SCHÄFFER
POESCHEL

Frank Ritz

Betriebliches Sicherheitsmanagement

Aufbau und Entwicklung widerstandsfähiger Arbeitssysteme

2015
Schäffer-Poeschel Verlag Stuttgart

Gedruckt auf chlorfrei gebleichtem, säurefreiem und alterungsbeständigem Papier

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
Druck und Bindung: BELTZ Bad Langensalza GmbH, 99947 Bad Langensalza

Printed in Germany
März 2015

Schäffer-Poeschel Verlag Stuttgart
Ein Tochterunternehmen der Haufe Gruppe

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-

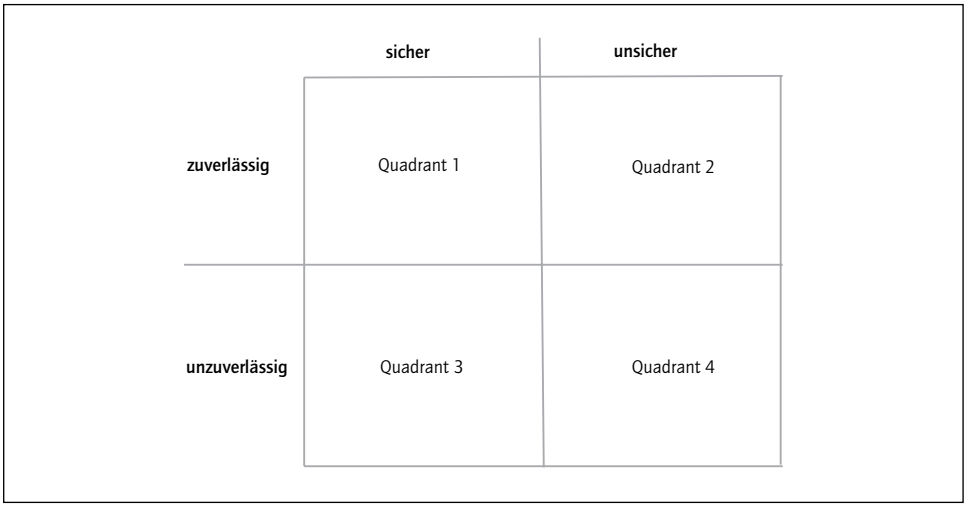

Abb. 1: Kombinationsmöglichkeiten von Sicherheit und Zuverlässigkeit in einem komplexen System als Vierfeldertafel visualisiert

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.

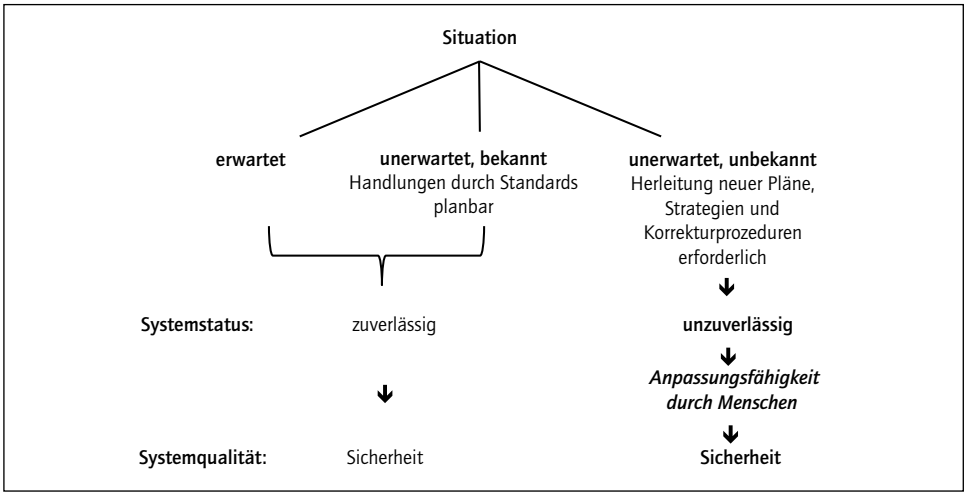

Abb. 2: Sicherheit im situationalen Kontext (nach Ritz et al., 2013, S. 5)

1.3 Sicherheit als Systemsicherheit

Aus den bisherigen Ausführungen wird bereits deutlich, dass der Begriff Sicherheit in unterschiedlichen Kontexten in seiner Bedeutung stark variiert. In soziotechnischen Systemen (vgl. Kapitel 4) hängt Sicherheit von der Gestaltung der physischen und psychischen Bedingungen am Arbeitsplatz und den Arbeitshandlungen der operativ tätigen Personen ab. Diese Bedingungen werden durch die Organisation – in Abhängigkeit vom jeweiligen Produktions- oder Dienstleistungsprozess – in Form von Personal, Technik, Strukturen, Prozessen, prozeduralen Vorgaben, Routinen, Regeln und räumlichen Voraussetzungen bereitgestellt. Damit ist Sicherheit in zweierlei Hinsicht durch die Organisation geprägt:

- Erstens geht es um das Organisieren von Sicherheit auf der Organisationsebene, beispielsweise durch das Erstellen von Plänen, die Bereitstellung von Ressourcen und das Formulieren von koordinativen Vorgaben;
- zweitens geht es darum, operativ tätige Personen zur Verhaltenssicherheit zu befähigen, wozu neben der Bindung an Handlungsvorgaben auch die Möglichkeit zur Autonomie zählt.

Systemsicherheit geht vom soziotechnischen Systemansatz (vgl. Kapitel 4) aus und zielt auf den aktiven Schutz von Mensch und Umwelt vor Gefahren ab, die aus den Risiken eines organisationsinternen Produktionsprozesses entstehen können. Hoyos und Ruppert (1993, S. 113; zitiert nach Grote, 1997, S. 236) beschreiben Sicherheit als Ziel, das durch aktive Bemühungen auf allen Ebenen der Organisation resultiert:

> »Dem Begriff ›Gefahr‹ und den möglichen Folgen, die eintreten, wenn die potentiell schädigenden Energien wirksam werden, steht das Ziel ›Sicherheit‹ gegenüber als ein Ausdruck präventiven Bemühens und eine Abkehr von der Tendenz, sich allein auf die Analyse von Unfallursachen nach dem Eintritt von Schädigungen zu konzentrieren. Wir haben daher versucht, den sicheren Zustand eines Systems hypothetisch durch Leistung des Managements, der Führungskräfte und der Beschäftigten zu definieren. Die Ergebnisse dieser Leistungen sollen sich in Sicherheitskriterien niederschlagen, die von sicheren Betriebsmitteln bis zum sicherheitsförderlichen Führungsstil reichen. Wir betrachten sie als Bausteine für eine um Prävention bemühte Sicherheitsarbeit. Unsere Kenntnisse und die sicherheitswissenschaftliche Diskussion reichen indessen noch nicht aus, um eine begründete Liste solcher Kriterien aufzustellen.«

Das mit dem Produktionsprozess in soziotechnischen Systemen verbundene Gefährdungspotenzial kann über die eigentliche Organisation hinauswirken wie beispielsweise bei der Luftfahrt, dem Zugverkehr oder der kerntechnischen Stromproduktion. Organisationen, die in Branchen mit hohem Gefährdungspotenzial agieren, haben deshalb ausgefeilte Organisations- und Koordinationsformen (vgl. Abschnitt 2.1.2) entwickelt, um Risiken kontrollieren und Systemsicherheit aktiv erzeugen zu können. Systemsicherheit wird nach Fahlbruch und Wilpert (1999, S. 56) in Anlehnung an Roland und Moriarty (1990) definiert als »Qualität eines Systems, die es dem System gestattet, ohne größere Zusammenbrüche unter vorgegebenen Bedingungen und mit einem Minimum unbeabsichtigten Kontrollverlusts oder Schadens für die Organisation und die Umwelt zu funktionieren.«

Dieser Definition liegt ein prozesshaftes Verständnis von Sicherheit zugrunde, das davon ausgeht, dass es sich bei Sicherheit nicht um einen stabilen Zustand handelt, sondern dass Sicherheit in einem System aktiv gebildet werden muss. Systemsicherheit ist demzufolge als Bestandteil des Primärziels eines Arbeitssystems (vgl. Abschnitt 4.1.2) zu verstehen. Sie entsteht gleichzeitig mit dem eigentlichen risikobehafteten Produktionsprozess sowie dessen Randbedingungen und weist damit auch eine starke Beziehung zur Arbeitssicherheit auf. Systemsicherheit umfasst Arbeits- und Prozesssicherheit auf organisationaler Ebene und sicherheitsgerichtetes Verhalten auf individueller Ebene.

1.3.1 Arbeits- und Prozesssicherheit

Den Hauptansatzpunkt der Systemsicherheit bildet die Prozesssicherheit (Process Safety), die trotz thematischer Überschneidungen von der Arbeitssicherheit (Occupational Safety) abzugrenzen ist.

Arbeitssicherheit ist definiert als »Zustand der Arbeitsbedingungen, bei denen keine oder nur vertretbare arbeitsbedingte Gesundheitsgefährdungen und Belastungen auftreten« (Lehder & Skiba, 2005, S. 25). Belastungen sind hierbei zu verstehen als physische und psychische Faktoren, die während einer Arbeitstätigkeit auf eine Person einwirken (vgl. Abschnitt 5.4). Das Konzept der Arbeitssicherheit zielt auf den Schutz von Personen vor arbeitsbedingten Gefahren ab. Die Schutzspanne reicht von der Reduzierung eher allgemeiner Gefahren (z. B. Schnitt- oder Sturzverletzungen) bis hin zu den mit-

unter äußerst spezifischen Gefahren (z. B. radioaktive Strahlung), die mit dem direkten Produktionsprozess verbunden sind. Zur Reduzierung dieser Gefahren werden präventive Maßnahmen umgesetzt, z. B. die Bereitstellung von persönlicher Schutzausrüstung, die bestehen kann aus Helm, Gehörschutz, Arbeitsschuhen und aufgabenspezifischer Arbeitskleidung oder maschinellen Schutzeinrichtungen. Durch diese Maßnahmen wird nicht nur auf bekannte unmittelbar wirkende Gefahren reagiert, sondern auch auf längerfristig gesundheitsschädigende Auswirkungen der Arbeit. Dabei geht es auch um die Gestaltung von Arbeitsbedingungen, durch die bekannte Berufskrankheiten vermieden bzw. deren Auswirkungen reduziert werden können (z. B. ergonomiegerechte Gestaltung von Arbeitsplätzen). Es wird deutlich, dass Arbeitssicherheit als Sekundäraufgabe von soziotechnischen Systemen zu verstehen ist, die dazu dient, dass die Primäraufgabe ausgeführt werden kann. Die Schutzeinrichtung an einer Maschine (vgl. Beispiel 10) ist beispielsweise nicht erforderlich, um ein Produkt herzustellen, sondern um die arbeitende(n) Person(en) vor den Gefahren des Produktionsprozesses zu schützen. Hiervon ausgehend kann Arbeitssicherheit nach Grote (2007) grundsätzlich durch eine Beseitigung von Gefahren, durch die Trennung von Mensch und Gefahrenquelle, durch den Schutz vor den Auswirkungen der Gefahr oder durch eine möglichst sichere Interaktion von Mensch und Gefahr umgesetzt werden.

Maßnahmen der Arbeitssicherheit kennzeichnen sowohl die Verantwortungsübernahme der Organisation für die Sicherheit der Mitarbeitenden als auch Verhaltensanforderungen an die Mitarbeitenden, deren Einhaltung im Verantwortungsbereich der jeweiligen Person liegt. Diese Anforderungen sind z. B. die sachgemäße Verwendung von Schutzkleidung und Schutzeinrichtungen, das Beachten von Gefahrenhinweisen und die Beurteilung der Sicherheitsdienlichkeit von Sicherheitsvorrichtungen beim unplanmäßigen Verlauf von Arbeitsprozessen. Die genannten Verhaltensaspekte werden, z. B. als Reaktion auf Veränderungen, durch Maßnahmen zur Sicherheitsförderung durch die Organisation unterstützt. Dazu gehören die Vermittlung aktueller Kenntnisse über Gesundheitsgefährdungen und deren Vermeidung, die Reglementierung technischer Schutzeinrichtungen und die Installation von Schutz- und Warnvorrichtungen. Letztgenannte Maßnahmen markieren den Übergang zur Prozesssicherheit. Arbeitssicherheit wird anhand von Beispiel 10 praxisbezogen dargestellt; Prozesssicherheit wird anhand von Beispiel 11 exemplarisch veranschaulicht.

Prozesssicherheit bezieht sich auf die Primäraufgabe des Arbeitssystems, also den Schutz vor den Risiken, die von den meist hochtechnologischen Produktionsprozessen ausgehen, z. B. dem Fliegen eines Verkehrsflugzeugs oder der Stromproduktion durch ein Kernkraftwerk. Beispiel 11 veranschaulicht das Konzept der Prozesssicherheit, das auf das Ziel ausgerichtet ist, sichere Produktionsprozesse zu schaffen und zu erhalten. Eine Strategie von Organisationen, um dieses Ziel zu erreichen, ist die Automation von Arbeitsaufgaben (vgl. Abschnitt 4.2.5). Dabei wird menschliches Handeln zunehmend durch technische Prozesse unterstützt, eingegrenzt oder völlig übernommen. Zusätzlich wird Technik zum Schutz vor Komponentenausfällen an sicherheitskritischen Stellen etwa mit Redundanzen und Diversitäten ausgestattet.

- Unter einer Redundanz wird in diesem Zusammenhang eine baugleiche Ressource verstanden, die im normalen störungsfreien Betrieb nicht (oder nur teilweise) benötigt wird. Die Notstromversorgung in Beispiel 11 stellt eine solche Redundanz dar.

Weitere Beispiele für Redundanzen sind das doppelte Vorhandensein von Bremsen oder Triebwerken an einem Verkehrsflugzeug.

- Unter einer Diversität wird eine funktionsgleiche Komponente verstanden, die genau genommen auch als Redundanz fungiert, aber von der Bauart oder dem technischen Prozess her andersartig gestaltet ist. Beim Ausfall der elektrischen Stromversorgung beispielsweise fungieren Öllampen oder Kerzen als Lichtquellen. Der Verwendung von Diversitäten liegt die Idee zugrunde, dass ein Ausfallsrisiko dadurch minimiert wird, dass zwei auf unterschiedliche Arten realisierte technische Komponenten weniger anfällig auf eine spezifische Art von Störung reagieren.

Darüber hinaus werden verschiedene ingenieurwissenschaftliche Strategien verfolgt, mit denen zur funktionalen Sicherheit technischer Teilsysteme beigetragen wird, z. B. die räumliche Trennung von Diversitäten und Redundanzen. Weitere Hinweise zur funktionalen Sicherheit technischer Systeme finden sich etwa in den Normen DIN EN 61508-1 bis -3.

Die jeweilige Organisation trägt die Verantwortung für die Umsetzung entsprechender Normen und die Sicherheit des gesamten Produktionsprozesses. Die Verantwortung der handelnden Personen liegt in der Einhaltung der Vorgaben der Organisation und dem Informieren entsprechender Organisationseinheiten oder Funktionsträger (z. B. der Organisationseinheit Sicherheitsmanagement oder einer vorgesetzten Person) über auftretende Unsicherheiten, Schwankungen oder Störungen.

1.3.2 Bedingungen sicherheitsgerichteten Verhaltens

Aus den bisherigen Ausführungen wird deutlich, dass sicherheitsgerichtetes Verhalten in soziotechnischen Systemen in mehrfacher Hinsicht von Bedeutung ist. Im Sinne der Arbeitssicherheit zielt es darauf ab, dass sich eine Person unter Nutzung der durch die Organisation bereitgestellten Ressourcen vor arbeitsplatzbedingten Gefahren schützt. Das bedeutet, dass die Verantwortung für die körperliche und geistige Unversehrtheit der Person auf die Organisation und die Person selbst verteilt ist. Ausgehend vom Konzept der Prozesssicherheit bedeutet Sicherheitsgerichtetheit, dass eine Person durch von der Organisation bereitgestellte Ressourcen wie Arbeitsmittel, Standards, Routinen und Regeln sowie durch die Nutzung persönlicher Ressourcen (z. B. qualifikationsbedingtes Wissen und erfahrungsgestützte motorische Handlungen) eine Arbeitsleistung erbringt, die einen sichereren Produktionsprozess unterstützt.

Zusammengenommen erfordert die Sicherheitsgerichtetheit eines Betriebs, Personen zu befähigen, Routineaufgaben und Aufgaben bei bekannten unerwarteten Situationen durch qualifizierte Ausführungen organisationaler Standards sicherheitsorientiert zu erfüllen. Zusätzlich ist beim Auftreten unbekannter Situationen die Fähigkeit zur Entwicklung situationsadäquater Bewältigungsstrategien erforderlich, durch welche die Kontrolle über einen technischen Prozess aufrechterhalten oder schnellstmöglich zurückerlangt werden kann. Eine übergeordnete Voraussetzung für Verhaltenssicherheit bildet die jeweilige Organisationskultur, speziell die Sicherheitskultur (vgl. Kapitel 3). Kulturelle Bedingungen bilden Verhaltensnormen und Werte, die einen entscheidenden