Strategische Entwicklung des Sicherheitsmanagements zur Bewältigung neuartiger Gefahren in einer digitalisierten Arbeitswelt

Frank RITZ

Institut Mensch in komplexen Systemen,
Hochschule für Angewandte Psychologie, Fachhochschule Nordwestschweiz,
Riggenbachstrasse 16, CH-4600 Olten

Kurzfassung: Arbeitssysteme, deren Organisation darauf ausgerichtet ist, Produktionsprozesse mit einem hohem Gefährdungspotenzial zu betreiben, werden durch die Digitalisierung mit einer wachsenden Anzahl neuartigen, unbekannten Gefahren konfrontiert. Im vorliegenden Beitrag werden zwei Strategien vorgeschlagen, um diesen Gefahren aktiv entgegenwirken zu können: 1. Eine stärkere und explizite Nutzung menschlicher Adaptivität und 2. eine konzeptionelle Integration von „Safety“ und Security zu Systemsicherheit. Ziel ist es, das Sicherheitsmanagement an die Anforderungen des digitalen Zeitalters heranzuführen.

Schlüsselwörter: Systemsicherheit, Gefahrenprävention, Gefahrenbewältigung, Safety, Security, menschliche Adaptivität, Digitalisierung

1. Bedeutung von Gefahrenbewältigung

In Organisationen hohen Gefährdungspotenzials wird das vorherrschenden Paradigma der „Insellösung“, also des weitestgehend autarken Organisierens von Arbeitssystemen bei fortschreitender Digitalisierung, zunehmend weniger praktikabel und voraussichtlich nur durch eine höhere, kostenintensive Ressourcenaufbringung aufrecht zu erhalten sein. So werden bspw. Diagnose und Wartung technischer Anlagen häufiger im „Online-Modus“ (also via digitale Netzwerke) erforderlich werden, wozu der Auf-/Ausbau und die Instandhaltung einer digitalen Infrastruktur notwendig wird. Diese kann Einfallstor für z.T. unbekannte externe Gefahren, z.B. fehlerhafte Ferndiagnosen und/oder digitale Sabotage werden. Dies erfordert eine Neuausrichtung der Strategien zur Gefahrenabwehr. Insgesamt bedingt ein Mehr an Möglichkeiten hier nicht nur ein Mehr an Gefahren, sondern auch eine beschleunigte GefahrenevolutionDa Organisationen als offene Systeme umweltbedingten Veränderungen unterliegen, sind sie per se gefordert, mit einem Mix von Maßnahmen zur Stabilisierung und Flexibilisierung auf Veränderungen zu reagieren, um sich organisationserhaltend anpassen zu können. Gefahren können dabei entweder fraktal (spontan sprunghaft) entstehen, oder aus einer langfristigen Entwicklung hervorgehen.

Grundsätzlich lassen sich drei Arten von Gefahren unterscheiden:

1. Geschäftsmodellspezifische Gefahren (z.B. ökonomische Bedrohungen oder gesellschaftliche Veränderungen),
2. Inhärente Gefahren durch den Produktionsprozess, die bei der Erfüllung der Primäraufgabe einer Organisation entstehen (z.B. radioaktive Strahlung bei der Stromproduktion durch kerntechnische Anlagen) oder
3. Gefahren, die im Zusammenhang mit den Sekundäraufgaben von Organisationen entstehen (z.B. Schutzmaßnahmen gegen Security-Bedrohungen).

Um diesen Gefahren aktiv zu begegnen, bedienen sich Organisationen zweier Strategien der Gefahrenabwehr, die sich einerseits auf die Stabilisierung und andererseits Flexibilisierung der Organisation beziehen (Grote, 2004; Ritz, 2015b):

1. Der Gefahrenprävention durch sorgfältige Planung organisationaler Standards, wie Prozeduren und Regeln zur Stabilisierung der Organisation sowie
2. der Gefahrenbewältigung, die als adäquate Anpassungsleistungen an konkrete situative Anforderungen zu verstehen ist und auf die Flexibilisierung der Organisation abzielt. Gefahrenbewältigung ist dann erforderlich, wenn unerwartete oder unbekannte Situationen auftreten, aus denen sicherheitsgerichtete Anforderungen entstehen, die nicht allein durch die bloße Anwendung organisationaler Standards erfüllt werden können, um eine unmittelbar erforderliche Aufrechterhaltung und/oder Widererlangung der Kontrolle über einen riskante Produktionsprozess und dessen potenziellen Auswirkungen zu erreichen.

Insbesondere in Organisationen aus hoch-regulierten Branchen, wie der Kerntechnik, der Luftfahrt oder dem Schienenverkehr, ist zu beobachten, dass der Gefahrenprävention durch Planung und Standardisierung gegenüber der Gefahrenbewältigung bislang eine überproportionale Bedeutung eingeräumt wird (Ritz, 2015b). Da jedoch auch durch zunehmend detailliertere Planung und stärkere Standardisierung zukünftige Gefahren nur bedingt zu vermeiden sein werden (viele Gefahren sind im Vorfeld ihres Auftretens naturgemäß noch nicht bekannt), droht sich die skizzierte Überakzentuierung negativ auf die Fähigkeit zur Gefahrenbewältigung auszuwirken (Ritz 2015b). Organisationen und ihre Mitglieder sind sich dann beim Auftreten unerwarteter/unbekannter Gefahren ihrer Anpassungsfähigkeit nicht im ausreichenden Masse bewusst und operative Bewältigungskompetenzen sind zu wenig trainiert. Das führt dazu, dass unter zeitkritischen Bedingungen kostbare Ressourcen mit der Suche nach passenden Standardprozeduren gebunden werden, anstelle durch Bündelung bestehender Wissens- und Fertigkeitsbestände eine anforderungsorientierte Problemlösung zu erarbeiten, durch die ein sicherheitskritischer Produktionsprozess unter Kontrolle gebracht und drohenden Schädigungen entgegengewirkt werden kann.

Da durch Digitalisierung eine weitere Steigerung der Dynamik zwischen externen und internen Anforderungen an Organisationen zu erwarten ist, aus deren Wechselwirkungen eine steigende Anzahl unerwarteter und unbekannter Gefahren hervorgehen, ist indiziert, über die reine Gefahrenprävention hinaus die Gefahrenbewältigung explizit zu stärken. Als Ergänzung zur sicherheitsgerichteten Standardisierung organisationaler Strukturen und Prozesse sollte somit die systematisches Befähigung zur Bewältigung unbekannter situativer Anforderungen außerhalb (off-the-job) und während produktiver Arbeitsprozesse (on-the-job) gefördert werden.

Ein zeitgemässes Sicherheitsmanagementkonzept sollte einerseits die menschliche Fähigkeit zur Adaptivität stärker aktiv einbeziehen und andererseits wachsende Gefährdungspotentiale durch böswillige, externe Eingriffe berücksichtigen.

2. Bedeutung menschlicher Adaptivität für das Sicherheitsmanagement

Die Reduzierung unsicherer Handlungen ist eines der Hauptziele der Manager von komplexen soziotechnischen Arbeitssystemen mit hohem Gefährdungspotenzial.

Ermittelte Unzuverlässigkeit im Produktionsprozess wird im Sinne einer Abweichung bei der Transformation betrieblicher Ist- in Sollzustände als ungewollte Variabilität bewertet (Reason 2008). Zur Vermeidung von Unzuverlässigkeit wird dabei das Konzept verfolgt, sowohl die menschliche Handlung als auch die Systemleistung insgesamt durch zunehmend detailliertere Standardisierung von Prozeduren zu begrenzen. Als höchstmögliche Form der Standardisierung, wird hierzu die Automatisierung bereits seit geraumer Zeit vorangetrieben. Automatisierung bedeutete die Übertragung von zumeist operativen Aufgaben des Menschen auf Maschinen.

Mit der Digitalisierung, als Erweiterung von Automatisierung, werden nun auch Kontroll- und Überwachungsaufgaben vom Menschen auf Maschinen übertragen. Das bedeutet, dass Maschinen direkt kommunizieren und in vernetztem Zusammenwirken Produktionsprozesse weitgehend autonom von menschlicher Einflussnahme realisiert werden können. Bei dieser Entwicklung droht menschliche Variabilität immer stärker eingegrenzt zu werden. Vielversprechend scheint dies auf den ersten Blick hinsichtlich zu erwartender Produktivitätssteigerungen. Bei näherer Betrachtung stellt sich – neben den artikulierten Befürchtungen u.a. vor Lebenzweckentfremdung ohne Arbeit sowie der damit verbunden Frage, ob und wie Konsum und Absatzmärkte zukünftig existieren können – die Frage, wie Sicherheit unter diesen Bedingungen zukünftig zu erzeugen ist.

Was komplexe Arbeitssysteme in einer von Ungewissheit, Intransparenz und Dynamik geprägten Welt vor dem Zusammenbruch bewahrt, ist menschliche Adaptivität. Sie ermöglicht, über kompensierende Anpassungshandlungen variierenden, situativen Anforderungen gerecht zu werden, um unbekannte sicherheitskritische Situationen zu bewältigen. Kompensiert werden hierbei v.a. fehlende organisationale Standards, die sich auf den Umgang mit akuten, bedrohlichen Systemzuständen beziehen, welche naturgemäß bei der zeitlich vorgelagerten organisationalen Planung nicht abdeckt werden können, da keine Erfahrungswerte dazu vorliegen. Bewältigungshandlungen sind somit als ad hoc zu entwickelnde Anpassungsleistungen zu betrachten, die stark von erfolgskritischen Faktoren wie der Qualifikation von Mitarbeitenden und organisationalen Rahmenbedingungen wie der aktiven Gestaltung und Erhaltung von Handlungsspielräumen abhängen. Die Methode PUMA (vgl. Koch et al. 2017) ist ein geeignetes Beispiel dafür, wie menschliche Adaptivität als Gefahrenbewältigungskompetenz strategisch in Organisationen integriert werden kann. Die Entwicklung und Implementierung der Methode, die auf die Steigerung der organisationalen Resilienz abzielt, ist in Ritz et al. (2016) beschrieben.

3. Sicherheit (Safety) und Security als Bedingungen für Systemsicherheit

Sicherheitsmanagement befasst sich derzeit mit „Safety“ und umfasst die Bereiche Prozesssicherheit und Arbeitssicherheit. Im Bereich Prozesssicherheit wird sich damit beschäftigt, wie Gefahren, die mit dem jeweiligen technischen Produktionsprozess inhärent verbunden sind (z.B. nukleare Sicherheit, Luftfahrtsicherheit, Patientensicherheit,...), zu detektieren und Schädigungen zu vermeiden sind. Im Bereich Arbeitssicherheit geht es darum, Gefahren und Risiken, die den Arbeitsschutz der Mitarbeitenden systematisch gefährden, stetig aufzuzeigen, um diesen durch systematische organisationale Gegenmaßnahmen (z.B. Ausstattung mit persönlicher Schutzausrüstung) geeignet entgegenzuwirken (vgl. Ritz 2015a). In beiden Bereichen wird dabei das grundlegende Konzept der bestmöglichen Trennung von

Mensch und Gefahr verfolgt. Bei der Prozesssicherheit dient dies über den Schutz von Mitarbeitenden und Organisation hinaus grundsätzlich auch dem Schutz der Organisationsumwelt.

Digitalisierung ermöglicht hinsichtlich Arbeitssicherheit im Routinebetrieb, eine nahezu unbegrenzte räumliche Distanz zu Gefahrenquellen während riskanter Produktionsprozesse. Bspw. befinden sich Leitwarten grosstechnischer Anlagen weit entfernt von der Produktion, unbemannte Passagierbeförderung auf der Schiene ist bereits Realität und ferngelenkte zivile Luftfahrt ein diskutiertes Thema. Wissenschaftliche Evidenzen zu Folgen der Automatisierung zeigen bereits seit geraumer Zeit negative Konsequenzen der zunehmenden Trennung von Mensch und Produktionsprozess auf, wie bspw. Verlust des „Situationsbewusstsein“ durch „out-of-the-loop-unfamiliarity“ (Endsley & Kiris 1995), Fertigkeitsverlust (Endlsey et al. 2003) oder dem Verlust an Wissensbeständen zur Steuerung technischer Systeme (Kluwe 2006). Paradoxer Weise handelt sich dabei um Voraussetzungen für menschliche Kompensation zur Bewältigung gefährlicher Situation, z.B. dann wenn automatisierte, resp. digitalisierte Systeme ausfallen und nicht verfügbar sind.

In der betrieblichen Praxis wird trotz Digitalisierung auch langfristig weiterhin eine Überschneidung zwischen den Bereichen Arbeits- und Prozesssicherheit bestehen. Bspw. kann eine Mitarbeitende, die einen drohenden Kontrollverlust im Arbeitssystem antizipiert, zur Vermeidung oder Abmilderung einer drohenden Schädigung (resp. zur Aufrechterhaltung der Prozesssicherheit) gegen Regeln zur Arbeitssicherheit verstossen, um die Prozesssicherheit aufrechtzuerhalten. Oder, ein Mitarbeiter verstösst z.B. gegen spezifische Regeln, in relevanten Arbeitsbereichen seine persönliche Schutzausrüstung zu tragen und verletzt sich dabei, wodurch es zu einem Arbeitsverzug kommt, der die Prozesssicherheit zumindest partiell gefährdet. Diese Beispiele lassen erahnen, welche Wechselwirkungen in komplexen Arbeitssystemen allein zwischen den Arbeits- und Prozesssicherheit entstehen können.

Angesichts vorschreitender Digitalisierung und situativ variierender terroristischer Gefährdungslagen sind die konzeptionellen Grundlagen für das Sicherheitsmanagement zu erweitern. Die Bedeutung von Security, im Sinne eines systematischen „Schutz vor böswilligen Angriffen“ (Ritz 2015a, S. 2), steigt angesichts neuer, digitalisierter Zugangsmöglichkeiten zu Organisationen, die (derzeit) weder hinsichtlich ihres Umfangs bekannt sind, noch hinsichtlich der von ihnen ausgehenden Risikopotenziale näher spezifiziert werden können. Evident scheint bislang nur, dass Security - ebenso wie „Safety“ - eine wichtige Voraussetzung für die Systemsicherheit ist, wobei die Produktion (output) und deren Konsequenzen für die Mitarbeitenden, die Organisation und die Organisationsumwelt (outcome) schadlos zu halten sind. Was bislang zu wenig Berücksichtigung bei der konzeptionellen Gestaltung des Sicherheitsmanagements findet, ist der Aspekt, dass auch zwischen „Safety“ (Arbeits- und Prozesssicherheit) und Security jeweils Wechselwirkungen existieren, die durch Digitalisierung mutmasslich zur Dynamisierung von Anforderungen an die Organisation durch eine Evolution von Gefahren beitragen.

Ausgehend davon, dass mit einem gesellschaftlich legitimierten Produktionsprozess (z.B. kerntechnische Stromproduktion, Personenbeförderung via Flugzeug) ein inhärentes Risikopotenzial akzeptiert wird und dem profitierenden Unternehmen der Schutz des Produktionsprozesses vor Zweckentfremdung obliegt, ist auch der Bereich Security in den konzeptionellen Rahmen des Sicherheitsmanagement zu intergieren.

Beim operativen Betrieb bestehen, ebenso wie für die Bereiche Arbeitssicherheit und Prozesssicherheit zuvor skizziert, Wechselwirkung zwischen Sicherheit („Safety“) und Security. Bspw. sorgen erfolgreiche Zutrittskontrollen - im Sinne einer Prävention vor zweckentfremdeter Nutzung mit schädigender Intention - dafür, dass ein sicherer Produktionsprozess aufrechterhalten werden kann. Umgekehrt können sich Zutrittskontrollen auch negativ auf die Prozesssicherheit auswirken. Z.B. wenn beigezogene externe Organisationen, zur Vermeidung oder Schadensbegrenzung von sicherheitsrelevanten Vorfällen, bedingt durch intensive Zutrittskontrollen erst verzögert ihre Tätigkeit aufnehmen und die damit verbundenen Aufgaben erledigen können. Ermittelte Wechselwirkungen führen bislang meist zu problemspezifischen Einzellösungen, bei denen im Sinne von „single-loop-learning“ (Argyris & Schön 1996) oder bestenfalls durch „double-loop-learning“ (Argyris & Schön 1996) ermittelte Schwachstellen sukzessive beseitigt werden. Um das Sicherheitsmanagement weiterzuentwicklen, ist hingegen „deutero-learning“ (Argyris & Schön 1996) erforderlich, was bedeutet, zu steuern, was auf der Metaebene zu lernen ist. Bezogen auf den zuvor skizzierten Zusammenhang bedeutete dies, das „Safety“ (Arbeits- und Prozesssicherheit) und Security sowie deren operative Wechselwirkungen ins Sicherheitsmanagementkonzept einzubeziehen sind.

4. Diskussion: Systemsicherheitsmanagement quo vadis?

Digitalisierung bietet Chancen, u.a. für eine Effizienzsteigerung der Produktion. Damit diese vorwiegend ökonomischen Chancen genutzt werden und Digitalisierung längerfristig nicht mehr Schaden als Nutzen bringt, ist es allerdings wesentlich, den Prozess der Digitalisierung aktiv sicherheitsgerichtet auszulegen und zu steuern. Für die Domäne Systemsicherheit sind dazu kontinuierlich Forschungsergebnisse zu erbringen und zu hinterfragen, bevor und während Arbeitssysteme und deren Bestandteile digitalisiert werden. Wichtige Hinweise über bekannte Problembereiche liefert bereits die Forschung zur Automatisierung. Allerdings kann bei der rasanten technologischen Entwicklung und Vermarktung entsprechender Infrastruktur, die strategische Entwicklung des Sicherheitsmanagements nicht mithalten. Hier ist politische Regulation notwendig, durch die sichergestellt werden kann, dass Digitalisierung zur Produktivitätssteigerung nur erfolgen kann, wenn noch zu entwickelnden Sicherheitskriterien erfüllt werden. Was das für die ökonomische Konkurrenzfähigkeit in globalisierten Märkten bedeutet, ist noch nicht abzusehen.

Den skizzierten Zusammenhängen liegen verschieden Prämissen zugrunde, die eine sukzessive Überprüfung von wissenschaftlicher Seite erfordern. Dazu gehören u.a., dass Wechselwirkungen zwischen den Bereichen der Systemsicherheit durch Digitalisierung tatsächlich hinsichtlich Dynamik und Auftretenswahrscheinlichkeit einen Zuwachs erfahren. Die Ableitung dieser Hypothese bezieht sich bislang vorwiegend auf Beobachtungen und Einschätzungen von Experten. Gleiches gilt für die explizite Integration der Gefahrenbewältigung in die strategische Ausrichtung der Gefahrenprävention. Implizit wird Gefahrenbewältigung von Mitarbeitenden im operativen Betrieb bereits gefordert, wobei diese sich gleichzeitig damit konfrontiert sehen, oftmals gegen organisationale Standards und juristische Regeln verstossen zu müssen, um die Systemsicherheit und Produktivität aufrechterhalten zu können. Auch hier ist der Gesetzgeber gefordert, die Priorisierung von Sicherheit gegenüber Regelkonformität rechtsfähig zu ermöglichen.

Resümierend kann festgehalten werden, dass zukünftige Trends im Systemsicherheitsmanagement darauf angewiesen sein werden, menschliche Adaptivität stärker als Chance zu begreifen, um Herausforderungen (nicht nur) durch die Digitalisierung sicherheitsgerichtet zu managen. Insgesamt wird es erforderlich sein, um die Systemsicherheit („Safety“ und Security) von Organisationen mit hohem Gefährdungspotenzial dauerhaft zu erzeugen, menschliche Adaptivität im Denken und Handeln schon beim Systemdesign wertschätzend zu berücksichtigen und aktiv zu nutzen.

5. Literatur

Argyris C, Schön D (1996) Organizational learning II: Theory, method, and practice. Reading: Addison-Wesley.

Endsley M R, Bolté B, Jones D G (2003) Designing for situation awareness. London: Taylor & Francis.

Endsley M R, Kiris E O (1995) The out-of-the-loop performance problem and level of control in automation. Human Factors, 37, 381-394.

Grote G (2004) Uncertainty management at the core of system design. Annual Reviews in Control 28:267-274.

Kleindienst C, Koch J, Ritz F, Brüngger J (2015) Förderung von Resilienz durch organisationales Lernen - Ein Schulungskonzept für Leitwartenteams in einem Kernkraftwerk. In: Mühlfelder M & Steffanowski A (Eds.), Themenheft Resilienz: Aktuelle Perspektiven und Konzepte aus der Wirtschaftspsychologischen Forschung und Praxis", Wirtschaftspsychologie 4:53-61.

Kluwe R H (2006) Informationsaufnahme und Informationsverarbeitung. In. B. Zimolong & U. Konradt (Hrsg.) Ingenieurpsychologie, Enzyklopädie der Psychologie. Themenbereich D, Serie III, Band 2. Göttingen: Hogrefe, 35-70.

Koch J, Brüngger J. Ritz F (2017, in dieser Ausgabe) Strukturierung der Teaminteraktion für eine erfolgreiche Bewältigung sicherheitskritischer Situationen - Eine Interventionsmethode für die Kernkraftwerksleitwarte.

Reason J (2008) The human contribution - Unsafe acts, accidents and heroic recoveries. Ashgate: Farnham.

Ritz F (2015a) Betriebliches Sicherheitsmanagement - Aufbau und Entwicklung widerstandsfähiger Arbeitssysteme. Stuttgart: Schäffer-Poeschel.

Ritz F (2015b) Organisationale Resilienz - Paradigmenwechsel, Konzeptentwicklung, Anwendung. In: Bargstedt U, Horn G, van Vegten A (Eds.), Resilienz in Organisationen stärken - Vorbeugung und Bewältigung von kritischen Situationen. Frankfurt: Verlag für Polizeiwissenschaft, Schriftenreihe der Plattform Menschen in komplexen Arbeitswelten e.V., 3-24.

Ritz F, Kleindienst C, Koch J, Brüngger J (2016) Entwicklung einer auf Resilienz ausgerichteten Organisationskultur. Gruppe. Interaktion. Organisation. Zeitschrift für Angewandte Organisationspsychologie, 47:151-158.

Gesellschaft für
Arbeitswissenschaft e.V.

Soziotechnische Gestaltung des digitalen Wandels – kreativ, innovativ, sinnhaft

63. Kongress der
Gesellschaft für Arbeitswissenschaft

FHNW Brugg-Windisch, Schweiz

15. – 17. Februar 2017

GfA Press

Bericht zum 63. Arbeitswissenschaftlichen Kongress vom 15. – 17. Februar 2017

FHNW Brugg-Windisch, Schweiz

Herausgegeben von der Gesellschaft für Arbeitswissenschaft e.V.
Dortmund: GfA-Press, 2017
ISBN 978-3-936804-22-5

NE: Gesellschaft für Arbeitswissenschaft: Jahresdokumentation

Als Manuskript zusammengestellt. Diese Jahresdokumentation ist nur in der Geschäftsstelle erhältlich.

Schriftleitung: Matthias Jäger
im Auftrag der Gesellschaft für Arbeitswissenschaft e.V.

USB-Print: Dr. Philipp Baumann, Olten

Screen design und Umsetzung
© 2017 fröse multimedia, Frank Fröse
office@internetkundenservice.de · www.internetkundenservice.de