TeleTrusT
Pioneers in IT security.

Risikoquantifizierung - Sind schwarze Schwäne in der IT denkbar?

Quantitative Methoden zur Bestimmung von operationellen Risiken und deren Aggregation auf Management Ebene

von
Dr. Wolfgang Böhmer

TU-Darmstadt, Computer Science Dep.
Security Engineering Group

COMPETENCE CENTER FOR
APPLIED SECURITY TECHNOLOGY
CAST

© TeleTrusT Deutschland e.V.

Agenda - Risikoquantifizierung

- Motivation,
  - Der langfristige Einfluss von BASEL II auf die Wirtschaft
  - Der ambitionierte Ansatz (AMA)
- ..von der ordinalen Risikobetrachtung zur Risikoquantifizierung
  - Was ist Risikoquantifizierung?
  - Unterschiede zwischen Zeitreihenanalyse und Prozessanalyse des Geschäftsbetriebes
  - Weg der Risikoquantifizierung am Beispiel eines Kraftwerkes im Bereich der SCADA Systeme
- ..vom Einzelrisiko zum Gesamtrisiko – Aggregation von Risiken
  - Der Einfluss der „Fat-tails“
  - Die kollektive Risikotheorie und die Verallgemeinerte Pareto Verteilung
  - Aggregation von Risiken auf Standort eben und Aggregation Risiken auf Holding Ebene (Kategorien)
- Fazit .... vom Risikomaß zur Sicherheitsmetrik
  - Die Rolle der Standards der ISO Familie ISO 27000, 27001, 27003, 27005

© TeleTrusT Deutschland e.V.

Motivation - Risikoquantifizierung

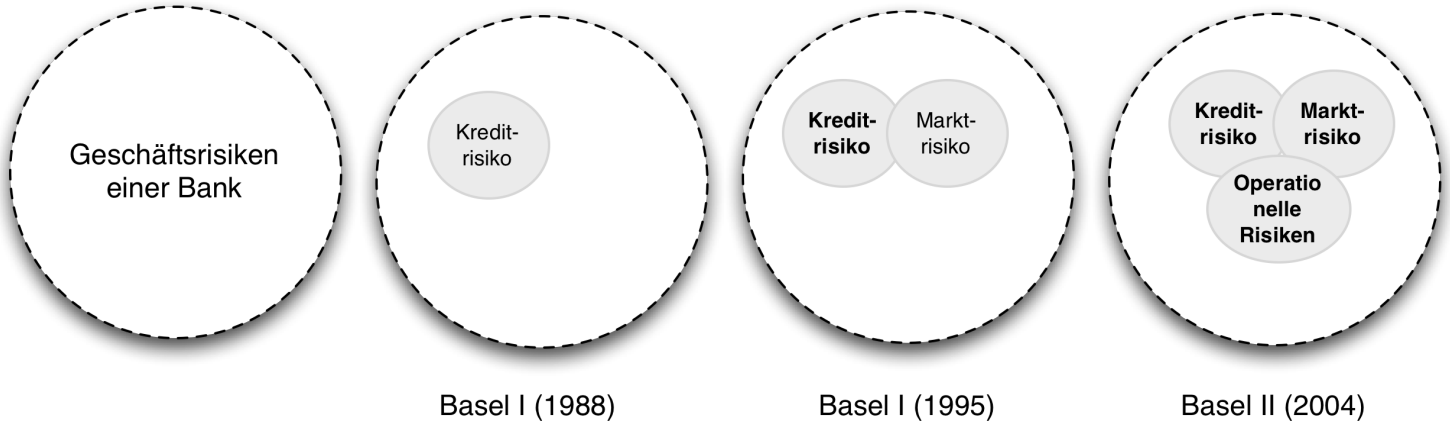


Fig. 1: Skizzierung der BASEL II Entwicklung

- Der Accord zu BASEL II wurde im Jahr 2001 publiziert und im Jahr 2004 weiter konkretisiert.
- „*Das operationelle Risiko ist definiert als die Gefahr von Verlusten infolge unzulänglicher oder fehlgeschlagener interner Prozesse, Systeme oder Mensche sowie von externen Ereignissen. Diese Definition beinhaltet das Rechtsrisiko, schließt aber strategisches –und das Reputationsrisiko aus“.*
- Es sind drei Ansätze vorgesehen, von denen der ambitionierte Ansatz (AMA) der anspruchsvollste Ansatz ist.

© TeleTrusT Deutschland e.V.

Motivation - Risikoquantifizierung

- Die Bestimmung der operationellen Risiken können nach BASEL II mit unterschiedlichen Ansätzen bestimmt werden.
- Der anspruchsvollste Ansatz ist der so genannte Advanced Measurement Approach (AMA).
- Wurde dieser Ansatz zunächst in den ersten Jahre nach BASEL II vermieden, wird dieser nun überall in den Banken und in der Industrie verwendet.

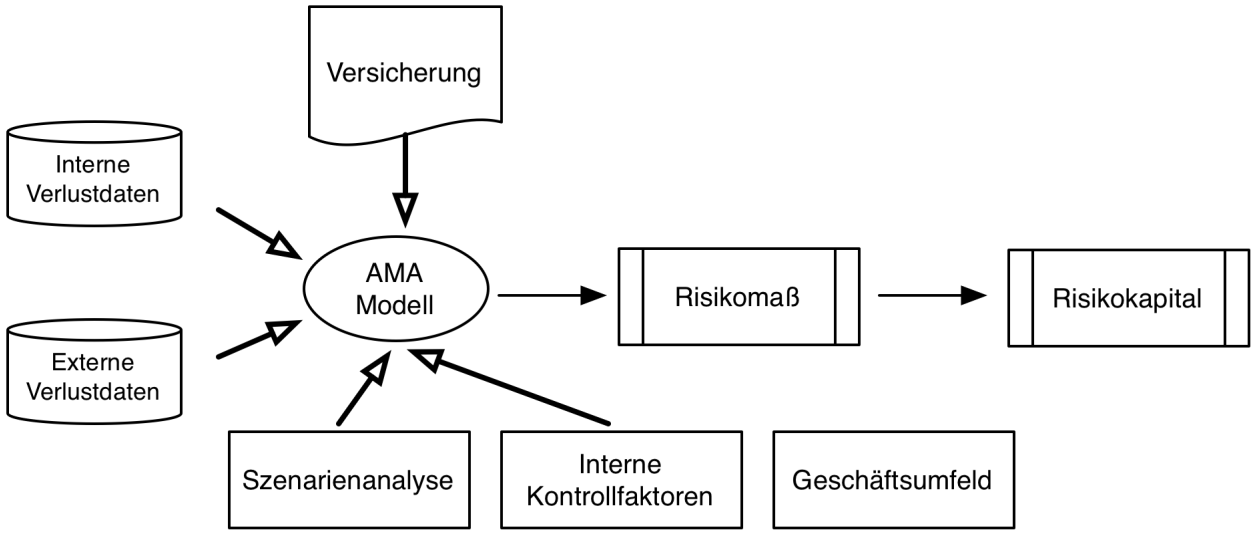


Fig. 2: Skizzierung der Durchführung eines AMA konformen Ansatzes

© TeleTrusT Deutschland e.V.

Motivation - Risikoquantifizierung

- Einfluss von BASEL II auf die Informationssicherheit Management Systeme (ISMS) nach ISO 27001:2005, Kapitel 1.1, Zitat:“ *This International Standard specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented ISMS within the context of the organization’s overall business risks*”
- In der ISO 27005:2008 wird weiter konkretisiert, Zitat, Kapitel 5, Seite 4 „*Risks being assessed in terms of their consequences to the business and the likelihood of their occurrence“.*
- Wie Geschäftsprozesse zu betrachten sind vor dem Hintergrund einer ISMS Implementierung ist aus der ISO 27003:2010 zu entnehmen, Zitat: Kapitel 7, Seite 25: *a) select the important organizational business processes and process steps concerning information security requirements, b) create a comprehensive flow chart covering the organization’s main processes including infrastructure (logical and technical), if this is not already present or performed during the organization analysis.*
- These: Die Richtung ist damit vorgegeben für die Bestimmung von operationellen Risiken

© TeleTrusT Deutschland e.V.

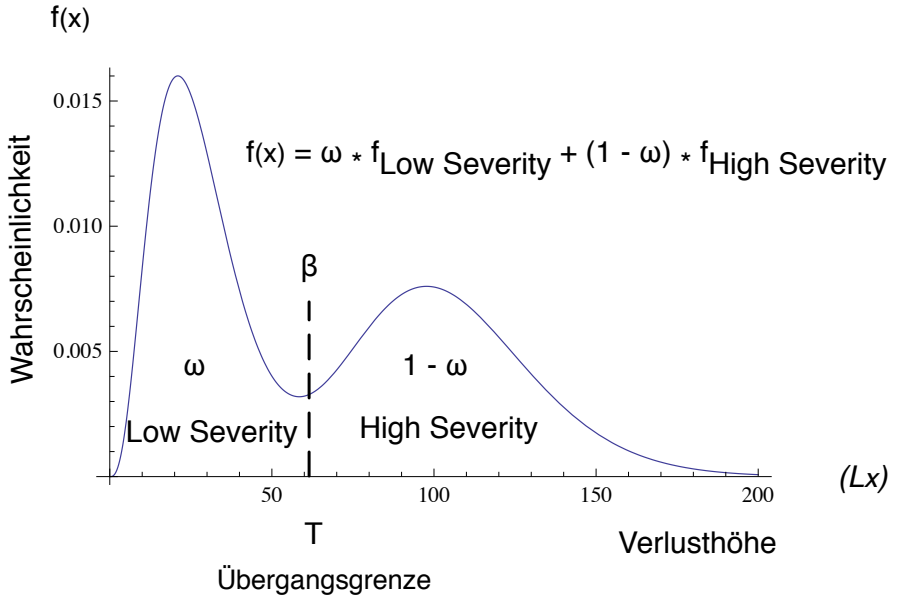
Agenda - Risikoquantifizierung

- Motivation,
  - Der langfristige Einfluss von BASEL II auf die Wirtschaft
  - Der ambitionierte Ansatz (AMA)
- ..von der ordinalen Risikobestimmung zur Risikquantifizierung
  - Was ist Risikoquantifizierung?
  - Unterschiede zwischen Zeitreihenanalyse und Prozessanalyse des Geschäftsbetriebes
  - Darstellung der Risikoquantifizierung am Beispiel eines Kraftwerkes im Bereich der SCADA Systeme
- ..vom Einzelrisiko zum Gesamtrisiko – Aggregation von Risiken
  - Der Einfluss der „Fat-tails“
  - Die kollektive Risikotheorie und die Verallgemeinerte Pareto Verteilung
  - Aggregation von Risiken auf Standort eben und Aggregation Risiken auf Holding Ebene (Kategorien)
- Fazit .... vom Risikomaß zur Sicherheitsmetrik
  - Die Rolle der Standards der ISO Familie ISO 27000, 27001, 27003, 27005

© TeleTrusT Deutschland e.V.

- Was ist Risikoquantifizierung: Historie?
  - Historisch, vor ca. 100 Jahren, wurde in der Versicherungsmathematik mit der kumulativen Risikotheorie der so genannt *Loss Distribution Approach, LDA* eingeführt.
  - Das Cramér-Lundberg Modell beherrschte zu der Zeit die Versicherungen. Es betrachtet die Fälle mit großer Häufigkeit aber einer Low-Severity (geringer Auswirkung) und einer geringen Häufigkeit mit einer High Severity (hohe Auswirkung) getrennt.
  - Darstellung einer zusammen-gesetzten Gamma Funktionen, so dass eine bimodale Dichtefunktion entsteht. Die erste Gama Fkt. hat Die Parameter α = 4 und θ = 7 für einen Mode von 21 und die zweite hat die Parameter α = 15 und θ = 7 mit einem Mode von 98

$$f(x) = 0.5\frac{x^3 e^{-x/7}}{3!7^4} + 0.5\frac{x^{14} e^{-x/7}}{14!7^{15}}$$



© TeleTrusT Deutschland e.V.

- Was ist Risikoquantifizierung?
  - Die Idee einer Risikoquantifizierung besteht in der Zuweisung eines Wertes (Wx) bzw. Verlustgröße (Lx) bei einem Ereignis das einer Zufallsvariable widerfährt. Das Risiko wird als Zufallsvariable (X) verstanden, das sich innerhalb eines Wahrscheinlichkeitsraumes Ω bewegt.

$$L_X = W_X := X(\Omega) = \{x \in \mathbb{R} \mid \exists\, \omega \in \Omega \text{ mit } X(\omega) = x\}. \qquad (1)$$

  - Ein einfaches Beispiel: Wir werfen eine ideale Münze dreimal
  - Vorbereitung:
    - Ergebnismenge $\Omega := \{K, W\},\ \text{es ist } \omega_1 = K,\ \omega_2 = W$
    - Die Zufallsvariable X bezeichnet *die Gesamtzahl* der Würfe mit „Kopf“
    - Beispielweise gilt X (K W K) = 2 und X(K K K) = 3
    - X hat den Wertebereich W_X = {0,1,2,3}
  - Jetzt ist obige Zuweisung zwischen einem Wert und einer Zufallsvariable zu verstehen
  - Eine Zufallsvariable ist die Abbildung: $X : \Omega \longrightarrow \mathbb{R}$

© TeleTrusT Deutschland e.V.

- Wir werfen die Münze dreimal
  - Wenn „Pr“ die Wahrscheinlichkeit ist, dann folgt für den Wahrscheinlichkeitsraum:

$$\Pr[\mathrm{X}=0]=\Pr[\mathrm{W\ W\ W}]=\tfrac{1}{8}$$

$$\Pr[\mathrm{X}=1]=\Pr[\mathrm{K\ W\ W}]+\Pr[\mathrm{W\ K\ W}]+\Pr[\mathrm{W\ W\ K}]=\tfrac{3}{8}$$

$$\Pr[\mathrm{X}=2]=\Pr[\mathrm{K\ K\ W}]+\Pr[\mathrm{K\ W\ K}]+\Pr[\mathrm{W\ K\ K}]=\tfrac{3}{8}$$

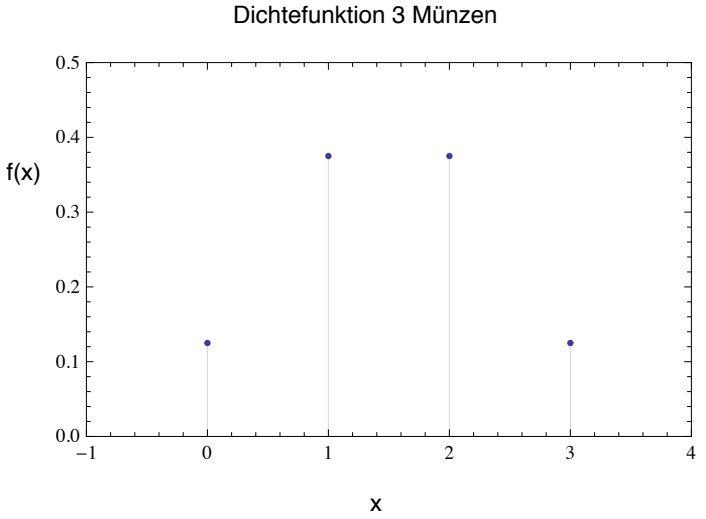
$$\Pr[\mathrm{X}=3]=\Pr[\mathrm{K\ K\ K}]=\tfrac{1}{8}$$

  - Wie sieht nun die Dichtfunktion und die Verteilung aus?
  - Dichte und Verteilungsfunktionen sind wichtige Informationen zur Ermittlung eines Risikomaßes und Aggregation von Risiken

© TeleTrusT Deutschland e.V.

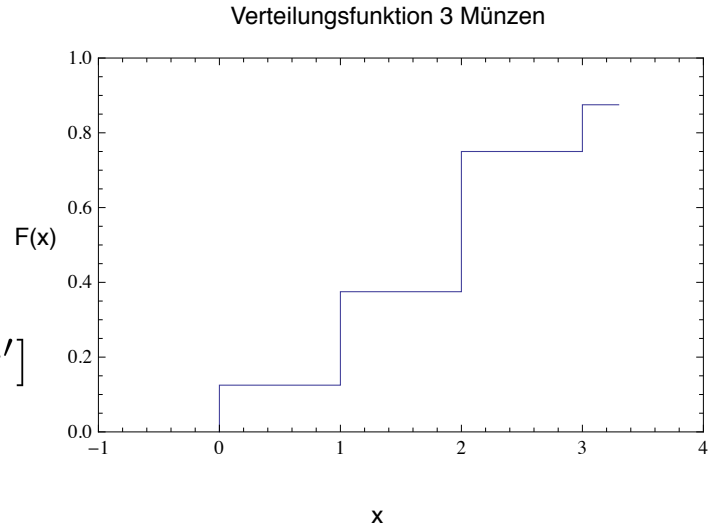
- Dichte und Verteilung der Zufallsvariable X

$$\Pr[X = 0] = \frac{1}{8} = 0.125$$
$$\Pr[X = 1] = \frac{3}{8} = 0.375$$
$$\Pr[X = 2] = \frac{3}{8} = 0.375$$
$$\Pr[X = 3] = \frac{1}{8} = 0.125$$



Dichtefunktion

$$f_x : \mathbb{R} \to [0,1], \quad x \mapsto Pr[X = x]$$



Verteilungsfunktion

$$F_x : \mathbb{R} \to [0,1],\ x \mapsto Pr[X \leq x] = \sum_{x \in W_x : x' \leq x} Pr[X \leq x']$$

© TeleTrusT Deutschland e.V.

- Erwartungswert ($\mathbb{E}$) von der Zufallsvariable (X),
- *was kann man im Mittel erwarten*?

$$\mathbb{E} := \sum_{x \in W_x} x \cdot Pr[X = x] = \sum_{x \in W_x} x \cdot f_x(x)$$

- Zur Veranschaulichung berechnen wir den Erwartungswert von $\mathbb{E}[X]$

$$\mathbb{E}[X] = \sum_{i=0}^{3} i \cdot Pr[X = x] = 1 \cdot Pr[X = 1] + 2 \cdot Pr[X = 2] + 3 \cdot Pr[X = 3]$$

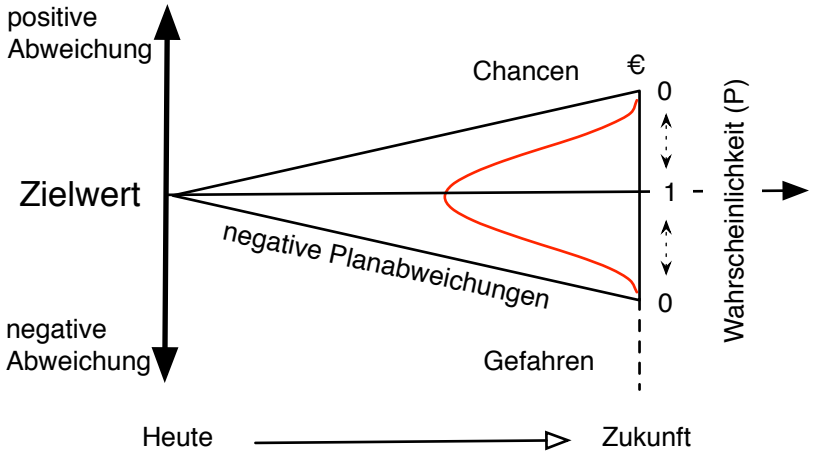
$$\mathbb{E}[X] = 1 \cdot \tfrac{3}{8} + 2 \cdot \tfrac{3}{8} + 3 \cdot \tfrac{1}{8} = \tfrac{3}{2}$$

- Entsprechend kann die Varianz und Standardabweichung im Wahrscheinlichkeitsraum gebildet werden
- Mit Standardabweichung und Varianz kann eine Verteilung ausreichend beschrieben werden

© TeleTrusT Deutschland e.V.

..von der ordinalen Risikobetrachtung zur Risikoquantifizierung

- Entwicklung des Index als Zeitreihe
- Betrachtung einer Aktie zu einem bestimmten Zeitpunkt (t) und deren Entwicklung Δt kann mittels Normalverteilung (bedingt) betrachtet werden
- Abweichungen bleiben in Grenzen „bedingt“ gering.



NASDAQ100 (09. Juni 2010)

© TeleTrusT Deutschland e.V.

- Unterschiede zwischen Risiken im Bereich der Finanzdienstleistungen und den operationellen Risiken (OpRisk)
  - Während Risiken im Finanzsektor bewusst eingegangen werden, sind die OpRisk inhärent mit dem Geschäftsbetrieb verbunden.
  - Während es im Finanzsektor im Kern nur zwei Möglichkeiten gibt mit Risiken umzugehen, a.) Risiken erst gar nicht einzugehen, b.) Risiken zu streuen (Diversifizierung) z.B. ein Aktienportfolio anzulegen, gibt es im OpRisk Bereich präventive (ISMS) und reaktive (BCMS) Möglichkeiten mit Risiken umzugehen.
  - Während Risiken sich im Finanzsektor auf das Verhalten einer bzw. mehreren Zeitreihe beziehen, die ggf. korreliert sind, müssen Risiken im Bereich OpRisk über die Betrachtung von Prozessen behandelt werden.
  - Während extreme, unerwartete Schwankungen der Eingangsgrößen im Bereich der Finanzrisiken „hingenommen“ werden müssen, ist i.d.R. im Bereich der OpRisik ein Notfallplan und Business Continuity Prozesse (BCP) vorhanden.

© TeleTrusT Deutschland e.V.

Weg der Risikoquantifizierung am Beispiel eines Kraftwerkes im Bereich der SCADA Systeme

- Skizzierung: Prozesshierarchie eines Kraftwerkes
- Es gibt drei Hauptprozesse (P1, P2, P3)
- z.B. wird Prozess Dampf + Strom erzeugen näher untersucht
- Prozesse der Leittechnik (PL) und der Prozessdatenverarbeitung (PDV) (SCADA Systeme) werden näher untersucht.
- Gegenstand der Untersuchung ist der Einfluss von PDV/PLT auf den Wertschöpfenden Prozess Dampf + Strom erzeugen

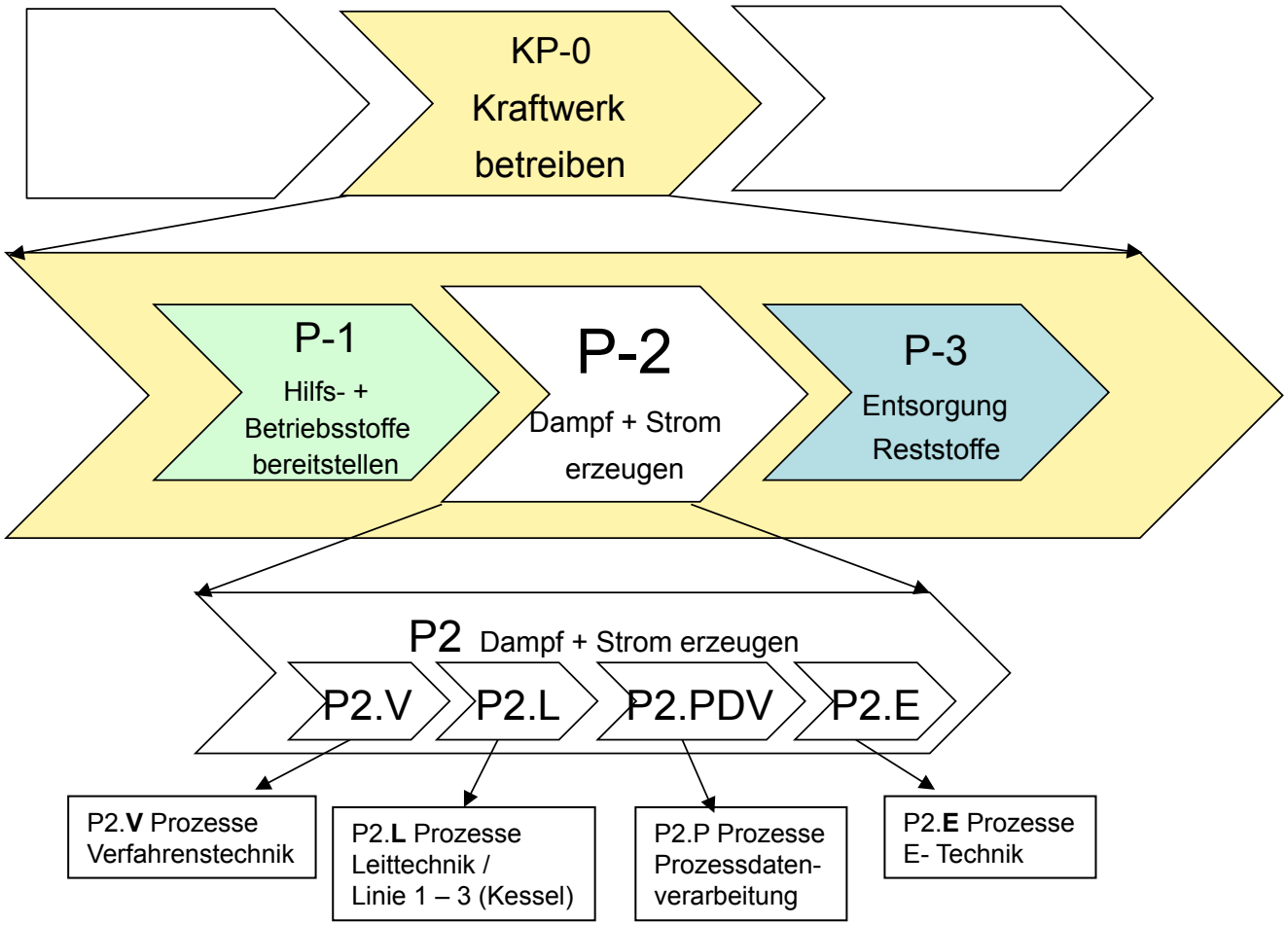


Fig.1: Ausschnitt der Prozesslandschaft zum Kernprozess „Kraftwerk betreiben“

© TeleTrusT Deutschland e.V.

Weg der Risikoquantifizierung am Beispiel eines Kraftwerkes im Bereich der SCADA Systeme

- Prozessanalyse auf Ebene der Prozesselemente
- Einfluss der Prozess-Risiken (Regelbetrieb) auf den Prozess Dampf & Strom erzeugen
- Die Risiken werden mittels Risikoszenarien erfasst
- Ein Risikoszenario ist ein stochastisches Ereignis das sich in der Zukunft abspielen könnte und aus dem Rückschlüsse (ggf. Maßnahmen) auf die Gegenwart gezogen werden können
- Einer von vielen Prozessen in der Prozesslandschaft

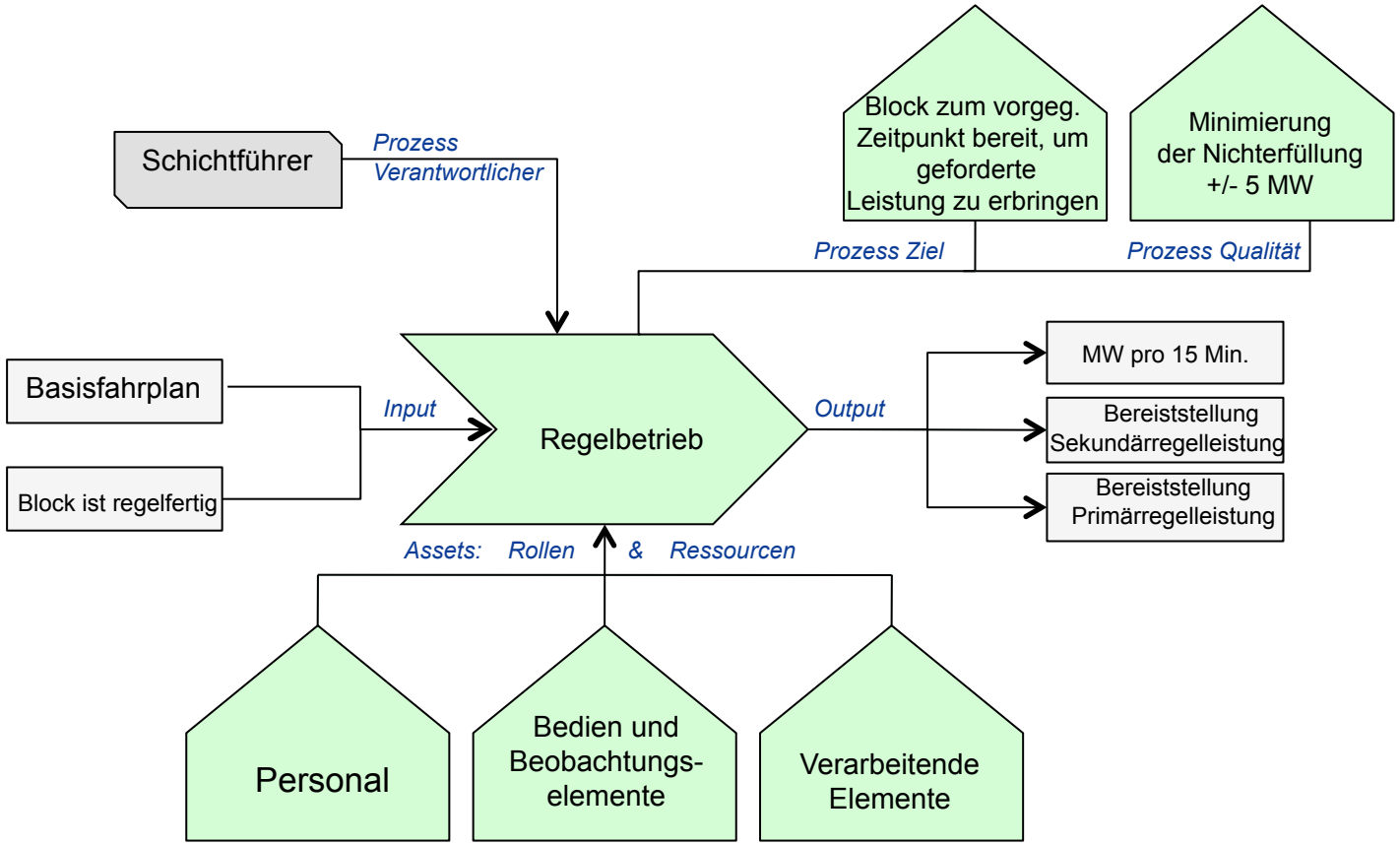


Fig.2: Illustration der Prozesselemente eines der Teilprozesse des Prozess „Dampf & Strom Erzeugen“

© TeleTrusT Deutschland e.V.

- Ablauf der Risikoquantifizierung:
  - Identifizieren der relevanten Prozesselemente pro Prozess
  - Analyse der Schwachstellen und möglichen Bedrohungen pro Prozess
  - Entwicklung von Risikoszenarien pro Prozess unter Einbeziehung der Assets pro Prozess
  - Ein Risikoszenario ist ein bestimmtes (Risiko)-Ereignis für die Zufallsvariable (X) bezogen auf die Schnittmenge (M5) der relevanten Assets, Schwachstellen und Bedrohungen. (Assets, Bedrohungen und Schwachstellen werden im Sinne der ISO 27001 aufgefasst)
  - Das Risikoereignis ist im Sinne der Ergebnismenge Ω zu verstehen. D.h. es handelt sich um die Zuweisung (x_i) eines potentiellen Schadens. Der Schaden wird nach Schwere (Severity) und ist eine Funktion der Eintrittswahrscheinlichkeit.
  - Es werden drei Risikoszenarien pro Asset in jedem Prozess „durchgespielt“. Dabei bedeutet die Zuweisung x_i = „best case“, x_j = „most likely case“ und x_k „worst case“.
  - Es hat die Projekterfahrung gelehrt, dass es für die Beteiligten einfacher ist ein Szenario zu beurteilen als die Parameter einer Verteilung zu bestimmen.
  - Aus den jeweiligen drei Einzelszenarien (x_i , x_j , x_k) wird eine Verteilungsfunktion ermittelt. Dies geschieht mittels Monte Carlo Simulation, um die fehlenden Werte der Verteilung zu ermitteln.

© TeleTrusT Deutschland e.V.

Weg der Risikoquantifizierung am Beispiel eines Kraftwerkes im Bereich der SCADA Systeme

- Risikoquantifizierung entspricht einer Schadenszuweisung einer Zufallsvariable
- Nur die Schnittmenge M5 ist relevant für die interessante Ergebnismenge
- Es werden drei Varianten eines möglichen Ereignisses betrachtet.
- Die Ereignisse werden mit den Prozessbeteiligten (*Expert Opinion*) vor Ort ermittelt.
- Die Experteneinschätzung ist wichtiger als eine bestimmte Verteilung bzw. Schätzmethode zu nutzen. Denn die Expertenschätzung stellt die Wesentliche „Input“ Größe dar.
- Aus den Einzelwerten wird auf die Verteilung geschlossen (Simulation)
- Alternative: Schätzung mit der Maximum Likelihood Methode

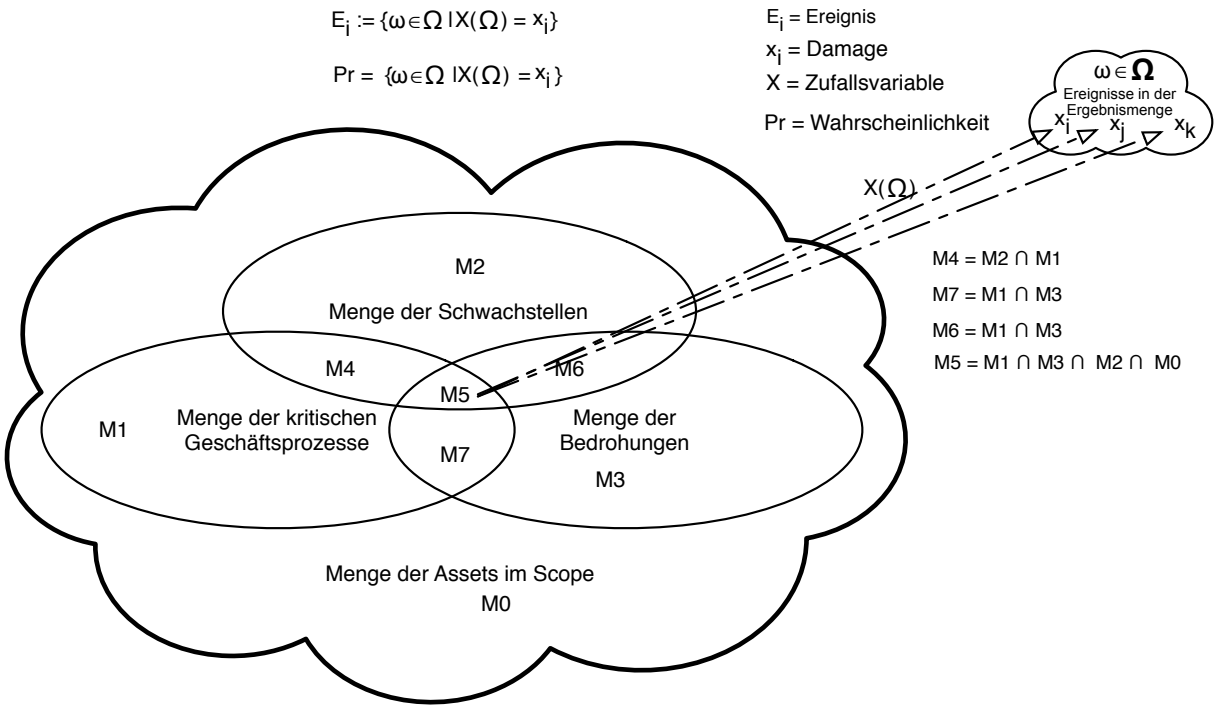


Fig.3: Illustration der Zuweisung der Zufallsvariable X

© TeleTrusT Deutschland e.V.

- Risikoquantifizierung entspricht der Schadenszuweisung einer Zufallsvariable
  - Pro Prozess (Dampf & Strom erzeugen, Entsorgung Brennstoffe, Hilfs- & Betriebsstoffe bereitstellen) entstehen eine Reihe von Einzelsrisikozenarien, die zunächst als disjunkt (keine Copulafunktion) behandelt werden.
  - Es werden Einzelszenarien pro Prozess nach der Vertraulichkeit, Verfügbarkeit und Integrität gemäß den Unterprozessen (P2V, P2L, P2PDV,P2E) unterschieden.
  - Die Einzelrisiken bzw. deren Verteilungen (i(x), j(x),g (x), h(x) werden anschließend durch eine math. Faltung zu einer Gesamtverteilung für den o.g. Prozess zusammengefügt.
  - Denn die Einzelrisiken bilden eine Partitionierung des Wahrscheinlichkeitsraumes
  - Für die Gesamtverteilung wird anschließend ein kohärentes Risikomaß genutzt.
  - Das kohärente Risikomaß, C-VaR, wird für die o.g. Prozesse erarbeitet und in eine Matrix (siehe Folie 23) eingetragen.

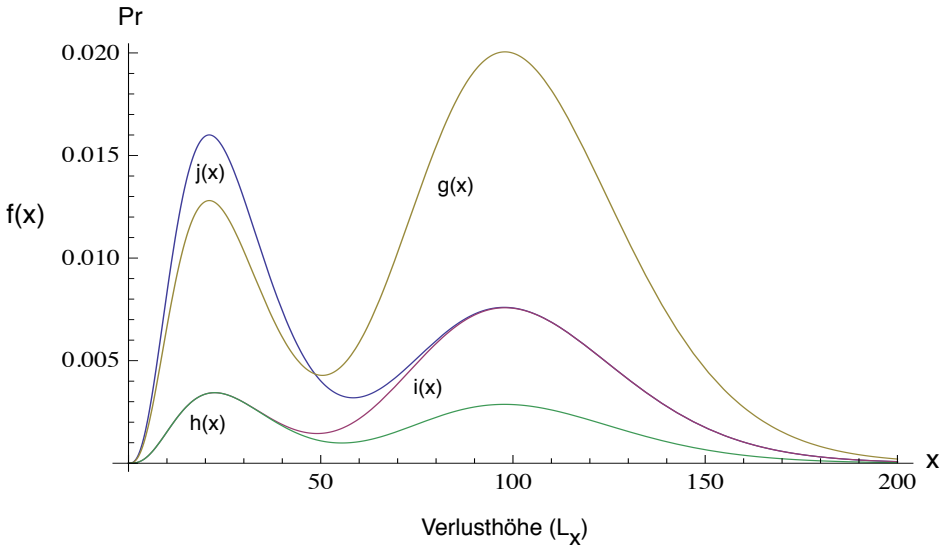


Fig.4: Verteilungen von Zufallsvariablen,

© TeleTrusT Deutschland e.V.

- Warum können wir das Risiko messen?
  - Zum Messen wird eine Mass- Funktion benötigt und zwar im Wahrscheinlichkeitsraum. Denn das Risiko kann als Zufallsvariable im Wahrscheinlichkeitsraum verstanden werden
  - Betrachtet man nun konkreter einen endlichen Wahrscheinlichkeitsraum, dann ist $(\Omega, \mathcal{A}, \mathbb{P})$, mit $\mathbb{P}$ als Wahrscheinlich-keitsmaß und X als Zufallsvariable auf $(\Omega, \mathcal{A}, \mathbb{P})$ der Verlust (Lx) nach einer Zeitperiode (t)

Sei $\mathcal{A}$ eine σ-Algebra über eine Menge (Ergebnismenge) Ω. Dann heißt die Abbildung

$$\mu : \mathcal{A} \to [0, \infty]$$

ein Maß auf $\mathcal{A}$, falls für μ gilt:

- μ ist σ-additiv, d.h. $\mu(\sum_{i=1}^{\infty} \mathcal{A}_i) = \sum_{i=1}^{\infty} \mu(\mathcal{A}_i)$ für paarweise disjunkte $\mathcal{A}_i$.
- $\mu(0) = 0$.

Das Tripel $(\Omega, \mathcal{A}, \mu)$ heißt dann Maßraum.

ρ = Risikofunktion bzw. Riskomaß

$$\rho = \mathcal{G} \longrightarrow \mathbb{R}$$

mit $\mathcal{G}$ als eine nicht leere Menge an messbaren Zufallsvariablen (X)

„ Man kann das Risikomaß als dasjenige Kapital interpretieren, das man z.B. für einen Prozess vorhalten muss, so dass das Risiko ein Verlust zu erleiden gleich Null wird “

© TeleTrusT Deutschland e.V.

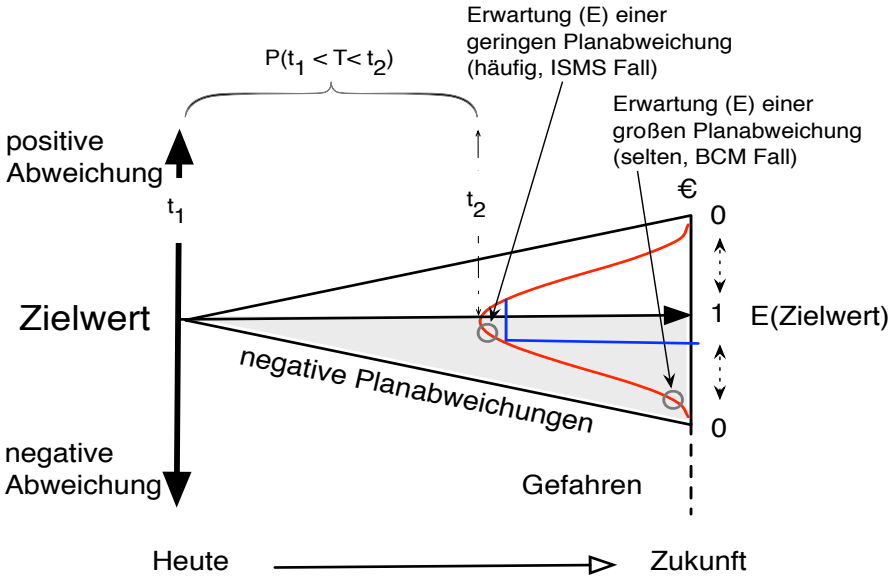
Agenda - Risikoquantifizierung

- Motivation,
  - Der langfristige Einfluss von BASEL II auf die Wirtschaft
  - Der ambitionierte Ansatz (AMA)
- ..von der ordinalen Risikobetrachtung zur Risikoquantifizierung
  - Was ist Risikoquantifizierung?
  - Unterschiede zwischen Zeitreihenanalyse und Prozessanalyse des Geschäftsbetriebes
  - Weg der Risikoquantifizierung am Beispiel eines Kraftwerkes im Bereich der SCADA Systeme
- ..vom Einzelrisiko zum Gesamtrisiko – Aggregation von Risiken
  - Der Einfluss der „Fat-tails“
  - Die kollektive Risikotheorie und die Verallgemeinerte Pareto Verteilung
  - Aggregation von Risiken auf Standort eben und Aggregation Risiken auf Holding Ebene (Kategorien)
- Fazit .... vom Risikomaß zur Sicherheitsmetrik
  - Die Rolle der Standards der ISO Familie ISO 27000, 27001, 27003, 27005

© TeleTrusT Deutschland e.V.

Negativbeispiel einer einfachen Aggregation und der Einfluss der „fat tails“

- Ein großer Vorteil des Maßes „erwarteter Verlust“ ist seine gute Nachvollziehbarkeit und seine einfache Berechnung. Wegen der Additivität des Erwartungswerts können die Erwartungswerte der einzelnen Risiken einfach addiert werden, um ein Gesamtrisiko anzugeben. Wenn das übergeordnete Ziel des Risikomanagementprozesses das Management und die Minderung der Risiken ist, könnte der erwartete Verlust deshalb ggf. besser geeignet sein diese Ziele zu unterstützen als komplizierter Risikomaße.
- **Nachteil:** So berücksichtigt dieser Wert nicht das Risiko, das aus einer breiteren Streuung der möglichen Gesamtverlusthöhe resultiert. Auch unterscheidet der Erwartungswert nicht zwischen seltenen, aber gravierenden Risiken („low frequency, high severity“) und häufigen, aber nicht so gravierenden Risiken („high frequency, low severity“).



Der Erwartungswert als statistisches Maß für ein Risiko hat sich in der Literatur durchgesetzt, jedoch wird häufig die Varianz (blaue Linie) des Erwartungswerts als Risikomaß für eine Aggregation hergenommen. Generell wird jedoch nur das *Downside Risikomaß* genommen (graue Fläche), denn es ist nur die negative Abweichung von Interesse.

Der Value-at-Risk zum Konfidenzniveau α (VaR) ist definiert durch

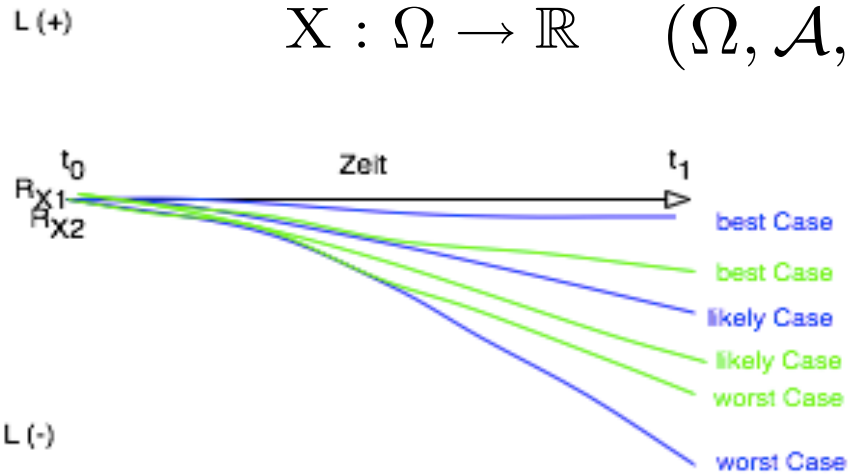
$$VaR_\alpha(X) = min\{x|(P(X \leq x) > \alpha)\}$$

© TeleTrusT Deutschland e.V.

Bedeutung der Drei-Punkt-Schätzung (DPS)

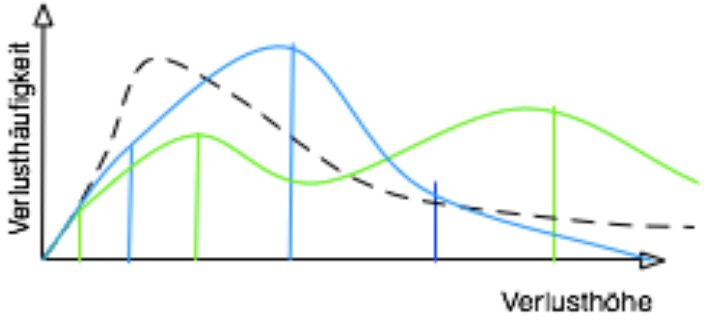
Loss distribution Approach (LDA)

- Die einfache DPS ermöglicht es über eine Simulation zu einer Verteilung zu gelangen.
- Mittels Verteilung kann dann die Varianz der Verteilung bezogen auf ein Konfidenzniveau berechnet werden.
- Damit kann eine Aussagen über den wahrscheinlichen nicht überschrittenen Verlust bezogen auf ein Zeitintervall angegeben werden (VaR). Ein VaR reicht jedoch nicht aus.
- G sei eine nichtleere Menge von *A*-messbaren Zufallsvariablen. Dabei ist A eine σ-Algebra
- Durch Verwendung keiner Normalverteilung z.B. einer GPD, siehe Folie 7, entsteht ein kohärentes Risikomaß



$$X : \Omega \rightarrow \mathbb{R} \qquad (\Omega, \mathcal{A}, \mathbb{P})$$

$$\rho = \mathcal{G} \rightarrow \mathbb{R}$$

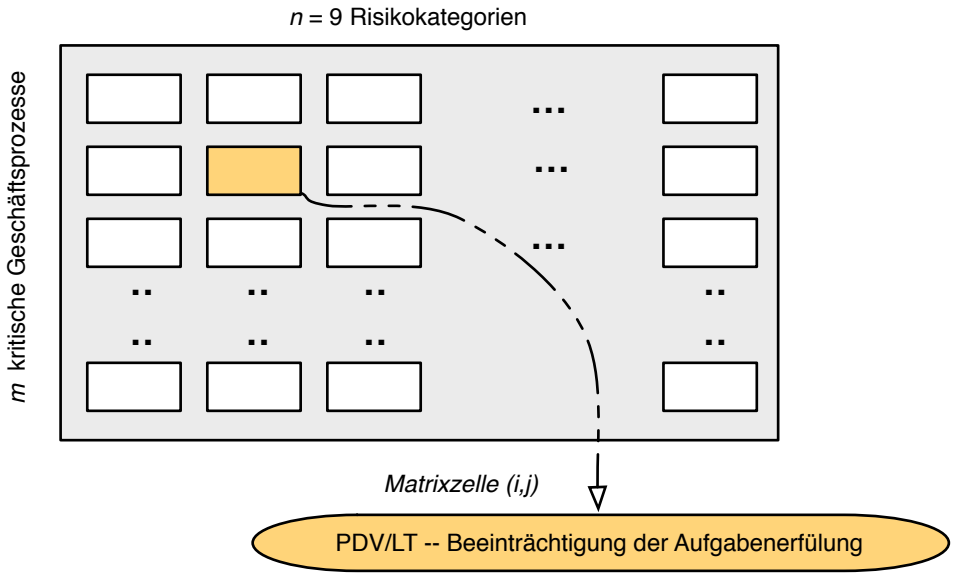


mit $\mathcal{G}$ als eine nicht leere Menge an messbaren Zufallsvariablen (X)

© TeleTrusT Deutschland e.V.

Aggregation von Einzelrisiken auf Standortebene

- Um Einzelrisiken aggregieren zu können muss ein Risikomaß pro Zelle vorliegen.
- Im AMA Ansatz werden als Zellen die Geschäftsbereiche verwendet.
- In der Industrie (in diesem Fall) ist es sinnvoll die wertschöpfenden Prozesse zu nehmen
- Es gibt bei dem EVU 9 Risikokategorien (Umwelt, Arbeitsleistung, rechtliche Aspekte, Geschäftsentwicklung, etc.) diese werden auf die kritischen Geschäftsprozessen bezogen. Auf den entstehenden Zellen jeweils ein Risikomaß berechnet worden
- Die Zellen bzw. die Verteilungen können mit einer Faltung kombiniert werden. Damit ergibt sich dann das Gesamtrisiko pro Standort.



© TeleTrusT Deutschland e.V.

Beispiel einer Risikoaggregation eines EVU

Verlusterwartung in einem Zeitinterval bezogen auf ein Konfidenzniveau

- Aggregation auf höherer Ebene nach Kategorien (Marktrisiken, Finanzrisiken, Geschäftsrisiken, Umfeldrisiken, sonstige Risiken.
- Aggregation auf der ersten Ebene nach Standorten und dort nach verschiedenen Kriterien (vf, vt, In) bezogen auf die kritischen Prozesse.
- Erfassung der Einzelrisiken (VVI) auf der PDV/LT Ebene (zukünftig ggf. mehr Ebenen.
- Aggregiert wird auf allen Ebenen mit einem kohärenten Risikomaß, dem C-VaR.
- Vorteil: Es kann eine Konzernsteuerung bzgl. der Betriebsrisiken auf allen Ebenen erfolgen.

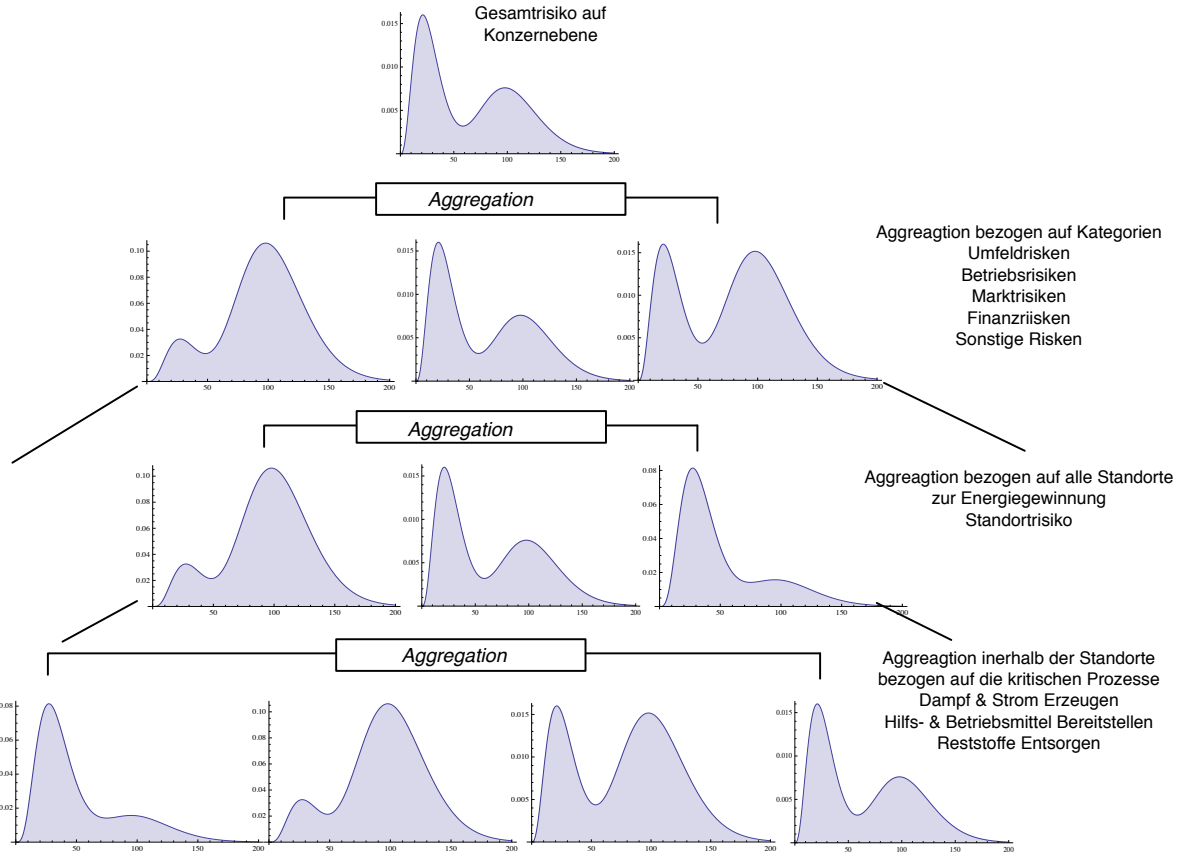
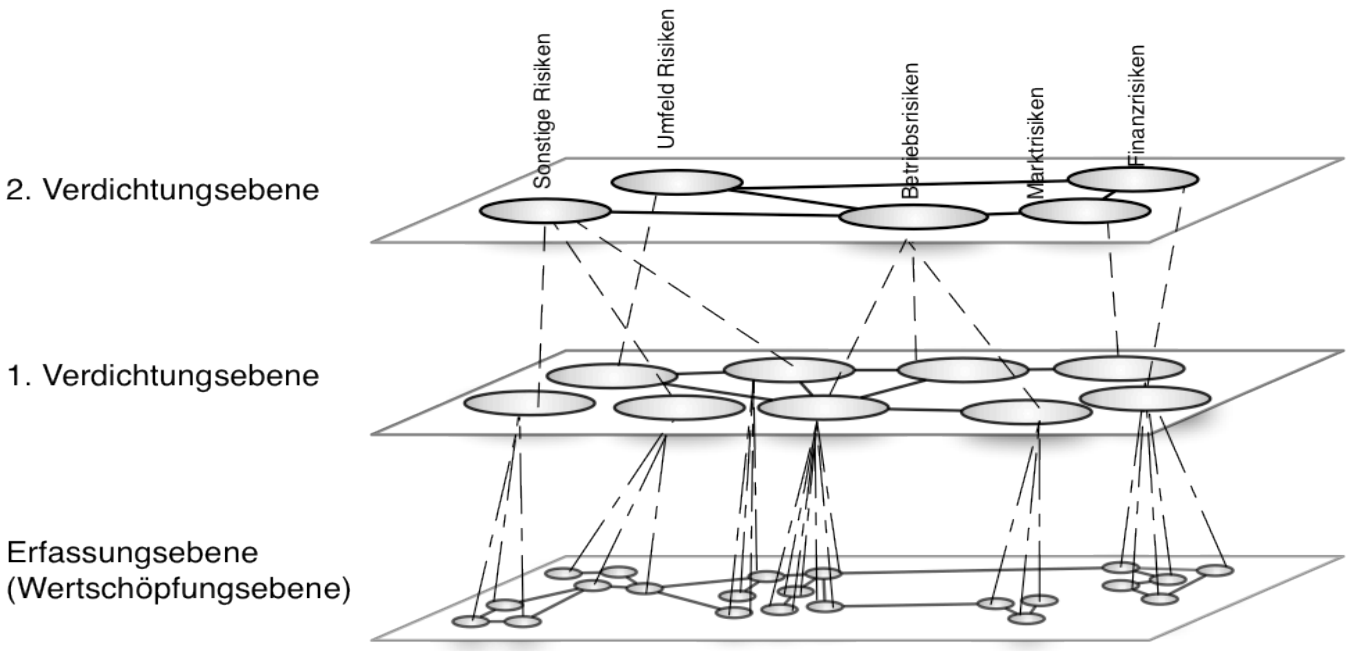


Fig.6: Illustration der Aggregation mit einem kohärenten Risikomaß

© TeleTrusT Deutschland e.V.

Hierarchie der Risikomeldungen, in Form von aggregierter Risiken



2. Stufe der Risikoverdichtung / Risikomeldung mit 5 Kategorien (obere Management Ebene) z.B. Risikomanagement nach Vorgabe, basierend auf 1. Stufe allerdings mit Umrechnungen

1.Stufe der Risikoverdichtung/ Risikomeldung mit 8 Kategorien (Management Ebene) z.B. Informationssicherheit

Basis: 6x8 Matrix, verschieden Auswertungen nach potentielle Schäden (€) *(Severity Level)*

Unterste Ebene oder Stufe der Risikoerfassung (untere hierarchische Ebene) z.B. bei den EVU-Standorten

*Die dargestellten Linien zeigen die Möglichkeit auf das Risiken, von einer oberen Verdichtungsebene, ggf. bis auf die Erfassungsebene, zurückverfolgt werden können. Das Risiko hat eine monetäre Einheit (€). Diese wird bestimmt durch die mögliche Schadenshöhe, die mit anzugeben ist. Eine Verdichtung kann immer nur auf den gleichen Sachverhalt bezogen werden.

© TeleTrusT Deutschland e.V.

Fazit

- Die Risikobetrachtung ist einem starken Wandel im Bereich der operationellen Risiken unterworfen
  - Der Trend geht in Richtung „Risikoquantifizierung“
  - Risikoaggregation ist erforderlich, so bald nicht mehr nur Einzelrisiken von Interesse sind. Damit wird eine Risikoskalierung z.B. nach der Norton Skala obsolet
  - Die Risikosteuerung von Unternehmen setzt sich mehr und mehr auch im Bereich operationelle Risiken (Betriebsrisiken) durch.
  - Da sich Risiko und Sicherheit diametral (*Bernoulli Verteilung*) gegenüber stehen, kann mittels einem Risikomaß auch eine Aussage zur Geschäftssicherheit formuliert werden.
  - Die Vorgehensweise erfordert allerdings gewisse Hintergrundinformationen über die Wahrscheinlichkeitstheorie und deren Anwendung
  - Das Wissen hierüber ist in den Unternehmen noch „*dünn gesät*“
  - Es gibt kaum Schulungsunternehmen die diese Lücke derzeit füllen

© TeleTrusT Deutschland e.V.