Frank Ritz

Betriebliches Sicherheitsmanagement

Aufbau und Entwicklung widerstandsfähiger Arbeitssysteme

eBook
SCHÄFFER POESCHEL

SCHÄFFER
POESCHEL

Frank Ritz

Betriebliches Sicherheitsmanagement

Aufbau und Entwicklung widerstandsfähiger Arbeitssysteme

2015
Schäffer-Poeschel Verlag Stuttgart

Bibliografische Information der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Print ISBN 978-3-7910-3302-0 Bestell-Nr. 20488-0001
EPDF ISBN 978-3-7992-6738-0 Bestell-Nr. 20488-0150

www.schaeffer-poeschel.de
info@schaeffer-poeschel.de

Lektorat: Michael Bauer, Mainz
Einbandgestaltung: Löffelhardt Willy/Petra Rehr
Satz: Johanna Boy, Brennberg

März 2015

Schäffer-Poeschel Verlag Stuttgart
Ein Tochterunternehmen der Haufe Gruppe

Vorwort

Allein während der kurzen Zeit, in der dieses Buch entstanden ist, haben sich weltweit zahlreiche Katastrophen und Unfälle ereignet. Da sind z. B. der verschollene Flug MH 370, bei dem ein Flugzeug mit 239 Insassen auf dem Flug von Kuala Lumpur nach Peking spurlos verwand, und ein Fährunglück in den Gewässern Südkoreas, bei dem mindesten 270 Menschen das Leben verloren. Es ereignete sich ein Zugunglück in der Nähe von Tiefencastel in der Schweiz, in dessen Folge ein Mensch starb. Bei der Explosion einer Hochdruckgasleitung im deutschen Ludwigshafen verloren zwei Bauarbeiter das Leben, zahlreiche Menschen wurden verletzt und es entstand hoher Sachschaden. Dem Ausbruch einer Ebola-Epidemie in Westafrika erlagen dort bis jetzt schon tausende Menschen und die globalen Konsequenzen sind derzeit noch nicht absehbar. Viele andere Ereignisse haben sich zugetragen, die hier unerwähnt bleiben.

Wenn wir mit derartigen Ereignissen konfrontiert werden, fragen wir uns sowohl, wie es zu deren Entstehung kommen konnte, als auch, wie gleichartige Ereignisse zukünftig verhindert werden können. Genau mit diesen beiden Fragen beschäftigen sich die Sicherheitswissenschaften. Dabei kooperieren in multidisziplinärer oder interdisziplinärer Zusammenarbeit Personen aus unterschiedlichen Disziplinen wie den Ingenieurwissenschaften, der Politikwissenschaft, der Psychologie, den Rechtswissenschaften, der Soziologie und den Wirtschaftswissenschaften.

Dieses Buch richtet sich vorwiegend an Personen, die sich professionell mit dem Thema Sicherheitsmanagement in der betrieblichen Praxis auseinandersetzen wollen oder solche, die sich dafür qualifizieren möchten. Es ist weniger an Wissenschaftlerinnen und Wissenschaftler gerichtet, auch wenn die Hoffnung besteht, dass es ebenfalls in dieser Personengruppe gelesen wird. Zur Zielgruppe gehören vorrangig diejenigen, die als Sicherheitsverantwortliche oder Führungskräfte in Unternehmen arbeiten, deren Produktions- oder Dienstleitungsprozesse mit einem hohen Gefährdungspotenzial verbunden sind, z. B. in Branchen wie Luftfahrt, Kerntechnik, Medizin, Pharmazeutik, Reedereien, Schienenverkehr oder chemische Industrie. Hinzu kommen Personen, die in Organisationen arbeiten, welche regulativen Einfluss auf Unternehmen aus den genannten Branchen nehmen, z. B. von Aufsicht führenden Behörden, Risikobewertungsunternehmen, Rückversicherern, öffentlichen Interessensverbänden oder Personen aus der Politik.

Das zentrale Anliegen dieses Buches ist eine Sensibilisierung für das Thema Systemsicherheit in Kombination mit der Befähigung, sich aktiv mit der Gefahrenprävention und Gefahrenbewältigung in und zwischen Organisationen auseinanderzusetzen. Dieses Buch beansprucht nicht, eine vollumfängliche Zusammenfassung aller Theorien und Konzept zum Thema betriebliches Sicherheitsmanagement zu geben. Dies ist allein schon aufgrund der Verschiedenartigkeit von Branchen und Organisationen, die Sicherheitsmanagement auf unterschiedliche Arten betreiben, nicht möglich.

Es werden vielmehr diejenigen Theorien und Konzepte vermittelt, die sich in den vergangenen Jahren bei der Aus- und Weiterbildung für die Teilnehmerinnen und Teilnehmer als besonders hilfreich erwiesen haben.

Dieses Buch ist in sieben Kapitel gegliedert, die aufeinander aufbauend wesentliche Erkenntnisse vermitteln, wie einerseits Gefahren entstehen und andererseits widerstandsfähige Arbeitssysteme aufgebaut und weiterentwickelt werden.

Dazu werden in Kapitel 1 umgangssprachlich oft synonym verwendete Termini wie Risiko, Sicherheit und Zuverlässigkeit erklärt. Anschließend werden grundsätzliche Definitionen und Konzepte vermittelt, die thematisch mit Sicherheit in Verbindung stehen. Zusätzlich wird ein erster Blick auf diejenigen Faktoren der Organisationsumwelt geworfen, welche die Systemsicherheit einer Organisation systematisch beeinflussen.

Kapitel 2 beschäftigt sich mit der Entstehung von Unsicherheit und Schäden. Dabei wird ein Überblick über die einflussreichsten sicherheitswissenschaftlichen Theorien gegeben und es werden Modelle der Ereignisentstehung vermittelt, die beschreiben, durch welche Wirkzusammenhänge Unfälle in komplexen Systemen hervorgerufen werden.

Sicherheit und Unsicherheit entstehen unter dem Einfluss kultureller Bedingungen einer Organisation. Sicherheitskultur ist deshalb Gegenstand von Kapitel 3, das neben der Funktion von Kultur auch Ansätze zur Entwicklung von Sicherheitskultur beschreibt und diese gegenüber ähnlichen Konzepten wie Sicherheitsklima und Sicherheitsmanagement abgrenzt.

In Organisationen kommt in zunehmenden Maße Technik zum Einsatz, besonders durch Digitalisierung. Die Implementierung technischer Komponenten führt mitunter zu einer wachsenden Komplexität und Dynamik in Organisationen, obwohl man sich dadurch eine Vereinfachung versprochen hat. Kapitel 4 befasst sich mit dem soziotechnischen Systemansatz und der Gestaltung von Mensch-Maschine-Systemen, wobei ein Schwerpunkt dem Thema Automatisierung gewidmet ist. Dieses Kapitel akzentuiert die Bedeutung der komplementären Gestaltung von Arbeit durch Technikentwicklung in Wechselwirkung mit sozialen/menschlichen Prozessen, wobei diejenigen Gefahren beschrieben werden, die beim Zusammenwirken von Mensch und Technik entstehen.

Um diesen Gefahren schon bei der Systemgestaltung gezielt entgegenwirken zu können, werden in Kapitel 5, Human Factors, die wichtigsten Themen menschlicher Leistungsfähigkeit und ihrer Begrenzungen zur Gestaltung von Produkten und Prozessen differenziert dargeboten.

Kapitel 6 widmet sich dem Thema Organisation und führt in Prinzipien der Organisationsgestaltung ein. Dabei werden Aspekte wie Führung, Regeln, Prozeduren, Standardisierung und Anpassungsfähigkeit veranschaulicht und auf Sicherheit bezogen.

Kapitel 7 behandelt die wesentlichen Methoden, die zum Aufbau und zur Entwicklung widerstandsfähiger Arbeitssysteme verwendet werden, sowie die Beschreibung der Rahmenbedingungen für effektives Sicherheitsmanagement.

Es ist der Anspruch dieses Buches, einen Beitrag zur Professionalisierung des Sicherheitsmanagements zu leisten.

Auf eine geschlechtsneutrale Verwendung von Begriffen wird geachtet. Sofern in Beispielen oder anderen Textstellen einmal die männliche, ein anderes Mal die weibliche Form verwendet wird, ist dies keineswegs mit Wertungen verbunden.

Danksagung

Ich möchte die Gelegenheit nutzen und mich bei all denjenigen bedanken, die in unterschiedlicher Weise zum Gelingen dieses Buches beigetragen haben. Viele wertvolle Anregungen haben die Teilnehmerinnen und Teilnehmer betrieblicher Weiterbildungen, die ich durchgeführt habe, gegeben. Zahlreiche Anmerkungen stammen von Studierenden aus den Studiengängen in der Aus- und Weiterbildung, in denen ich als Dozent und/oder Leiter tätig bin. Für die tollen Anmerkungen und intensiven Diskussionen richte ich einen herzlichen Dank an alle, v. a. auch dafür, dass mir ein Teil meiner wissenschaftlichen Flausen ausgetrieben wurde.

Einen herzlichen Dank richte ich an die Leitung der Hochschule für Angewandte Psychologie der Fachhochschule Nordwestschweiz, die mir mit der großzügigen Bewilligung eines Forschungsfreisemesters die erforderliche Zeit zum Abfassen dieses Buches bereitgestellt hat.

Daneben gibt es eine Reihe von Kolleginnen und Kollegen, mit denen ich in unterschiedlicher Form und bei unterschiedlichen Gelegenheiten habe zusammenarbeiten und unterschiedliche Standpunkte habe diskutieren dürfen. Die zahlreichen Hinweise sind sicher in dieses Buch eingeflossen ebenso wie die praktischen Erfahrungen von Industriepartnern aus Forschungs- und Entwicklungsprojekten bei der gemeinsamen Umsetzung von Methoden in die betriebliche Praxis.

Außerdem danke ich den Mitgliedern der Plattform Sicherheitsmanagement. Sie haben ein stabiles Netzwerk etabliert, durch das Schaffende aus betrieblicher und wissenschaftlicher Praxis unter dem Eindruck aktueller Herausforderungen bei der Professionalisierung des Sicherheitsmanagements praxisbezogen wirken können. Für dieses Buch waren unsere gemeinsamen Sitzungen eine stetige Quelle der Inspiration.

Mein besonderer Dank richtet sich an Helmut Beloch für die wertvollen Diskussionen zum und den Korrekturarbeiten am Manuskript. Michael Bauer danke ich sehr für sein gründliches und inspirierendes Lektorat.

Mein abschließender und tief empfundener Dank gilt meiner Partnerin Esther für alles, was Du in vielfältiger Weise zu diesem Buch beigetragen hast. Und insbesondere dafür, mich während der vergangenen Monate ertragen zu haben.

Basel, im Oktober 2014 Frank Ritz

Inhaltsverzeichnis

Vorwort V
Danksagung VII
Abbildungsverzeichnis XIII
Beispielverzeichnis XVI

1 Sicherheit: Begriffsbestimmung und Systematisierung 1
1.1 Statisches Verständnis von Sicherheit 2
1.2 Dynamisches Verständnis von Sicherheit 4
1.2.1 Sicherheit als Prozess 5
1.2.2 Umgang mit Ungewissheit 5
1.2.3 Das Verhältnis von Sicherheit und Zuverlässigkeit 6
1.3 Sicherheit als Systemsicherheit 8
1.3.1 Arbeits- und Prozesssicherheit 9
1.3.2 Bedingungen sicherheitsgerichteten Verhaltens 11
1.4 Einflussfaktoren der Systemumwelt auf die Systemsicherheit 12

2 Sicherheitswissenschaftliche Theorien und Ereignisentstehungsmodelle 17
2.1 Sicherheitswissenschaftliche Theorien 17
2.1.1 Normal Accidents Theory 17
2.1.2 High Reliability Organization Theory 19
2.1.3 Resilience Engineering 21
2.1.4 Zusammenfassender Vergleich sicherheitswissenschaftlicher Theorien 23
2.2 Modelle der Ereignisentstehung 24
2.2.1 Lineare Ereignisentstehung: Das Dominosteinmodell 24
2.2.2 Komplexe, lineare Ereignisentstehung: Das Schweizer-Käse-Modell 27
2.2.3 Systemische Ereignisentstehung: Drift to Danger 30
2.2.4 Zusammenfassende Bewertung der Modelle 35

3 Sicherheitskultur 37
3.1 Allgemeiner Kulturbegriff 37
3.2 Psychologisches Kulturmodell 38
3.3 Entwicklung von Sicherheitskultur 42
3.3.1 Organisationales Lernen 42
3.3.2 Transformation aktionsfähigen Wissens 47
3.4 Funktion von Sicherheitskultur in Organisationen 49
3.4.1 Sicherheitskultur als Erklärungsmodell der Ereignisentstehung 49
3.4.2 Sicherheitskultur als normatives Modell 51
3.4.3 Reifegradmodell der Sicherheitskultur 54
3.4.4 Sicherheitskultur als informierte Kultur 55
3.5 Weiterentwicklung von Sicherheitskultur durch Organisationale Resilienz . . 57
3.6 Abgrenzung und Einordnung von Sicherheitskultur 60

4 Soziotechnischer Systemansatz und Mensch-Maschine-Systeme 63
4.1 Soziotechnischer Systemansatz 63
4.1.1 Entstehung des soziotechnischen Systemansatzes 63
4.1.2 Aufbau soziotechnischer Systeme. 64
4.2 Mensch-Maschine-Systeme 66
4.2.1 Historische Entwicklung der Mensch-Maschine-System-Forschung 67
4.2.2 Systematisierung von Mensch-Maschine-Systemen 68
4.2.3 Ebenen technischen Handelns 69
4.2.4 Gestaltung der Mensch-Maschine-Interaktion 70
4.2.5 Automatisierung 72
4.2.6 Usability 82
4.2.7 Interaktion zwischen Mensch und Maschine. 84

5 Human Factors 87
5.1 Mentale Repräsentation 87
5.2 Wissen zur Steuerung und Kontrolle technischer Systeme 88
5.3 Situationsbewusstsein 90
5.4 Belastung und Beanspruchung. 92
5.5 Aufmerksamkeit und Informationsverarbeitung 94
5.5.1 Vigilanz 94
5.5.2 Erregung. 95
5.5.3 Selektive Aufmerksamkeit 96
5.5.4 Ressourcenmodelle 99
5.6 Kognitive Handlungskontrolle 103
5.7 Modell der Entscheidungsleiter 106
5.8 Menschliche Fehler 108
5.8.1 Basisfehlertypen 109
5.8.2 Dynamische Entstehung von Fehlern 110
5.9 Motorische Kontrolle 111
5.9.1 Parameter der Bewegungsausführung 114
5.9.2 Fehler bei Bewegungen 114
5.10 Sozialpsychologische Faktoren 115
5.10.1 Soziale Kognition 116
5.10.2 Attribution 119
5.10.3 Kognitive Dissonanz 121
5.10.4 Soziale Normen und Konformität 123
5.10.5 Einstellung und Einstellungsänderung 123
5.10.6 Verantwortungsdiffusion 126
5.10.7 Gruppeneffekte am Beispiel Groupthink 127
5.10.8 Konflikt und Kooperation zwischen Gruppen 129

6 Organisation 131
6.1 Organisationsprinzipien. 131
6.1.1 Unterteilung in funktionale Einheiten 132

6.1.2 Führung . . . 133
6.1.3 Sinnstiftung . . . 136
6.1.4 Selbstregulation . . . 138
6.1.5 Planung . . . 139
6.1.6 Lose Kopplung: Bindung versus Autonomie . . . 140
6.1.7 Standards und Anpassungsfähigkeit . . . 143
6.1.8 Regeln und Routinen . . . 147
6.1.9 Aufgaben . . . 151
6.2 Veränderung in Organisationen . . . 154
6.2.1 Fortwährende Verbesserung . . . 154
6.2.2 Veränderungsmanagement . . . 156

7 Sicherheitsmanagement . . . 159
7.1 Methoden des Sicherheitsmanagements . . . 160
7.1.1 Risikoidentifikation und Risikoverringerung . . . 162
7.1.2 Sicherheitsschulungen und Sicherheitstrainings . . . 165
7.1.3 Monitoring der Sicherheitsleistung . . . 167
7.1.4 Meldesysteme . . . 168
7.1.5 Ereignisanalyse . . . 173
7.1.6 Auditierung . . . 177
7.1.7 Berichts- und Prozesswesen . . . 179
7.2 Rahmenbedingungen . . . 180
7.2.1 Sicherheitspolitik im Unternehmen . . . 180
7.2.2 Ressourcen für Sicherheitsleistung . . . 183
7.2.3 Verantwortung für Sicherheit . . . 186

Schlusswort . . . 193

Literaturverzeichnis . . . 195

Stichwortverzeichnis . . . 211

Der Autor . . . 214

Abbildungsverzeichnis

Abb. 1: Kombinationsmöglichkeiten von Sicherheit und Zuverlässigkeit in einem komplexen System als Vierfeldertafel visualisiert 7
Abb. 2: Sicherheit im situationalen Kontext (nach Ritz et al., 2013, S. 5) 8
Abb. 3: Soziotechnisches System involviert in Risikomanagement (nach Rasmussen, 1997, S. 185) 15
Abb. 4: Vier Grundsteine der Resilienz (nach Hollnagel, 2011, S. xxxvii) 22
Abb. 5: Ratio von Heinrich (1931) als Eisbergmetapher illustriert 25
Abb. 6: Dominomodell (aus Heinrich, 1950, S. 13) 26
Abb. 7: Das Entfernen des zentralen Faktors »unsichere Handlung und mechanische Gefahr« (aus Heinrich, 1950, S. 13) 26
Abb. 8: Das Entfernen des zentralen Faktors unterbricht den Unfallentstehungsprozess (aus Heinrich, 1950, S. 13) 26
Abb. 9: Modell der linearen, komplexen Ereignisentstehung (nach Reason, 1990, S. 208) 28
Abb. 10: Organisationale Perspektive der Ereignisentstehung (nach Reason, 1997, S. 17) 29
Abb. 11: Komplexes Muster des Fährunglücks in Zeebrügge (nach Rasmussen, 1997, S. 188) 32
Abb. 12: Drift-to-danger-Modell der systemischen Ereignisentstehung (nach Rasmussen, 1997, S. 190) 34
Abb. 13: Kulturmodell (nach Schein, 1990) 39
Abb. 14: Organisationales Lernen (nach Argyris & Schön, 1996) 43
Abb. 15: Wissensspirale (nach Nonaka & Takeuchi, 1995) 48
Abb. 16: Stadien der Ereignisentstehung (nach Turner & Pidgeon, 1997, S. 72) 51
Abb. 17: Normatives Modell der Sicherheitskultur in kerntechnischen Anlagen (nach INSAG-15, 2002, S. 2) 53
Abb. 18: Reifegradmodell der Sicherheitskultur (nach Hudson, 2007, S. 704) 55
Abb. 19: Vier Elemente von Sicherheitskultur als informierte Kultur (nach Reason, 1997) 56
Abb. 20: Zusammenwirken von technischem und sozialem Teilsystem bei der Erfüllung des Systemzwecks (nach Ulich, 2005, S.195) 65
Abb. 21: Historische Entwicklungsphasen der Mensch-Maschine-System-Forschung (nach Timpe & Kolrep, 2002, S. 35) 67
Abb. 22: Systematisierung eines Mensch-Maschine-Systems (nach Timpe & Kolrep, 2002) 69
Abb. 23: Wirkzusammenhänge zwischen den Ebenen technischen Handelns (nach Timpe & Kolrep, 2002, S. 15) 70
Abb. 24: Einfaches Modell menschlicher Informationsverarbeitung (nach Parasuraman et al., 2000, S. 287) 74
Abb. 25: Stufen der Automatisierung und Handlungsauswahl (nach Parasuraman et al., 2000, S. 287) 75

Abb. 26: Taxonomie möglicher Automatisierungsstufen (nach Endsley & Kaber, 1999, S. 466) 76
Abb. 27: Beispiel einer MABA-MABA-Liste (Fitts, 1951; nach Hauß & Timpe, 2002, S. 55) 78
Abb. 28: Auswahl beitragender Faktoren zum Verlust des Situationsbewusstseins durch Out of the Loop Unfamiliarity (nach Endsley, Bolté & Jones 2003) 82
Abb. 29: Aspekte der Benutzbarkeit technischer Komponenten (nach Baggen & Hemmerling, 2002, S. 241) 83
Abb. 30: Drei Einflussfaktoren auf die Interaktion mit technischen Systemen (nach Norman, 1988, S. 190) 86
Abb. 31: Wissen über technische Systeme (nach Kluwe, 2006, S. 42) 89
Abb. 32: Situationsbewusstsein (nach Endsley, 1995. S. 35) 91
Abb. 33: Prozess der Bildung des Situationsbewusstseins, abgekürzt SB (nach Endsely, 2000, S. 9) 91
Abb. 34: Belastung und Beanspruchung (nach DIN ISO 10075-1, 2000) 92
Abb. 35: Konzeptuelle Zusammenhänge von Faktoren psychischer Belastung und Beanspruchung 93
Abb. 36: Zusammenhang zwischen Erregung und Leistung im Vergleich: Yerkes-Dodson-Gesetz (1908) und monoton wachsende Funktion nach Kahneman (1973) 96
Abb. 37: Filtertheorie (nach Broadbent, 1958, S. 299) 98
Abb. 38: Dämpfungstheorie (nach Treismann, 1964) 98
Abb. 39: Theorie der späten Verarbeitung (nach Deutsch & Deutsch, 1963) 99
Abb. 40: Veranschaulichung der Performance Ressource Function (nach Norman & Bobrow, 1975, S. 48) 100
Abb. 41: Veranschaulichung von Lerneffekten bei der Aufgabendurchführung durch die Performance Ressource Function (nach Norman & Bobrow, 1975, S. 61) 101
Abb. 42: Modell der multiplen Ressourcen (nach Wickens & Hollands, 2000, S. 449) 102
Abb. 43: Ebenen der kognitiven Handlungskontrolle (nach Rasmussen, 1987, S. 54) 104
Abb. 44: Schematische Darstellung der Informationsverarbeitungsprozesse bei Steuerungs- und Kontrollentscheidungen im Mensch-Maschine-System (nach Rasmussen, 1986, S. 104) 107
Abb. 45: Systematisierung der Basisfehlertypen (nach Reason, 1990, S. 207) 109
Abb. 46: Dynamik der Fehlerentstehung im generischen Fehlermodellierungs-system GEMS (nach Reason, 1990, S. 64) 110
Abb. 47: Charakteristika von Regelung und Steuerung als motorische Kontrollarten (nach Konczak, 2008, S. 742) 114
Abb. 48: Zweiphasenmodell des Handelns nach automatischem oder kontrolliertem Denken 118
Abb. 49: Zwei Schritte im Attributionsprozess 120
Abb. 50: Ablaufdiagramm für die Entscheidung zur Hilfeleistung durch eine zuschauende Person (nach Aronson, Wilson & Akert, 2008, S. 368) 127

Abb. 51: Management von Unsicherheit in Organisationen (nach Grote, 2004, S. 268) 140
Abb. 52: Beispiele für Zielregeln, Prozessregeln und Handlungsregeln aus dem Manual einer europäischen Fluggesellschaft (nach Grote, 2014, S. 5) . . . 149
Abb. 53: Merkmale der Aufgabengestaltung (aus Ulich, 2005, S. 202) 153
Abb. 54: Plan-Do-Check-Act-Zyklus bzw. PDCA-Zyklus (nach Deming, 1986, S. 88) 156
Abb. 55: Systematisierung von Methoden und Verfahren des Sicherheitsmanagements nach prädiktiver, reaktiver und proaktivier Ausrichtung. 161
Abb. 56: Beispielhafte Darstellung eines Fehlerbaums 163
Abb. 57: Exemplarische Prüfliste für ein betriebsinternes Arbeitssicherheitsaudit (nach Suva, 2014, S. 4) 178
Abb. 58: Verortung des Sicherheitsmanagements am Beispiel einer Stab-Linien-Organisation 182
Abb. 59: Wirkungsmechanismen gesellschaftlicher und politischer Verantwortungsübernahme auf die Verantwortlichkeit für Sicherheit in Organisationen (nach Parker, 2010, S. 60) 188

Beispielverzeichnis

Beispiel 1: Feuerausbruch in Flugzeugkabine (Perrow, 1992, S.182) 18
Beispiel 2: Entstehungsverlauf des Fährunglücks der »Herald of Free Enterprise« (nach Ritz, 1998, S. 80–81, CXXII) 31
Beispiel 3: Verkehrssicherheit – Einführung der Verpflichtung zum Anlegen von Sicherheitsgurten während des Führens von Personenkraftwagen 40
Beispiel 4: Der mutige Druckmaschinenhersteller 44
Beispiel 5: Notlandung eines Airbus A320 auf dem Hudson River. 47
Beispiel 6: Auswirkungen unterschiedlicher Abbaumethoden in einem englischen Kohlebergwerk (aus Cherns, 1989, S. 483ff., zitiert nach Ulich, 2005, S. 189.) 64
Beispiel 7: Handlungskontrolle am Beispiel eines Pkw-Lenkers. 106
Beispiel 8: Entscheidung beim Aufleuchten einer Warnleuchte im Pkw. 108
Beispiel 9: Kognitive Dissonanz beim Nichtverwenden persönlicher Schutzausrüstung 122
Beispiel 10: Manipulation der Schutzeinrichtung an einer Maschine. 137
Beispiel 11: Störfall im Kernkraftwerk Forsmark 1 am 25.07.2006 (nach HSK, 2006; KSA, 2007) 141

1 Sicherheit: Begriffsbestimmung und Systematisierung

Die Sicherheitswissenschaften beschäftigen sich als interdisziplinäre und angewandte Wissenschaften mit der Erforschung von Bedingungen bei der Entstehung, Bewältigung und Vermeidung von Gefährdungspotenzialen, die im Zusammenhang mit Arbeits- und Produktionsprozessen innerhalb und zwischen Arbeitssystemen entstehen und die Unversehrtheit von Mensch, Organisation und Umwelt bedrohen.

Wir beachten Sicherheit für gewöhnlich nicht als spezielles Charakteristikum von Arbeitssystemen und Organisationen, während wir deren Angebote nutzen. So ist es beispielsweise selbstverständlich, nach einer Bahnfahrt aus dem Zug auszusteigen, ohne sich über die damit verbundenen Risiken bewusst zu werden. Bremst jedoch z. B. ein Zug während der Fahrt auf offener Strecke aus hoher Geschwindigkeit plötzlich stark ab und kommt abrupt zum Stehen, wobei Menschen aneinanderstoßen und Gepäckstücke umfallen, dann wird uns kurzfristig das Risiko bewusst, dass wir beim Nutzen dieses soziotechnischen Systems eingehen. Erst das spontane Auftreten starker Kräfte lenkt unsere Aufmerksamkeit auf die Wahrnehmung situativer Unsicherheit. Als involvierte Passagiere beschäftigen wir uns während der Weiterfahrt dann möglicherweise mit sicherheitsbezogenen Fragen, warum es z. B. in einem Zug, der teilweise mit über 200 km/h fährt, nicht möglich ist sich anzuschnallen oder warum es keine Gepäckklappen gibt, die uns vor herausfallenden Gepäckstücken schützen. Mit derartigen Überlegungen befinden wir schon mitten in Gestaltungsfragen soziotechnischer Systeme.

Bleiben wir zunächst jedoch noch beim Beispiel des unverhofften Zugstops und nehmen an, wir kommen als eine Gruppe von Passagieren und Bahnangestellten während der Weiterfahrt in ein Gespräch darüber, welche Anstrengungen das Bahnunternehmen für die Sicherheit unternimmt. Durch Ausführungen der Zugbegleiterinnen wird uns klar, dass ein hoher Organisationsaufwand im Unternehmen erforderlich ist, um technische Systeme kontinuierlich zu verbessern und das Personal im Umgang mit Mensch und Technik zu schulen. Während der Diskussion wird auch klar, dass das Bahnunternehmen zwar für die Sicherheit von Mensch und Umwelt verantwortlich ist, dass allerdings verschiedene externe Organisationen, z. B. Aufsicht führende Behörden, zuliefernde Unternehmen, Beratungs- und Forschungsorganisationen oder Fahrgastverbände Einfluss auf die Sicherheit im Bahnbetrieb nehmen. Wenn der Zug seinen Bestimmungsbahnhof erreicht, kommen wir möglicherweise noch zu der abschließenden Erkenntnis, dass sich bestimmte organisationskulturelle Bedingungen auf die Sicherheit auswirken, und wir werten die offene Diskussion mit dem Bahnpersonal als einen guten Indikator dafür, dass für die Sicherheit im Unternehmen Sorge getragen wird. Das animiert uns dazu, auch weiterhin unbesorgt Bahn zu fahren. Bei der nächsten planmäßig verlaufenden Bahnfahrt fällt uns dann die Sicherheit wieder nicht mehr auf.

Die umgangssprachliche Verwendung des Begriffs Sicherheit ist von einer Vielzahl impliziter Bedeutungen geprägt. Im deutschsprachigen Raum werden Diskurs und Konzeptentwicklung durch ein unklares Begriffsverständnis von Sicherheit zusätzlich erschwert. Im Englischen wird sprachlich zwischen Safety und Security unterschieden. Security zielt auf eine Sicherung zum Schutz vor meist externen Gefahren durch bös-

willige Angriffe, Spionage und Sabotage ab. Security kann als Bestandteil von Sicherheit (»Safety«) verstanden werden, da Angriffe i. d. R. darauf abzielen, einen Produktionsprozess für bestimmungsfremde Zwecke zu missbrauchen. Daraus resultiert entweder eine direkte Prozessgefahr, z. B. bei einer Flugzeugentführung im Falle einer terroristischen Bedrohung, oder es wird Know-how entwendet, wodurch zum einen die Organisation in wirtschaftliche Gefahr gerät oder zum anderen durch die unsachgemäße Reproduktion und Verwendung eines entwendeten Know-hows neue technologische Risiken entstehen.

Obwohl die allermeisten der im weiteren Verlauf vorgestellten Theorien und Konzepte problemlos auf den Bereich Security übertragen werden könnten, wird in diesem Buch auf den Schutz vor böswilligen Angriffen thematisch kein Bezug genommen. Dieses Unterfangen würde sowohl den Umfang dieses Buches sprengen als auch zu einer weiteren konzeptionellen Unklarheit bezüglich des Gebrauchs beider Begriffe führen. Dieses Buch bezieht sich im Sinne von Safety auf die Sicherheit beim Betrieb von komplexen soziotechnischen Systemen, die auch als Systemsicherheit (System Safety) bezeichnet wird.

Sicherheit kann einerseits statisch als Zustand verstanden werden und andererseits dynamisch als Prozess. Der Begriff Sicherheit ist darüber hinaus geprägt von unterschiedlichen Definitionen verschiedener sicherheitswissenschaftlicher Fachgebiete, was zu seiner Vielschichtigkeit beiträgt. In diesem Kapitel werden unterschiedliche Sichtweisen von Sicherheit systematisiert und – unter Definition und Einbeziehung zentraler Begriffe wie Risiko, Ungewissheit und Zuverlässigkeit – zu einem umfassenden Verständnis von Sicherheit zusammengeführt.

1.1 Statisches Verständnis von Sicherheit

Sicherheit kann allgemein und mathematisch als 100 %ige Wahrscheinlichkeit dafür verstanden werden, dass ein Ereignis genauso eintritt, wie es zuvor prognostiziert wurde (Fahlbruch, Schöbel & Marold, 2012; Ritz, 2011). Bezogen auf die Sicherheit eines Arbeitssystems bedeutet dies, dass kein sicherheitsrelevantes Ereignis wie beispielsweise ein Unfall oder ein Beinaheunfall eintritt. Dieser Negativlogik folgend ist Sicherheit ein Zustand, der durch die Verhinderung des Eintretens schädigender Ereignisse zu erreichen ist. Sicherheit hat zudem einen idealtypischen Charakter, da nicht davon auszugehen ist, dass sie in allen zukünftig auftretenden Situationen aufrechtzuerhalten ist.

Ingenieurwissenschaftlich wird Sicherheit definiert als der Zustand der vorschriftsmäßigen und gefahrenfreien Funktion eines Systems (siehe International Organization for Standardization, ISO/IEC Guide 51, 1999). Das bedeutet, Sicherheit wird als das Vorliegen eines Sollzustandes verstanden. Somit wird hier Sicherheit mit Zuverlässigkeit gleichgesetzt. Zuverlässigkeit ist definiert als Eignung einer Einheit, innerhalb vorgegebener Zeitspannen bei vorgegebenen Anwendungsbedingungen definierte Funktionsanforderungen zu erfüllen. Sie wird quantitativ als Wahrscheinlichkeit angegeben. Ein System gilt beispielsweise nach der Industrienorm DIN 40041 (siehe Deutsches Institut für Normung e.V., DIN 40041, 1990) als zuverlässig, wenn eine geforderte Funktion

unter gegebenen Bedingungen während einer festen Zeitdauer ausfallfrei ausgeführt wird.

Diese implizite Gleichsetzung ist insbesondere dahin gehend problematisch, dass sie suggeriert, Sicherheit sei beim Vorliegen von Zuverlässigkeit automatisch existent. Leveson (2004, 2011) zeigt allerdings anhand zahlreicher Beispiele, dass sicherheitsrelevante Ereignisse wie Unfälle auch in Systemen auftreten, die während der Ereignisentstehung vollkommen zuverlässig agiert haben.

In der Verkehrspsychologie und der Unfallforschung versteht man unter Sicherheit einen »Zustand ohne Schädigung oder Wahrnehmung eines Zustands ohne Schädigung oder potenzielle Schädigung« (Echterhoff, 2004, S. 861). Zustand bezieht sich dabei auf »Individuen in natürlicher, sozialer oder technischer Umgebung« (Echterhoff, 2004, S. 862).

Ingenieurwissenschaftlich wird Sicherheit unter Einbeziehung des Aspekt des Risikos definiert als

> »Zustand, dass für eine Sachlage (Produkt, Verfahren, Arbeitssystem,...) innerhalb eines bestimmten Zeitraumes keine Schädigung von Personen, der Umwelt und von Sachwerten eintritt, das heißt Sicherheit ist ein Zustand, bei dem das Risiko einer Gefährdung kleiner ist als das Grenzrisiko« (Lehder & Skiba, 2005, S. 26).

Risiko ist definiert als

> »Kombination der Wahrscheinlichkeit und des Schweregrades (Schadensausmaß) einer Schädigung (Gesundheitsschädigung) in einer Gefährdungssituation« (Lehder & Skiba, 2005, S. 26).

Das Grenzrisiko wird erklärt als das größte noch vertretbare Risiko, das einem bestimmten technischen Vorgang oder Zustand innewohnt. Insgesamt betrachten Lehder und Skiba (2005) Sicherheit nicht nur als einen »gefahrlosen« Zustand, sondern auch als »Zustand mit einem vertretbaren, akzeptablen Restrisiko, für das Maßnahmen festgelegt werden müssen zum Abbau des Restrisikos« (S. 27). Das Restrisiko beschreibt die Gesamtgefahr, die mit einem Arbeitsprozess verbunden ist. Die Gesamtgefahr besteht aus einem bekannten und einem unbekannten Anteil. Zur Abschätzung des Restrisikos können die Auftretenswahrscheinlichkeiten bekannter Gefahren über die Kumulation der Zuverlässigkeitsquotienten aller an einem Prozess beteiligten technischen und menschlichen Akteure ermittelt werden. Das Restrisiko kann durch wachsende Erfahrungswerte so ständig aktualisiert werden. Die Risikoakzeptabilität erleichtert ein »Urteil über die Tolerierbarkeit von Risiken aufgrund vorgegebener Kriterien« (Grote, 1997, S. 236). Eine solche Definition ermöglicht es, Entscheidungen über das Betreiben oder Nichtbetreiben risikoreicher Systeme treffen zu können. Sie ist allerdings zur Gestaltung soziotechnischer Systeme unzureichend (Grote, 1997). Hierzu ist die Berücksichtigung von Prinzipien der Systemgestaltung erforderlich (vgl. Kapitel 4).

Die alleinige Bindung von Sicherheit an das bekannte Risiko, das mit einem Zustand verbunden ist, suggeriert eine a priori nicht bestehende situative Stabilität. In realen Arbeitssituationen verändert sich jedoch ein Zustand durch dynamische, umweltbedingte Einflüsse ständig, wodurch unbekannte Anteile von Risiko entstehen.

1.2 Dynamisches Verständnis von Sicherheit

In einem dynamischen Verständnis von Sicherheit wird Risiko als eine Kombination aus der Auftretenswahrscheinlichkeit eines sicherheitsrelevanten Ereignisses und dem Schweregrad dessen potenzieller Konsequenzen (Leveson, 1995) betrachtet. Eine Risikoerhöhung erfolgt, wenn die Auftretenswahrscheinlichkeit für einen Ausfall im System oder das Ausmaß von Verlusten ansteigt. Verschiedene Faktoren beeinflussen diese beiden Risikodimensionen. Einige Faktoren, die im Kontext der aktuellen Entwicklung besonders relevant sind, beziehen sich auf das Auftreten neuer, unbekannter Gefahren und das Ansteigen von Komplexität, Beanspruchung, Energie, Automation, Zentralisierung und Geschwindigkeit der technologischen Entwicklung in den Systemen.

Andere Faktoren gehen aus Kombinationen der genannten Faktoren vor dem Hintergrund der gesellschaftlichen Entwicklungen hervor, beispielsweise durch den Trend, dass Menschen immer weniger auf dem Land und in stärkerem Maße in städtischen Ballungsräumen, also auf immer engerem Raum zusammenleben. In diesen Regionen wächst der Schweregrad potenzieller Ereignisse allein durch den Anstieg der Bevölkerungsdichte an. Damit steigt automatisch auch das Risiko unabhängig von der Auftretenswahrscheinlichkeit an, weil eine größere Anzahl von Menschen betroffen sein kann. Häufig entstehen Risikoanstiege auch durch kollektive Verhaltensänderungen, wodurch sich immer größere Teile der Bevölkerung auch direkt potenziellen Risiken aussetzen, z. B. durch wachsende Mobilität. Das Verkehrsaufkommen wächst, immer mehr Passagiere werden befördert, die Passagierkapazität in Flugzeugen oder Zügen wird erhöht, immer mehr Energie ist erforderlich und immer leistungsfähigere Kraftwerke werden gebaut.

Die stärkere Verbreitung und der vermehrte Einsatz technischer Geräte, deren Nutzung mit einem Risiko behaftet ist, ist eine weitere Quelle für einen beinahe unbemerkten Risikozuwachs. Zum Beispiel werden immer mehr Menschen bei Zahnarztbesuchen ohne konkrete Indikation vor oder während der Behandlung geröntgt und somit vermeidbaren Strahlungspotenzialen durch technische Geräte ausgesetzt. Für den einzelnen Patienten entsteht dabei der Eindruck, dass es sich bei den jeweiligen Strahlenexpositionen um Einzelfälle handelt und/oder dass diese keine negativen Auswirkungen haben können, weil es Ärzten ja darum geht, die Gesundheit zu erhalten oder herbeizuführen. Insgesamt betrachtet steigt jedoch durch einen gesamthaften Anstieg des Röntgens sowohl das Risiko für die Person, die geröntgt wird, durch die kumulative Erhöhung der Dosisleistung, die sie aufnimmt (vgl. z. B. Gigerenzer, 2013), als auch das Risiko, dass durch die Fehlkalibrierung einzelner Geräte eine große Gruppe von Patienten betroffen ist, wie das Beispiel von 206 Patienten veranschaulicht, die durch einen Computertomografen verstrahlt wurden (siehe U.S. Food and Drug Adminstration, 2009).

Beide Risikoarten betreffen natürlich auch das behandelnde Personal. Insgesamt betrachtet steigt also das Risiko für strahlungsbedingte Schädigungen durch den verbreiteteren Technikeinsatz. So haben einzelne Ereignisse wie Fehlhandlungen oder Unfälle schwerwiegendere Konsequenzen, und durch die großflächigere Verbreitung bestimmter risikobehafteter Technik sind mehr Menschen über größere Räume hinweg von ähnlichen Risiken betroffen. Die skizzierten Zusammenhänge veranschaulichen,

dass zu einem angemessenen Verständnis von Sicherheit der Aspekt der Veränderung zu berücksichtigen ist.

1.2.1 Sicherheit als Prozess

Weick (1987, S. 118) definiert Sicherheit (High Reliability) unter einem prozesshaften Verständnis als »dynamisches Nicht-Ereignis«. Er beschreibt, wie Organisationen Arbeitsprozesse, die mit einem hohen Gefährdungspotenzial verbunden sind, durch zuverlässige Anpassungen an situationsbedingte Veränderungen erfolgreich managen. Sicherheit ist eine Systemeigenschaft (Leveson, 2004), die in Organisationen fortlaufend durch das Zusammenwirken von Strukturen, Prozeduren, Regeln und operativen Handlungen der Organisationsmitglieder erzeugt wird. Dabei werden Anforderungen, die innerhalb der Organisation entstehen und die von außerhalb auf die Organisation einwirken, bewältigt. Das Sicherheitsmanagement (vgl. Kapitel 7) widmet sich der strategischen Entwicklung organisationaler Maßnahmen zur Aufrechterhaltung von Sicherheit und zur sicherheitsgerichteten Koordination intra- und interorganisationaler Aktivitäten.

1.2.2 Umgang mit Ungewissheit

Organisationen werden stark beeinflusst durch Globalisierung, Technologiesprünge und zunehmende Ökonomisierung (Rasmussen, 1997). Das Management nimmt diesen situationalen Kontext oftmals als bedrohlich wahr und entwickelt ein kritisches Bewusstsein für die Ungewissheit der eigenen Organisation hinsichtlich zukünftiger Entwicklungen. Ungewissheit bedeutet, etwas nicht sicher zu wissen, und ist in Anlehnung an Galbraith (1973) zu charakterisieren als »die Differenz zwischen der Menge an Informationen, die zur Durchführung einer Aufgabe erforderlich ist, und der Menge an Informationen, die eine Organisation bereits besitzt« (übersetzt nach Grote, 2009, S.12). Zusätzlich wird Ungewissheit durch die Mehrdeutigkeit vorhandener Informationen hervorgerufen, wodurch beim Eintreten unbekannter Situationen eine Vielzahl möglicher Bedeutungen entsteht (Weick, 1979). Wird Ungewissheit vorwiegend als negativ betrachtet, schlägt sich das im Verhalten von und in Organisationen nieder. Die Angst vor dem Eintreten zukünftiger Risiken wird überbewertet gegenüber den Chancen zur Weiterentwicklung der Organisation, die durch eine erfolgreiche Gefahrenbewältigung entstehen können.

Der Umgang mit Ungewissheit auf der organisationalen Ebene kann auf individueller Ebene zu Verhaltensunsicherheit führen, die durch gleichzeitiges Wissen und Unwissen entsteht und begleitet wird von einem meist unangenehmen Spannungszustand, der das Bestreben auslöst, möglichst schnell aufgelöst zu werden (Ritz, in Druck). Es besteht die Gefahr, dass zwar schnell, aber unsicher gehandelt wird. Um dieser Gefahr entgegenzuwirken, entwickeln Organisationen differenzierte Standards, damit Organisationseinheiten und Mitarbeitende zuverlässig handeln können. Damit wird das Ziel der Gefahrenprävention verfolgt, wobei durch die zentrale Planung von formalen Vor-

gaben eine Handlungsorientierung oder gar Handlungseinschränkung erzeugt wird, um zuverlässiges Handeln zu ermöglichen (vgl. Abschnitt 6.1.5).

Zuverlässigkeit gibt Organisationen angesichts wahrgenommener Ungewissheit Stabilität. Stabilität wird fälschlicherweise häufig mit Sicherheit gleichgesetzt (Ritz et al., 2013). Zur Aufrechterhaltung der Sicherheit ist zusätzlich Flexibilität erforderlich. Das bedeutet, dass neben der Gefahrenvermeidung durch Standards auch die Fähigkeit zur Gefahrenbewältigung durch Anpassungsfähigkeit erforderlich ist (vgl. Abschnitt 6.1.6).

1.2.3 Das Verhältnis von Sicherheit und Zuverlässigkeit

Zuverlässigkeit ist als eine Systemeigenschaft zu verstehen, die zur Sicherheit beitragen kann, die aber nicht zwangsläufig zu Sicherheit führt. Leveson (2011) kommt durch die Analyse sicherheitsrelevanter Ereignisse zu dem Fazit, dass die Sicherheit eines Systems aus den komplexen Wechselwirkungen zwischen dessen Komponenten in einem spezifischen situationalen Kontext entsteht. Zuverlässigkeit ist hingegen eine Eigenschaft, anhand derer sich jede einzelne Systemkomponente isoliert beschreiben lässt.

Das bedeutet für Systeme, dass durch unbekannte Veränderungen in der Systemumwelt, bei denen zwar alle Einzelkomponenten zuverlässig funktionieren, durch fehlende situationsadäquate Anpassung unvorhersehbare Wechselwirkungen entstehen, die zu Unsicherheit führen. Das Verhältnis von Sicherheit und Zuverlässigkeit eines Systems wird in Abb. 1 als Vierfeldertafel veranschaulicht.

- Die Kombination, die dadurch entsteht, dass ein System – wie im 1. Quadranten dargestellt – sicher und zuverlässig agiert, ist in Organisationen aus hochregulierten Branchen die wahrscheinlichste. Sie gilt als Normalfall und findet meist wenig oder keine Beachtung, da alle Systemvorgänge wie geplant verlaufen und die Anforderungen durch den situativen Kontext im erwarteten Bereich liegen. Der technische Teil eines Systems arbeitet also zuverlässig und menschliche Akteure vollziehen bei Überwachungsaufgaben entweder keine in den Produktionsprozess eingreifenden Handlungen oder nur Regulationen, die im Rahmen ihres Handlungsspielraums liegen und deshalb unbemerkt bleiben.
- Quadrant 2 bildet die Kombination, in der ein System zwar zuverlässig agiert, aber durch ungeplante Variationen der situativen Anforderungen an einen Produktionsprozess Unsicherheit entsteht, die in ein sicherheitsrelevantes Ereignis münden kann. Dabei wird die Entstehung eines Ereignisses gerade dadurch begünstigt, dass ein technisch zuverlässig verlaufender Prozess nicht das situativ erforderliche Anpassungsspektrum bietet und/oder dass menschliche Akteure die erforderliche Anpassung von Systemvariablen nicht vornehmen können oder wollen.
- Quadrant 3 beschreibt, dass ein System sicher sein kann, obwohl oder gerade weil es unzuverlässig agiert. In diesem Fall passen menschliche Akteure die durch Regeln oder Prozeduren vorgegebenen Handlungen über den durch die Organisation legitimierten Handlungsspielraum hinaus an. Dadurch wird Systemkontrolle erlangt und Sicherheit aufrechterhalten.
- Quadrant 4 kombiniert die Eigenschaften Unzuverlässigkeit und Unsicherheit eines Systems. Die Interaktion dieser Systemeigenschaften wird oftmals erst durch das Auf-

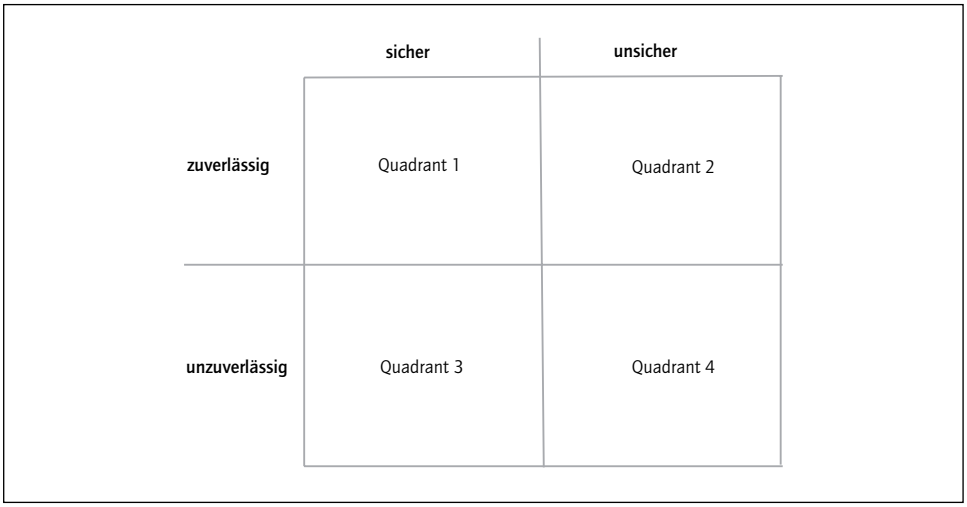

Abb. 1: Kombinationsmöglichkeiten von Sicherheit und Zuverlässigkeit in einem komplexen System als Vierfeldertafel visualisiert

treten eines sicherheitsrelevanten Ereignisses (vgl. Kapitel 2) erkannt, obwohl während dessen Entstehung bereits Informationen, die auf eine konkrete Gefährdung hinweisen, vorliegen (vgl. Abschnitt 3.4.1). Nach einem Ereignis wird dessen ursächliche Entstehung häufig auf von Standards abweichende menschliche Handlungen, sogenannte Fehlhandlungen, attribuiert. Hierbei besteht die Gefahr, einen fundamentalen Attributionsfehler (vgl. Abschnitt 5.10.2) zu begehen. Letztendlich ließe sich in einer radikalen Sichtweise jedes sicherheitsrelevante Ereignis eines Systems auf den Menschen zurückführen. Wenn man nur zeitlich und räumlich weit entfernt genug sucht, wird sich eine Person finden, die in ihrer Funktion als Systemdesigner, Systemkonstrukteur, Manager oder Operateur einen potenziellen Fehler begangen hat, zu dem eine Verbindung mit dem Ereignis besteht oder konstruiert werden kann.

Ritz et al. (2013) beschreiben die Aufrechterhaltung von Sicherheit in komplexen soziotechnischen Systemen als Qualität des Systems. Durch Zuverlässigkeit kann in Situationen, in denen die Bedingungen eines Produktionsprozesses erwartungskonform bestehen, Sicherheit erzeugt werden. Bei unerwarteten Situationen, die bekannt sind und zu deren Kompensation Handlungspläne in Form von Prozeduren vorliegen oder auf die durch automatisierte Abläufe reagiert werden kann, wird ebenfalls durch Zuverlässigkeit Sicherheit erzeugt. Unerwartete und unbekannte Situationen erfordern die Herleitung neuartiger Handlungsprozeduren, durch die dahin gehend unzuverlässig gehandelt wird, dass von bestehenden Plänen abgewichen werden muss oder neuartige Handlungsstrategien entwickelt und umgesetzt werden müssen. Durch sicherheitsgerichtete Anpassungshandlungen können abweichende Systemparameter kompensiert werden und Sicherheit wird erzeugt. Besonders in unplanbaren Situationen ist die menschliche Anpassungsfähigkeit für die Aufrechterhaltung von Sicherheit von zentraler Bedeutung.