Wie unsicher ist sicher genug?

IT-SiBe Jahrestagung 2016

Brühl, 13. September 2016

Professor Dr. Gerhard Banse

gerhard.banse@partner.kit.edu

„Wenn wir annehmen, der ‚schlimmste Fall' könne jederzeit eintreten, wenn wir also Vorsorge treffen und der ‚''schlimmste Fall' bleibt dann doch aus, so ist das allemal weniger gefährlich, als wenn wir uns so verhalten, als könne der ‚schlimmste Fall' nicht eintreten – und er tritt dann doch ein."

(Wolfgang Krüger: „Verantwortung" für den „Super-Gau"? Anmerkungen zu einem Aufsatz von Günter Ropohl. In: EuS. Ethik und Sozialwissenschaften. Zeitschrift für Erwägungskultur, Heft 1/1994, S. 160)

„Das Leben ist keine unlogische Angelegenheit; trotzdem stellt es für die Logik eine Falle dar. Es scheint eben ein klein bißchen mathematischer und regulärer, als es ist; seine Genauigkeit ist augenfällig, seine Ungenauigkeit aber verborgen; seine Unberechenbarkeit liegt im Hinterhalt“.

(Gilbert Keith Chesterton; zit. nach Peter L. Bernstein: Wider die Götter. Die Geschichte von Risiko und Risikomanagement von der Antike bis heute. München 1997, S. 424)

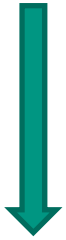
Ziel: Perspektiven-Wechsel *anregen*

(1) Ausgangs-Situation

⇒ Frage „Wie sicher ist sicher genug?“

↳ „Mit wieviel Sicherheit wollen wir leben?“

↳ normatives Problem (auf Mikro-, Meso- und Makroebene)
(Fixierung auf „Sicherheitsideal“ mit allen Konsequenzen)



(2) „Tatsachen“ der Lebenswelt

(3) Ziel-Situation

⇒ Frage „Wie unsicher ist sicher genug?“

↳ „Mit wieviel Unsicherheit müssen wir leben?“

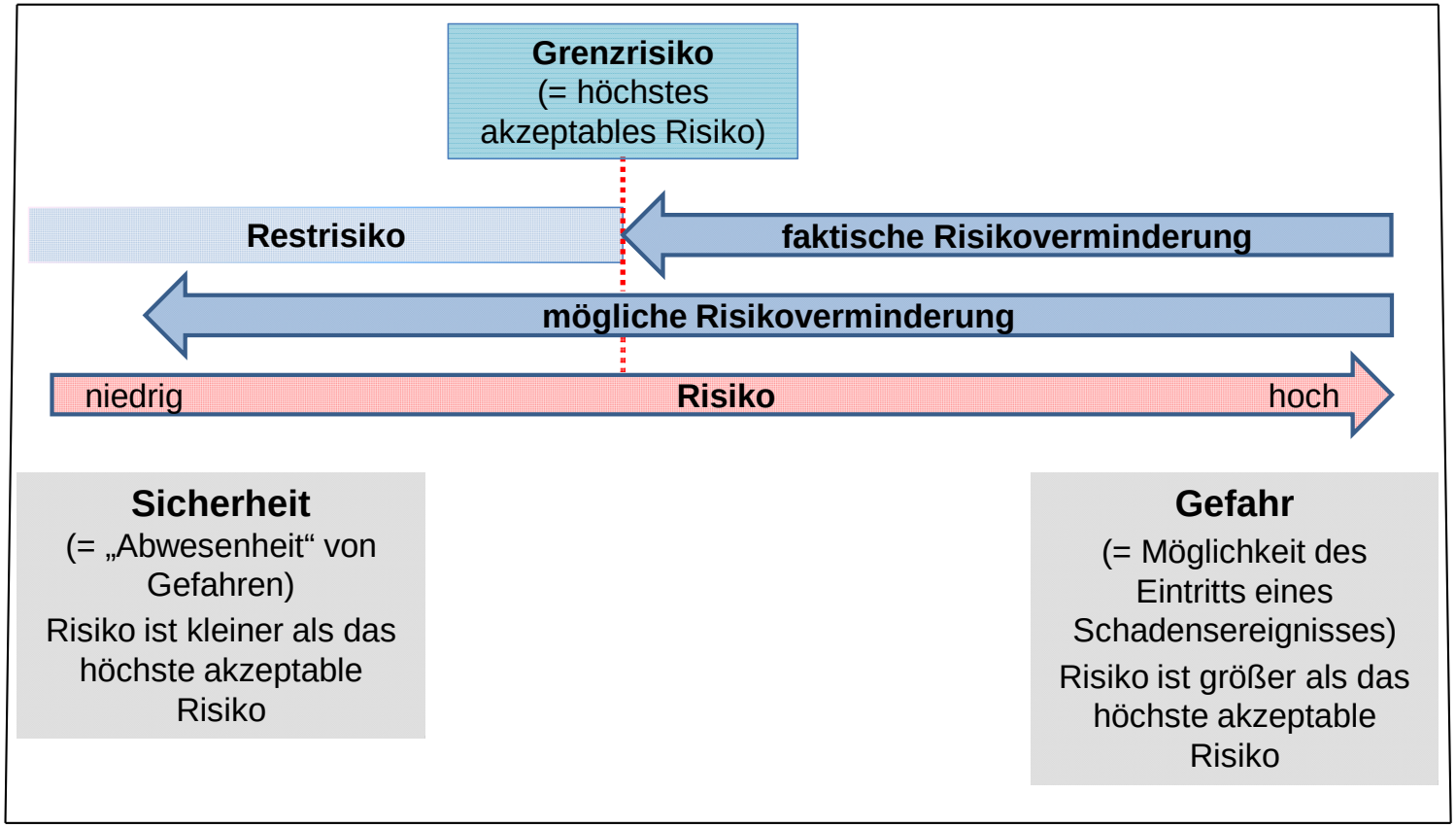
↳ deskriptives Problem (auf Mikro-, Meso- und Makroebene)

INHALT

INHALT

(1) Ausgangs-Situation – Konzeptioneller Hintergrund Ia

(I) Sicherheitsverständnis



(nach DIN 31000 „Allgemeine Leitsätze für das sicherheitsgerechte Gestalten von Produkten“; eigene Darstellung)

(1) Ausgangs-Situation – Konzeptioneller Hintergrund Ib

1. Die unterschiedlichen Risiko„anteile“ werden durch das jeweilige Maß an ***Akzeptanz*** unterschieden.

Unklar bleibt indes, wie es zur Festlegung bzw. Feststellung des „Akzeptablen“ kommt.

2. Zu klären ist, was sich hinter dem sogenannten ***„Restrisiko“*** verbirgt.

EN ISO 12100 „Sicherheit von Maschinen – Allgemeine Gestaltungsleitsätze – Risikobeurteilung und Risikominderung“ (2011):
Das Restrisiko ist jenes Risiko ist, dass verbleibt, nachdem Schutzmaßnahmen getroffen wurden, wobei es einen abschätzbaren und einen unbekannten (!!) Anteil gibt.

(1) Ausgangs-Situation – Konzeptioneller Hintergrund Ic

„Kalkar-Entscheidung“ des Bundesverfassungs-Gerichts vom 08. August 1978:
„In einer notwendigerweise mit Ungewißheit belasteten Situation“ gilt: „Für die Gestaltung der Sozialordnung muß es insoweit bei Abschätzungen anhand praktischer Vernunft bewenden. Ungewißheiten jenseits dieser Schwelle praktischer Vernunft sind unentrinnbar und insofern als sozialadäquate Lasten von allen Bürgern zu tragen.“

Restrisiko bedeutet, dass „die Wahrscheinlichkeit eines künftigen Schadens nicht mit letzter Sicherheit auszuschließen“ ist und „in Kauf“ zu nehmen sei.

(II) Technikverständnis

(a) „*traditionales*“ („mechanistisches“) TV

„Eindeutigkeit“
deterministisches System
statisches System
Wiederholbarkeit
Faktizität
exakte Beschreibung
Kontinuum
Einzelheit
technikzentriert/-orientiert
disziplinär

(1) Ausgangs-Situation – Konzeptioneller Hintergrund IIb

(b) (mehr oder weniger) *engeres* TV

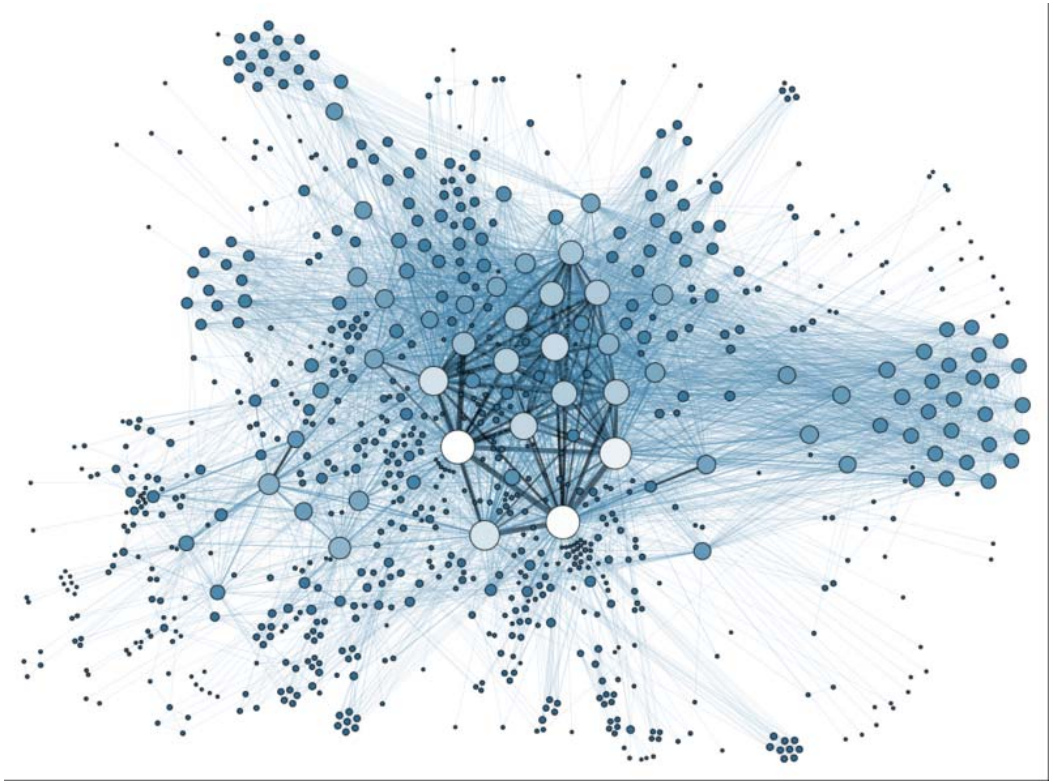
- Reduzierung vorrangig auf „Artefaktisches“ (technisches Sachsystem: technische Mittel zur Zweckerreichung);
- Reduzierung vorrangig auf unmittelbare Mensch-Technik-Interaktionen im Verwendungshandeln;
- Berücksichtigung zumeist nur des rechtlichen und des politischen (sowie des ökonomischen) „Kontextes“;
- Vernachlässigung weiterer relevanter „Kontexte“ (etwa des kulturellen) sowie des Herstellungshandelns (Implementierungen!).

INHALT

(2) Tatsachen“ der Lebenswelt Ia

(I) Technische Entwicklungen

(a) von (bekannten) Großrechnern über PC/Server/Mobiltelefonie zu (anonymen, ***vernetzten***) Großrechnern („Wolke“!!)



⇒ ***Intransparenz***

(https://upload.wikimedia.org/wikipedia/commons/9/9b/Social_Network_Analysis_Visualization.png)

(2) Tatsachen“ der Lebenswelt Ib

(b) von der Mensch-Computer-Interaktion/Kommunikation zur Computer-Computer-Interaktion/Kommunikation („Internet der Dinge“; IoT)

⇒ ***„Schwachstellen“*** (mehrere Mio. Programm-Zeilen!)

⇒ ***Komplexität*** (viele Variable, vernetzte Variable, nichtintendierte Wechselwirkungen, Eigendynamiken)

(c) „ubiquitous computing“ im umfassendsten Sinn (einschließlich Home/Building Automation, Automotive, Industrie 4.0, …)

⇒ ***Verletzlichkeit***

(d) „wireless“ // ***vereinheitlichte*** und ***autonome*** Grundkomponenten („Algorithmen“; „Codes“)

⇒ ***umfassende Kompromittierbarkeit***

↳ IT-Sicherheit ist unter z.T. undefinierten / nichtdefinierbaren Bedingungen zu gewährleisten!

(II) Entwicklungen von Handlungspraxen und Nutzungsmustern

- ***Technologie*** als „Treiber“ (Was ist technisch möglich? ≠ Was ist technisch sinnvoll?)
- ***Lebensweise*** als „Treiber: „Internet to go“ / „Cyberlife“ („Leben 2.0“) / „Digitale Teilhabe bedeutet soziale Teilhabe!“

☞ (a) wahrnehmbare Differenz zwischen 1983 („Volkszählungsurteil“) und heute (nur Verhältnis „Freiwilligkeit vs. [staatlicher] Zwang“ oder „kultureller Wandel“?)

(b) Verschiebungen zwischen „Öffentlichem“ und „Privatem“

(c) „Entgrenzungen“: räumlich, zeitlich, rechtlich, sprachlich, altersmäßig, sittlich, „quantitativ“, … / „Bequemismus“

(d) zunehmende Abhängigkeiten („Sachzwänge“, Gruppenzwänge“)

(2) Tatsachen“ der Lebenswelt IIb

(e) ***Nutzungssituation***

WER nutzt? - Subjekt (Mensch)

WAS wird genutzt? - Mittel (techn. Sachs.)

WOFÜR wird genutzt? - Ziel/Zweck

WIE wird genutzt? - Modalitäten

Unter WELCHEN Bedingungen wird genutzt? - „Kontext“

IT-Sicherheitsrelevanz u.a. durch

WER? – Wissen / (Sach-, Personal-, Sozial-, Methoden-)Kompetenzen

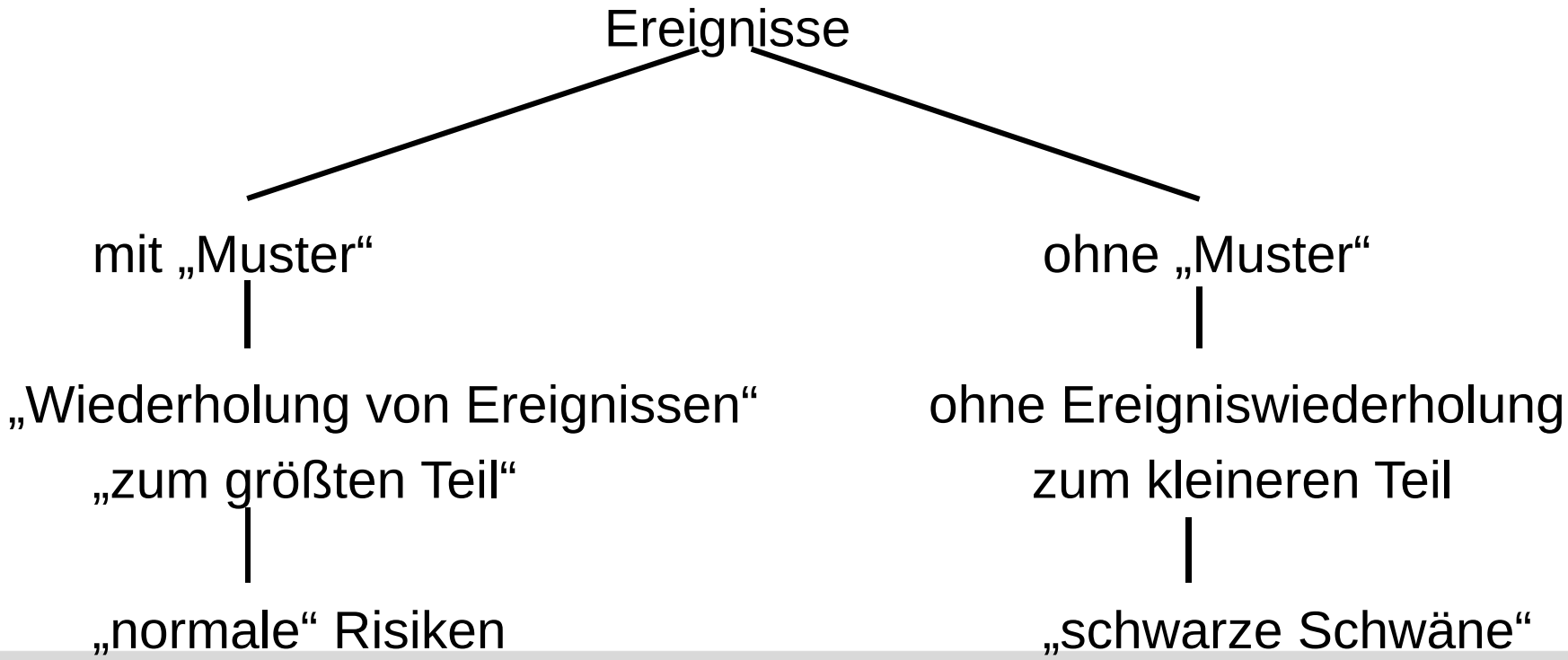
WAS? – Usability; „Infrastruktur“

WOFÜR? – Informieren (über mich / über andere); Kommunizieren; Kooperieren; Enter-/Infotainment

(III) „Alternative“ Denkansätze

(a) *Gottfried Wilhelm Leibniz*: Brief an Jacob Bernoulli vom 3. Dezember 1703

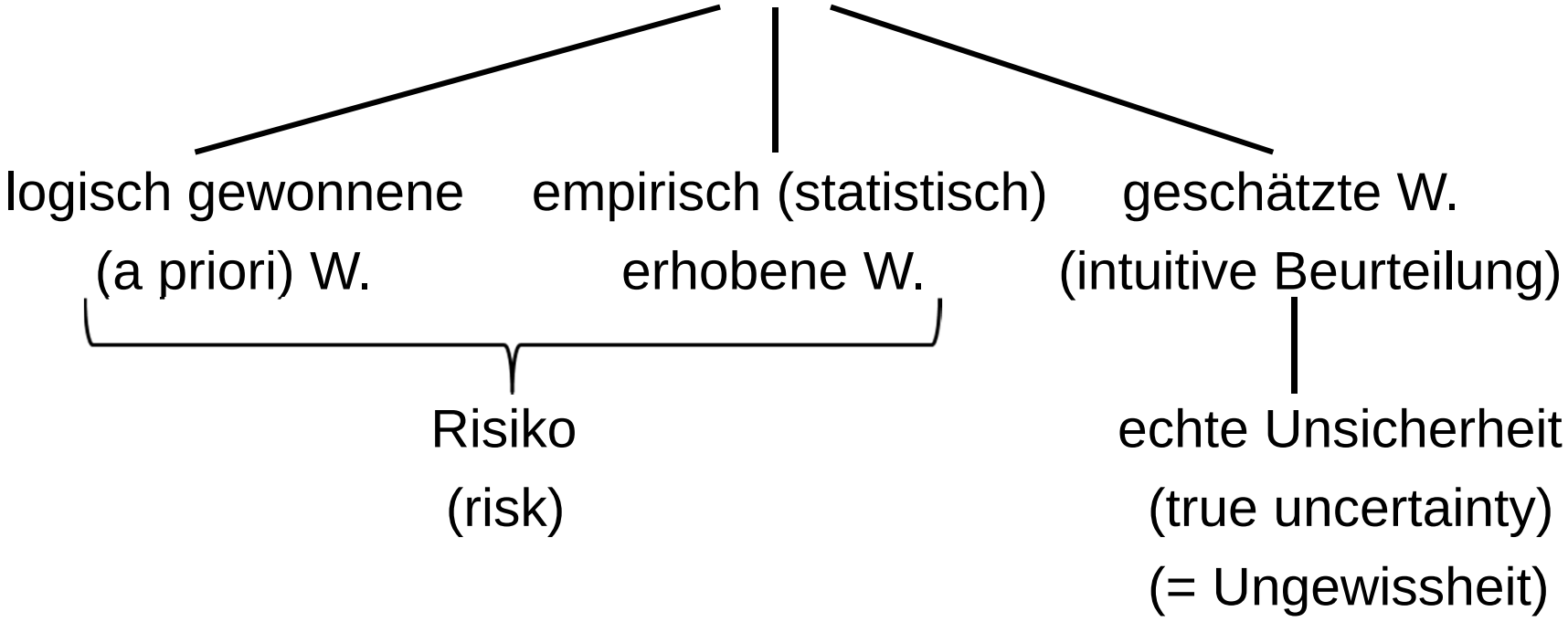
Die „Natur [hat] Muster eingerichtet [...], die zur Wiederholung von Ereignissen führen, aber nur zum größten Teil“.



(2) Tatsachen“ der Lebenswelt IIIb

(b) *Frank Knight*: „Risk, Uncertainty, and Profit“ (1921)

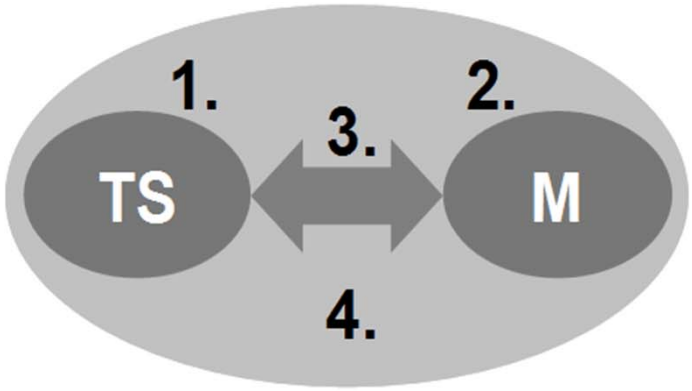
3 Arten von Unsicherheiten (Wahrscheinlichkeitssituationen)



Für *echte Unsicherheit* existieren keinerlei Methoden, um eine objektive und quantitative Eintrittswahrscheinlichkeit anzugeben, da ihr Auftreten einzigartig ist und es wenig (bzw. keine) Erfahrungswerte gibt.

INHALT

(3) Ziel-Situation – Erweitertes Technikverständnis I



1. Technische Sachsysteme (TS)
2. Nutzer/Menschen (M)
3. Wechselwirkung zwischen Nutzer und technischem Sachsystem
4. Umfeld

➢ ***„Embedded Systems“***

„Sichere Gesamtzustände unter Beteiligung von Menschen haben andere Eigenschaften als technische Apparate. Das Hinzutreten des Menschen in diesen Systemzusammenhang ist wesentlich mit Schuld an den veränderten Eigenschaften. Unter Einfluß menschlichen Handelns werden die Systemzustände prinzipiell unvorhersagbar und selbst in ihrer Wahrscheinlichkeitsberechnung problematisch.“

(Reuter, H.; Wehner, Th.: Eine ganzheitspsychologische Betrachtung der Sicherheit im Umgang mit Industrierobotern. In: Banse, G. (Hg.): Risikoforschung zwischen Disziplinarität und Interdisziplinarität. Von der Illusion der Sicherheit zum Umgang mit Unsicherheit. Berlin 1996, S. 94)

(3) Ziel-Situation – Erweitertes Technikverständnis II

Die Sicherheit in Mensch-Technik-Interaktionen lässt sich gewährleisten bzw. verbessern durch „Investitionen“ in

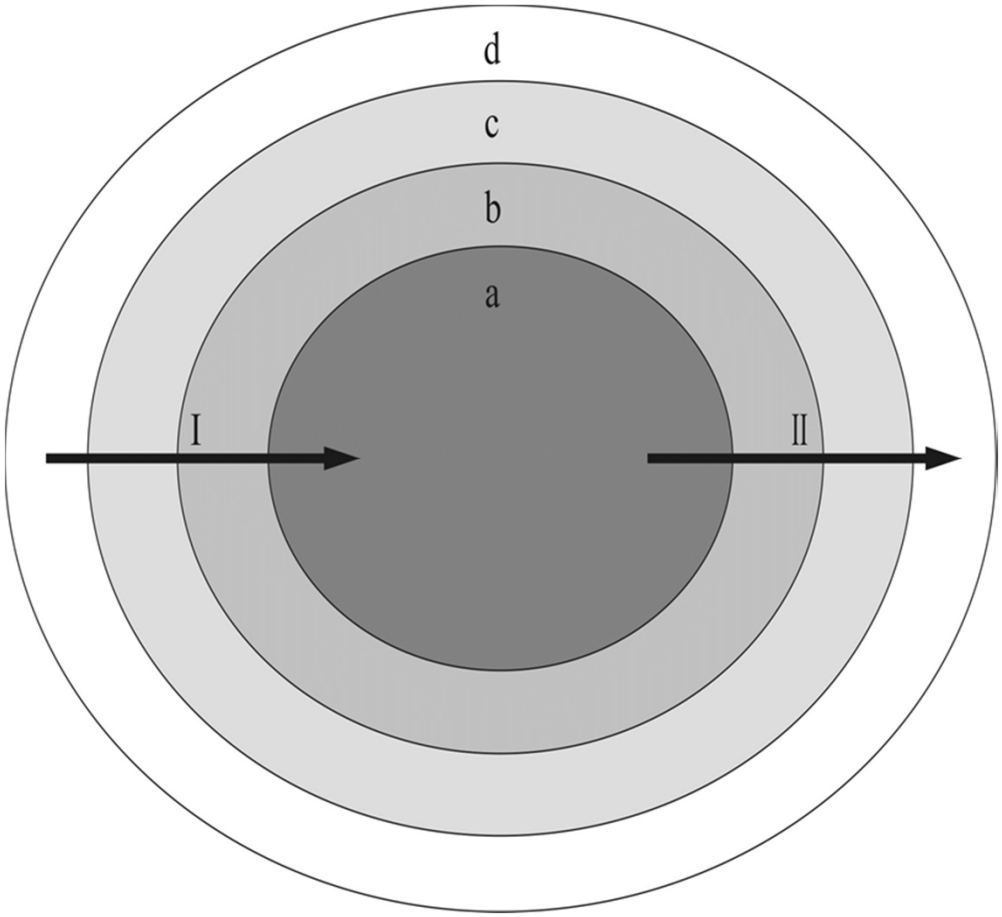
1. die technischen Sachsysteme (TS) bei deren konstruktiver Auslegung und produktionstechnischer Herstellung (etwa durch Verbesserungen hinsichtlich Zuverlässigkeit und Handhabbarkeit, der Schadensvorbeugung und der Gefährdungsabwehr);
2. die „Nutzer“ (M) technischer Sachsysteme (etwa durch die Ausprägung von Kompetenz und spezifischer Persönlichkeitseigenschaften);
3. die „Wechselwirkung“ von TS und M (etwa durch solche technischen Komponenten oder personellen Ausprägungen, die die Möglichkeit von Fehlern und/oder Irrtümern verringern);
4. das (rechtliche, soziale, **kulturelle**, …) „Umfeld“ der Technikherstellung, vor allem aber der Techniknutzung (z.B. „Sicherheitskultur“).

(3) Ziel-Situation – Erweitertes Technikverständnis III

Komplexes Technikverständnis

„Eindeutigkeit“	„Mehrdeutigkeit“
deterministisches System	stochastisches System
statisches System	dynamisches System
Wiederholbarkeit	(eingeschränkte) Wiederholb.
Faktizität	Hypothetizität
exakte Beschreibung	„unscharfe“ Beschreibung
Kontinuum	Vielheit / Komplexität
Einzelheit	Diskontinuum
technikzentriert/-orientiert	anthropo- / humanorientiert
disziplinär	multi- / transdisziplinär

(3) Ziel-Situation – Erweitertes Technikverständnis IV



(d) soziale, **kulturelle** Ebene

(c) rechtliche, ökonomische Ebene

(b) technisch-organisatorische Ebene

(a) technisches Sachsystem (als „Kern“)

I Sozialkonstruktivismus

II Technischer Determinismus

(verändert nach Krummeck, G.; König, R.: Chipkarten im Gesundheitswesen. Abschlußbericht. Bonn (BSI) 1994, S. 33)

(3) Ziel-Situation – „Instrumente“ I

(a) „Bedrohungstypen“ und Sicherheitsanforderungen ***zeitgemäß*** analysieren

(Vertraulichkeit; Integrität; Verfügbarkeit; Zurechenbarkeit; Authentizität; Unabstreitbarkeit; Zugriffskontrolle; Unbeobachtbarkeit; Anonymität; Unverkettbarkeit;

Identitätstäuschung; Datenverfälschung; Abstreiten von Handlungen; Ausspähen; Programmverfälschung; Unterlassen von Handlungen; Diebstahl; Vorgangsverfälschung; Abstreiten der Urheberschaft; Restriktion von System-Ressourcen; Missbrauch von System-Ressourcen)

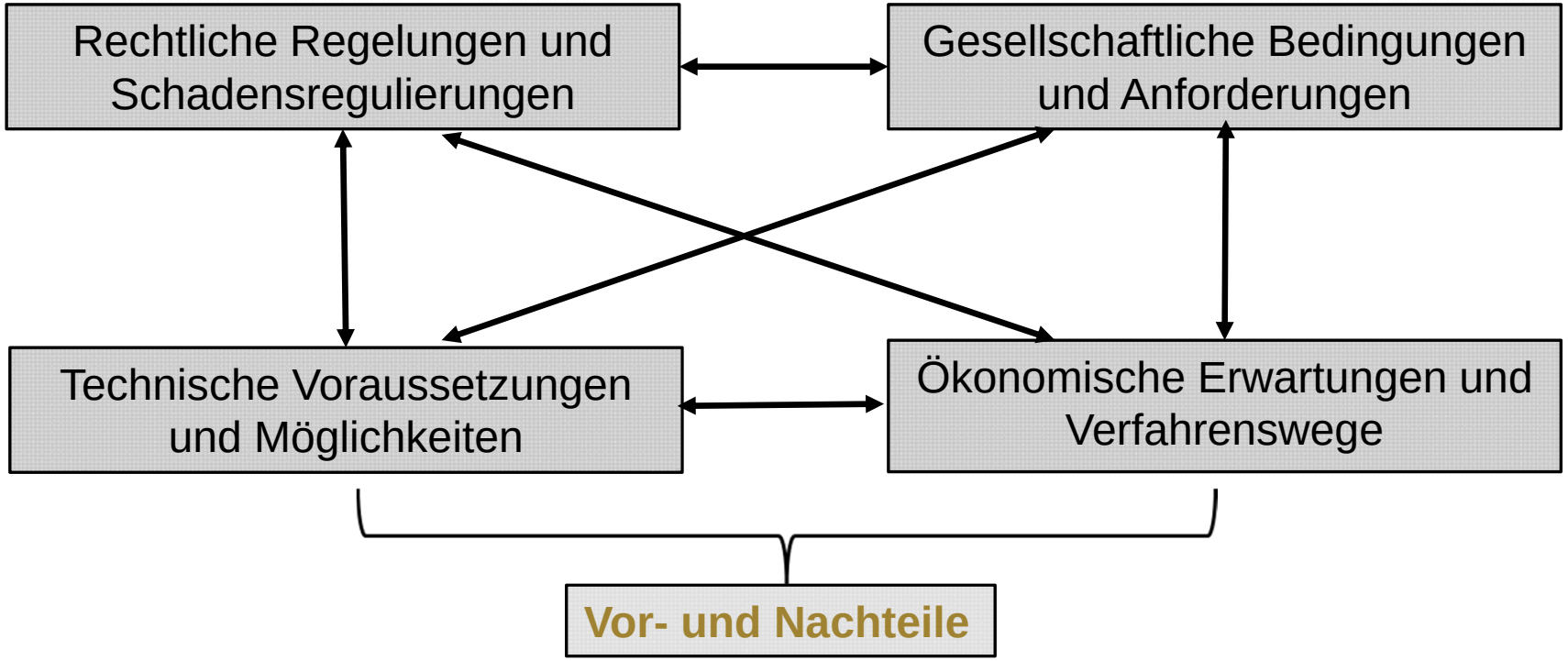
⇒ ***Beeinflussbares / Nicht-Beeinflussbares*** (z.B. Software-Implementierungen)

⇒ „***Verletzlichkeit*** der Informationsgesellschaft“, „Blackout“

(3) Ziel-Situation – „Instrumente“ II

(b) ***Abwägungen*** im Bereich der IT-Sicherheit: **„Quadrupel“**

(nach Zoche, P.; Kornetzky, S.; Harmsen, D.-M. (1998): Folgen durch fehlende oder unzureichende IT-Sicherheitsvorkehrungen im elektronischen Zahlungsverkehr. Technikfolgen-Abschätzung im Auftrag des Bundesamtes für Sicherheit in der Informationstechnik. Karlsruhe (ISI) Mai (Manuskript), S. 17)



besser **„Pentrupel“**: Ergänzung um individuelle Erwartungen / Erfahrungen

(3) Ziel-Situation – „Instrumente“ IIIa

(c) stärkere Berücksichtigung des ***„Kulturellen“***

- ***„Fehlerkultur“*** (als Teil der Unternehmens- oder „Behörden“kultur)

- ***Sicherheitskultur*** (als Teil der Mensch-Technik-Interaktion auf der Mikro- und der Meso-Ebene)

„Beeinflußt werden die Charakteristika einer Sicherheitskultur durch technische, ökonomische und organisatorische Zwänge, repräsentiert werden sie durch sicherheitstechnische Vorrichtungen, Regelwerke, Vorschriften, Aufsichtsdienste und Praktiken einerseits sowie informelle Praktiken, individuelle und kollektive Sinnvorstellungen der Mensche andererseits. Sicherheitskulturen bieten für den einzelnen Menschen folglich einen Rahmen, der die Ordnung der menschlichen Wahrnehmung erst ermöglicht.“

(Hartmann, A.: „Ganzheitliche IT-Sicherheit“: Ein neues Konzept als Antwort auf ethische und soziale Fragen im Zuge der Internationalisierung von IT-Sicherheit. In: BSI – Bundesamt für Sicherheit in der Informationstechnik (Hg.): Fachvorträge 4. Deutscher IT-Sicherheitskongreß 1995, (Sektion 7, BSI 7165), S. 10)

(3) Ziel-Situation – „Instrumente“ IIIb

- (mehr) **„theoretische“** Ebene (vor allem in Form von Anweisungen, Regeln, Vorschriften, Statements, Codes usw.)
- (mehr) **„praktische“ Ebene** (als gelebte und praktizierte Sicherheitskultur)

  ⇒ sicherheitsbezogene handlungsrelevante/-leitende Einstellungen, Werte und grundlegende Überzeugungen der Mitarbeiter

***Kommunikation*:** Wie wird über Techniksicherheit kommuniziert?

***Handeln/Verhalten*:** Welche sicherheitsrelevanten Handlungspraxen haben sich im Umgang mit Technik(en) bzw. technischen Systemen herausgebildet und wie sind diese institutionalisiert?

***Denken*:** Welche Kompetenzen und welchen Informationsstand haben die Akteure?

***Fühlen/Empfinden*:** Wie zufrieden sind die Individuen mit der Arbeitsumgebung? Welche Strukturen der Anerkennung und Motivation existieren?

(3) Ziel-Situation – „Instrumente“ IIIc

↳ - Individuelle Sicherheitskulturen (Mikroebene) enthalten ***implizite*** Anteile (unreflektierte Denkgewohnheiten und Handlungsroutinen).

- Transindividuelle Sicherheitskulturen (ab Mesoebene) sind zumeist ***heterogen*** und zunehmend ***„hybrid“*** (Kontexte von Intrakulturalität).
- Sicherheitskultur lässt sich nur indirekt über ***Indikatoren*** „messen“.

Ausgewählte Indikatoren der Sicherheitskultur			
Tech. Anlagen/ unterstützende tech. Systeme	Sicherheitsrelevante Störungen an Maschinen	Fehlbedienung von Maschinen und Anlagen	
Dokumentation	Verständlichkeit der sicherheitsrelevanten Vorschriften	Kommunikation der sicherheitsrelevanten Vorschriften	Dokumentation und Analyse sicherheitsrelevanter Vorfälle
Bedingungen/ Gebäude	Sauberkeit	Ergonomische Bedingungen	
Faktor Mensch	Strukturwissen der Mitarbeiter	Verhalten der Mitarbeiter in kritischen Situationen	Sicherheitsbewusstsein der Mitarbeiter
Organisation	Wertesystem im Unternehmen	Prävention	Sicherheitsfokussierung
Produkt	Reklamationen	Rückrufaktionen	

(übersetzt aus Belyová, L.; Banse, G.: Safe Innovations, Innovative Safety. In: Loudín, J.; Hochgerner, J. (eds.): Social and Cultural Dimensions of Innovation in Knowledge Societies. Prague 2011, p. 73)

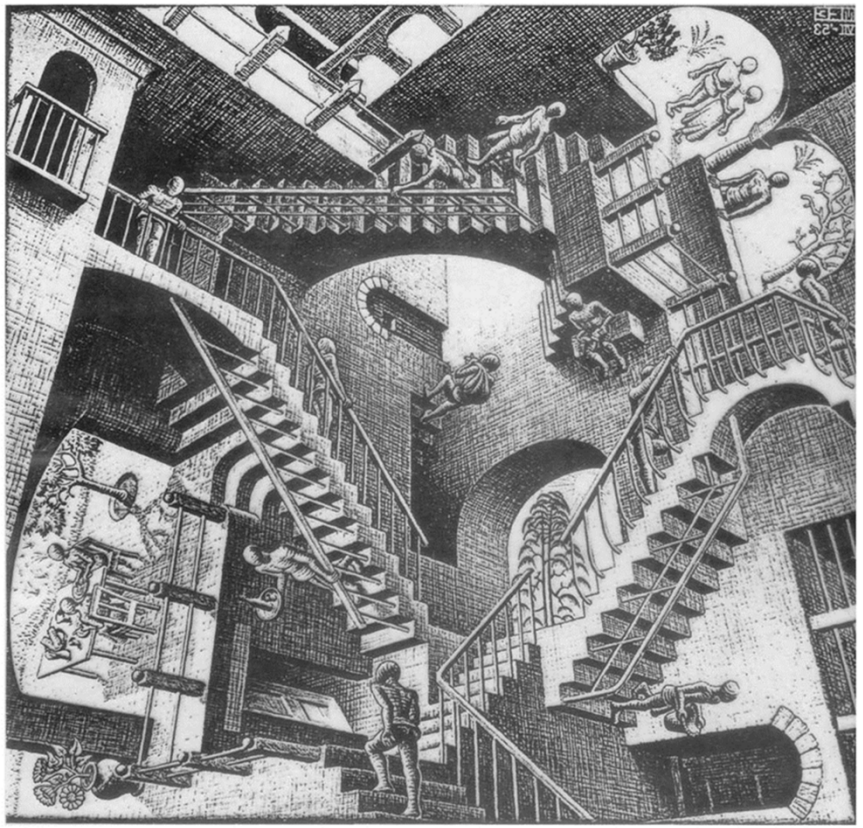
INHALT

Fazit I

- Die nach wie vor vorherrschende Fixierung auf das Ideal vollständiger Sicherheit muss ***überwunden***, zumindest ***relativiert*** werden (Perspektivenwechsel).
- Es gilt: Die Unbestimmtheit hinsichtlich der zukünftigen Wirkungen heutiger Entscheidungen und Handlungen ist eine bestimmende Größe unseres Lebens, d.h. die „Risikobehaftetheit“ ist ***irreduzibel*** – Leben unter Unbestimmtheit (in einem unbestimmten Ausmaß!) ist Normalität.
- Reduzierung, Limitierung oder Eingrenzung der Unbestimmtheit sowohl hinsichtlich der Eintrittswahrscheinlichkeit (ursachenorientiert) als auch des zu erwartenden Schadensausmaßes (wirkungsorientiert), d.h. eine ***zielgerichtete Einflussnahme*** und ***produktive Handhabung*** („Beherrschung“) von Unbestimmtheit ist präventiv durch verschiedene Vorgehensweisen jedoch möglich.

Fazit II

- Neue technische Lösungen stellen oftmals einen ***Kultur(um)bruch*** dar (d.h. einen gravierenden Wandel im menschlichen Handeln), der mit „Irritationen“ bei den Nutzern (z.B. in Form von Handlungsfehlern oder inadäquaten Handlungsroutinen) verbundenen sein kann.
- Unbestimmtheiten auch hinsichtlich IT-Sicherheit werden individuell unterschiedlich, z.T. konträr wahrgenommen, registriert und bewertet – damit ist eine ***Vielfalt von möglichen Sichtweisen*** verbunden.



(Escher, M. C.: Ineinanderverschlungene Perspektiven. In: „Relativität“. 1953)

„Katastrophen sind selten, [jedoch könne man] daraus wenig Trost beziehen.“

„Systemunfälle sind ungewöhnlich, sogar selten; dennoch ist diese Tatsache alles andere als beruhigend, wenn sie eine Katastrophe nach sich ziehen können.“

(Charles Perrow: Normale Katastrophen. Die unvermeidbaren Risiken der Großtechnik. Frankfurt am Main/New York 1989, S. 13, 18)