- Verlässlichkeit -

Thesen zur Förderung wissenschaftlicher Grundlagenforschung

Initiative des Themennetzwerkes - Sicherheit -
der Deutschen Akademie für Technikwissenschaften (acatech)

Prof. Jürgen Beyerer
Universität Karlsruhe

Prof. Eckehard Schnieder
Universität Braunschweig

Prof. Petra Winzer
Bergische Universität Wuppertal

acatech
DEUTSCHE AKADEMIE DER TECHNIKWISSENSCHAFTEN

Inhalt

Sicherheit umfasst im Allgemeinen und im fachsprachlichen Sprachgebrauch viele Aspekte aus allen Lebenslagen in Gesellschaft, Wirtschaft und Technik.

Der Sicherheitsbegriff erstreckt sich von:

- Gewissheit,
- Vertrauenswürdigkeit,
- Zuverlässigkeit,
- Schutz vor Gefährdungen,
- Bedrohungen von innen und außen,
- Risiko sowie bis hin zu
- Resilienz.

Verlässlichkeit wird als erweitertes Sicherheitsverständnis aufgefasst!

Die **Verlässlichkeit**: „… bezeichnet die Gesamtheit der **vier Eigenschaften**“ von Systemen, d.h. „**Überlebensfähigkeit** (engl. Reliability; oftmals auch als Zuverlässigkeit bezeichnet), **Verfügbarkeit** (engl. Availability), **Instandhaltbarkeit** (engl. Maintainability), **Sicherheit** (engl. Safety für Schutz der Umwelt vor negativen Auswirkungen des Betrachtungssystems sowie Security für Schutz des Systems vor Fremdeinwirkungen)“ [Schnieder 2013, S. 57]. Ergänzend kommen Vertrauenswürdigkeit, Korrektheit und Gewissheit hinzu.

Gewissheit,
Vertrauenswürdigkeit,
Zuverlässigkeit,
Schutz vor Gefährdungen,
Bedrohungen von innen und außen,
Risiko sowie bis hin zu
Resilienz.

Verlässlichkeit

Sicherheit

Vorarbeiten/ Analyse des Standes der Wissenschaft und Forschung u.a.:

und zahlreiche Diskussionen führten zum vorliegenden Thesenpapier.

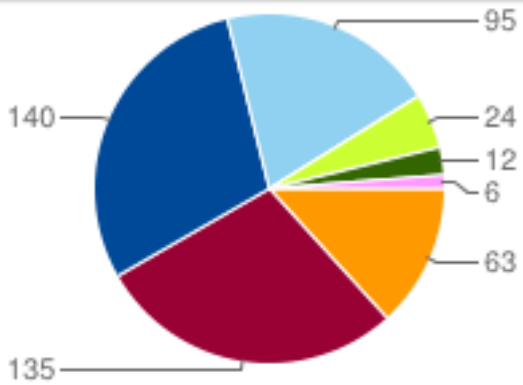
Initiatoren des Thesenpapiers	Unterstützer des Thesenpapiers
Prof. Jürgen Beyerer **(Universität Karlsruhe)** **Prof. Eckehard Schnieder** **(Universität Braunschweig)** **Prof. Petra Winzer** **(Bergische Universität Wuppertal)**	Prof. Reiner Anderl (Technische Universität Darmstadt) Prof. WilhBauer (Fraunhofer-Institut für Arbeitswirtschaft und Organisation IAO, Stuttgart) Prof. Christina Berger (Technische Universität Darmstadt) Prof. Bernd Bertsche (Universität Stuttgart) Prof. Jürgen Gausemeier (Universität Paderborn) Prof. Norbert Gronau (Universität Potsdam) Prof. Claudia Eckert (TU München) Prof. Eva-Maria Jakobs (RWTH Aachen) Prof. Roland Jochem (Technische Universität Berlin) Prof. Michael Lauster (Fraunhofer Institut für Naturwissenschaftlich-Technische Trendanalysen INT) Prof. Joern Müller-Quade (Karlsruher Institut für Technologie, KIT) Prof. Ortwin Renn (Universität Stuttgart) Prof. Klaus Thoma (Universität Freiburg) Prof. Wilhelm Schäfer (Universität Paderborn) Heinz Schmersal (Schmersal Gruppe) Prof. Dieter Spath (Wittenstein AG) Prof. Klaus Vieweg (Universität Erlangen) Prof. Anette Weisbecker (Fraunhofer-Institut für Arbeitswirtschaft und Organisation IAO, Stuttgart) Prof. Kai-Dietrich Wolf (Bergische Universität Wuppertal/ ISS Velbert) Prof. Liggesmeyer (Fraunhofer-Institut IESE und Präsident der Gesellschaft für Informatik) Prof. Dr.-Ing. Karsten Lemmer (Institut für Verkehrssystemtechnik des DLR)

Wissenschaftliche Problemlage:

- sehr viele angewandte nationale und internationale Forschungsprojekte zu den Themen Safety, Security, Resilienz,
- keine fachübergreifende Grundlagenforschung zum Thema Verlässlichkeit,
- divergente Sichten verschiedenster Wissenschaftsdisziplinen auf das Themenfeld der Sicherheit sowie eine unzulängliche Kommunikationsgrundlage zur Überwindung dieser,
- keine einheitliche Definition der vielschichtigen Begriffe Sicherheit, Unsicherheit, Risiko, Gefahr sowie insbesondere eine getrennte Betrachtung von Safety und Security sowie
- kein systemtheoretischer Ansatz, der Safety und Security übergreifend betrachtet.

Sicherheitsforschung in Deutschland:

475 Institutionen in Deutschland



Anzahl	Kategorie
63	Großunternehmen
135	KMU
140	Hochschulforschung
95	Forschungsinstitute
24	Netzwerke
12	Behörden
6	Verbände

Quelle: www.securityresearchmap.de

BMBF-geförderte Projekte seit 2007:
Szenarienorientierte Sicherheitsforschung: 92
Querschnittsorientierte Sicherheitsforschung: 54

Quelle : www.bmbf.de/de/11770.php

7. Forschungsrahmenprogramm der EU:
Themenbereich „Sicherheit“ (2007-2013) 1,4 Milliarden Euro

Quelle : www.bmbf.de/de/13012.php

Es fehlt eine systematische Grundlagenforschung!

Wissenschaftliche Fragestellungen:

- Können durch das transdisziplinäre Betrachten der verschiedenen sicherheitsrelevanten Forschungsfelder Zusammenhänge erkannt, Doppelungen vermieden und Synergien gestiftet werden?

- Gibt es Möglichkeiten zukünftige Herausforderungen durch erstmalig fachdisziplinübergreifende Modellkonzepte und ihre einheitliche Formalisierungen zu analysieren und ihnen vorzubeugen (z.B. infolge der Verwundbarkeit intensivierter oder digitaler Vernetzungen der Infrastrukturen oder infolge ausgeschöpfter Ressourcen)?

- Ist die Änderung der Blickrichtung von der reaktiven zu einer konstruktiven Sichtweise, d. h. integrierte Prävention zur Gewährleistung der Verlässlichkeit soziotechnischer Systeme möglich?

Wissenschaftliche Zielstellung:

Etablieren der wissenschaftlichen Grundlagenforschung
für das Forschungsgebiet der Verlässlichkeit

Zentraler Ansatz für das erweiterte Sicherheitsverständnis – als Verlässlichkeit bezeichnet – ist eine *systemische Betrachtung*, in der *allgemeine und spezielle Konzepte sowie Methoden* der Systemtheorie
aus der Technik (Systems Engineering, Regelungstechnik, Nachrichtentechnik), der Statistik und Stochastik sowie der Sozialwissenschaften *mittels formalisierter Modelle transdisziplinär integriert werden*.

Deutschland als Garant für Verlässlichkeit

Schwerpunkte einer transdisziplinären Verlässlichkeitsforschung sind:

- durch Abstraktion gemeinsame Konzepte zu identifizieren, diese dann zu modellieren,

- geeignete Termini und Beschreibungsmittel symbolischer und formaler Natur zu finden, welche zu konsistenten Begriffsgebäuden und akzeptablen oder sogar universellen Metriken der Verlässlichkeit führen können,

- methodische/systematische Vorgehensweisen der verschiedensten Wissenschaftsdisziplinen so zu bündeln, dass ein transdisziplinärer methodischer Ansatz der Verlässlichkeitsforschung entwickelt werden kann.

Transdisziplinäre Theorie der Verlässlichkeit

Thesen zur Verlässlichkeit im Überblick:

- These 1: **Überwindung der Vielfalt**
- These 2: **Integration von Safety und Security**
- These 3: **Kommunikation und Begriffsbildung (Terminologie)**
- These 5: **Metriken der Verlässlichkeit**
- These 4: **Sicherheit ist eine emergente Verhaltenseigenschaft**
- These 6: **Verlässlichkeit ist konstruierbar**

These 1: Überwindung der Vielfalt

Die Verlässlichkeit technischer und soziotechnischer Systeme kann nur nachhaltig gewährleistet werden, wenn die disziplin- und domänenspezifische Aufspaltung des Wissenschaftsgebietes „Sicherheit“ überwunden wird.

Problemlage:

- Diversifikation

Wissenschaftliche Fragestellung:

- Domänen- und techniktypübergreifende Konzeptualisierung möglich?

Lösungsansatz: Abstraktion, Integration und Formalisierung

Aktuelle Unzuverlässigkeitsfälle

31.01.2013

„Dreamliner"-Desaster kostet Airline Millionen

Wegen der Probleme mit Batterien müssen alle „Dreamliner" am Boden bleiben.

Quelle: Focus

11.04.2013

Millionen-Rückruf wegen Airbag-Problem

Die japanischen Autohersteller Toyota, Honda, Mazda und Nissan bitten wegen fehlerhaften Beifahrer-Airbags weltweit insgesamt 2,9 Millionen Autos in die Werkstatt. Auch in Deutschland sind Fahrzeuge betroffen.

Quelle: auto-motor-sport

20.03.2013

VW holt 384.000 Autos in die Werkstatt

VW bittet bei einer Rückrufaktion in China mehr als 380.000 Autos in die Werkstatt. Der Grund ist ein Problem mit dem DSG-Getriebe

Quelle: auto-motor-sport

Quelle: Bernd Bertsche: Ähnlichkeiten und Unterschiede zwischen Sicherheit und Zuverlässigkeit. Vortrag. 26. VDI-Fachtagung Technische Zuverlässigkeit 2013 Produkt- und Prozessgestaltung. 23./24. April 2013, Leonberg bei Stuttgart.

These 1: Überwindung der Vielfalt

In Anlehnung an These 3, Prof. Schnieder, Folie 30.

Fazit:

- 130 unterschiedliche Sicherheitsdefinitionen allein in deutschen Normen
- Sicherheit und Zuverlässigkeit wird:
  - in der Datenbank DIN-Term
  - im internationalem Vokabular der Elektrotechnik
  - im VDI-Handbuch Technische Zuverlässigkeit
- Vielzahl von unterschiedlichsten sicherheitsmethodischen Vorgehensweisen.
- Gesetzliche Regelungen trennen zwischen Entwurfs- und Herstellungs- bzw. Nutzungsprozess
- Erkenntnisse über sichere Produkte, Maschinen, Anlagen, Technologien, Gebäude, Dienstleistungen etc. müssen systematisch über deren PLC gesammelt und ausgewertet werden können

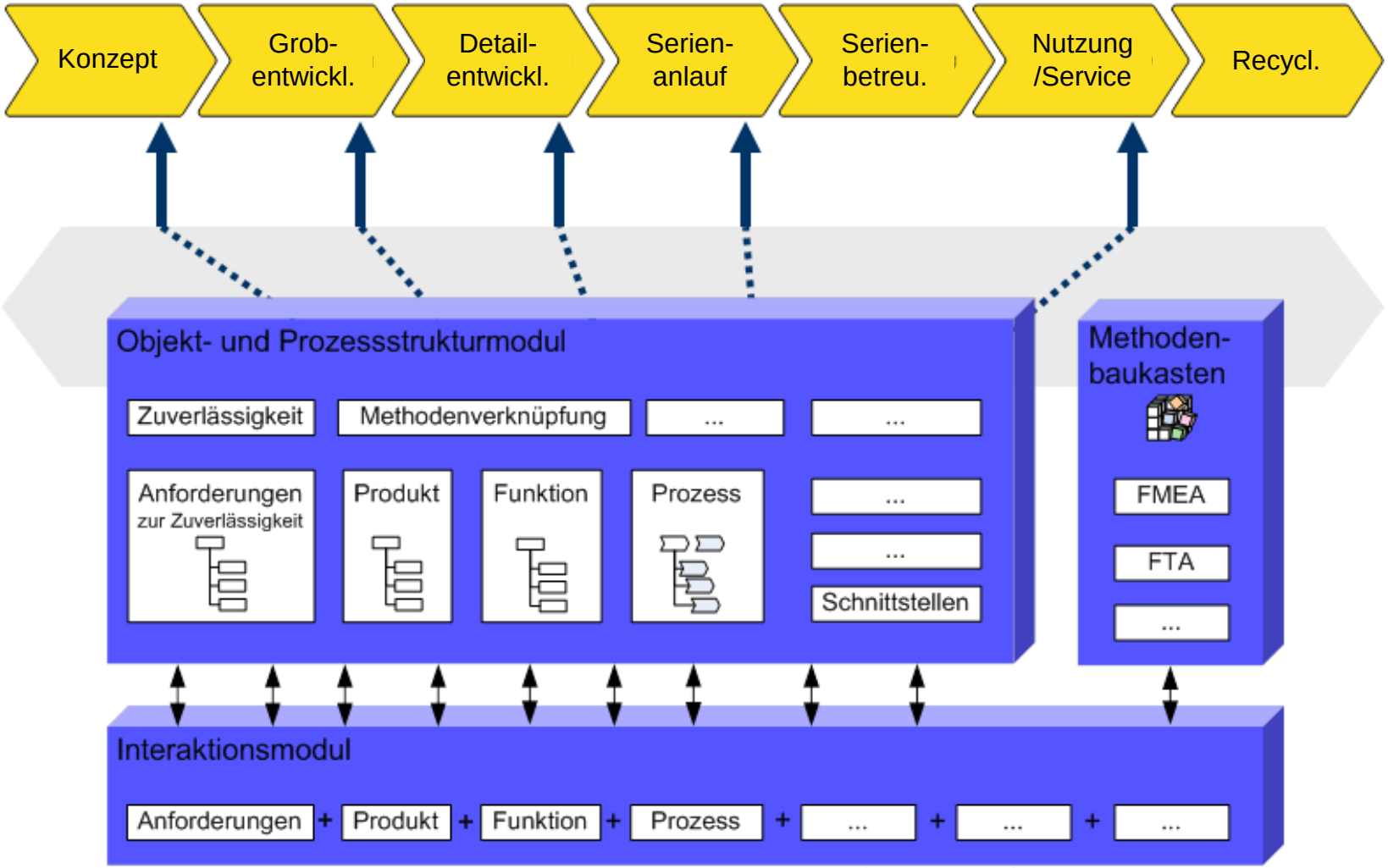
Zu lösende wissenschaftliche Fragestellungen:

- Wie sind die sicherheitsrelevanten Begriffe so zu vereinheitlichen, dass sie die Ingenieure fachdisziplinübergreifend bei PLC[1]-bezogenen Problemlösungen verstehen sowie umsetzen können?

- Wie können die verschiedensten Methoden zur Gewährleistung von Verlässlichkeit in die verschiedensten Phasen des PLC integriert werden?

[1]PLC=Product Life Cycle

These 1: Überwindung der Vielfalt



Quelle: Müller N., Winzer P. (2007) Vortrag Vorstellung Verbundprojekt PromeSys. VDI. Kaiserslautern

These 2: Integration von Safety und Security

Safety- und Security-Aspekte sind bei der Entwicklung technischer wie auch soziotechnischer Systeme integriert zu betrachten, um die Gemeinsamkeiten sowie die Wechselwirkungen beider z.Zt. isolierten Sichten zu erschließen und zu nutzen.

Daher ist eine Brücke zwischen Safety und Security zu entwickeln.

Problemlage:

- Trennung von Safety und Security

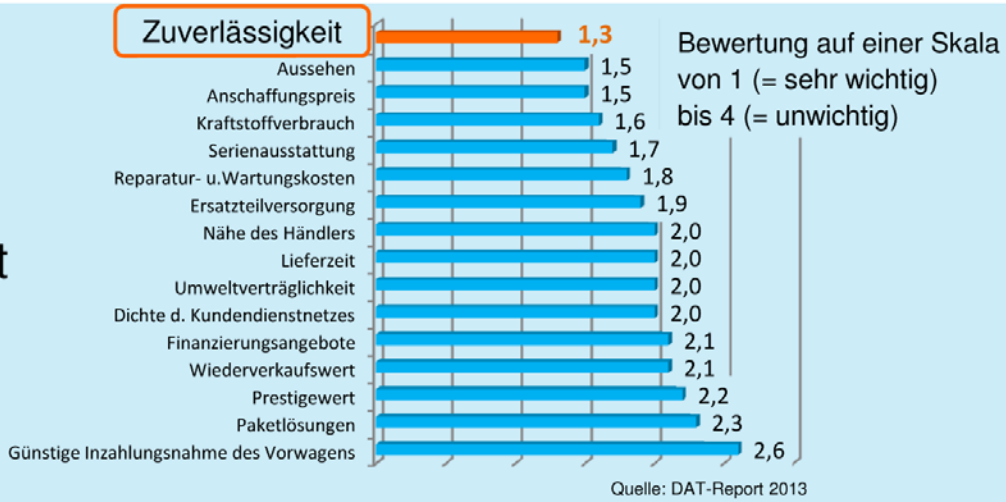
Wissenschaftliche Fragestellung:

- Ist eine synergetische Betrachtung und Beseitigung von Zielkonflikten möglich?

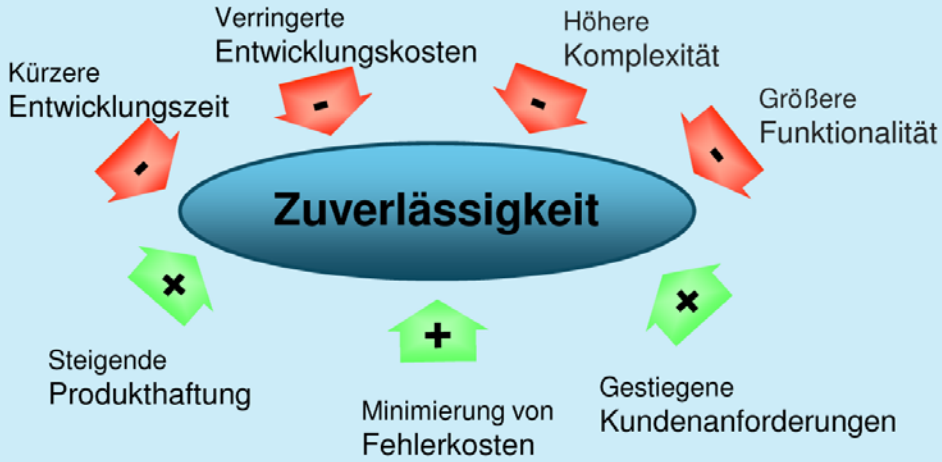
Lösungsansatz: Symbiose, abstrahierende Verdichtung

Bedeutung der Zuverlässigkeit

- Zuverlässigkeit ist eines der wichtigsten Kriterien
- Nahezu jeder Kunde ist mit Unzuverlässigkeit konfrontiert



- Viele Faktoren in der Produktentwicklung wirken unmittelbar auf die Zuverlässigkeit



Quelle: Bernd Bertsche: Ähnlichkeiten und Unterschiede zwischen Sicherheit und Zuverlässigkeit. Vortrag. 26. VDI-Fachtagung Technische Zuverlässigkeit 2013 Produkt- und Prozessgestaltung. 23./24. April 2013, Leonberg bei Stuttgart.

Keine Brücke zwischen Safety und Security

PLC des Materials

Safety-anforderungen

Security-anforderungen

an das Material

….

Produkt-entwicklung

Produktion

Nutzung

….

Safety-anforderungen

Security-anforderungen

an das Design

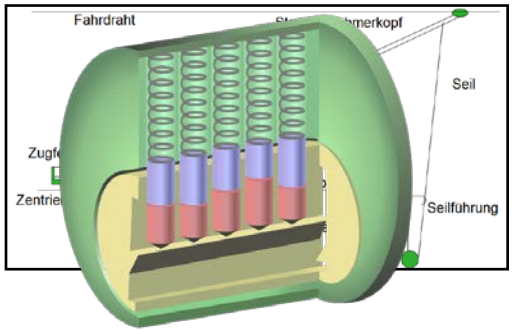
Safety-anforderungen

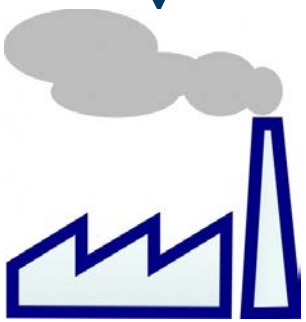
Security-anforderungen

Safety-anforderungen

Security-anforderungen

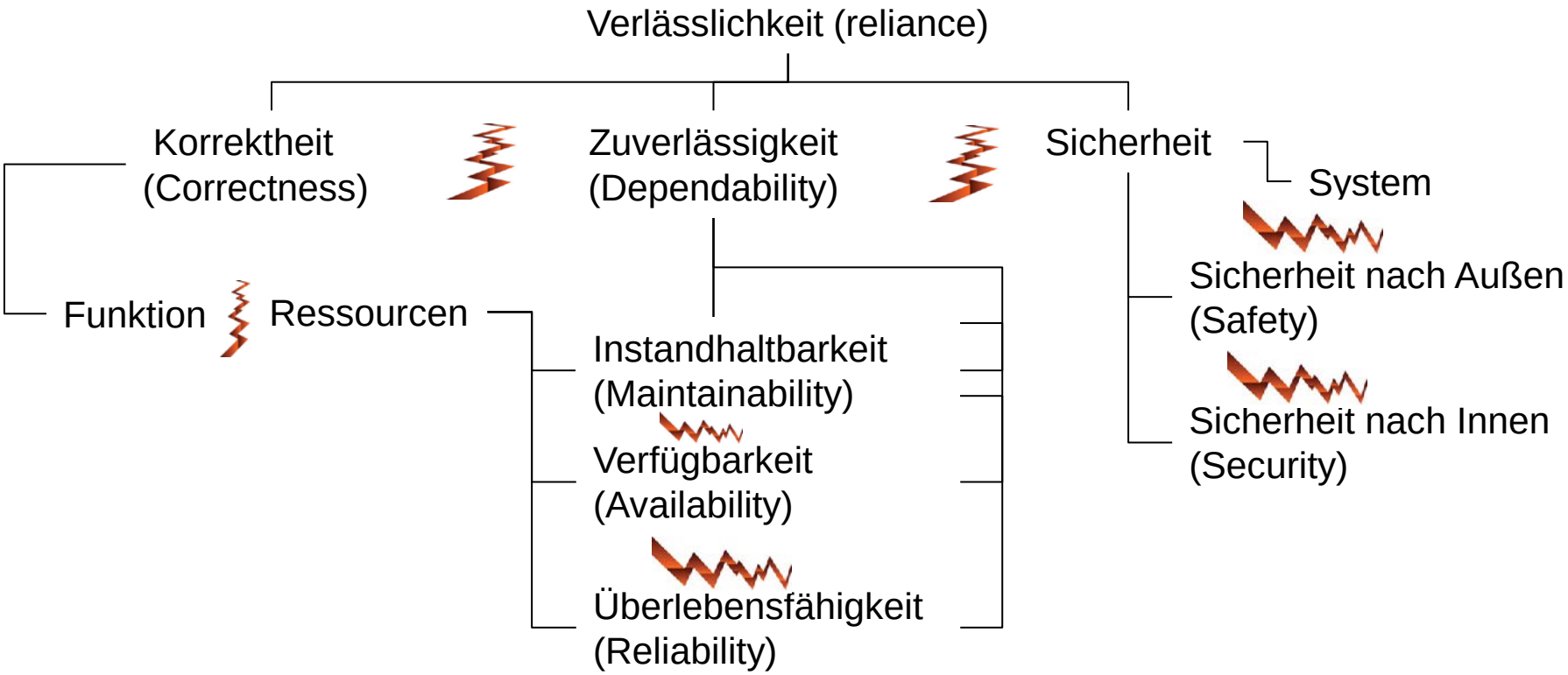
an die Nutzung





Quelle: In Anlehnung an Workshop …. Zur 3.Innosecure-kongress am 22.-24.04.2015

Klassifikationsmöglichkeiten von Begriffen fehlen



Quelle: in Anlehnung an Schnieder, Eckehard: Ähnlichkeiten und Unterschiede zwischen Sicherheit und Zuverlässigkeit. 26. VDI-Fachtagung Technische Zuverlässigkeit 2013

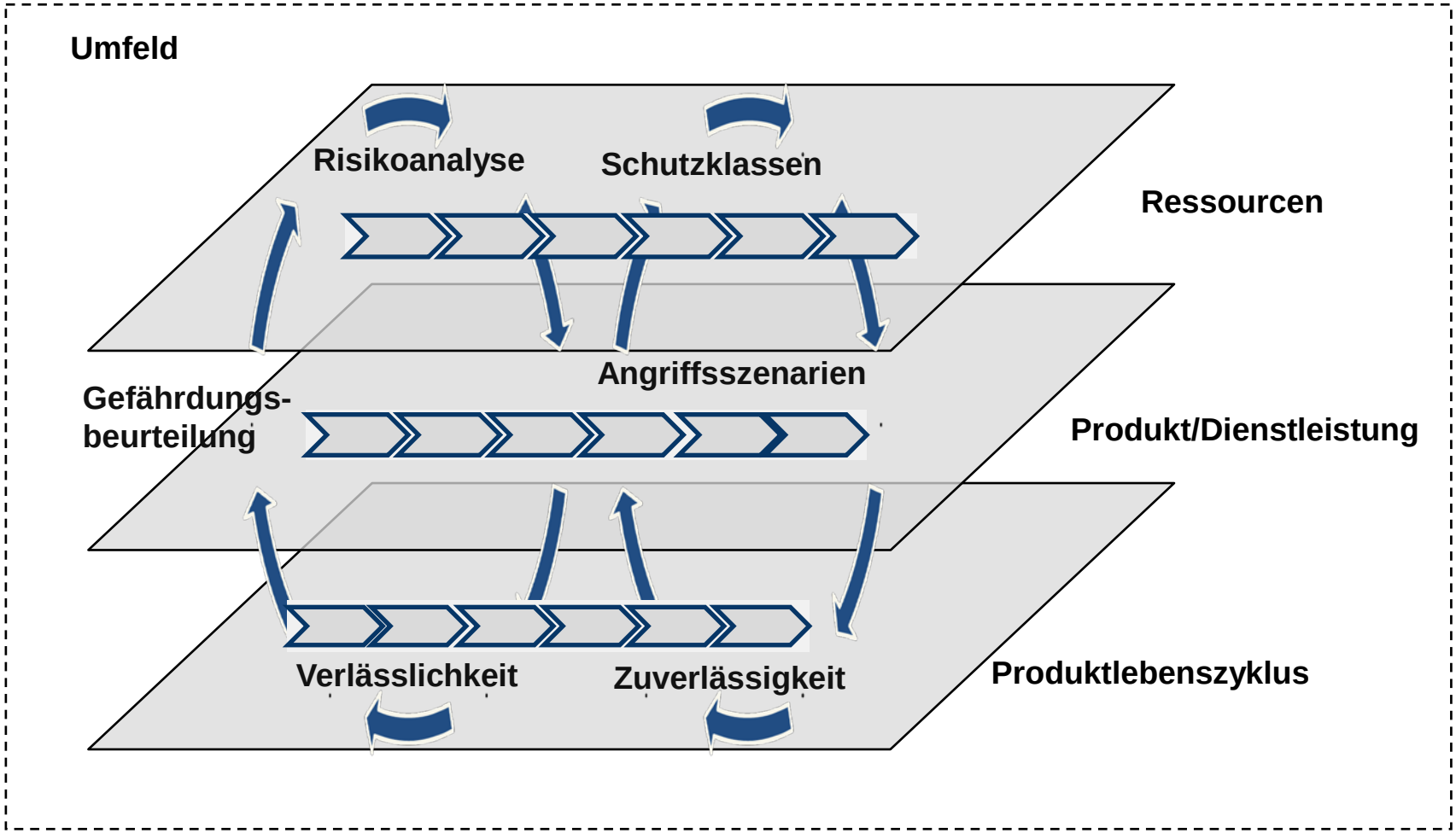
Zu lösende wissenschaftliche Fragestellungen:

- Kann eine Brücke zwischen Safety- und Security- Ansätzen in den PLC-Phasen durch ein Re-Design des Systems Engineering geschaffen werden?

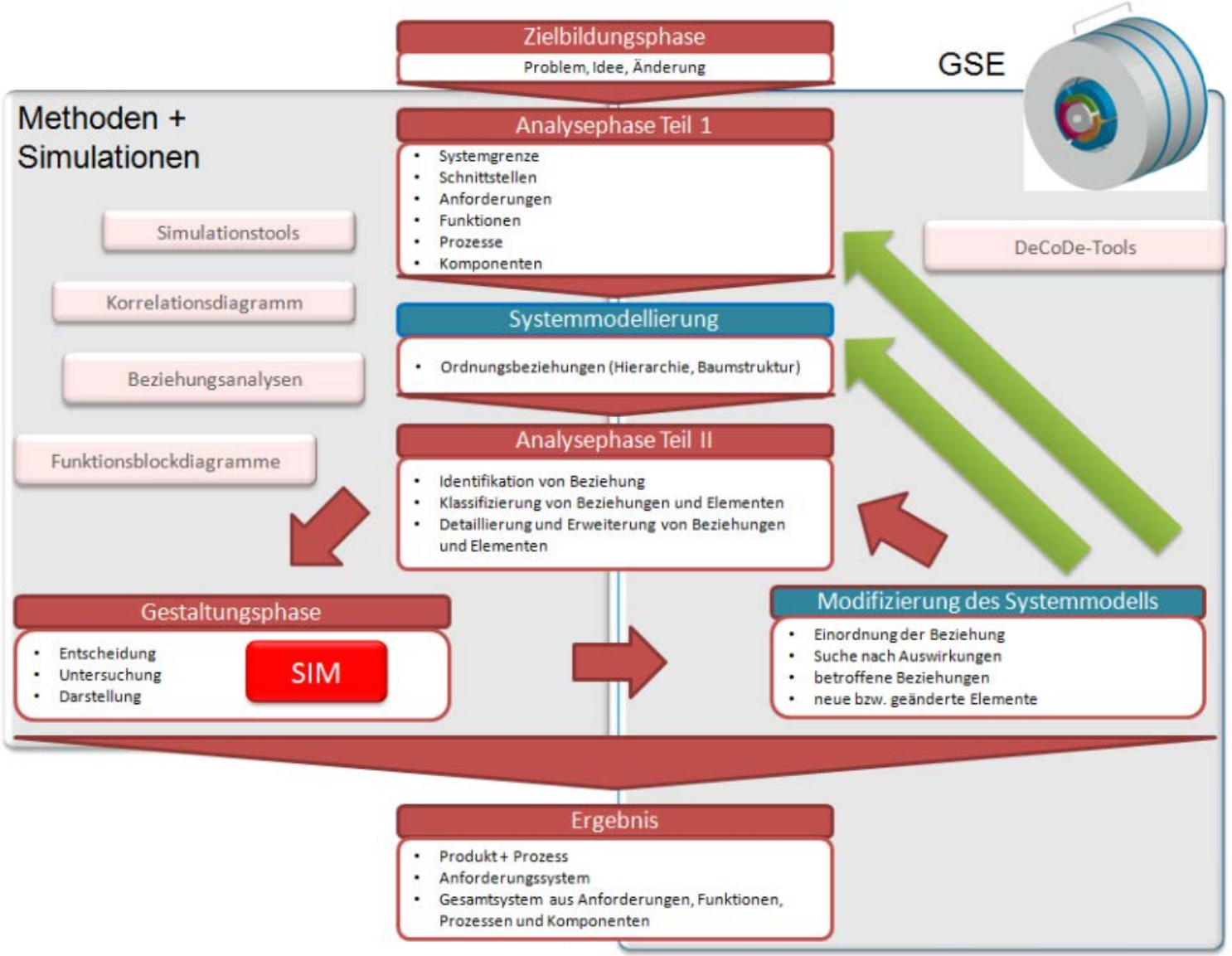
- Wie können sicherheitsrelevante Daten über den PLC gesammelt und für Sicherheitsprognosen in den frühen Phasen der Produktentwicklung verwendet werden?

Quellen: Schnieder, Eckehard: Ähnlichkeiten und Unterschiede zwischen Sicherheit und Zuverlässigkeit. 26. VDI-Fachtagung Technische Zuverlässigkeit 2013.
Berres, Axel, Schumann, Holger: Closing the safety process gap: Early integration of safety assessment methods into system engineering, in: Maurer, Maik, Schulze, Sven-Olaf (Hrsg):: Tag des Systems Engineering, Hanser, 2014.

These 2: Integration von Safety und Security

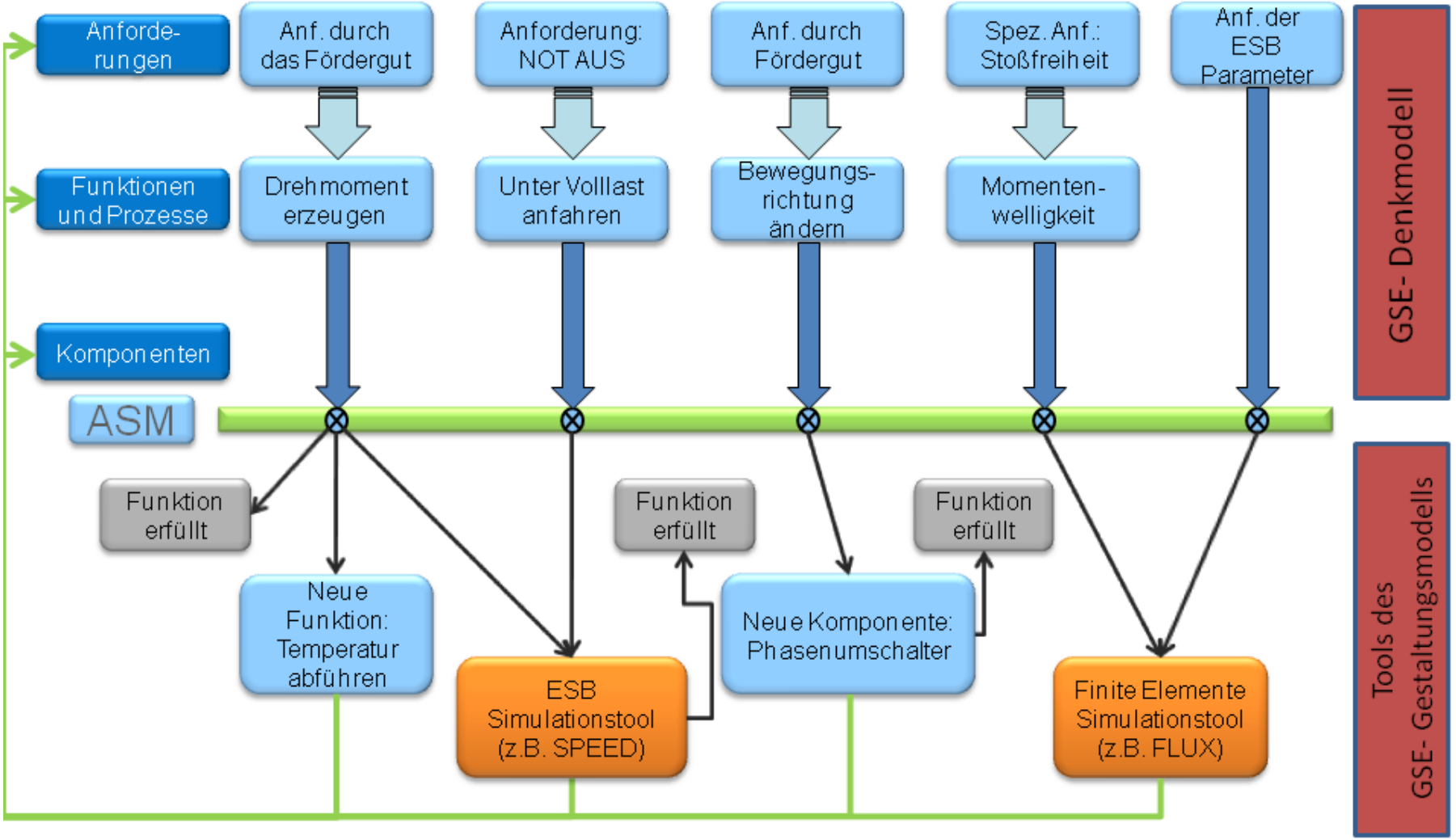


These 2: Integration von Safety und Security



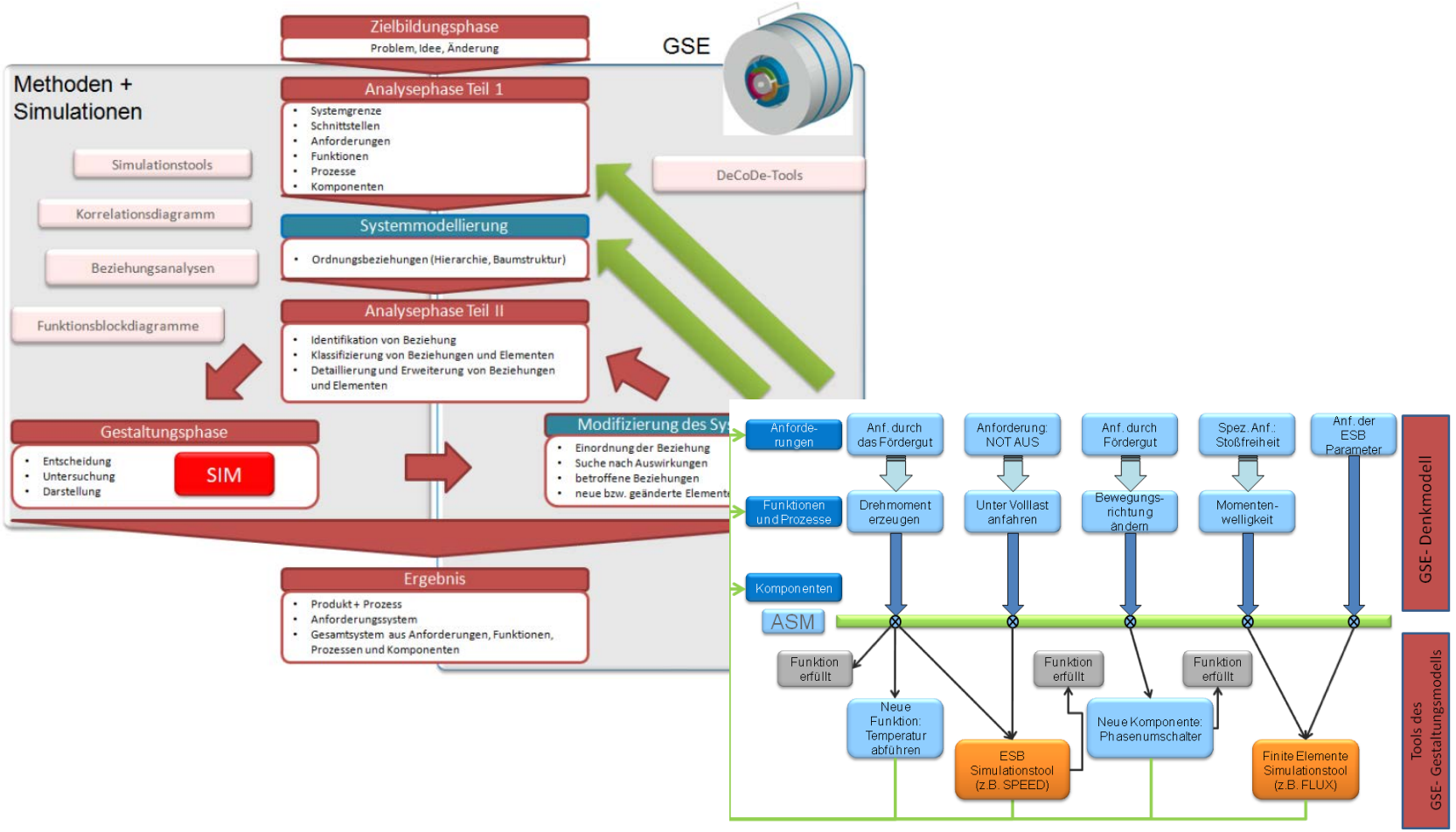
Quelle: Winzer, P.: Generic Systems Engineering - Ein methodischer Ansatz zur Komplexitätsbewältigung. Springer Vieweg Verlag 2013.

These 2: Integration von Safety und Security



Quelle: Winzer, P.: Generic Systems Engineering - Ein methodischer Ansatz zur Komplexitätsbewältigung. Springer Vieweg Verlag 2013

These 2: Integration von Safety und Security



Quelle: Winzer, P.: Generic Systems Engineering - Ein methodischer Ansatz zur Komplexitätsbewältigung. Springer Vieweg Verlag 2013

These 3: Kommunikation und Begriffsbildung (Terminologie)

Eine fachdisziplinübergreifende Sicherheitsforschung und -technologie erfordert eine gemeinsame Kommunikationsbasis mit harmonisierten Begriffen, Terminologien und Kommunikationsprozessen der menschlichen und organisatorischen Akteure.

Problemlage:

- Missverständnisse

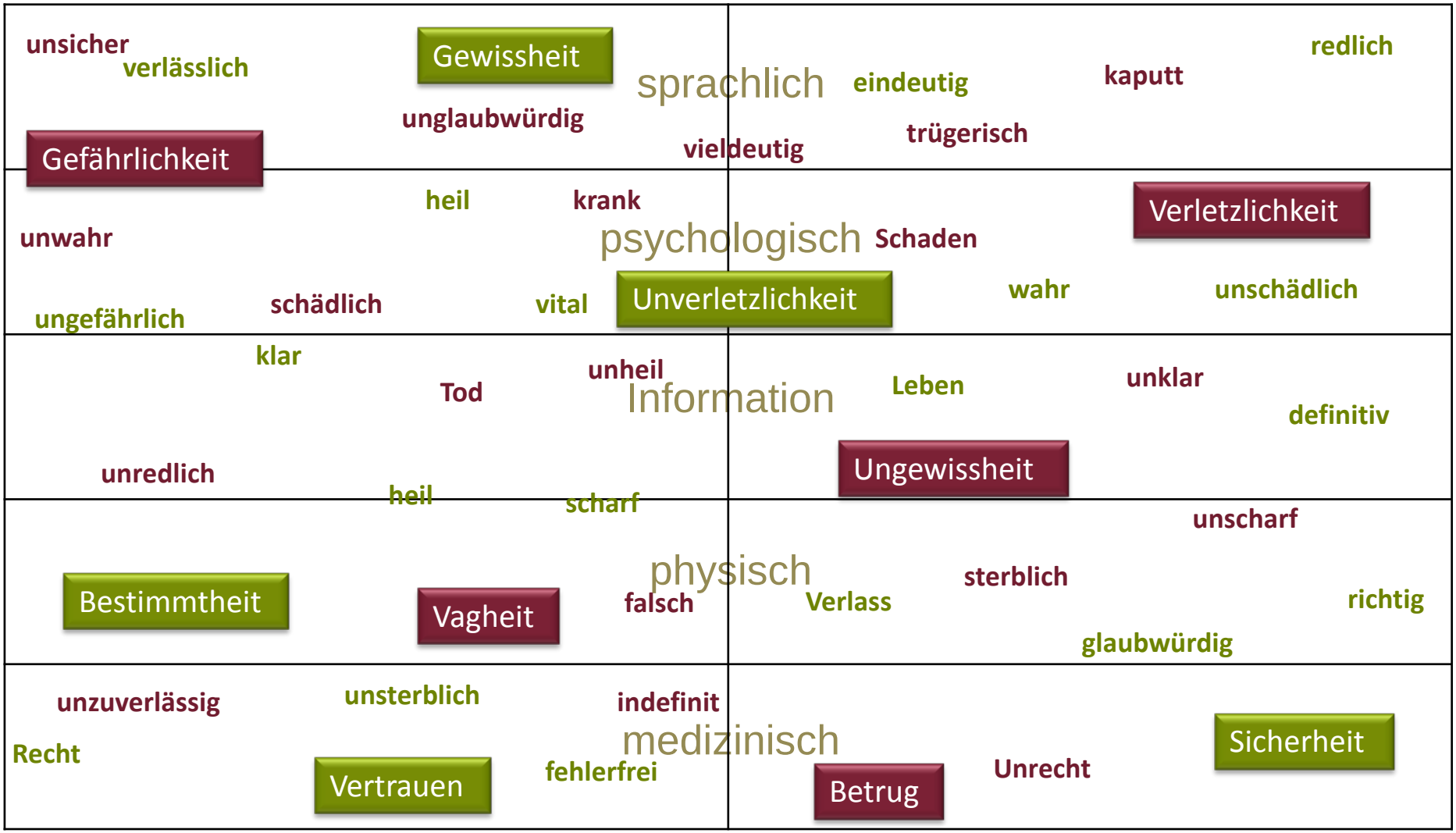
Wissenschaftliche Fragestellung:

- Wie ist ein formalisiertes und konsolidiertes Begriffsgebäude zu schaffen?

Lösungsansatz: harmonisierte Terminologie

These 3: Kommunikation und Begriffsbildung (Terminologie)

Sicherheit in Definitionen und Normen - **Sicherheit im Sprachgebrauch**



These 3: Kommunikation und Begriffsbildung (Terminologie)

Sicherheit in Definitionen und Normen – **DIN Term Extraktion und Analyse mit iglos**

Begriff	Generelle Nennung	Spezifische Definition
Sicherheit (safety)	2453	63
Gefährdung (hazard)	335	118
Gefahr (danger)	291	21
Risiko (risk)	496	130

These 3: Kommunikation und Begriffsbildung (Terminologie)

Sicherheit in Definitionen und Normen

Identisch Definition zu DIN 820-120

Risiko												
DIN 820-120: 2008	Kombi-nation	der			Wahr-scheinlichkeit	eines	Schadens-eintritts	und	seines	Schadensausmaß		
DIN EN 61508-4: 2009												
DIN EN 50126: 2001												
DIN EN 50128: 2001												
DIN EN 50129: 2003												
ISO CD 26262: 2008												
DIN EN 61511: 2005												
DIN EN ISO 12100-1:2004	Kombi-nation	der			Wahr-scheinlichkeit	des	Auftretens eines Schadens	und	seines	Schadensausmaß		
DIN EN ISO 14971:2007												
DIN EN ISO 14121:2007	Kombi-nation	der			Wahr-scheinlichkeit	des	Eintritts eines Schadens	und	seines	Schadensausmaß		

These 3: Kommunikation und Begriffsbildung (Terminologie)

Sicherheit in Definitionen und Normen

Synonym zu Definition DIN 820-120

Risiko												
DIN 820-120: 2008	Kombi-nation	der			Wahr-scheinlichkeit	eines	Schadens-eintritts	und	seines	Schadensausmaß		
DIN EN 61508-4: 2009	Kombi-nation	aus der			Wahr-scheinlichkeit	mit der ein	Schaden auftritt	und	dem	Ausmaß	dieses	Schadens
DIN EN 50126: 2001												
DIN EN 50128: 2001												
DIN EN 50129: 2003	Combi-nation	of the		freq uenc y	or probability	and	the consecence	of	a	sepcific		hazardous event
ISO CD 26262: 2008	Combi-nation	of the			probability	of	occurance of harm	and	the	severity	of that	harm
DIN EN 61511: 2005	Kombi-nation	der			Wahr-scheinlichkeit	des	Auftretens eines Schadens	und	des	Schwere-grad	dieses	Schadens
DIN EN ISO 12100-1:2004	Kombi-nation	der			Wahrschein-lichkeit	des	Eintritts eines Schadens	und	seines	Schadensausmaßes		
DIN EN ISO 14971:2007	Kombi-nation	der			Wahr-scheinlichkeit	des	Eintritts eines Schadens	und	des	Schwere-grades	dieses	Schadens

These 3: Kommunikation und Begriffsbildung (Terminologie)

Risikobegriff - Starke Abweichung zur Definition aus DIN 820-120

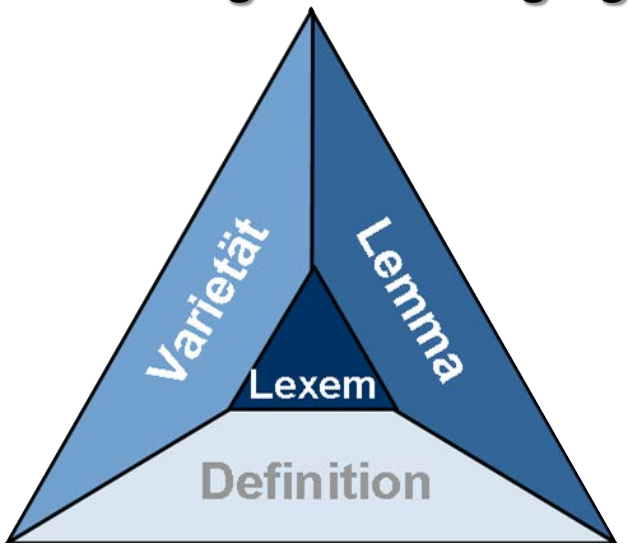
Risiko												
DIN 820-120: 2008	Kombi-nation	der			Wahr-scheinlichkeit	eines	Schadens-eintritt	und	seines	Schadensausmaß		
DIN EN 61508-4: 2009												
DIN EN 50126: 2001												
DIN EN 50128: 2001	Kombi-nation	der	Häufig-keit	oder	Wahr-scheinlichkeit			mit	den	Auswir-kungen	eines	spezifizier-ten gefährlichen Ereignisses
DIN EN 50129: 2003	Kombi-nation	aus	Häufig-keit	oder	Wahr-scheinlichkeit			und	den	Folgen	eines	spezifizier-ten gefährlichen Ereignisses
ISO CD 26262: 2008												
DIN EN 61511: 2005												
DIN EN ISO 12100-1:2004												
DIN EN ISO 14971:2007												
DIN EN ISO 14121:2007												
DIN EN ISO 14738:2004	--	--	--	--	--	--	--	--	--	--	--	--

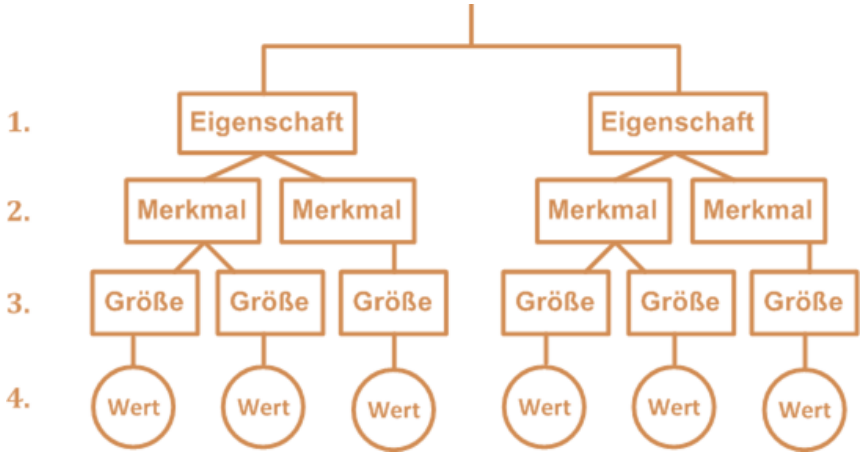
These 3: Kommunikation und Begriffsbildung (Terminologie)

Risiko												
DIN 820-120: 2008												
DIN EN 61508-4: 2009												
DIN EN 50126: 2001		Die			Wahr-scheinlichkeit	des	Auftretens einer Gefahr, die einen Schaden verursacht	sowie	der	Schwere-grad	eines	Schadens
DIN EN 50128: 2001	Kombi-nation	der	Häufig-keit	oder	Wahr-scheinlichkeit			mit	den	Auswir-kungen	eines	spezifizier-ten gefährlichen Ereignisses
DIN EN 50129: 2003	Kombi-nation	aus	Häufig-keit	oder	Wahr-scheinlichkeit			und	den	Folgen	eines	spezifizier-ten gefährlichen Ereignisses
ISO CD 26262: 2008												
DIN EN 61511: 2005												
DIN EN ISO 12100-1:2004												
DIN EN ISO 14971:2007												
DIN EN ISO 14121:2007												
DIN EN ISO 14738:2004	--	--	--	--	--	--	--	--	--	--	--	--

Widersprüche innerhalb einer Normenreihe

Formalisierte Begriffsbildung: iglos-Zeichenmodell und Attributhierarchie





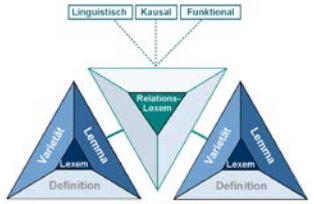
Attributhierarchie

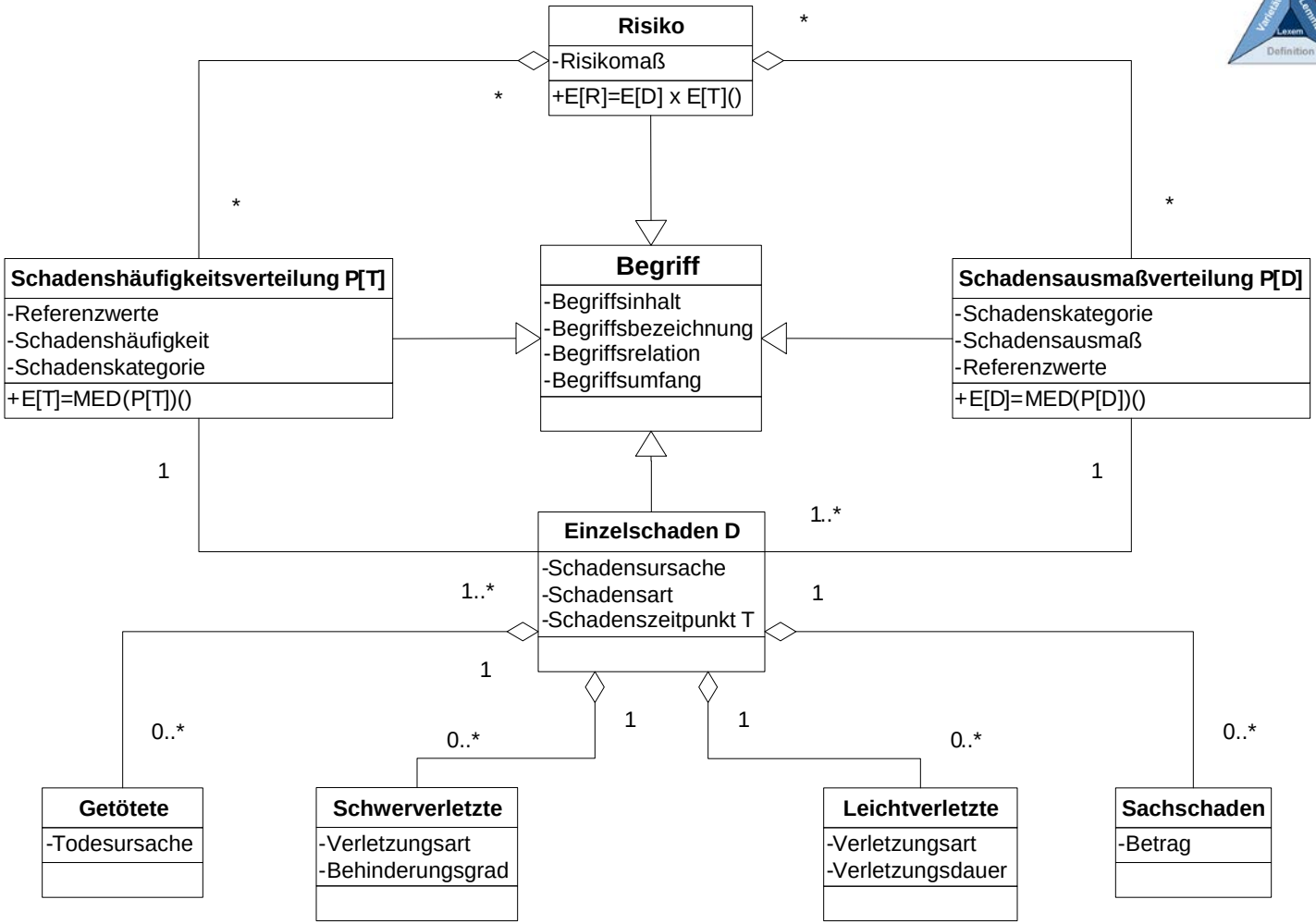
Ein Lexem (Begriff) besteht aus drei Konstituenten:

- **Lemma**: Die Benennung, eine Lautfolge oder Buchstabenfolge
- **Definition**: Die sprachlich gefasste Umschreibung der mentalen Einheit des Begriffs
- **Varietät**: Die fachsprachliche Domäne bzw. der fachliche Kontext, in dem das Lexem verwendet wird

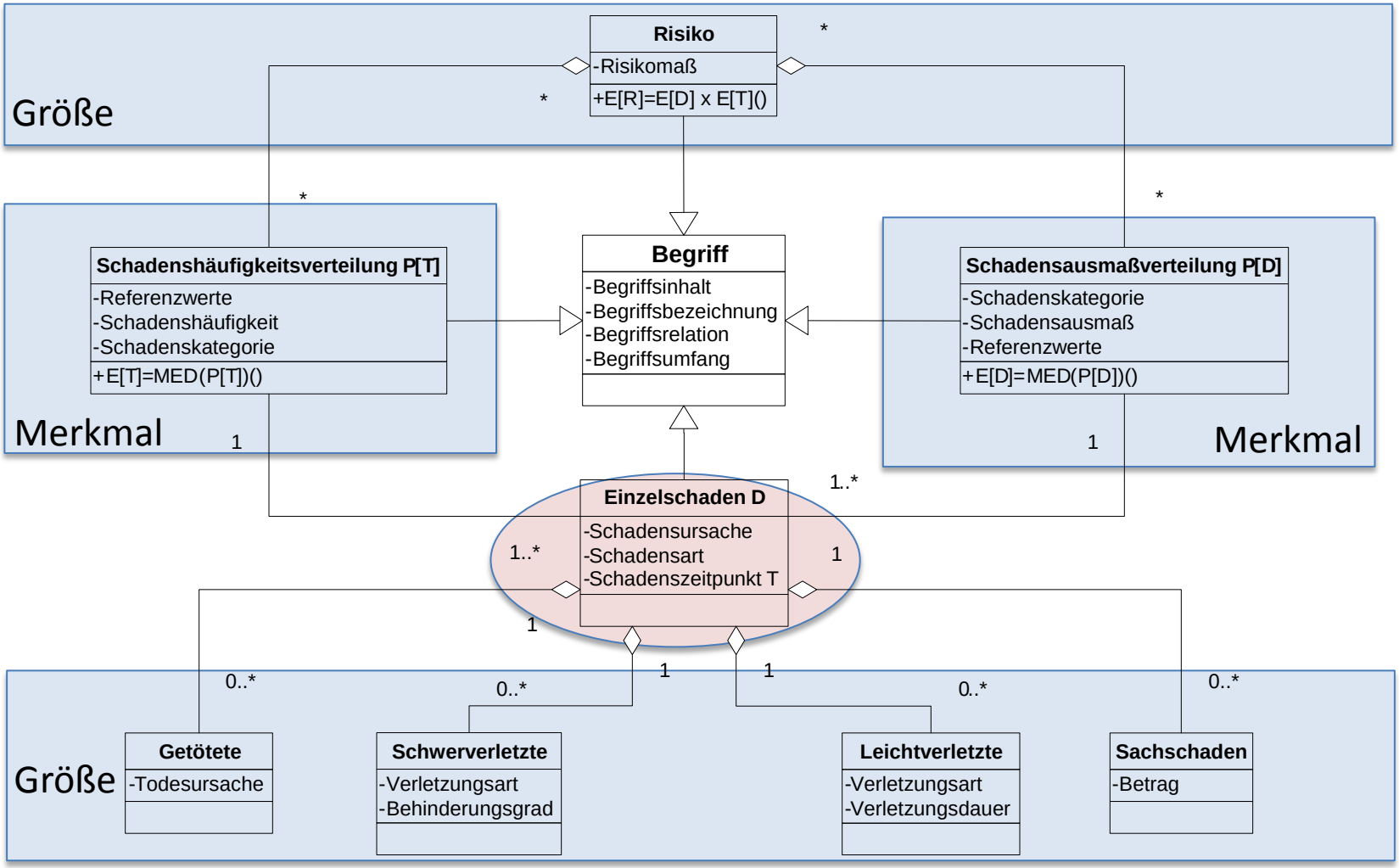
DIN 4002-4: (2013-09)
Merkmale und Geltungsbereiche zum Produktdatenaustausch - Teil 4: Terminologieregeln für Attribute für Strukturelemente
Verfahren zur Erarbeitung und Normung von Strukturelementen, kompatibel zu den internationalen Dokumentenreihen ISO/IEC Guide-77, ISO 13584, IEC 61360, ISO 29002,

Klassendiagramm zum Risikobegriff

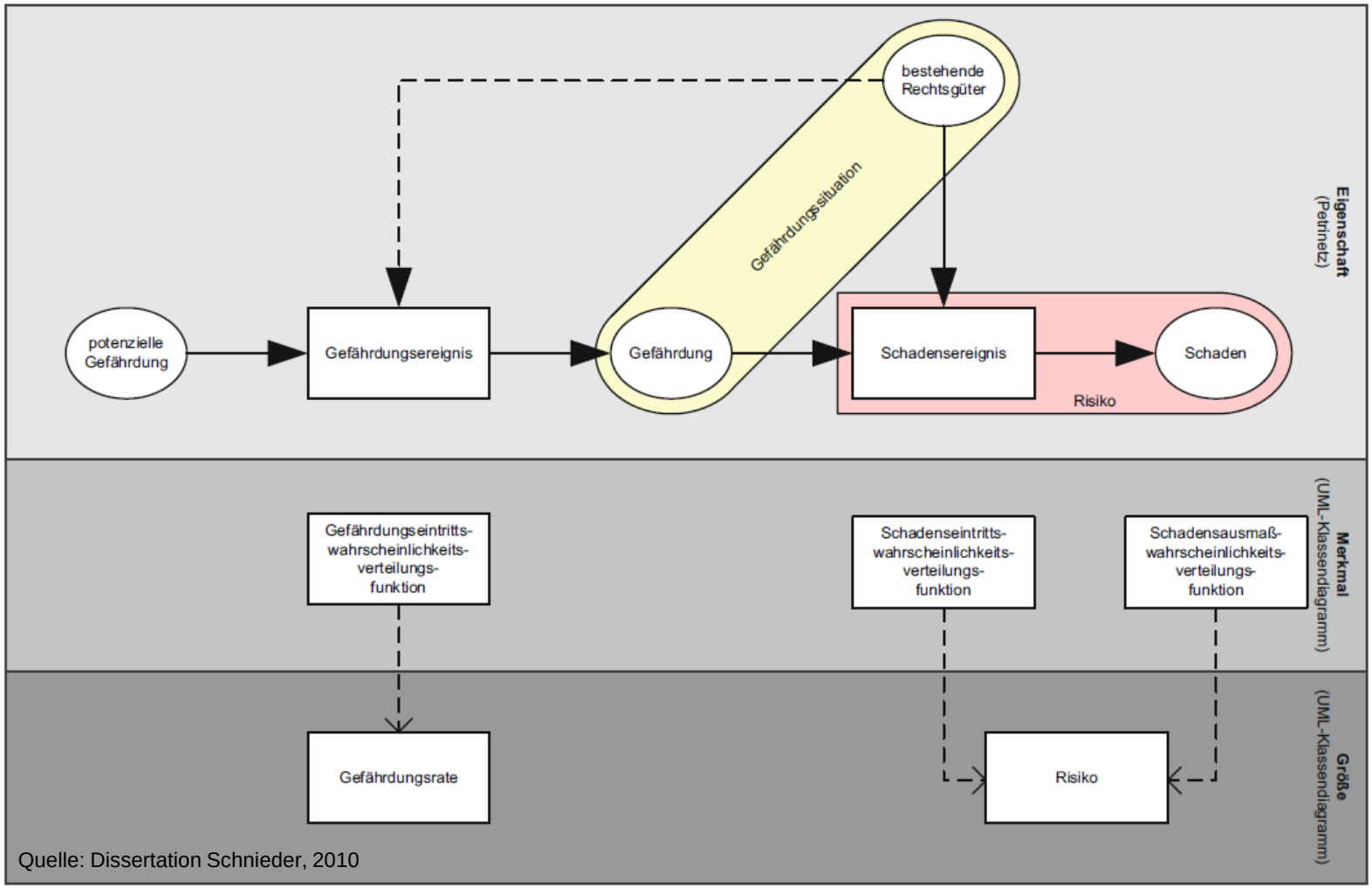




Klassendiagramm zum Risikobegriff

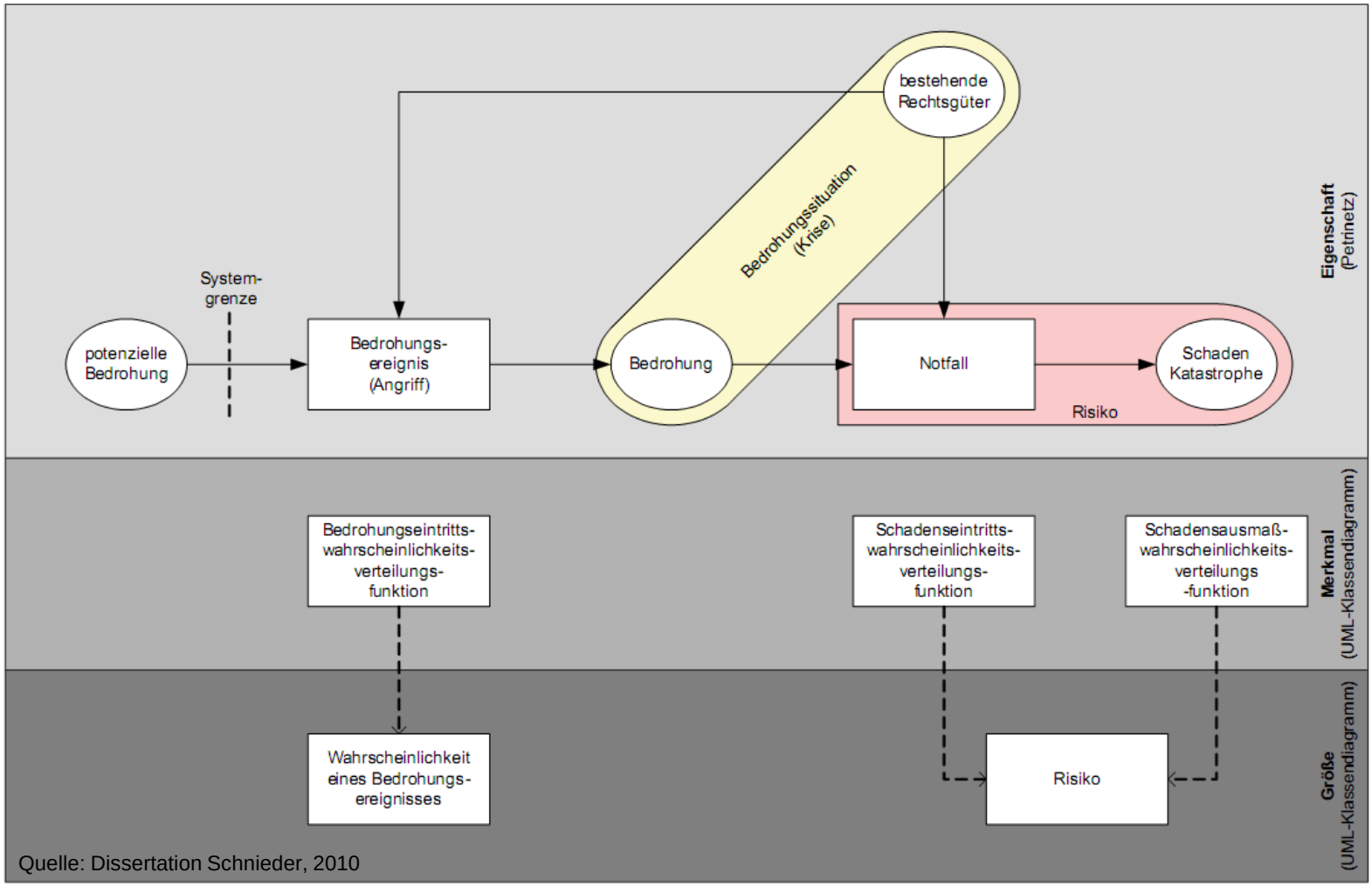


Risikogenesemodell (safety)
Formalisiertes Modell der Risikogenese – Safety (nach DIN-Fachbericht 144)



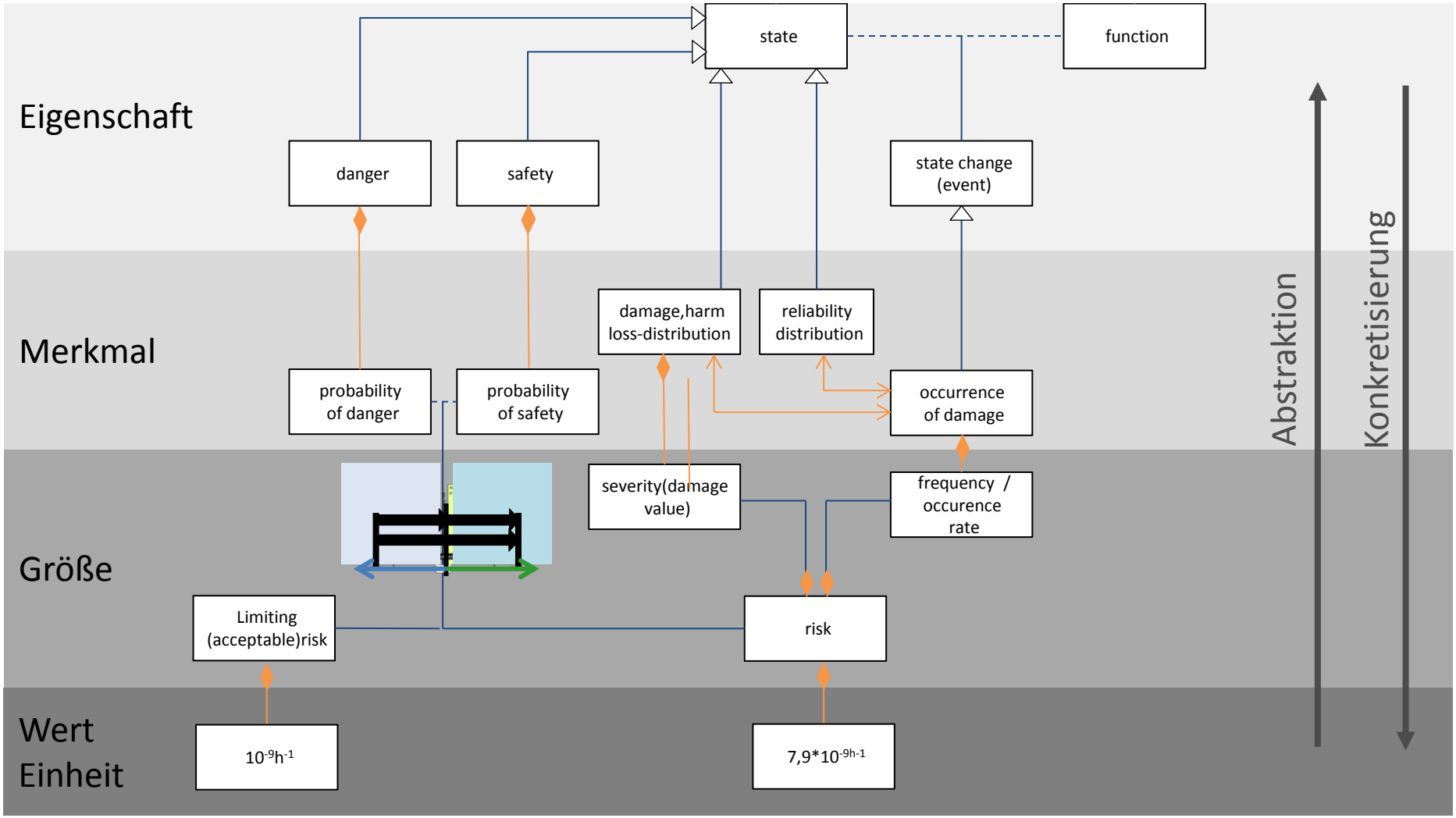
Quelle: Dissertation Schnieder, 2010

Risikogenesemodell (security)
Formalisiertes Modell der Risikogenese – Security (nach DIN-Fachbericht 144)



Quelle: Dissertation Schnieder, 2010

Definition von Sicherheitstermini durch Relationierung



These 4: Sicherheit ist eine emergente Verhaltenseigenschaft

Sicherheit ist als emergente Verhaltenseigenschaft komplexer Systeme modellierbar. Die zunehmende Komplexität von technischen wie auch soziotechnischen Systemen erfordert eine systemische Betrachtung auf deren Basis abstrahierte Modelle für die Sicherheit bzw. Verlässlichkeit dieser Systeme gebildet werden können. Somit ist eine Systemtheorie der Verlässlichkeit bzw. des erweiterten Sicherheitsverständnisses zu erarbeiten.

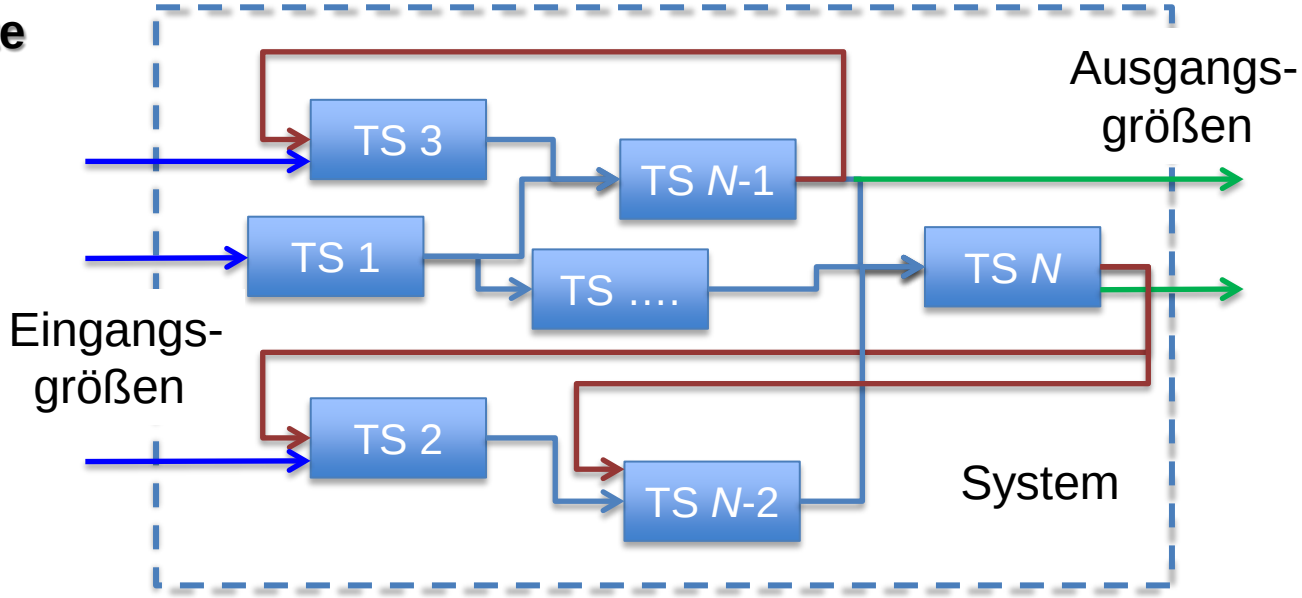
Problemlage:
Theoretische Fundierung

Wissenschaftliche Fragestellung:
- Kalkül zur Beschreibung, Analyse und Inferenz im Kontext Verlässlichkeit?

Lösungsansatz: Fachdisziplinübergreifende Modellierung

These 4: Sicherheit ist eine emergente Verhaltenseigenschaft

Sicherheit als emergente Systemeigenschaft



System = Hardware • Software • Orgware • Personal

System = TS 1 ∪ TS 2 ∪.... ∪ TS *N*-1 ∪ TS *N*

System: Rückkopplungen, Nichtlinearitäten, Stochastizitäten, Irrationalitäten, Komplexität

$$(\forall TS: Sicher(TS)) \overset{?}{\Leftrightarrow} Sicher(System)$$

Wie lässt sich von sicheren Teilsystemen auf sichere Systeme schließen?

Wie bricht man die Sicherheit eines Systems auf Teilsysteme und deren strukturelle Verknüpfung herunter?

Spieltheoretische Sicht auf Safety und Security

„Safety“ »Spiel gegen den Zufall«

→ Stochastisch eintretende Schadensereignisse

→ Statistische Analyse der Gefährdung

→ Passive Maßnahmen reichen oft aus

→ Bayes‘sche Modellierung systematischer Effekte

„Security“ »Spiel gegen die Absicht«

→ Gegner entzieht sich dem Verstandenwerden, handelt taktisch

→ Aktive, adaptive und lernende Prozesse sind notwendig

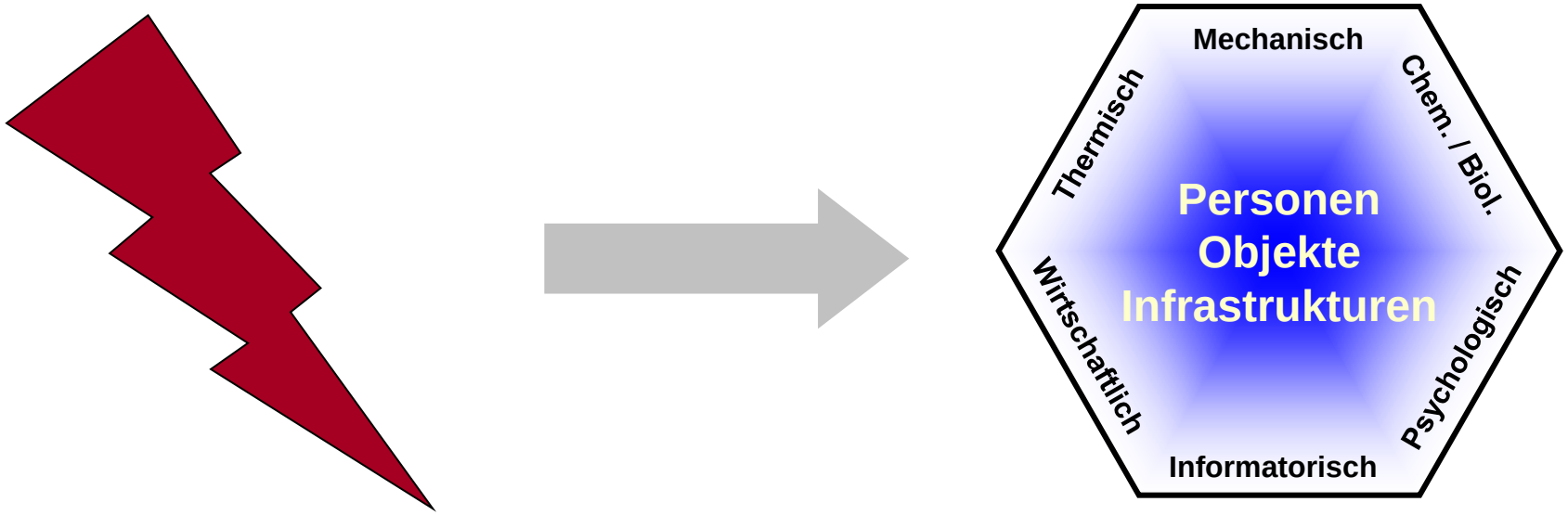
Gewährleistung von Security ist ein dynamischer Prozess!
→ Schutzprozesse werden Regelkreise.

Stufen der Gefahrenentfaltung und Flanken der Verwundbarkeit

Gefahrenquelle, Gefährder

Übertragungsweg

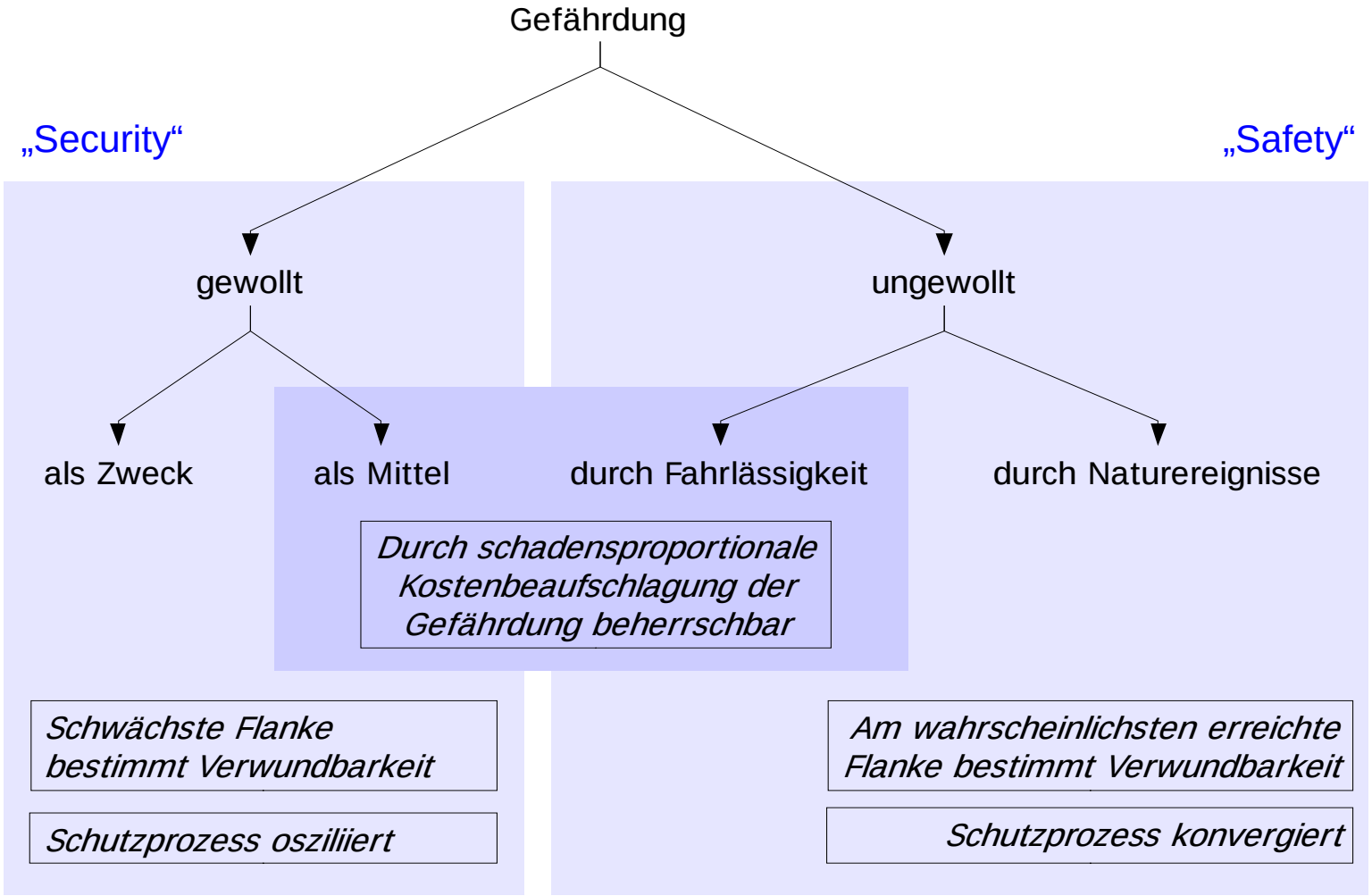
Gefahrensenke, Schutzbedürftiger



Flanken der Verwundbarkeit

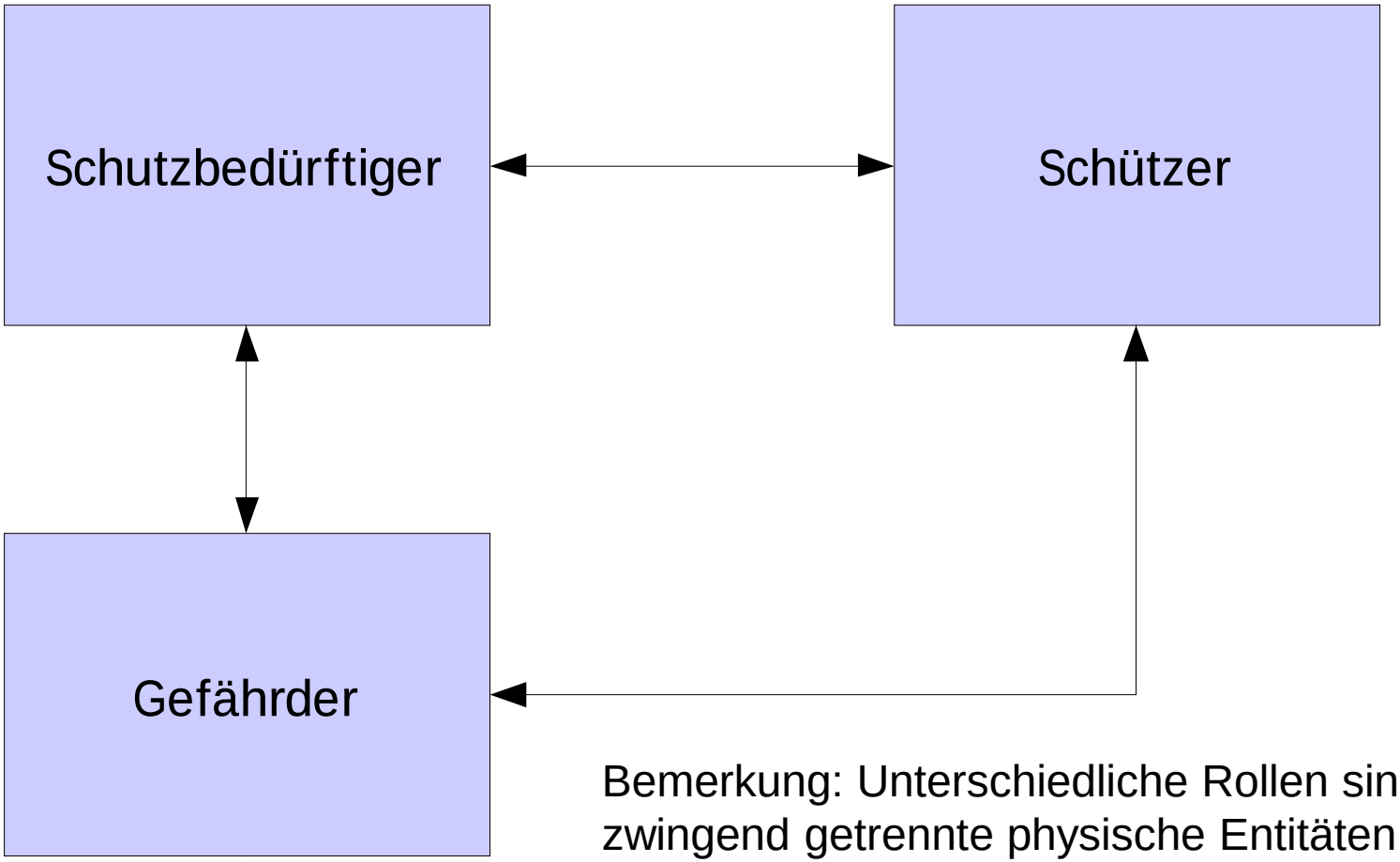
Minimalprinzip der Security:
Die schwächste Flanke ist bestimmend für die Verwundbarkeit.

Aufschlüsselung der Gefährdung



Quelle: Beyerer, J.; Geisler, J.; Dahlem, A.; Winzer, P.: Sicherhehit: Systemanalyse und –design. In: Winzer, P.; Schnieder, E.; Bach, F-W. (Hrsg.): acatech DISKUTIERT – Sicherheitsforschung – Chancen und Perspektiven, Springer, 2010, S. 39-72.

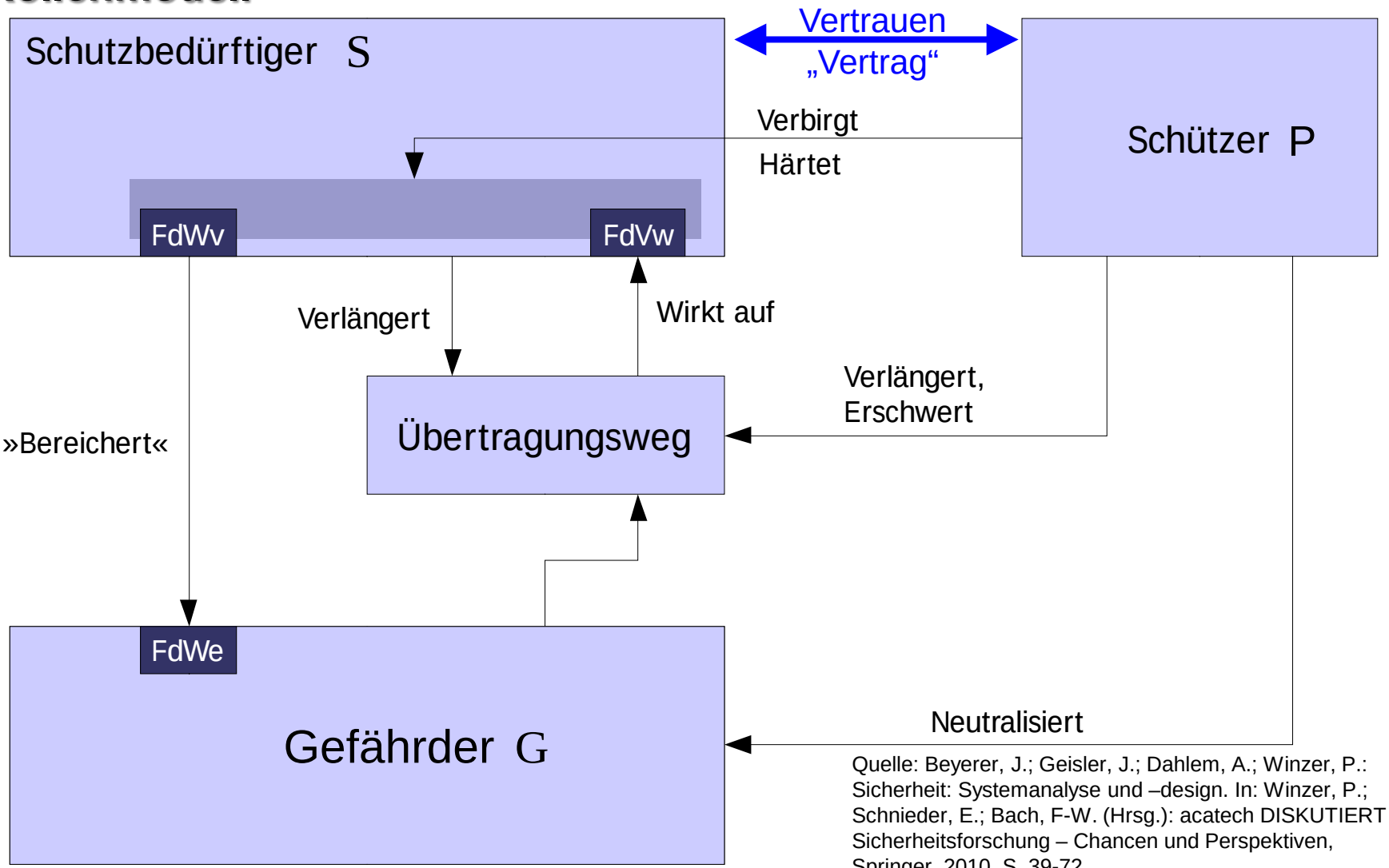
Rollenmodell



Bemerkung: Unterschiedliche Rollen sind nicht zwingend getrennte physische Entitäten.

Quelle: Beyerer, J.; Geisler, J.; Dahlem, A.; Winzer, P.: Sicherheit: Systemanalyse und –design. In: Winzer, P.; Schnieder, E.; Bach, F-W. (Hrsg.): acatech DISKUTIERT – Sicherheitsforschung – Chancen und Perspektiven, Springer, 2010, S. 39-72.

Rollenmodell



Quelle: Beyerer, J.; Geisler, J.; Dahlem, A.; Winzer, P.: Sicherheit: Systemanalyse und –design. In: Winzer, P.; Schnieder, E.; Bach, F-W. (Hrsg.): acatech DISKUTIERT – Sicherheitsforschung – Chancen und Perspektiven, Springer, 2010, S. 39-72.

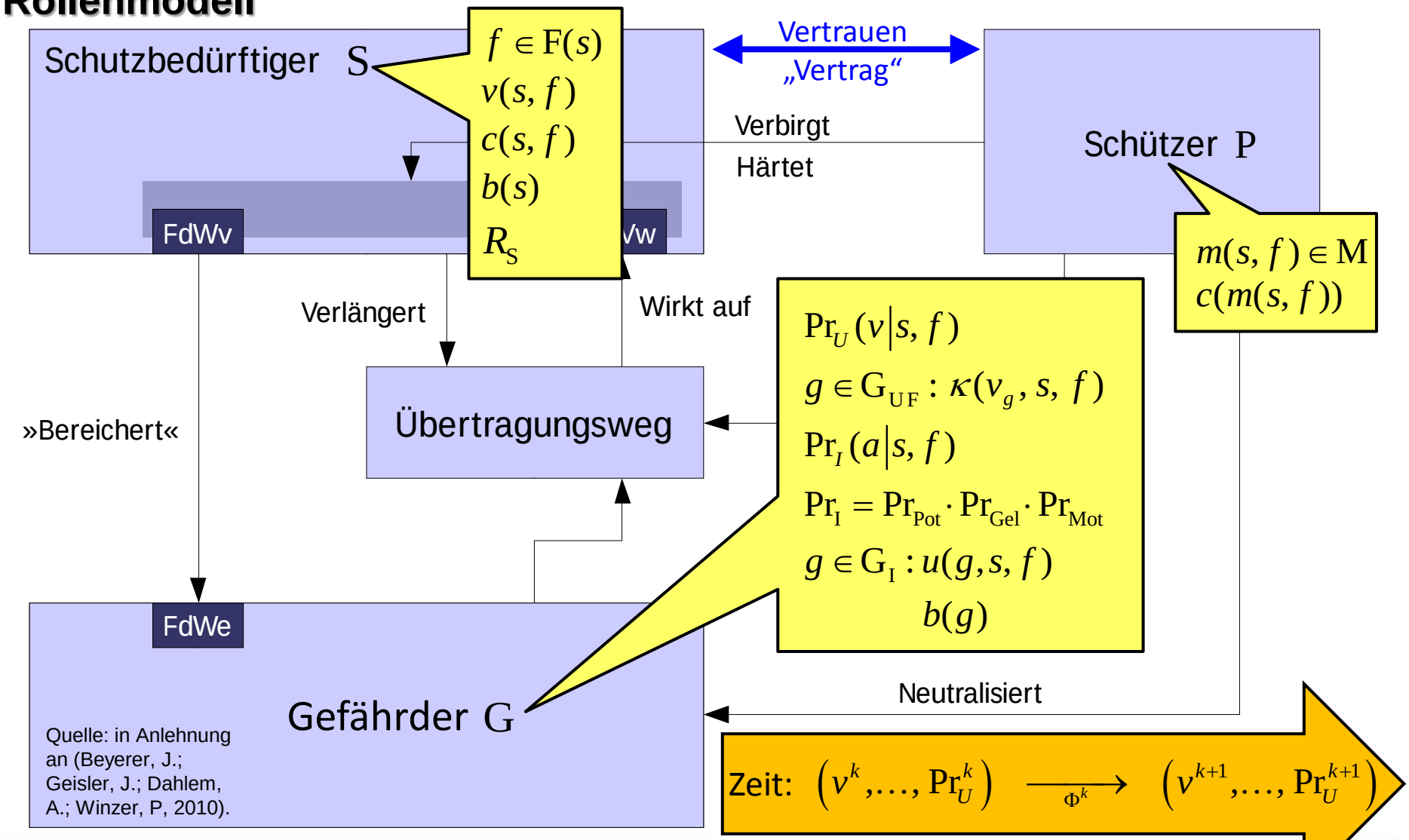
These 4: Sicherheit ist eine emergente Verhaltenseigenschaft

Modellgröße	Bedeutung
$S = S_{Personen} \cup S_{Objekte} \cup S_{Systeme}$	Menge S der Schutzbedürftigen *s*
$s \mapsto b(s)$ mit $s \in S$	Budget des Schutzbedürftigen
$f \in F(s)$	Flanken der Verwundbarkeit
$v(s, f) = \Pr\left(a \in A^* \middle| a, s, f\right)$	Vulnerabilität
$c(s, f) \in [0, \infty)$	Kosten eines Angriffs/Vorfalls
$g \mapsto b(g)$ mit $g \in G_I$	Budget des Gefährders
A	Menge der Angriffe
A*	Menge der erfolgreichen Angriffe
V	Menge der Vorfälle
V*	Menge der Vorfälle, die Schaden anrichten

These 4: Sicherheit ist eine emergente Verhaltenseigenschaft

Modellgröße	Bedeutung
$\kappa(v_g, s, f) \in [0, \kappa_{g\_\mathrm{Ruin}}]$	Kosten für fahrlässigen Gefährder $g \in \mathrm{G_{UF}}$
$m(s, f) \in \mathrm{M}$	Schutzmaßnahme
M	Menge verfügbarer Schutzmaßnahmen
M^*	Menge implementierter Schutzmaßnahmen
$c(m(s, f))$	Kosten für Schutzmaßnahme
$\sum_{m \in \mathrm{M}^*} c(m(s, f)) \quad \leq \quad b(s)$	Nebenbedingung Budgetbeschränkung
$R_{\mathrm{S\_absolut}} := \underbrace{R_{\mathrm{S}}}_{\text{Modell}} + \underbrace{R_0}_{\text{Nicht modellierbar}}$	Risiko des Schutzbedürftigen
$\Pr_U(v_g \mid s, f)$	Eintrittswahrscheinlichkeit eines Vorfalls
$\Pr_I(a_g \mid s, \tilde{f}) = \Pr_{\mathrm{Pot}} \Pr_{\mathrm{Gel}} \Pr_{\mathrm{Mot}}$	Eintrittswahrscheinlichkeit eines Angriffs
$u(g, s, f) \in [U_{\min}, U_{\max}]$	Utility für Gefährder

Rollenmodell



Quelle: in Anlehnung an (Beyerer, J.; Geisler, J.; Dahlem, A.; Winzer, P, 2010).

These 5: Metriken der Verlässlichkeit

Sicherheit ist eine emergente Verhaltenseigenschaft komplexer Multisysteme. Durch die Formalisierung und Metriken ist eine Basis für die Vergleichbarkeit zu schaffen.

Grundlage dafür sind neben Sicherheitsreferenzwerten geeignete Modellkonzepte mit formalisierter Beschreibung, welche qualitative Analysen und quantitative Berechnungen zulassen.

Problemlage:
Kommensurabilität

Wissenschaftliche Fragestellung:

- Wie lassen sich kommensurabler Größen und Beziehungen der Verlässlichkeit finden?

Lösungsansatz: Von der Numerik zur Metrik

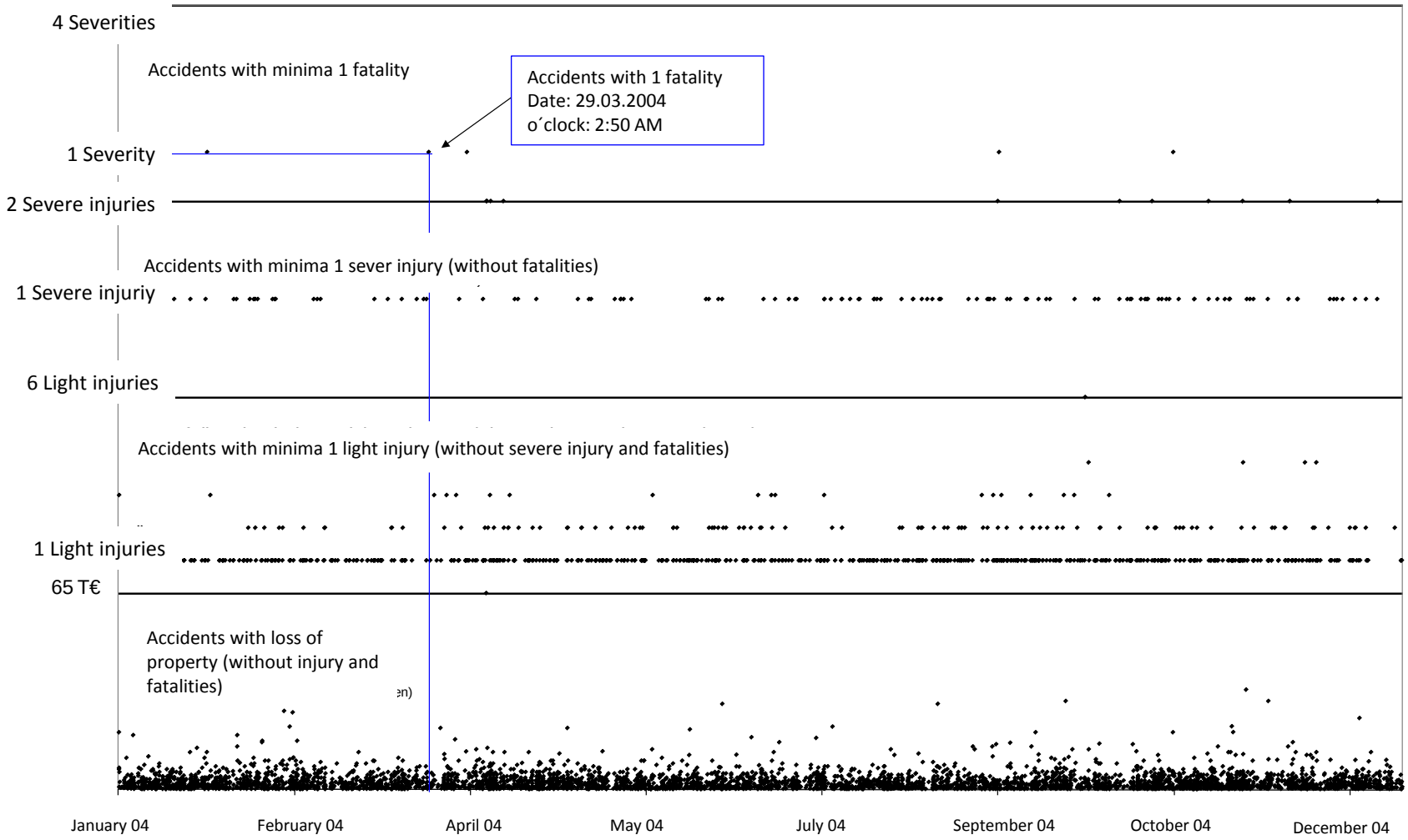
These 5: Metriken der Verlässlichkeit

Bemessung der Sicherheit - Unterschiedliche Risikomaße aus verschiedenen Regularien

Risk Metric	Name	Standard/Regulation
Residual mishap risk	RMR	MIL-STD-882-D
Average probability of failure on demand	PFD	IEC 61508
Probability of a dangerous failure per hour	PDFH	IEC 61508
Hazard rate	HR, SIL, ASIL, SAS, SPAD	EN 50126/EN 50129,IEC 61508, SIRF
Mean time between hazardous events	MTBHE	IEEE 1483
Safety targets	MEM,GAMAB,ALARP FWSI	EN 50126, 402/2013/EC
Disability-Adjusted Life Year	DALY	World Health Organization Family of International Classifications
Arbeitsplatzgrenzwert	AGW (MAK,TRK,BGW)	GefStoffV
Sicherheitspotenzial	SIPO	ESN ARS 27/2003/BMVBS2003

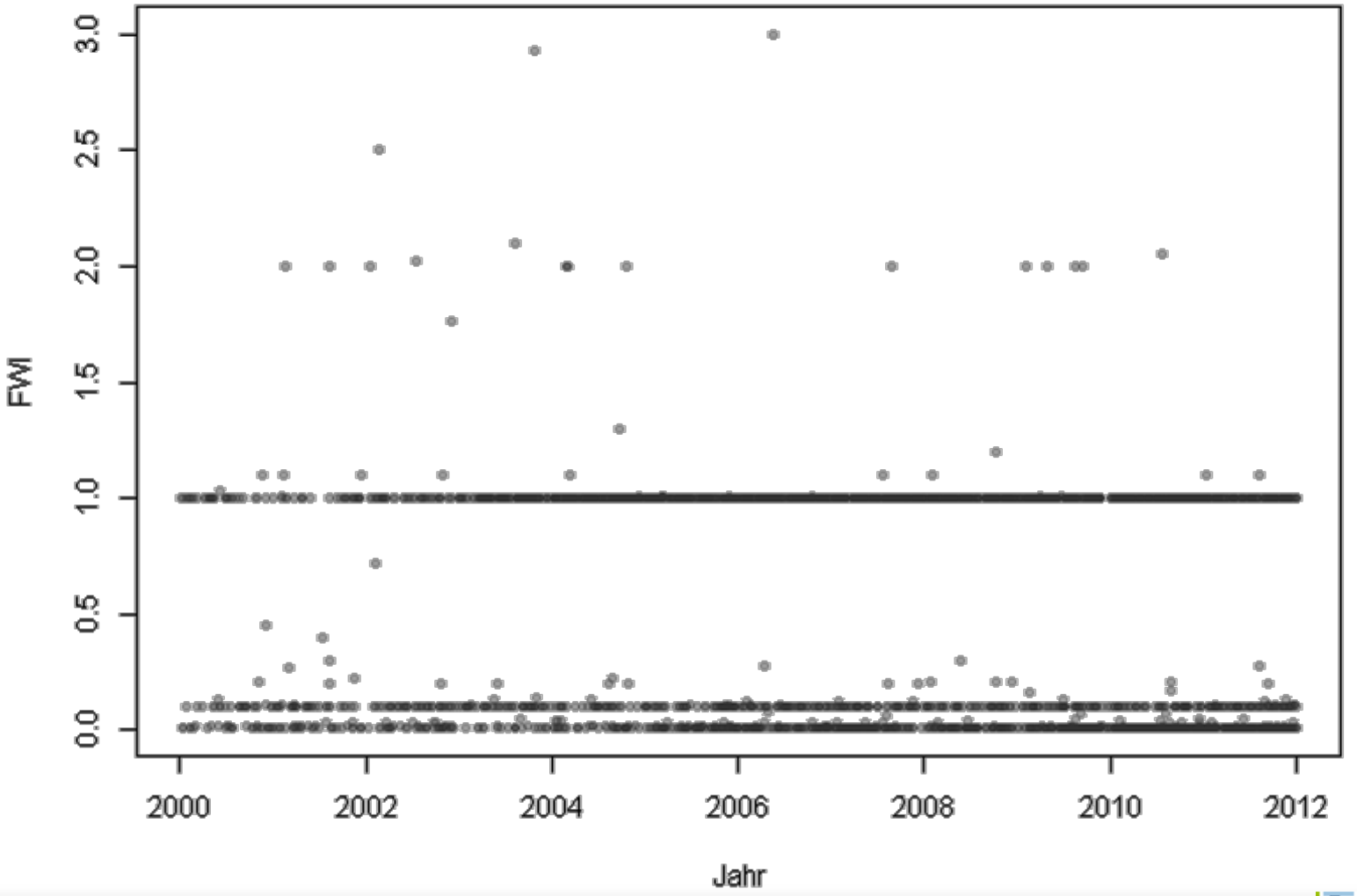
Bemessung der Sicherheit

Auswertung von Unfallberichten der Stadt Braunschweig 2004 - Ereignisse



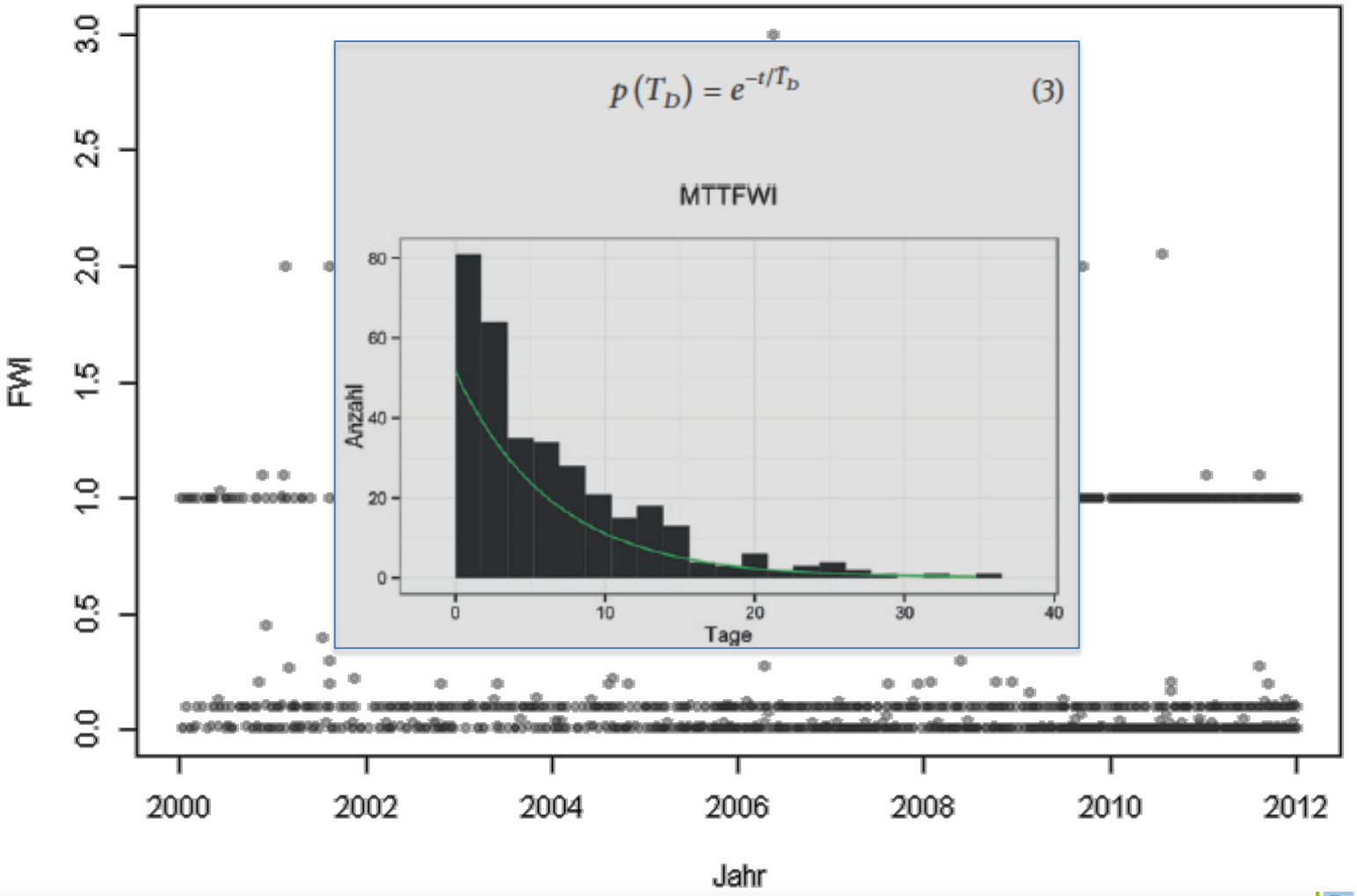
Bemessung der Sicherheit

Untersuchung FWI Eisenbahn Schweiz 2000 – 2011 - Ereignisse



Bemessung der Sicherheit

Untersuchung FWI Eisenbahn Schweiz 2000 – 2011 - Ereignisabstandsverteilung

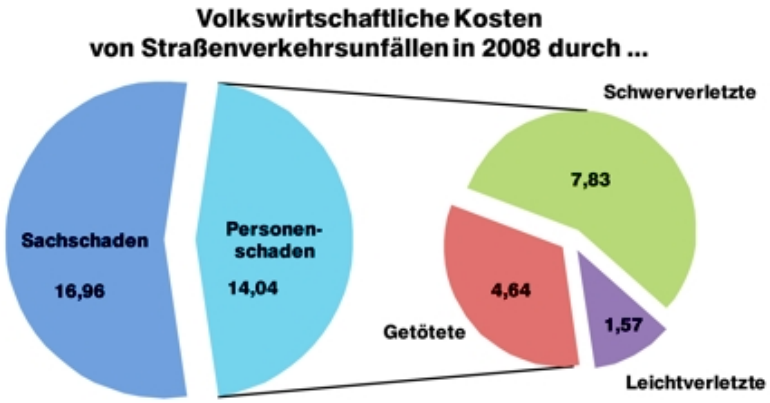


Bemessung der Sicherheit - Messwerte: Kosten der Verkehrssicherheit

BASt Bericht M208 von 2010

„Die neu berechneten Unfallkosten betragen im Jahr 2005 annähernd 31,477 Milliarden Euro. Die Personenschäden hatten daran einen Anteil von 15,226 Milliarden Euro, die übrigen 16,252 Milliarden Euro entfielen auf die Sachschäden.“

Kostensätze für Personenschäden (je verunglückte Person)	
Getötete	1.035.165
Schwerverletzte	110.506
Leichtverletzte	4.403
Kostensätze für Sachschäden (je Unfall)	
Unfall mit Getöteten	40.242
Unfall mit Schwerverletzten	19.436
Unfall mit Leichtverletzten	12.775
Schwerwiegender Unfall mit nur Sachschaden	19.035
Übriger Sachschadenunfall (einschließlich Alkoholunfall)	5.550



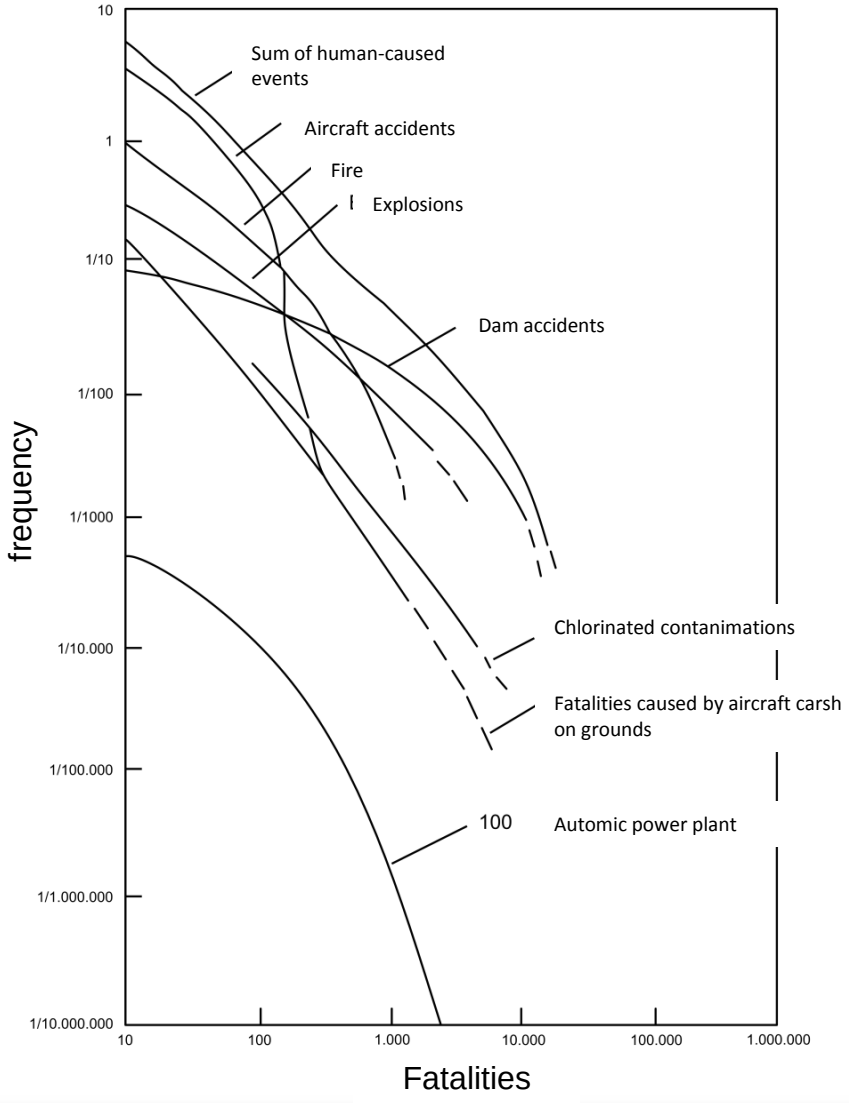
in Milliarden Euro.

Bemessung der Sicherheit - Skalen für Erdbeben

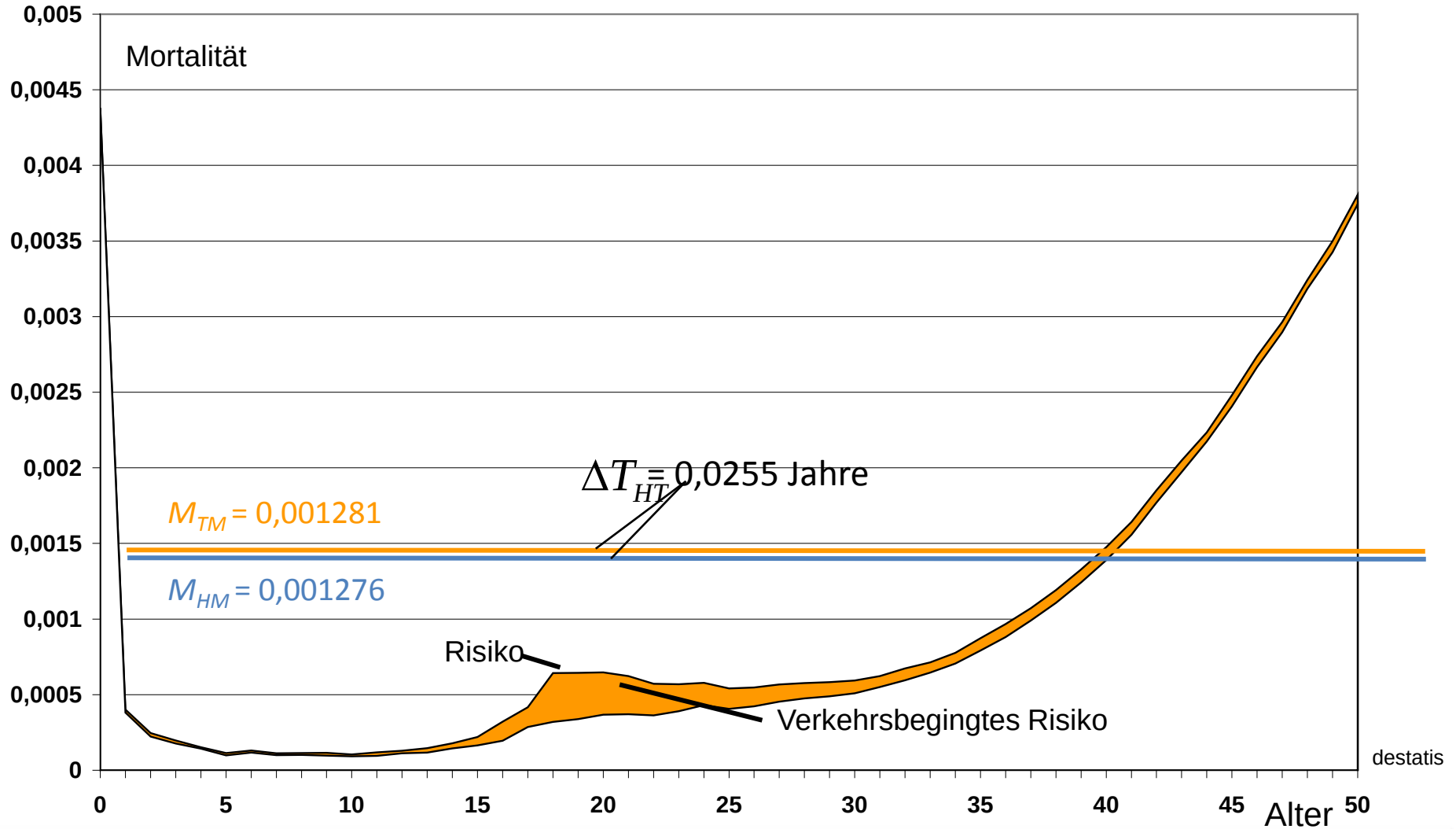
Richterskala	Mercalliskala	Energieäqivalent/TNT (Kilotonne TNT) = $4{,}184 \cdot 10^{12}$ J = 1,162 GWh	Anzahl jährlicher Erdbeben
0 to1,9	I	0,001–0,7	Sehr hoch
2 to 2,9	II	1–22	300.000
3 to 3,9	III	30–700	49.000
4 to 4,9	IV to V	$(1–22)x10^3$	6.200
5 to 5,9	VI	$(30\text{-}700)x\ 10^3$	800
6 to 6,9	VII to IX	$(1–22)x\ 10^6$	120
7 to 7,9	X to XI	$(30–700)x\ 10^6$	18
8 to 8,9	XII	$(1–22)x\ 10^9$	Alle 5 Jahre
9,0 and above	-	-	Unbekannt, 10 bis100 Jahre

Quelle: wikipedia

Bemessung der Sicherheit - Quantitative Skalierung im Farmer Diagramm



Bemessung der Sicherheit - Lebensaltersabhängige Mortalität



Bemessung der Sicherheit - Sicherheitsmaße: Mortalität und Verkürzung der Lebensdauer

Sicherheitsindex = Negatives Logarithmisches Verhältnis $\left(\frac{\text{Verkürzung der mittl. Lebensdauer}}{\text{Mittlere Lebensdauer}} \right)$

$$\Psi_H = -\lg \frac{\Delta T_{HT}}{T_{HM}}$$

These 6: Verlässlichkeit ist konstruierbar

Die präventive Gestaltung komplexer technischer und soziotechnischer Systeme gemäß des erweiterten Sicherheitsverständnisses erfordert eine methodische Vorgehensweise zum Entwurf integrierter Verlässlichkeitskonzepte.

Problemlage:
Systematischer Entwurf verlässlicher Systeme

Wissenschaftliche Fragestellung:
- Synthesefähigkeit eines Kalküls für Verlässlichkeit?

Lösungsansatz: Konvergente Methodik

Verlässlichkeit konstruieren

Systemabgrenzung → Deskription → Analyse → Inferenz → **Synthese** verlässlicher Systeme

Methodische Ansätze:

- Systems Engineering,
- Informatik,
- Statistische Entscheidungstheorie,
- Spieltheorie,
- Regelungstheorie, Kybernetik,
- Evolutionstheorie.

Konstruktionsprinzipien:

- Minimal-Prinzip Security,
- passive ←→ aktive Schutzmaßnahmen (Safety ←→ Security),
- Optimierungskriterien: Minimales mittleres Risiko ←→ Minimales maximales Risiko,
- Closed world ← → open world: Adaptierbarkeit, Lernfähigkeit, Erweiterbarkeit.

Verlässlichkeit konstruieren

Systemabgrenzung → Deskription → Analyse → Inferenz → Synthese verlässlicher Systeme

Wissenschaftliche Herausforderungen:

- Eruierbarkeit der Modellgrößen,
- Taxierung von Kosten (materielle und immaterielle),
- Schätzung von Wahrscheinlichkeiten (DoBs, seltene Ereignisse),
- Übergang von Szenario-orientiertem zu Szenarien-übergreifendem Entwurf
- Dynamisierung der Modelle,
- Beherrschung der Komplexität (Berechnung, Optimierung, Simulation).

Risikomodellierung → Basis für Risikominimierung, Basis für Systementwurf

Risiko für die Schutzbedürftigen:

$$R_S = \sum_{g \in G_U} \sum_{s \in S} \sum_{f \in F(s)} c(s,f) \cdot v(s,f) \cdot \Pr_U(v_g \mid s,f)$$

$$+ \sum_{g \in G_I} \sum_{s \in S} c(s,\tilde{f}) \cdot v(s,\tilde{f}) \cdot \Pr_I(a_g \mid s,\tilde{f}) + \sum_{s \in S} \sum_{m \in M^*} c(m(s,f))$$

mit $\tilde{f} := \arg\max_{f \in F(s)} \{u(g,s,f)\}$

$u(g,s,f) \in [U_{\min}, U_{\max}]$: Utility für Gefährder $g \in G_I$ aus seiner Sicht.

$\tilde{f}$ ist aus Sicht des Gefährders die Flanke der Verwundbarkeit von s, die ihm das beste Kosten/Nutzenverhältnis bietet.

Empfehlung zur Grundlagenforschung der Verlässlichkeit

- Verlässlichkeit (⊃ Sicherheit) braucht eine **Basistheorie**, die alle beteiligten Disziplinen übergreift und von konkreten Technologien abstrahiert.
- Eine Basistheorie für Verlässlichkeit soll eine einheitliche symbolische Beschreibung, Analyse, Synthese und Optimierung von Verlässlichkeit erlauben.
- In bisherige Förderprogramme der Sicherheitsforschung passte die Erforschung und Entwicklung einer solchen Basistheorie nicht hinein.
- Die Autoren und Unterstützer dieser Thesen empfehlen die **Institutionalisierung der Verlässlichkeitsforschung** im Rahmen der Grundlagenforschung**.**
- Die Autoren und Unterstützer dieser Thesen regen an, dass die DFG ein entsprechendes **Schwerpunktprogramm** einrichtet.