Fachhochschule Nordwestschweiz
Hochschule für Angewandte Psychologie

Institut Mensch in komplexen Systemen (MikS)

Sicherheitskultur und der Faktor Mensch als Garant der Informationssicherheit

Prof. Dr. Frank Ritz

Komm.ONE
Cybersecurity-Tag 2025
Kongresszentrum Kornwestheim, 26. Juni 2025

Inhalt

- Systematisierung: Von Systemsicherheit zu Informationssicherheit & Cybersicherheit
- Human Factors
- Soziotechnischer Systemansatz
- Ironien der Automatisierung und die Rolle des Menschen
- «Drift-to-Danger-Modell»
- Sicherheitskultur
- Organisationales Lernen
- Fazit: Die Rolle des Menschen bei aktiver Erzeugung von Sicherheit

Informationssicherheit eine Kulturfrage …

Sicherheit zwischen allgemeinem Verständnis und Zuverlässigkeit

- **Mathematische Definition**: ergebnisorientierte Aussage für 100%ige Wahrscheinlichkeit des Eintretens eines Ereignisses oder Zutreffens einer Prognose

- Sicherheit **entzieht sich i.d.R. unserer Wahrnehmung**, wir beobachten Unsicherheit

- **Ingenieurwissenschaftliche Definition von Sicherheit**: „Zustand der vorschriftsmässigen und gefahrenfreien Funktion eines Systems“ (ISO/IEC Guide 51, 1999)
  - System ist sicher, wenn „geforderte Funktion unter gegebenen Bedingungen während fester Zeitdauer ausfallsfrei ausgeführt“ (DIN 40041, 1990)
  - Sicherheit als positiver Sollzustande **= Zuverlässigkeit**

- **Definitorische Problematik**:
  - Sicherheit & Zuverlässigkeit sind unabhängige Qualitäten von Arbeitssystemen, die sprachlich synonym verwendet und mit anderen Begriffen und Konzept vermischt werden
  - Resultat: Verwirrung und Desorientierung!

Zuverlässigkeit

- **Allgemein:** Eignung einer Einheit, innerhalb einer vorgegebenen Zeitspanne bei vorgegebenen Anwendungsbedingungen definierte Funktionsforderungen zu erfüllen (quantitativ als Wahrscheinlichkeit angegeben)

  – Kriterien:
  - **Korrektheit** (Verlauf nach Vorgaben)
  - **Robustheit** (auftretende Störungen können ausgeglichen werden)
  - **Ausfallsfreiheit** (definierte Sicherheit gegen einen Ausfall)

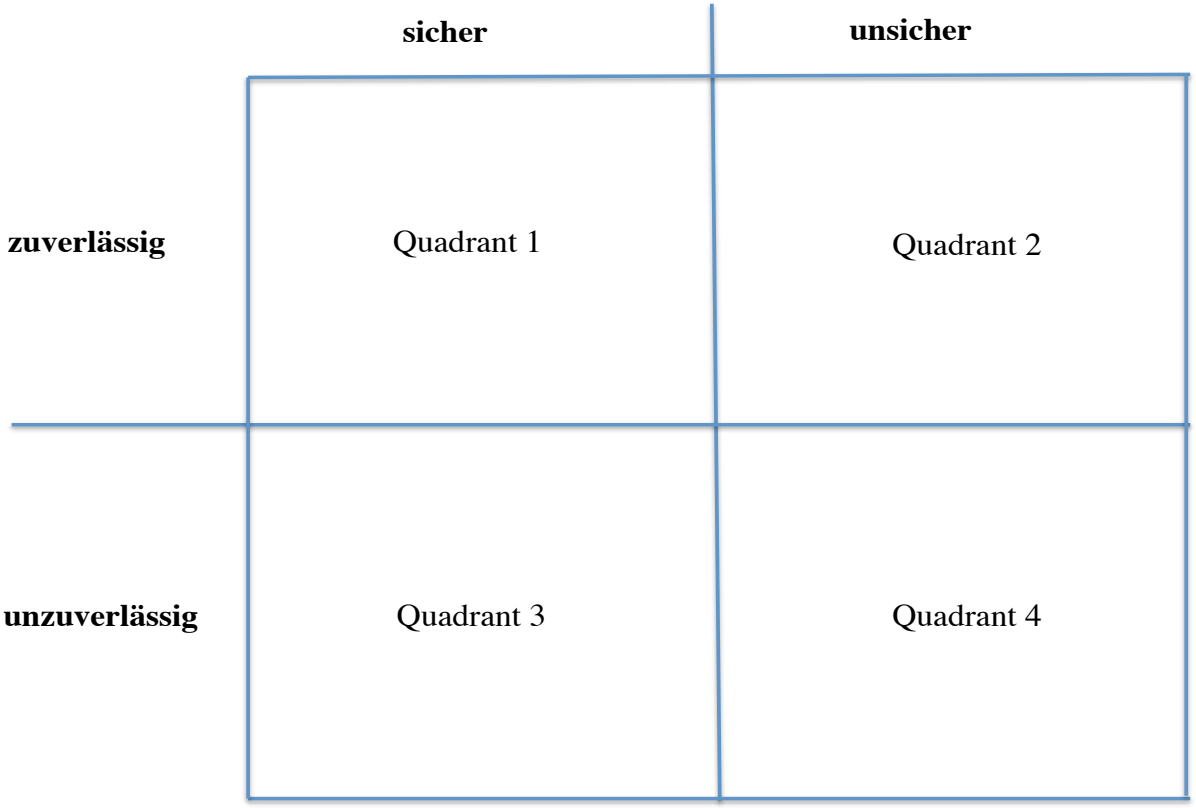
- **von Maschinen**

  – Fähigkeit, eine geforderte Funktion unter spezifischen Bedingungen und für einen vorgegebenen Zeitraum *ohne Fehler* auszuführen (Methode: Probabilistische Risikoanalyse)

- **von Menschen**

  – Fähigkeit des Menschen, eine Aufgabe unter vorgegebenen Bedingungen für ein gegebenes Zeitintervall im Akzeptanzbereich durchzuführen (Methode: Human Reliability Analysis)

Sicherheit und Zuverlässigkeit in komplexen Systemen (Ritz, 2015; S. 6 ff.)



Systemsicherheit, eine umfassende Definition…

- … als prozesshafte, organisationale Qualität:

  „…*a quality of a system that allows the system to function without major breakdowns under predetermined conditions with an acceptable minimum of accidental loss and unintended harm to the organization and its environment*“ (Fahlbruch & Wilpert, 1999; Roland & Moriarty, 1990)

- **„…Qualität, die es einem System gestattet, ohne größere Zusammenbrüche unter vorgegebenen Bedingungen und mit einem Minimum unbeabsichtigten Kontrollverlusts oder Schadens für die Organisation und die Umwelt zu funktionieren“**

Systemsicherheit: eine integrative Systematisierung (nach Ritz, 2015a)

- **Arbeitssicherheit**: „*Zustand der Arbeitsbedingungen, bei denen keine oder nur vertretbare arbeitsbedingte Gesundheitsgefährdungen und Belastungen auftreten*“ (Lehder & Skiba, 2005, S. 25)
- **Prozesssicherheit**: „*...bezieht sich auf die Primäraufgabe des Arbeitssystems, also den Schutz vor den Risiken, die von hoch-technologisierten Produktionsprozessen ausgehen*“ (Ritz, 2015a, S. 10)
- **Verhaltenssicherheit**: „*Befähigung, Routineaufgaben und Aufgaben bei unerwarteten Situationen durch von der Organisation bereitgestellte Ressourcen... sicherheitsgerichtet zu erfüllen ... sowie unbekannte Situationen ergänzt durch (kooperative Bündelung von) individueller Fähigkeiten sicherheitsgerichtet zu bewältigen*“ (Ritz, 2015b)
- **Psychological safety**: „*a shared belief that the team is safe for interpersonal risktaking. For the most part, this belief tends to be tacit-taken for granted and not given direct attention either by individuals or by the team as a whole*“ (Edmondson,1999, S. 354)
- **Security** ist auch ein Bestandteil von Systemsicherheit: „*Schutz vor Schädigungen durch böswillige Eingriffe in Organisationen*“ (Ritz, 2017)
  - **zunehmende digitale Transformation wird alle Bereiche der Systemsicherheit verstärkt bedrohen, wachsende Bedeutung von: IT-Security: u.a., Informationssicherheit, Datensicherheit, Cybersicherheit, …**

Informationssicherheit & Cybersicherheit (nach BAuA, 2022)

- Vielfältige Anforderungen und definitorische Grundlagen, z.B.:
  - **Informationssicherheit** ist ein Zustand von technischen oder nicht-technischen Systemen zur Informationsverarbeitung und -speicherung, der die **Schutzziele Vertraulichkeit**, **Verfügbarkeit** und **Integrität** sicherstellen soll**. Informationssicherheit dient dem Schutz vor Gefahren bzw. Bedrohungen**, **der Vermeidung von wirtschaftlichen Schäden und der Minimierung von Risiken**.

  - Die Gefahr, dass Unternehmen oder Organisationen Opfer eines Angriffs auf ihre IT-Systeme werden oder digitale Produkte ungewollt verändert werden, ist real und darf auch bei der Produktsicherheit nicht vernachlässigt werden.

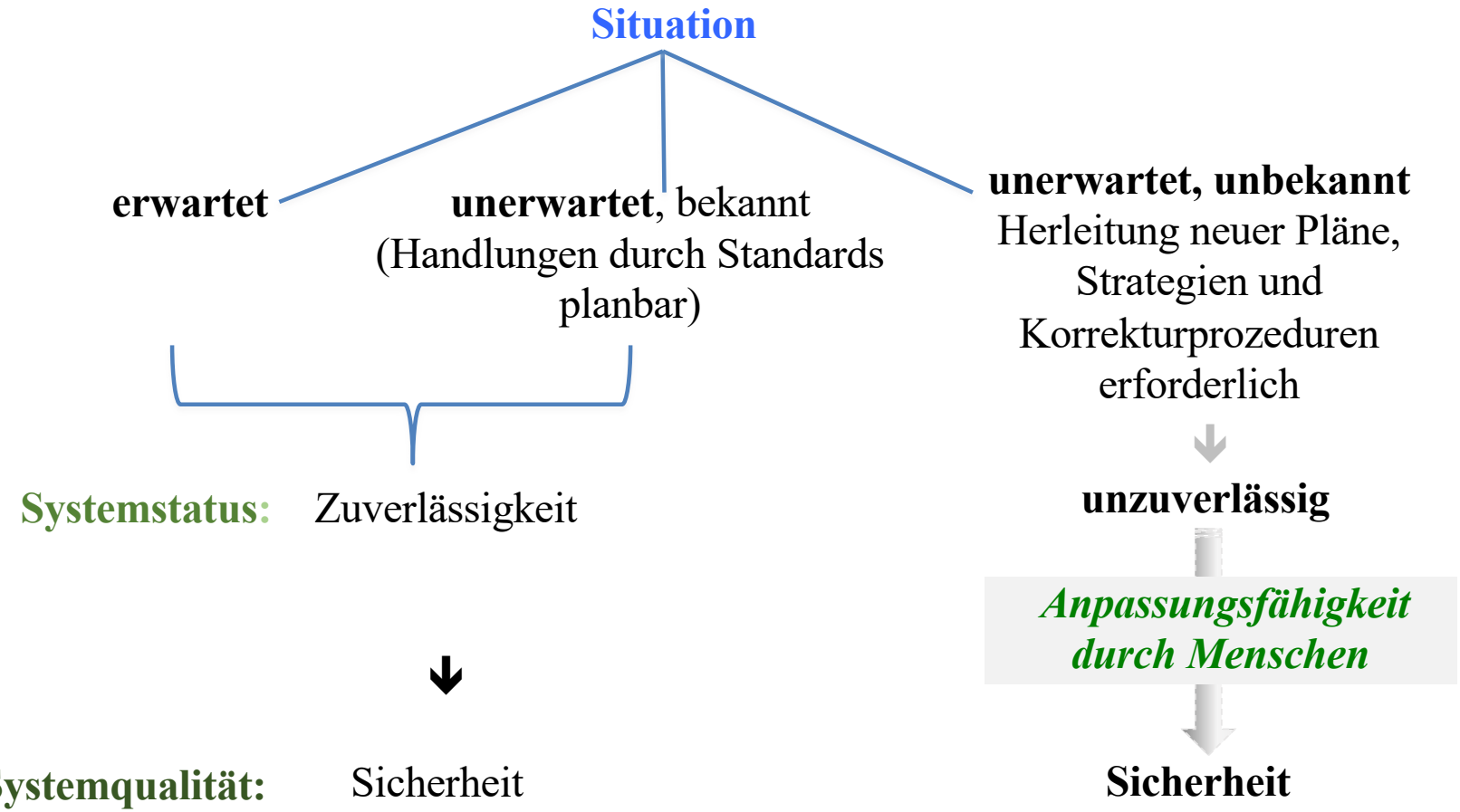
  - Das Fachgebiet der Safety (u.a. Maschinensicherheit) hat die Gesundheit des Menschen als Schutzziel. Ist das Schutzziel die **Datensicherheit** von Systemen, so ist die **IT-Security** zuständig. Da es Überschneidungen und Wechselwirkungen zwischen den beiden Fachgebieten gibt, ist eine abgestimmte Zusammenarbeit, das sogenannte Co-Engineering, oft zwingend erforderlich.

  - Co-Engineering-Ansatz auf Basis bestehender Normen und wo regulatorische und normative Verbesserungsmöglichkeiten werden kontinuierlich ausgearbeitet (https://link.baua.de/mna) und über „Technische Regel für Betriebssicherheit **Cybersicherheit** für sicherheitsrelevante Mess-, Steuer- und Regeleinrichtungen TRBS 1115 Teil 1“.

Systemsicherheit im Prozessverständnis

- Definition: „**dynamisches Nicht-Ereignis**“ (Weick, 1987)
  - Fortwirkendes Zusammenwirken von Strukturen, Prozeduren, Regeln und operativen Handlungen in Organisationen
  - ist geprägt von **Ungewissheit**:
    - Differenz zwischen der Menge an Informationen, die zur Durchführung einer Aufgabe erforderlich ist und der Menge an Informationen, die eine Organisation bereits besitzt (Galbraith, 1973; Grote, 2009)
    - **Widersprüchlichkeit** von Informationen (z. B. Weick, 1979)
- Als Gefahr resultiert oft eine Fixierung auf eine planungsbasierte **Gefahrenprävention**, bei gleichzeitiger Vernachlässigung von Maßnahmen zur **Gefahrenbewältigung**

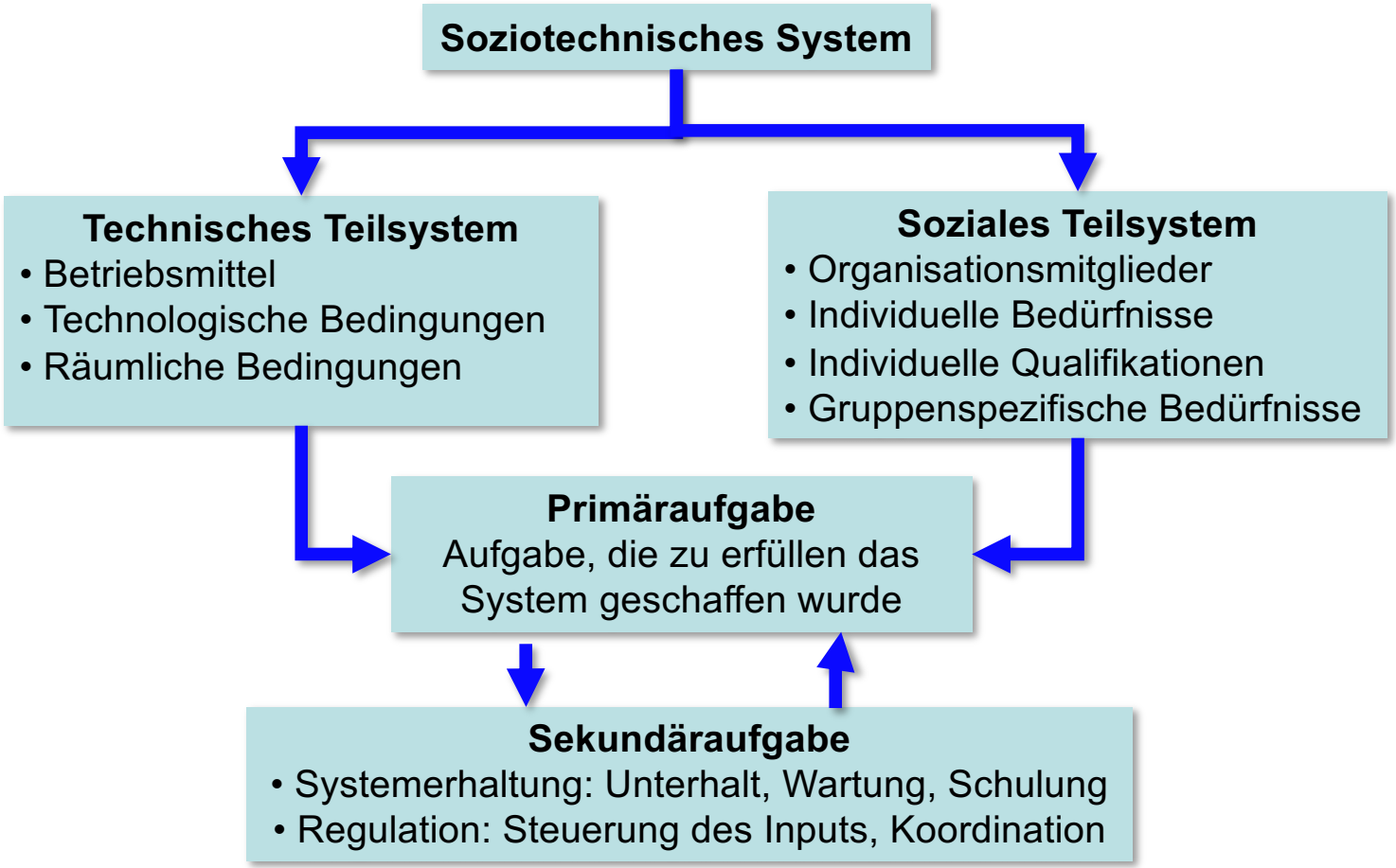
Sicherheit im situationalen Kontext (Ritz et al., 2013; Ritz, 2015)



Human Factors

- **Definition**: „Forschungsgegenstand, der sich damit beschäftigt, anwendungsorientiertes Wissen über die Faktoren **menschlicher Leistungsfähigkeit und ihre Begrenzung** zur Analyse, Gestaltung und Optimierung von Produkten, Prozessen und soziotechnischen Systemen zu erschließen“ (Ritz, 2015, S. 87)
- **Komplementäre Ausrichtung:**
  1. Verhalten in spezifisch gestalteten Umgebungen zu vermitteln, erklärbar zu machen und die gewonnenen Erkenntnisse zur **Gestaltung der jeweiligen Umgebung** (z. B. Arbeitsplatz mit physikalischen, psychologischen und sozialen Anforderungen während der Aufgabenbewältigung) zu nutzen.
  2. Ein zweiter Fokus ist darauf gerichtet, konkrete **Qualifikationsanforderungen** festzustellen, um möglichst effektive Aus-, Trainings- und Weiterbildungsprogramme ausarbeiten zu können.
- **Human Factors sind nicht per Definition negativ!**
- **Human Factors unterscheiden sich von Human Errors!**
- **Designfehler haben massive negative Auswirkungen auf menschliche Leistungsfähigkeit!**

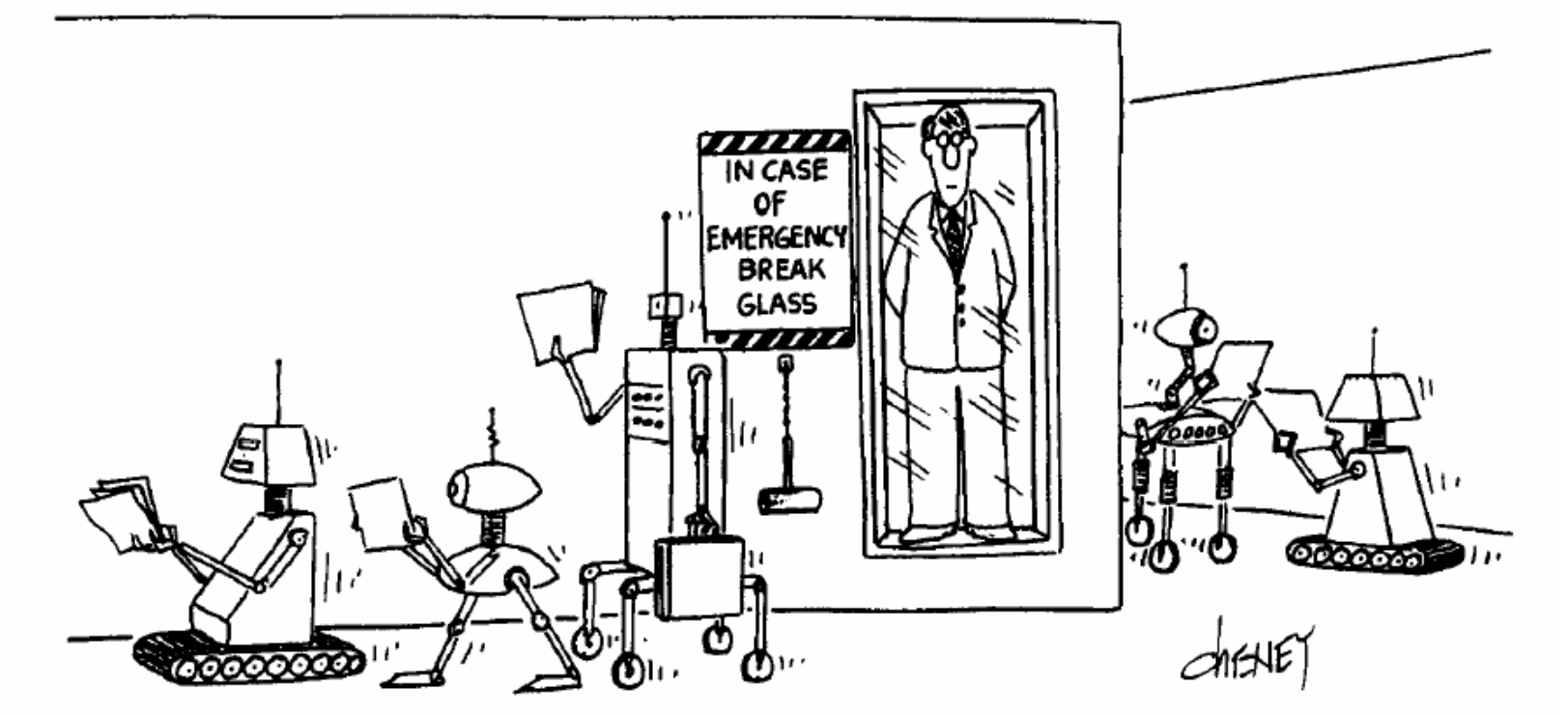
Soziotechnischer Systemansatz (Ulich, 2005; aus Ritz, 2015, S. 65)



Ironien der Automatisierung (Bainbridge, 1983), unbewusst wirkende Mindsets…

- „Unzuverlässiger“ Mensch plant und entwirft als Designer*in automatisierte Arbeitssysteme.
- „Unzuverlässiger“ Mensch greift dann ein, wenn die „zuverlässige“ Technik versagt!
- Fertigkeiten, Erfahrungen, Kenntnisse zur Steuerung gehen verloren (Kompetenzverlust). Diese Fertigkeiten werden aber gerade dann benötigt, wenn die Automatik ausfällt.
- Unvereinbarkeit der Variabilität der Arbeitssituationen mit der Inflexibilität und Unvollständigkeit von Prozeduren.
- Arbeitsprozesse werden durch Prozeduren formalisiert, um Risiken zu reduzieren.
- Problematisches Vorgehen in hochvariablen Umgebungen, in denen Initiative des Operateurs als nicht akzeptable Abweichung von der formalen Aufgabe und Prozedur aufgefasst wird. Die Bedeutsamkeit und Übereinstimmung von formaler Aufgabe und Prozedur in Bezug auf verschiedene Situationen muss hier gewährleistet sein.

Ironien der Automatisierung



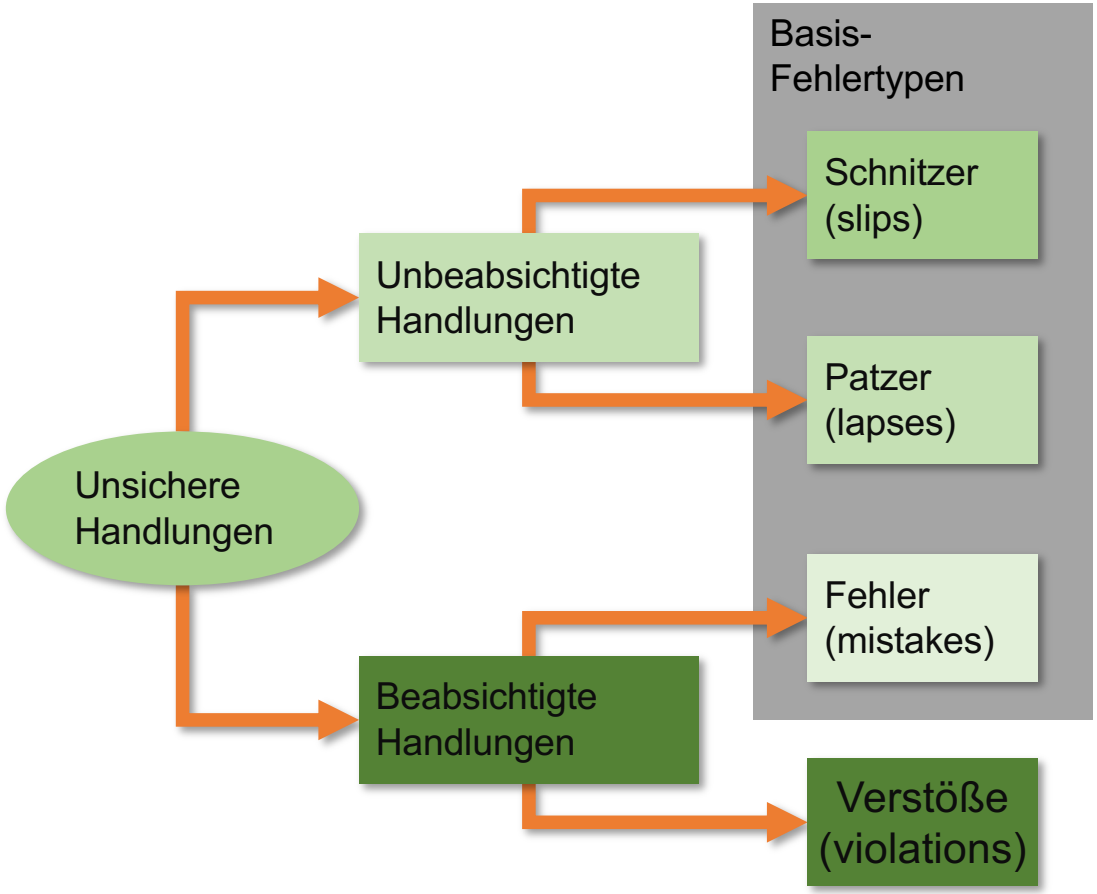
Weitere Auswirkungen der „Ironien der Automatisierung“

- Entwickler*innen automatisieren, was leicht zu beschreiben ist.
- Die schwierigen Aufgaben bleiben dem/der Operateur*in überlassen.
- In Situationen hoher Arbeitslast hilft die Automatik nicht.
- „ ... das „automatische Kontrollsystem“ ist eingeführt worden, weil es die Aufgaben besser erfüllen kann als der Operateur, und doch wird vom Operateur verlangt, dass er/sie das richtige Funktionieren des Systems überwacht“ (Bainbridge, 1983).
- Vermeintlich fehlerfreie automatisierte Systeme ersetzen den fehleranfälligen Menschen…?
- Aber, was ist eigentlich ein Fehler?

Begriffs- und Konzeptbestimmung: Fehler

- Es existiert **kein Antonym** zu Fehler!
- Die negativ **konnotierte Bezeichnung** Fehler wird umgangssprachlich verwendet für eine **Ursache**: z.B. ein Unfall ist durch „menschliche Fehler“ entstanden; **Handlung**: Nur die unplanmässige Handlung, nicht ihr Ergebnis, wird betrachtet; **Folge**: Nur das negative Ergebnis, nicht die Handlung, wird betrachtet, usw.
- „**Menschlicher Fehler**“: nachträgliche Attribution einer Ursache für ein beobachtetes (unerwünschtes) Ergebnis, das auf menschliches Handeln Bezug nimmt.
- „**Fehler**“ **im systemischen Verständnis**: „temporärer Schwachstelle eines Systems, die zum Schutz (Sicherheit)
  - **kurzfristig** vor Ort zu kompensieren sowie zu melden ist (Meldung),
  - **mittelfristig** professionell analysiert (Analyse) und
  - **langfristig** zur Steuerung des Organisationalen Lernens (bspw. Gestaltung von Massnahmen) zu nutzen sind“ (Ritz, in Vorbereitung, 2026).
- **Critical Incidents** (Flanagan, 1959): Lerngelegenheit über Schwächen und deren Kompensation (Stärken)

Basisfehlertypen (Reason, 1990; nach Ritz, 2015, S.109)



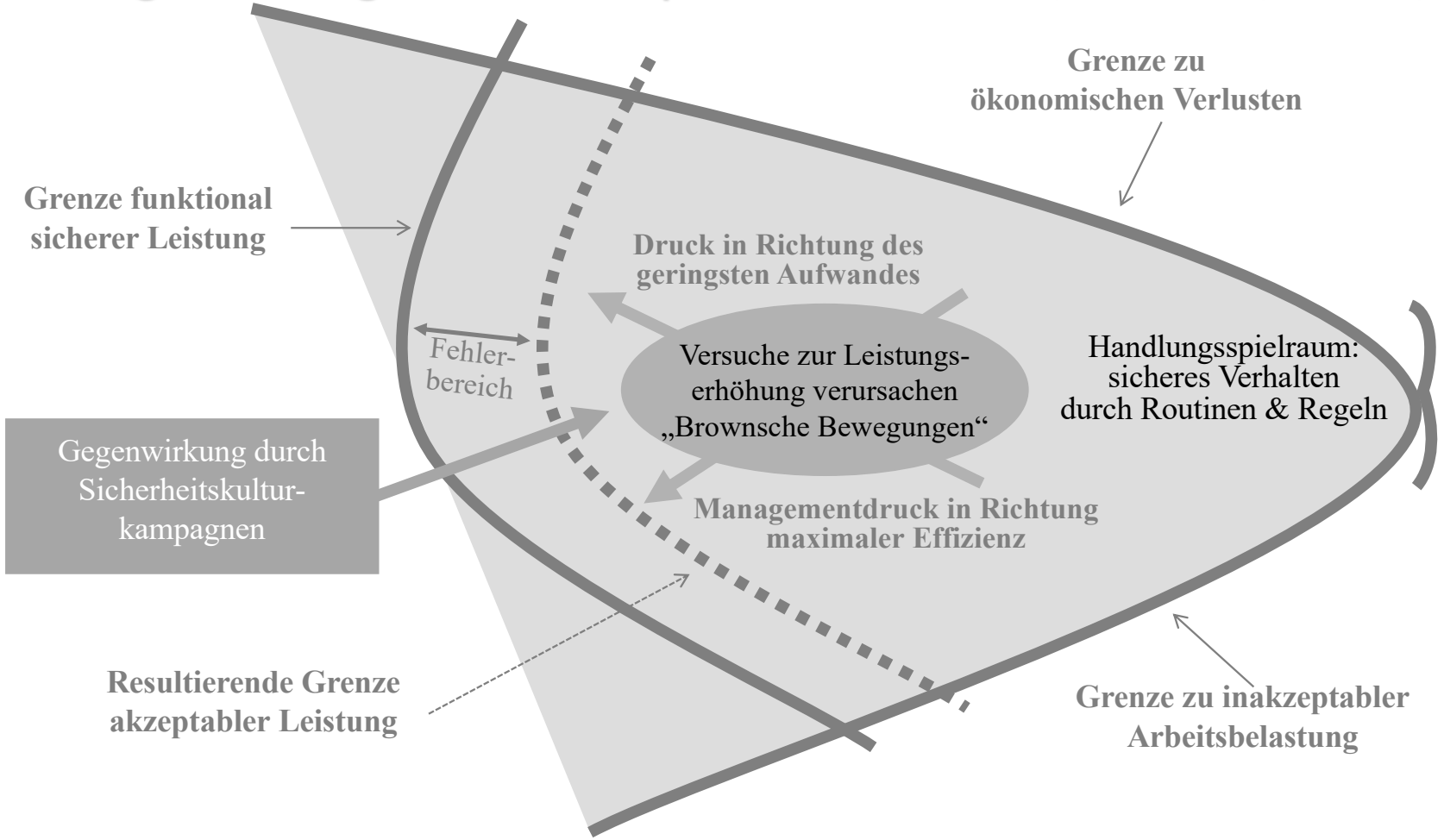
Ausführungsfehler
Störungen
Unterlassung
Vertauschung
Fehlbedienungen

Verarbeitungsfehler
Unterlassungen
Vergessen von Absichten
Verlust Stand der Dinge

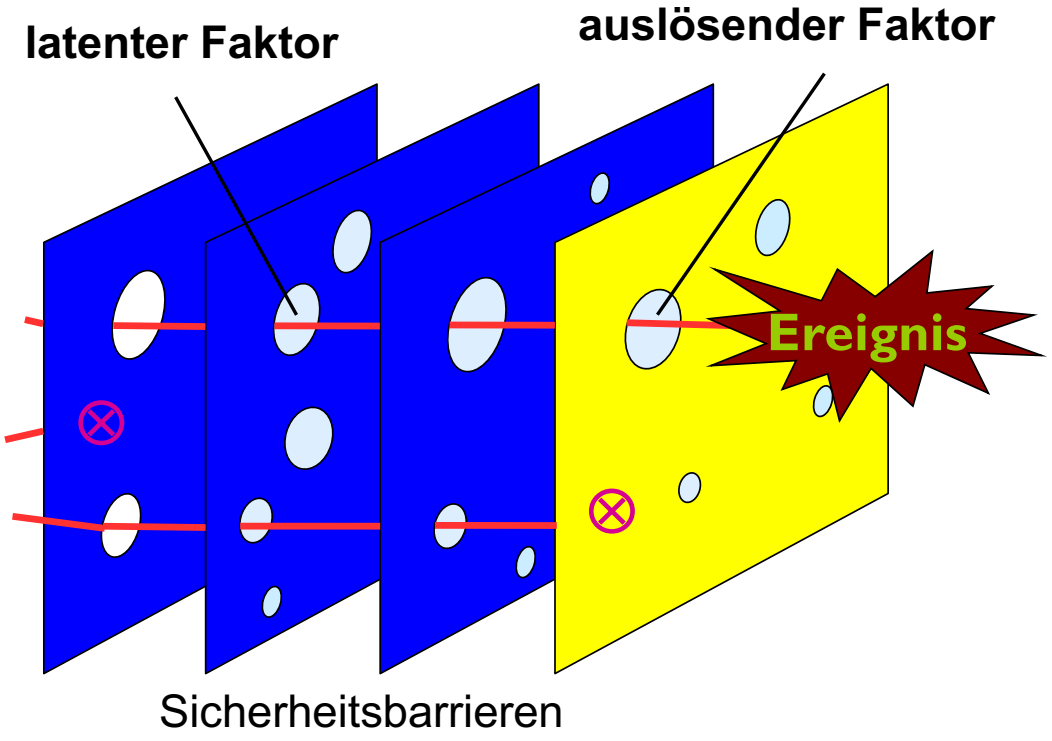
Planungsfehler
Regel-basiert
Wissens-basiert

Regelverstöße
Routine
Optimierung
Sabotage

«Drift-to-Danger» in Organisationen (Rasmussen 1997; aus Ritz, 2015a, S. 34)

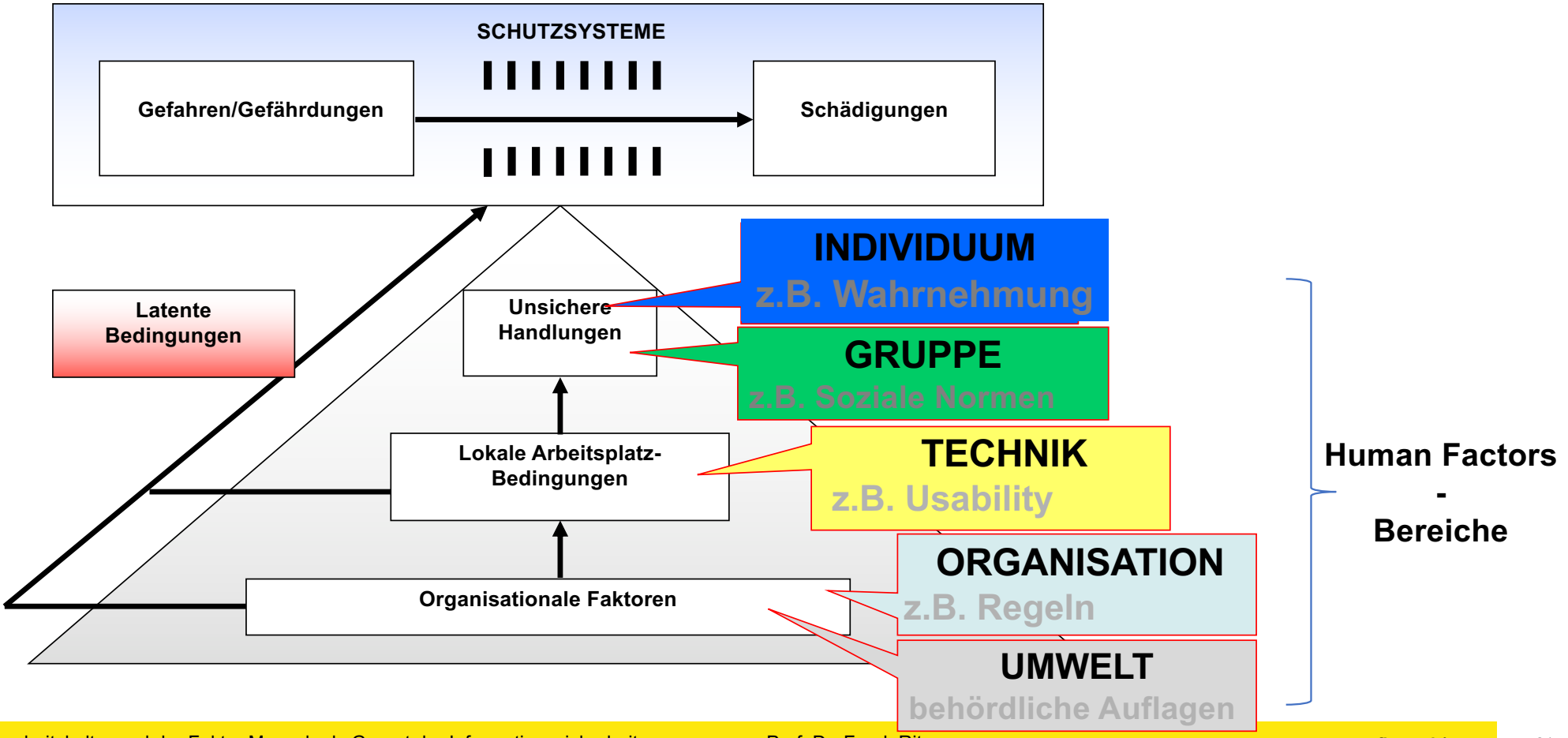


Ereignisentstehungsmodell (Reason, 1990; nach Ritz 2015a, S. 28)

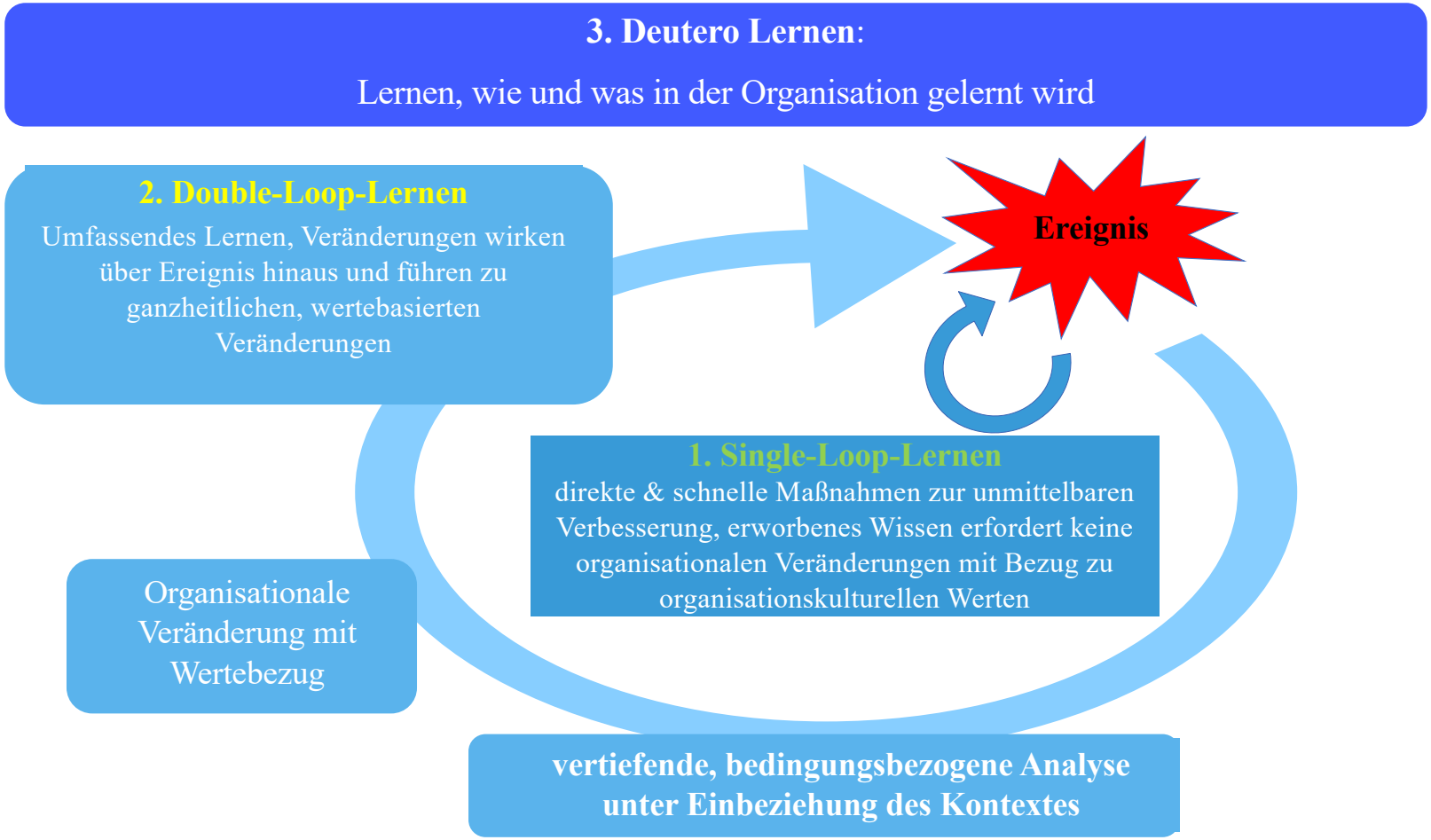


- Annahme:
  - Sicherheitsrelevante Ereignisse entstehen durch Wechselbeziehungen von unsicheren Handlungen und latenten Bedingungen.
- Analyse:
  - Pathogene bestehen im Durchbrechen von Barrieren.
- Ziel:
  - Sicherheit erzeugen, indem Löcher im Käse gestopft und damit Sicherheitsbarrieren verbessert werden.

Organisationale Ereignisentstehung (Reason, 1997; nach Ritz, 2015a, S. 29)



Organisationales Lernen (Argyris & Schön, 1996; nach Ritz, 2015a, S. 43)



Kulturdefinition nach Schein (1990) und Sicherheitskultur (IAEA, INSAG 15)

- „…ein **Muster gemeinsamer Grundannahmen**, das eine Gruppe bei der Bewältigung ihrer Probleme hat, das sich bewährt hat und als bindend gilt, und das daher an Mitglieder als rational und emotional korrekter Ansatz für den Umgang mit diesen Problemen weitergegeben wird...“
  - … Probleme beziehen sich:
    1. auf die Anpassung der Welt und
    2. die Übernahme von Aspekten der Welt als **Grundannahmen**“

  → Nationalkultur, Organisationskultur, **Sicherheitskultur**
  – Grundannahmen: „*collective programming of mind*“ (Hofstede, 1980)
- **Definition IAEA**: „Ganzheitliches Phänomen, das alle Organisationsmitglieder und beteiligte interorganisationale Akteure einbezieht und dessen Verhaltenswirksamkeit sich auf beobachtbare & psychologische Merkmale bezieht (INSAG-15, 2002)
- Anforderung: Sicherheitskultur als **informierte Kultur** durch Lernen (Reason, 1997; nach Ritz, 2015, S. 55ff.)

Kulturmodell von Schein (1990; nach Ritz, 2015a, S. 39)

⇒ **beobachtbare Aspekte**

Kleidung, Technik, Verhalten, Sprache,…

⇒ **nicht direkt beobachtbar**

Meinungsfreiheit, Vorgesetzten nicht widersprechen,…

⇒ **nur schwer ermittelbar**

„unbewusste Selbstverständlichkeiten“, unterstützen Verhalten in ungewohnten Situationen

Fazit: Die Rolle des Menschen bei aktiver Erzeugung von Sicherheit

- Der Mensch ist aufgrund seiner einzigartigen Fähigkeiten und seiner (juristischen) Verantwortlichkeit die wichtigste Quelle für Sicherheit.
- Menschliche Handlungsvariabilität ist größte Stärke und Schwäche zugleich; es gilt Anpassungsleistung zu fördern und Gelegenheiten für Fehler systematisch zu minimieren.
- Angesichts der wachsenden Bedeutung von Designfehlern (Ritz, 2015a) und den unvermeidlichen Risiken der Großtechnologie (vgl. z.B. Perrow, 1999) müssen Human Factors schon bei der Systemplanung berücksichtigt werden.
- Aufrichtiger Respekt vor Expert*innenwissen ist geboten.
- Fehler sind eine wichtige Quelle für kontinuierliche Verbesserungen.
- Sicherheitskultur bedeutet, Organisationales Lernen sicherheitsgerichtet auszurichten.
- Für die betriebliche Praxis biete sich an, an „**Workarounds**“ anzusetzen. Diese umfassen Schwachstellen in Systemen und menschliche Bewältigungshandlungen zur sicherheitsgerichteten Aufgabenbewältigung.

Literatur

Bainbridge, L. (1983). Ironies of Automation. *Automatica*, *19*, *775-779*.

Brüngger, J. & Ritz, F. (2023). Ausweitung sicherheitsbezogener Grauzonen: Unrealistische Planungsannahmen für operative Tätigkeiten durch Führungskräfte. Beitrag zur 69. Kongress der Gesellschaft für Arbeitswissenschaft e.V., Hannover, 01.-03.03.2023, *S. 1-6*. Sankt Augustin: GFA-Press. https://www.researchgate.net/publication/369269419

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

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

Ritz. F. (2017). Strategische Entwicklung des Sicherheitsmanagements zur Bewältigung neuartiger Gefahren in einer digitalisierten Arbeitswelt. Frühjahrskongress 2017 der Gesellschaft für Arbeitswissenschaft e.V. in Brugg (CH): *Soziotechnische Gestaltung des digitalen Wandels – kreativ, innovativ, sinnhaft –* Beitrag G.1.7, *S. 1-8*.

Ritz, F., Kleindienst, C., Brüngger, J. & Koch, J. (2015). Coping with unexpected safety-critical situations through adaptation - a concept for resilient (simulator) team training. In T. Ahram, W. Karwowski & D. Schmorrow. *Proceedings of the 6th International Conference on Applied Human Factors and Ergonomics AHFE*. Conference track: *2nd International Conference on Safety Management and Human Factors* (*pp. 5236-5242*). July 26th-30th 2015 in Las Vegas (USA).

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*. https://doi.org/10.1007/s11612-016-0318-6

Vielen Dank für Ihre Aufmerksamkeit!

Weitere Informationen:
https://www.fhnw.ch/de/personen/frank-ritz

Kontakt
Prof. Dr. Frank Ritz
frank.ritz@fhnw.ch