »Strategisches Denken aus dem Computer? Über den Nutzen eines Trainings allgemeiner Problemlösestrategien«, in: Ulrich Blötz (Hg.), Planspiele in der beruflichen Bildung: Auswahl, Konzepte, Lernarrangements, Erfahrungen, Bonn: Bundesinstitut für Berufsbildung 2005, Begleit-CD-ROM.

Bundesverwaltungsamt – Zentralstelle für Zivilschutz (Hg.): Stress im Katastrophenschutz: Zwischenbilanz und Forschungsbedarf. Ergebnisse eines Workshops, Bonn: Schriftenreihe WissenschaftsForum der Akademie für Krisenmanagement, Notfallplanung und Zivilschutz, Band 2, 2002.

Busby, Jerry/Hibberd, Ralph: »Mutual misconceptions between designers and operators of hazardous systems«, in: Research in Engineering Design 13 (2002), S. 132-138.

Dahlström, Nicklas/Dekker, Sidney: »Security and safety synergy: Advancing security with Human Factors knowledge«, in: John G. Voeller (Hg.), Wiley Handbook of Science & Technology for Homeland Security, Chichester, GB: John Wiley & sons 2008 (Online-Ausgabe, s. http://mrw.interscience.wiley.com/emrw/9780470087923/hhs/article/hhs298/current/abstract; zugegriffen am 24.2.2009).

Dekker, Sidney: 10 questions about human error: A new view of human errors and system safety, Hillsdale, NJ: Erlbaum 2005.

Dekker, Sidney/Dahlström, Nicklas/van Winsen, Roel/Nyce, James: »Crew resilience and simulator training in aviation«, in: Erik Hollnagel et al. (Hg.), Resilience Engineering Perspectives, Aldershot, UK: Ashgate 2008, S. 119-126.

Dörner, Dietrich: Bauplan für eine Seele, Reinbek bei Hamburg: Rowohlt 1999.

Durso, Frank/Gronlund, Scott: »Situation awareness«, in: Frank Durso (Hg.), Handbook of applied cognition, New York: Wiley 1999, S. 283-314.

Endsley, Mica: »Toward a theory of situation awareness in dynamic systems«, in: Human Factors 37 (1995), S. 32-64.

Hanzu-Pazara, Radu et al.: »Reducing of maritime accidents caused by human factors using simulators in training process«, in: Journal of Maritime Research 5 (2008), S. 3-18.

Heimann, Rudi: »Polizeikultur und Veränderung – ein Blick hinter die Kulissen«, Vortrag auf der Jahrestagung »Kultur und sicheres Handeln« der Plattform Menschen in komplexen Arbeitswelten, Dornburg 2008.

Hofinger, Gesine: »Teamtrainings für die Krisenbewältigung«, in: Cornelius Buerschaper/Susanne Starke (Hg.), Führung und Teamarbeit in kritischen Situationen, Frankfurt a.M.: Verlag für Polizeiwissenschaft 2008, S. 190-205.

Hollnagel, Erik/Nemeth, Christopher/Dekker, Sidney (Hg.): Resilience engineering perspectives: Remaining sensitive to the possibility of failure, Aldershot, GB: Ashgate 2008.

Horn, Günter/Strohschneider, Stefan: »Kommunikation im Krisenstab«, in: Gesine Hofinger (Hg.), Kommunikation in kritischen Situationen, Frankfurt a.M.: Verlag für Polizeiwissenschaft 2005, S. 101-120.

Huber, Stefanie et al.: »Situation awareness and lighting on airport taxiways: Should situation awareness measurement be situation-specific?«, Valencia, SP: Beitrag zur European Association of Aviation Psychology Conference 2008.

Janis, Irving: Victims of groupthink: A psychological study of foreign-policy decisions and fiascoes, Atlanta, GA: Houghton Mifflin 1972.

Johnson-Laird, Philip: »Mental models in cognitive science«, in: Cognitive Science 4 (1980), S. 71-115.

Klimoski, Richard/Mohammed, Susan: »Team mental model: Construct or metaphor?«, in: Journal of Management 20 (1994), S. 403-437.

Lützhöft, Margareta: »Studying the effects of technological change: Bridge automation and human factors«, in: Ortung und Navigation 2 (2002), S. 107-113.

Lützhöft, Margareta/Dekker, Sidney: »On your watch: Automation on the bridge«, in: The Journal of Navigation 55 (2002), S. 83-96.

Manzey, Dietrich: »Systemgestaltung und Automatisierung«, in: Petra Badke-Schaub/Gesine Hofinger/Kristina Lauche (Hg.), Human Factors: Psychologie sicheren Handelns in Hochrisikobranchen, Heidelberg: Springer Verlag 2008, S. 307-324.

McMaster, Richard/Baber, Chris: »Multi-agency operations: Cooperation during flooding«, Paper auf der Human Factors and ergonomics Society European Chapter Conference in Soesterberg, NL 2008.

Meck, Ute/Strohschneider, Stefan/Brüggemann, Ulrike: »Interaction design in ship building: An investigation in the integration of the user perspective in the design of ship bridges«, in: Journal of Maritime Studies (eingereicht).

Merat, Natasha: »Is drivers' situation awareness influenced by a fully

automated driving scenario?« Paper auf de HFES 8, Soesterberg NL 2008.
National Transportation Safety Board (Hg): We are all safer: Lessons learned and lives saved, Washington, DC: Safety Report/SR-07/01, 5. Auflage 2007.
Norris, Andy: »Laying the blame for bridge design«, in: Digital Ship, Oct. 2008, S. 34.
Parasuraman, Raja/Molloy, Robert/Singh, Indramani: »Performance consequences of automation-induced complacency«, in: The International Journal of Aviation Psychology 3(1) (1993), S. 1-23.
Paton, Douglas/Jackson, Duncan: »Developing disaster management capability: An assessment centre approach«, in Disaster Prevention and Management 11 (2002), S 115-122.
Pawlowsky, Peter/Mistele, Peter (Hg.): Hochleistungsmanagement: Leistungspotenziale in Organisationen gezielt fördern. Wiesbaden: Gabler Verlag 2008.
Poltrock, Steven/Grudin, Jonathan: »Organizational obstacles to interface design and development: Two participant-observer studies«, in: ACM Transactions on Computer-Human Interaction 1 (1994), S. 52-80.
Reason, James: Menschliches Versagen: Psychologische Risikofaktoren und moderne Technologien, Heidelberg: Spektrum Verlag 1994.
Sarter, Nadine/David Woods: »How in the world did we ever get into that mode? Mode error and awareness in supervisory control«, in: Human Factors 37 (1995), S. 5-19.
Schager, Bengt: »Accidents due to human error are increasing in the maritime industry«, in: The Swedish Club Letter, 2-2008 (2008), S. 12-13.
Schulz-Hardt, Stefan: Realitätsflucht in Entscheidungsprozessen: Vom Groupthink zum Entscheidungsautismus, Bern: Huber 1997.
Strohschneider, Stefan: »Kompetenzdynamik und Kompetenzregulation beim Planen«, in: Stefan Strohschneider/Rüdiger von der Weth (Hg.), Ja, mach nur einen Plan: Pannen und Fehlschläge – Ursachen, Beispiele, Lösungen, 2. Aufl., S. 35-51. Bern: Huber 2002.
Strohschneider, Stefan: »Human Factors Training«, in: Petra Badke-Schaub/Gesine Hofinger/Kristina Lauche (Hg.), Human Factors: Psychologie sicheren Handelns in Hochrisikobranchen, Heidelberg: Springer Verlag 2008, S. 289-306.
Van Winsen, Roel/Dahlström, Nicklas/Dekker, Sidney/Nyce, James: »Rule and role-retreat: An empirical study of procedures and resilience«, in: Journal of Cognitive Engineering and Decision Making (eingereicht).
Von der Weth, Rüdiger: »Risikoabwägung und Prozesssteuerung in kritischen Situationen«, in: Stefan Strohschneider (Hg.), Entscheiden in kritischen Situationen, Frankfurt a.M.: Verlag für Polizeiwissenschaft, 2. Auflage 2007, S. 41-54.
Wilson, Henry: »Emergency response preparedness: Small group training. Part 2 – training methods compared with learning styles«, in: Disaster Prevention and Management 9 (2000), S. 180-213.