TECHNISCHE UNIVERSITÄT DRESDEN

DRESDEN concept

Fakultät Informatik

Professur Softwaretechnologie

SOFTWAREMANAGEMENT

31_RISIKOMANAGEMENT

Prof. Dr. Uwe Aßmann
Dr.-Ing. Birgit Demuth
Sommersemester 2017

Überblick

- Grundlagen
- Risikomanagement-Prozess
- Risikobehandlung und -überwachung

Literatur (1)

- Dieter Köhnlein, Thomas Willert, Thomas Rauschen. Aktuarielle Software für Risikomanagement und Unternehmenssteuerung. Versicherungswirtschaft Heft 20/2006.

  [http://www.risknet.de/typo3conf/ext/bx_elibrary/elibrarydownload.php?&downloaddata=352]

- Werner Gleißner, Frank Romeike. Anforderungen an die Softwareunterstützung für das Risikomanagement. ZfCM – Zeitschrift für Controlling & Management, Gabler Verlag / GWV Fachverlage, Wiesbaden

  [http://www.risknet.de/typo3conf/ext/bx_elibrary/elibrarydownload.php?&downloaddata=190]

Literatur (2)

- Balzert, H. : Lehrbuch der SW-Technik; Bd 2 Spektrum- Verlag 2001
- Wallmüller, E.: Risikomanagement für IT- und Software-Projekte; Hanser Verlag 2004
- http://www.bsi.bund.de/
- http://www.risknet.de
- http://www.mittelstand-digital.de/DE/Wissenspool/elektronischer-zahlungsverkehr.html
- http://www.internet-sicherheit.de/

Grundlagen

Misserfolge internationaler Großprojekte

Projekt	Verspätung	Verlust
Deutsches Mautsystem „Toll Collect“	2 Jahre	rd. € 2,2 Milliarden
„YOU“-Projekt von Bank Vontobel	Abbruch nach 2 J.	CHF 256 Millionen
California PKW-Zulassung	3 Jahre	$ 54 Millionen
American Airlines Autovermietung	7 Jahre	$ 165 Millionen
Denver Flughafen Gepäckverteilung	2 Jahre	$ 750 Millionen
US Bundesfinanzamt Steuer	8 Jahre	$ 1600 Millionen
London, Elektronische Börse	12 Jahre	£ 800 Millionen
London, Krankenwagenleitsystem	5 Jahre	£ 12 Mill. und der Verlust von 46 Leben

Quelle: [Wallmüller, E.]

Die Verantwortung des Software-Ingenieurs

Software Engineering Code of Ethics and Professional Practice (Version 5.2)
[http://www.acm.org/about/se-code]

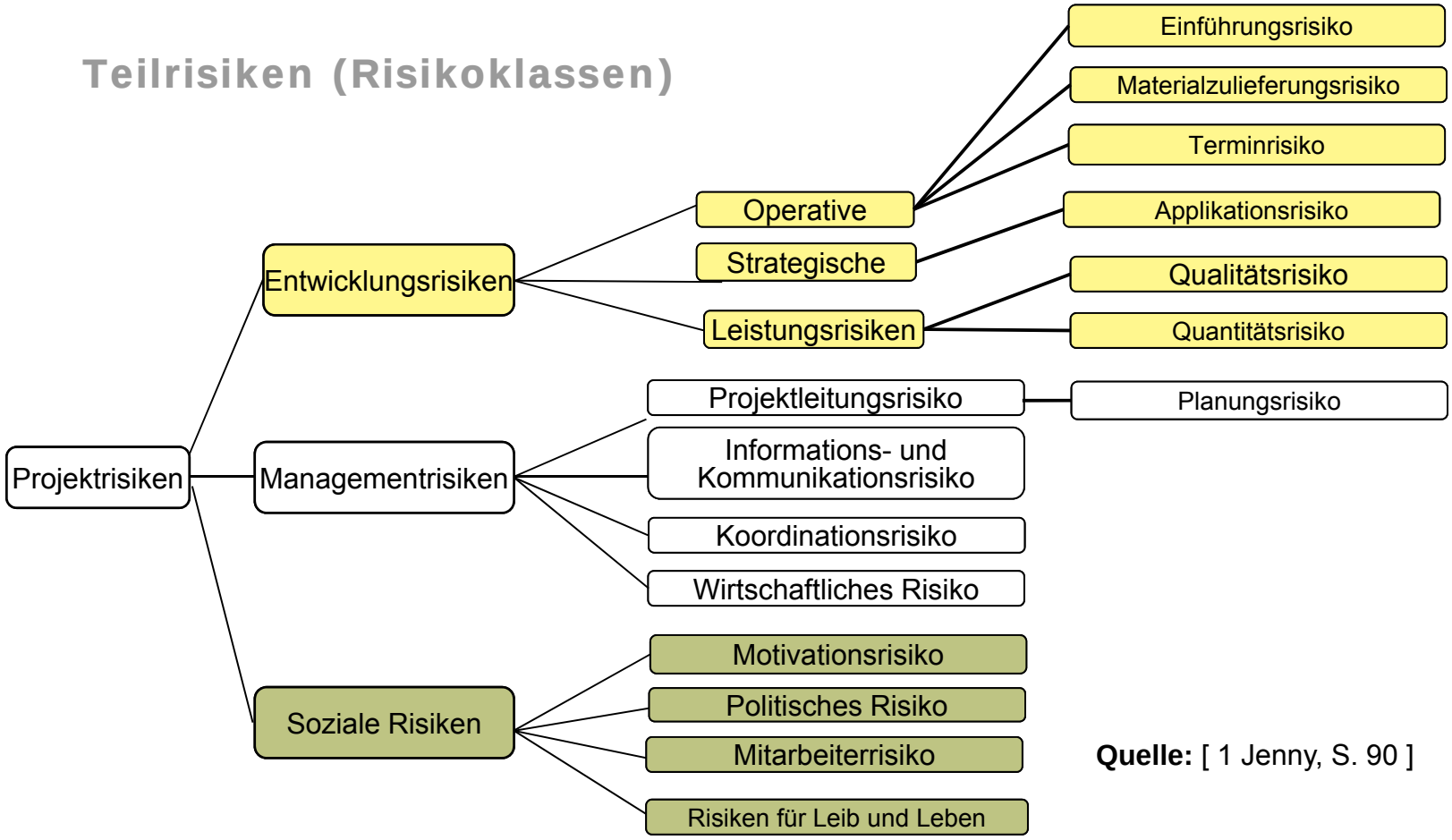
- Principle 1: **PUBLIC -** Software engineers shall act consistently with the public interest.
- Principle 2: **CLIENT AND EMPLOYER -** Software engineers shall act in a manner that is in the best interests of their client and employer, consistent with the public interest.
- Principle 3: **PRODUCT -** Software engineers shall ensure that their products and related modifications meet the highest professional standards possible.
- Principle 4: **JUDGMENT -** Software engineers shall maintain integrity and independence in their professional judgment.
- Principle 5: **MANAGEMENT -** Software engineering managers and leaders shall subscribe to and promote an ethical approach to the management of software development and maintenance.
- Principle 6: **PROFESSION -** Software engineers shall advance the integrity and reputation of the profession consistent with the public interest.
- Principle 7: **COLLEAGUES -** Software engineers shall be fair to and supportive of their colleagues.
- Principle 8: **SELF -** Software engineers shall participate in lifelong learning regarding the practice of their profession and shall promote an ethical approach to the practice of the profession.

Projektrisiken

Unter dem **Projektrisiko** wird die Höhe des Schadens verstanden, den ein Unternehmen erleidet, wenn die **Projektziele nicht erreicht** werden.

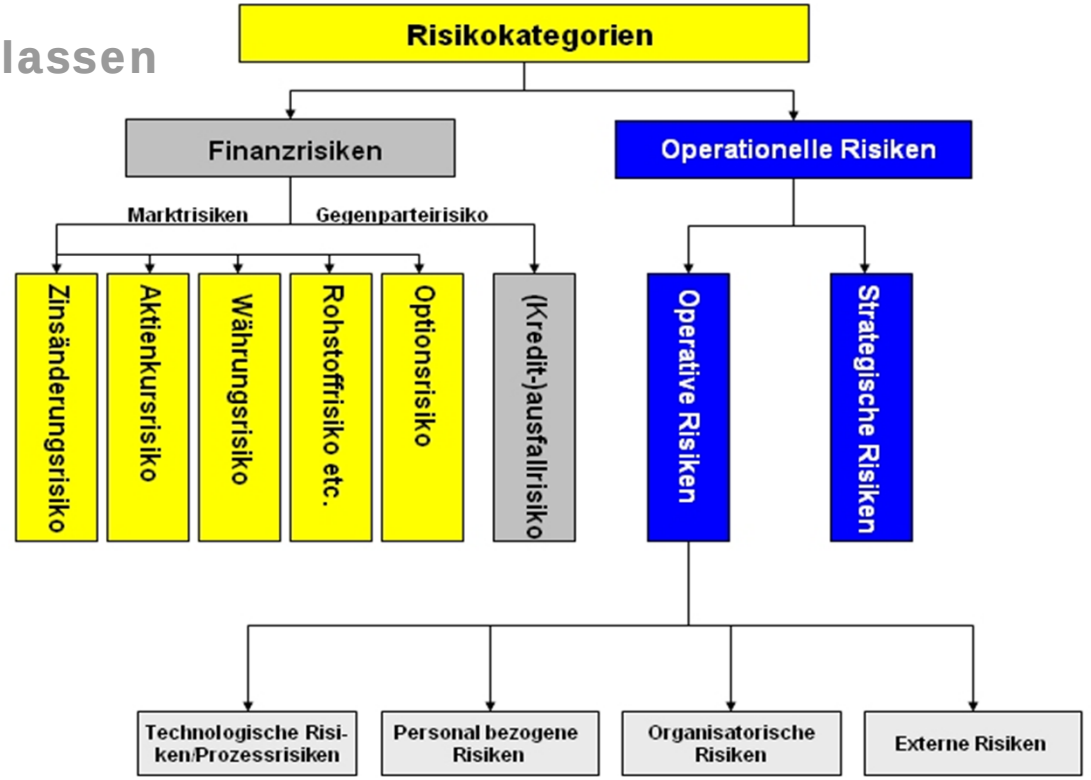
Das **Gesamtrisiko** lässt sich in Teilrisiken zerlegen…

Teilrisiken (Risikoklassen)



Quelle: [1 Jenny, S. 90]

Verfeinerung von Risikoklassen



[http://www.risknet.de/fileadmin/template_risknet/images_content/risikobaum_gr.jpg]

Risikomanagement

Ziel des **Risikomanagements** ist es, die Wechselbeziehungen zwischen Risiken und Erfolg zu formalisieren und in anwendbare Prinzipien und Praktiken umzusetzen.

Aufgabe des Risikomanagements ist es demzufolge

- Risiken zu identifizieren,
- sie zu analysieren,
- sie zu bewerten,
- sie anzusprechen,
- ihre Handhabung zu planen,
- sie zu beseitigen, bevor sie zur Gefahr oder zur Hauptquelle für Überarbeitung werden
- etwaige Schäden zu begrenzen oder beseitigen (Krisenmanagement).

Ein Risiko beschreibt die Möglichkeit, dass eine Aktivität oder ein Objekt einen Schaden haben könnte, dessen Folgen ungewiss sind.

Quelle: [Balzert, S. 176 – 185]

Probleme des Risikomanagement

- Probleme:
  - Risikoverbergung: Risiken werden unter den Teppich gekehrt
  - Informalität: Risikomanagement basiert häufig auf der Intuition der Betroffenen
  - Konzepte der Geschäftsführung sind selten mit gezieltem Risikomanagement auf der operativen Ebene in Projekten oder Organisationen verbunden.
  - Unpopularität: Der Überbringer schlechter Nachrichten wird zwar nicht mehr, wie im alten Griechenland, umgebracht, aber immer noch nicht ernst genommen.
- Notwendig: Schaffung eines effizienten internen Kontrollsystems einschließlich notwendiger Optimierungen
  - Risikobewusstsein und Risikotransparenz verbessern
- Risikomanagement setzt in der Praxis meist erst ein, wenn Risiken aufgrund verursachter Schäden augenfällig werden, d.h. materialisiert sind.
  - Wir sprechen im Falle der eigentlichen Intervention (Schadenbegrenzung, Schaden behebung) von Problem- bzw. Krisenmanagement

Ziele des Risikomanagements

Analyse

- Risiken sichtbar machen: systematisch Risikoursachen identifizieren;
- Potenzielle Gefährdungssituationen möglichst frühzeitig erkennen und erfassen;

Bewertung

- wo Risiken sind, sind auch Chancen;
- Risiken einschätzen und bewerten, um geeignetes Umgehen mit Risiken festzulegen

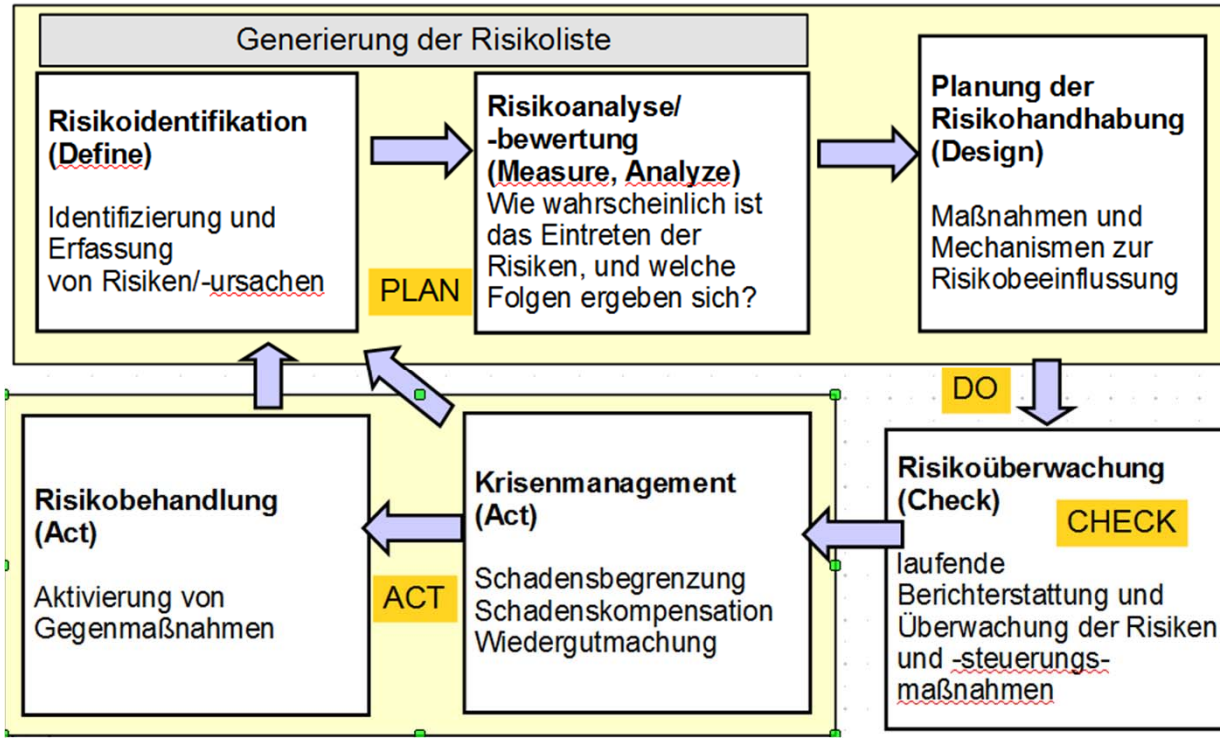
Behandlung bzw. Risikoreduktion

- Risiken kommunizieren und allen Beteiligten bewusst machen;
- Risikobehandlung durchführen

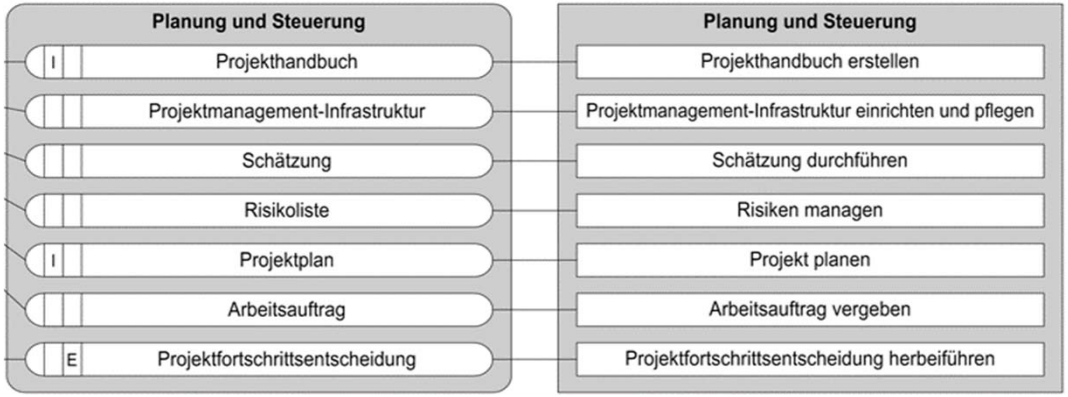
Kontrolle

- Risiken in ihrer Entwicklung verfolgen;
- Risiken eingrenzen und als bewusste Steuerungsgröße des Managements verwenden;
- Hilfsmittel zur Erkennung, Bewertung und Steuerung der Risiken bereitstellen und nutzen.

Risikomanagement-Prozess



Risikomanagement im V-Modell XT (Vorgehensbaustein Projektmanagement)



Produkt **Risikoliste**

Es werden

- die identifizierten Risiken ermittelt
- sie werden fortgeschrieben und verwaltet
- die geplanten Gegenmaßn. festgehalten.

Für die Risikoliste ist der PL verantwortlich

Aktivität **Risiken managen**

vorbeugend, in periodisch kurzen Schritten

- Risiken identifizieren, bewerten, Maßnahmen planen,
- Risiken überwachen und Wirksamkeit der Maßnahmen verfolgen.

Techniken zur Risikoidentifikation

Informell

- Szenariotechnik (Use Case, CRC-Karten)
- Brainstorming
- Strukturierte Interviews/Umfragen
- Workshops (Reviews)
- Checklisten
- Fragebögen

Formell

- Auswertung Planungs- und Controlling-Unterlagen
- Analyse von Prozessabläufen mit Flussdiagrammen, Sequenzdiagrammen u. ä.
- Fehlermöglichkeits- und Einflussanalyse (FMEA)
- Benchmarking

Risikodokumentation in Projekten

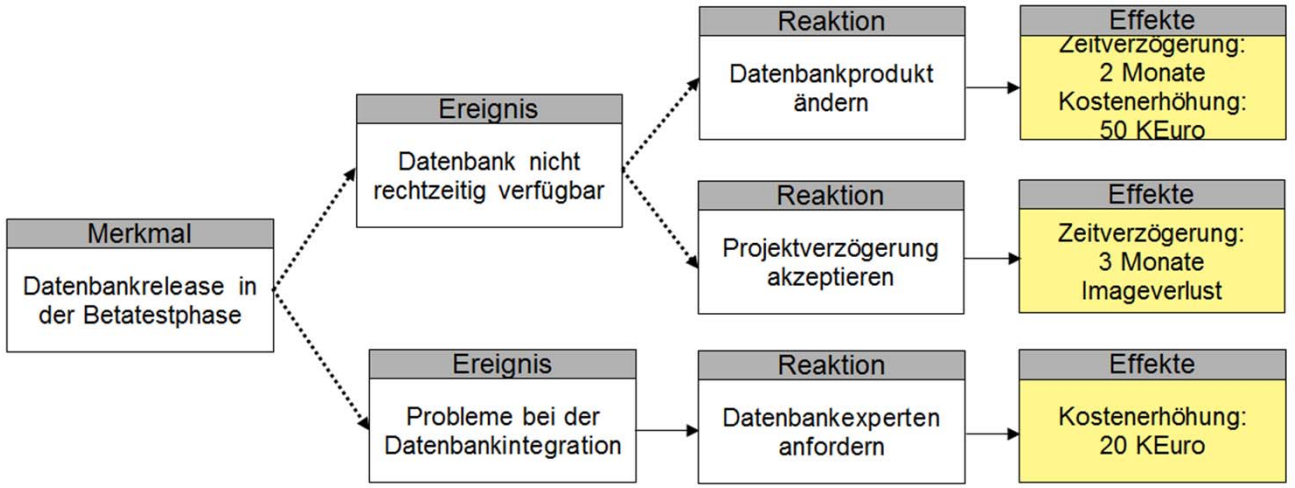
Risikodokumentation mit **Risikolisten**, -**katalogen** oder -**datenbanken**:

- Kurzbeschreibung
- Risikomerkmale
- mögliche technische Ausprägungen
- Alternativen
- zeitliche Lage des Risikos im Projekt

Zusätzlich: **Risiko-Szenario** mit **Ursache-Wirkungs-Graph**:

- Randbedingungen, die zum Eintreten des Risikos führen können
- Auswirkungen auf andere Bereiche des Projektes
- terminliche Auswirkungen

Beispiel eines Risikoszenario mit Ursache-Wirkungs-Graph



Ein Riskoszenario stellt einen ereignisbasierten Ursache-Wirkungsgraph auf:

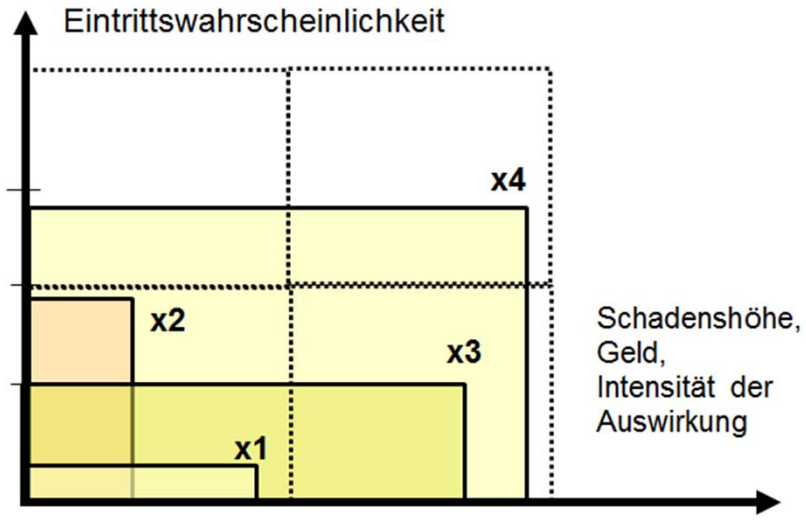
- **Risikomerkmal**: Merkmal mit Wahrscheinlichkeit für negatives Eintretens des Ereignisses
- **Risikoereignis** repräsentiert das Eintreten des negativen Vorfalls
- **Risikoreaktion**: Aktion, die bei Eintreten des Ereignisse ausgeführt wird
- **Risikoeffekt** beschreibt Auswirkungen des Risikoereignisses

Risikoanalyse / -bewertung

- Ziel: Priorisierung der Risikoliste
- Expertenbefragung: Risikodefinition + Risikodiskussion + Risikobewertung (Zeit, Kosten)
- **Eintrittswahrscheinlichkeitkeit** in % gibt an, wie wahrscheinlich ein Risikofall eintritt
- Die **Schadenshöhe** ist Bewertung in Geld: welchen Schaden wird das Risiko verursachen?
- **Risikopriorität** ergibt sich aus **Risikofaktor = Eintrittswkt. x Schadenshöhe**
- **Risikoreduktionskosten** bilden die Kosten der Risikobehandlung
- **Risikoreduktionsnutzen** beurteilt, ob Risikobehandlung sich lohnt

Risikoselektion mit Portfolio-Analyse

- Risikoselektion erfolgt mit Hilfe eines Portfolio aus Eintrittswahrscheinlichkeit und Schadenshöhe
- Der **Risikofaktor** ist die Fläche zwischen dem Ursprung und dem Punkt

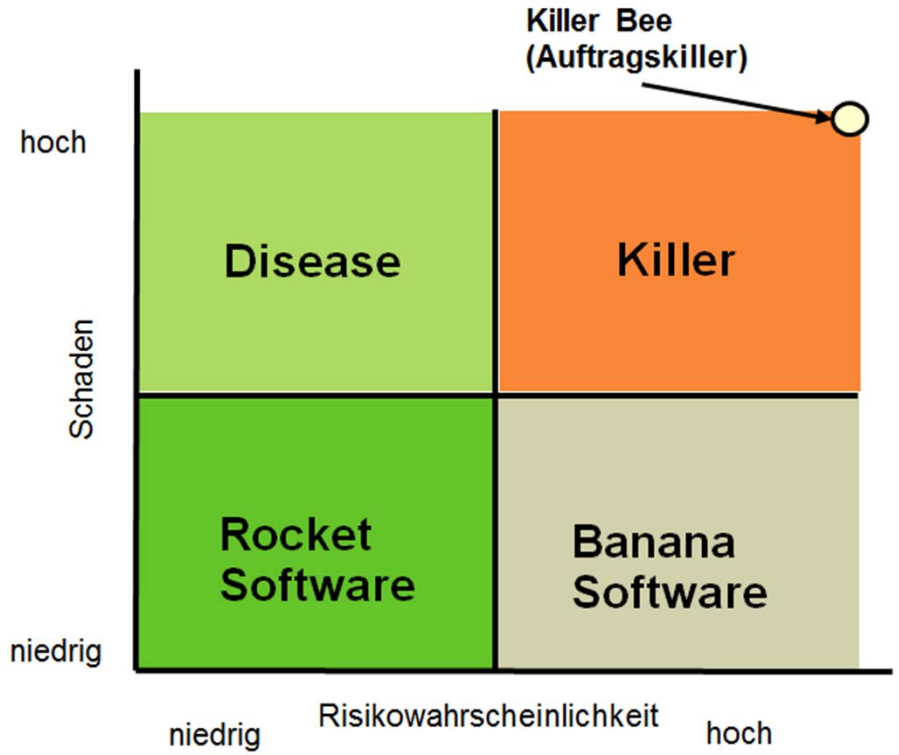


Risikobehandlungsplanung:

- **x1** u. U. Vernachlässigen
- **x2** vertraglich vorsorgen
- **x3** besonders beachten, z.B. mit Risikoversicherung
- **x4** Vorsorge treffen (Risikorückstellung); Risikowahrscheinlichkeit reduzieren

Auftragskiller-Projekte als Klassifikation der Produktrisiken

Die **“Auftragskiller”-Analyse** analysiert die Projekte nach **Produktrisiken**



Risikoreduktionsnutzen

Der **Risiko-Reduktions-Nutzen (RRN)** charakterisiert die Verbesserung des Risikofaktors im Verhältnis zu den Reduktionskosten

$$RRN := \frac{(RF'pre - RF'post)}{RRK}$$

RF'pre: Risikofaktor vor den Maßnahmen zur Reduzierung
RF'post: Risikofaktor nach diesen Maßnahmen
RRK: Risiko-Reduktionskosten

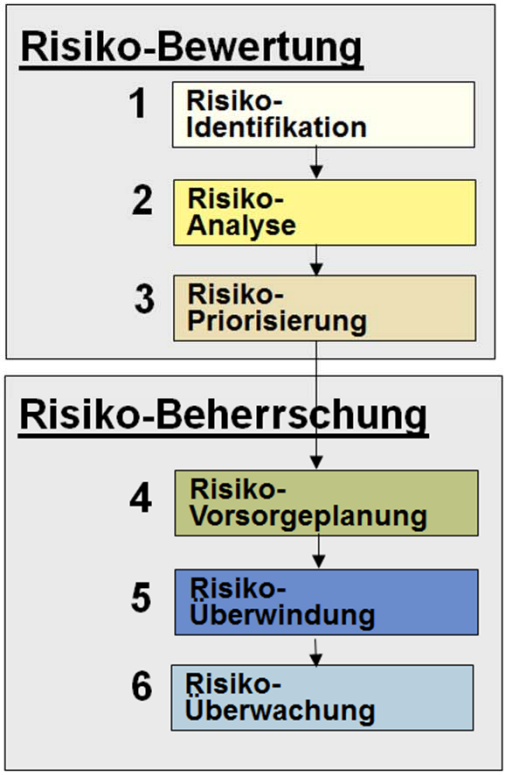
Beispiel: Schnittstellenfehler mit 30% Wahrscheinlichkeit würde Kosten von 1 M€ verursachen
Behandlung a) Senkung der Wahrscheinlichkeit auf 10% durch ein SS-Prüfprogramm von 20 000 €
Behandlung b) Senkung auf 5% durch ausgiebigen Test der Schnittstelle, Kosten = 200 000 €

RRN(a) = (1 M € * 0,3 - 1 M€ * 0,1) **:** 20 000 € = 10
RRN(b) = (1 M€ * 0,3 - 1 M€ * 0,05) **:** 200 000 € = 1,25

Top 10 Elemente der Risikoanalyse

#	Risikoelement	Risikomanagement-Techniken (Beispiele)
1	Personelle Defizite	Hochtalentierte Mitarbeiter einstellen, Teams zusammenstellen
2	Unrealistische Termin- und Kostenvorgaben	Detaillierte Schätzung mit mehreren Methoden, Inkrementelle Entwicklung, Wiederverwendung von Software, Anforderungen streichen
3	Entwicklung von falschen Funktionen und Eigenschaften	Benutzerbeteiligung, Prototypen, Frühzeitiges Benutzerhandbuch
4	Entwicklung der falschen Benutzungsschnittstelle	Prototypen, Aufgabenanalyse, Benutzerbeteiligung
5	Vergolden	Anforderungen streichen, Prototypen, Kosten/Nutzen-Analyse
6	Kontinuierliche Anforderungsänderungen	Hohe Änderungsschwelle, Inkrementelle Entwicklung (Änderungen auf spätere Erweiterungen verschieben)
7	Defizite bei extern gelieferten Komponenten	Leistungstest, Inspektionen, Kompatibilitätsanalyse
8	Defizite bei externen Aufträgen	Prototypen, Frühzeitige Überprüfung, Verträge auf Erfolgsbasis
9	Defizite in der Echtzeitleistung	Simulation, Prototypen, Leistungstest, Instrumentierung, Modellierung, Tuning
10	Überfordern der Softwaretechnik	Technische Analyse, Kosten/Nutzen-Analyse, Prototypen

Schritte des Risikomanagements nach Balzert



Quelle: [Balzert, S. 176 – 185]

Risikobehandlung und -überwachung

- Werkzeuge zur Risikobehandlung
- Paradoxon der Risikobehandlung
- Primäre Maßnahmen
- Sekundäre Maßnahmen
- Risikoüberwachung

Werkzeuge zur Risikobehandlung

- Die meisten Werkzeuge haben sich aus firmeninternen Vorgehensweisen zur Behandlung des Risikomanagements entwickelt
- Werkzeuge sind ähnlich zu Anforderungsmanagementsystemen oder Bugtracking-Systemen zu sehen
  - Risikopläne (einfache Dokumente)
  - Risikodatenbanken (verteiltes Risikomanagement)
  - Erweiterung von Projektmanagement-Werkzeugen um Komponenten zur Risikoanalyse und –überwachung
  - z.B. Microsoft Project erweitert um Add-In @RISK [http://www.palisade.com/risk/]
  - Weitere sind enthalten in der Übersicht [http://www.risknet.de/marktplatz/loesungsanbieter/]

Paradoxon der Risikobehandlung

- Risiken **unterschätzt**: Schaden tritt ein
  → Frust

- Risiken **überschätzt**: Vermeidbare Kosten; Verlust von Chancen
  → Frust

- Risiken **richtig eingeschätzt**: Nutzen nicht beweisbar, nachlassendes Risikobewusstsein
  → Frust

Primäre Maßnahmen

Primäre Maßnahmen sind vorbeugende Maßnahmen (“Risk mitigation plans”) zur Behandlung der Risikowahrscheinlichkeit bzw. Risikoeintritts

- **Risikovermeidung** ist kostenintensiv und wird nur praktiziert, wenn bei anderen Vorgehensweisen inakzeptables Gefahrenpotential verbleiben würde.
- **Risikoverminderung** beabsichtigt eine geringe Eintrittswahrscheinlichkeit und/oder einen geringen Schadensumfang im Eintrittsfall.

Beispiele für primäre Maßnahmen bei …

(1)technischen Risiken:	Simulation, Prototyping, Beratung,Reviews, Suche nach alternativen Konzepten, Erprobung von neuen Werkzeugen
(2)Risiken bezüglich Anforderungen/Kunden:	Verstärktes Bemühen um den Kunden, Kontaktpflege, Kundenworkshops, frühzeitige Abnahme von Zwischenergebnissen vereinbaren, Pflichten des Kunden vertraglich absichern
(3)Ressourcenproblemen:	Schulung/Coaching von Mitarbeitern/Projektleitern, Mitarbeitereinsatz in ähnlichen Projekten, Ressourcenzusage mit Management diskutieren
(4)Sonstiges:	Preisaufschläge einkalkulieren, Outsourcen von Risiken an Subunternehmer

Sekundäre Maßnahmen

Sekundäre Maßnahmen sind Maßnahmen zur Schadensbehandlung bzw. Kompensation

- **Risikostreuung** bedeutet eine Verteilung der Risiken, z.B. eine Verteilung von Aktien auf unterschiedliche Unternehmen bei Kapitalanlagen.
- **Risikoverlagerung (-ausschluss)** kann durch Vertragsbedingungen, z.B. Verlagerung der Risiken auf Lieferanten, Unterauftragnehmer usw. erreicht werden
- **Risikoversicherung** ist eine sichere aber auch sehr teure Form der Risikohandhabung (Kosten-/ Nutzenanalyse), u.U. mit Selbstbeteiligung
- **Notfallmaßnahmen** (“Contingency plans) für Risiken, die bewusst eingegangen werden
- **Risikoübernahme / Risikoakzeptanz** heißt, das Unternehmen akzeptiert das bestehende Risiko und trägt die Schäden der verbleibenden Risiken im Eintrittsfall.

Beispiel Notfallmaßnahmen

Aufbau von Rückzugspositionen bei technischen Risiken, z.B.

- Statt der Neuentwicklung alte SW-Komponenten einsetzen
- Alternative SW- oder HW-Konzepte bei Performanceproblemen
- Bei drohenden Versagen von Zukaufprodukten: Alternativen in der Hinterhand haben

Beispiele für Versicherungen

- Datenträger-Versicherung
- Haftpflichtversicherung
- Elektronikversicherung

Datenträger-Versicherung

Eine **Datenträger-Versicherung** versichert das Nichtfunktionieren der Datensicherung

- Wiedereingabe der Daten, z. B. 5 000 € für Wiedereingabe von 1MByte
- Wiederbeschaffung der Software und Daten
- Folgeschäden sind nicht versichert

Schäden werden ersetzt bei

- falsches oder zerstörtes Backup
- Störung oder Ausfall der DV-Anlage, der DFÜ, Stromvers., Klimaanl.
- Bedienungsfehler (falsche DT, falsche Befehlseingabe)
- Vorsatz Dritter (Sabotage, Progr.- oder Datenmanipulation, Hacker, Viren, Einbruch)
- Über- oder Unterspannung, elektrostat. Aufladung, elektromagn. Störung
- höhere Gewalt (Blitz, Hochwasser, Brand, ...)

Haftpflicht-Versicherung

Produkthaftung: der Hersteller ist für das Versagen seiner Produkte verantwortlich

- Personenschäden (können bei eingebetteter Software entstehen, wie Auto, Flugzeug, Bahn, U-Bahn)
- Sachschäden
- Ausfälle oder entgangene Gewinne (falls Produkt nicht rechtzeitig fertig wird)

Versicherungsarten am Beispiel einer Elektronikversicherung

(1) Sachträgerversicherung
→ Ersatz zum Nennwert der Anlage (Schaden durch Einwirkung von außen), Erweiterung: Leihgerät während Reparatur

(2) Datenträgerversicherung
→versichert ist nur das Nichtfunktionieren der eigenen Datensicherung

(3) Softwareversicherung
→ Bei Verlust /Veränderung auch ohne Sachschaden. Bsp.: DFÜ, Bedienfehler, Viren, Manipulation Dritter. Leistung: Kosten der Wiederherstellung

(4) Versicherung externer Netze

(5) Mehrkostenversicherung
→ z.B. Mehrkosten für ein Ausweichkonzept (Anmietung, Gebäude, Personal u.a.), max. 1 Jahr

(6) Elektronik-Betriebsunterbrechungs-Versicherung
→ für Folgeschäden eines sachschadenbedingten Ausfalls, wenn Ausweichmaßnahmen nicht möglich, für entgangenen Gewinn u. fortlaufende Kosten

Risikoüberwachung

Kontrollmaßnahmen

- regelmäßige Verfolgung des Projektfortschritts (Terminüberwachung) zu festgelegten Zeitpunkten
- Fortschritts- und Abweichungsberichte
- personelle und finanzielle Aufwandskontrolle
- regelmäßige Berichterstattung der für die Maßnahme Verantwortlichen
- Erkennen möglicher Veränderungen von Risikosituationen
- Aufzeigen von Sachverhalten, die Schadenshöhe und Eintrittswahrscheinlichkeit verändern
- Verfolgung der Top 10 Risiken

Ende

TECHNISCHE UNIVERSITÄT DRESDEN

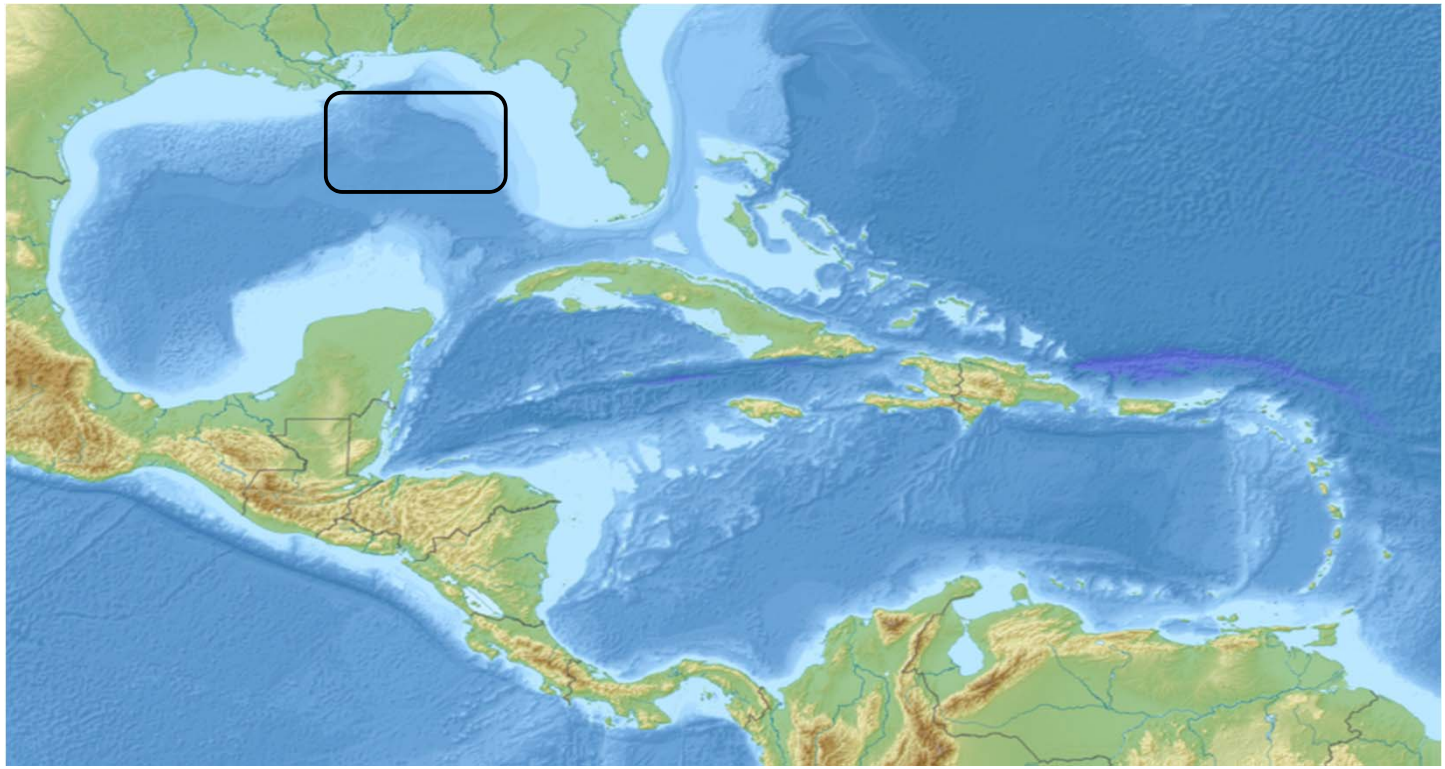
DRESDEN concept

Professur Softwaretechnologie

BACKUP

Prof. Aßmann SS 2016

- 5-6 Mrd Barrel (riesig) (Nordsee: 2,1 Mrd Barrel)



http://upload.wikimedia.org/wikipedia/commons/thumb/2/2c/Middle_America_relief_location_map.png/800px-Middle_America_relief_location_map.png

Explorationsplattform

Deepwater Horizon

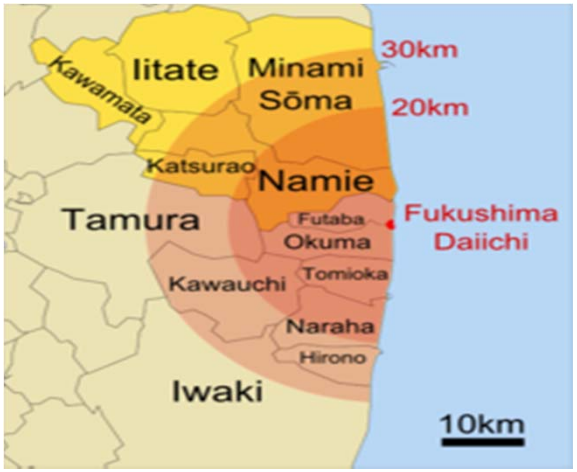
- 2.9.2009, Tiber-Ölfeld vor dem Missisippi-Delta: Meerestiefe 1250m, Tiefe 10685m
  - Oft Gaseinbrüche während der Bohrungen
  - BP-Manager bestanden darauf, einen zweiten Zement-Verschlussstopfens gegen Wasser zu tauschen (Kosten)
- 20.4.2010: Explosion beim Zementieren des Bohrloches, kurz vor Verschluß
  - Während einer Party für das 7jährige sichere Betreiben
  - Methangasexplosion aus eisförmigem Methanhydrat stammend, das im Ölfeld und auf dem Meeresgrund vorhanden ist
  - Angeblich 40% des Öls waren Methan (normal: 5%)
- Der Blow-out Preventer (BOP) versagte (7 min nach Explosio
  - Dichtgummi beschädigt, leere Batterien
  - Kontrollsystem außer Kraft gesetzt
- kein Verschlußsystem vorhanden

Menschliches Versagen

http://en.wikipedia.org/wiki/Deepwater_Horizon_explosion
http://de.wikipedia.org/wiki/Deepwater_Horizon

Fukushima Nuclear Desaster

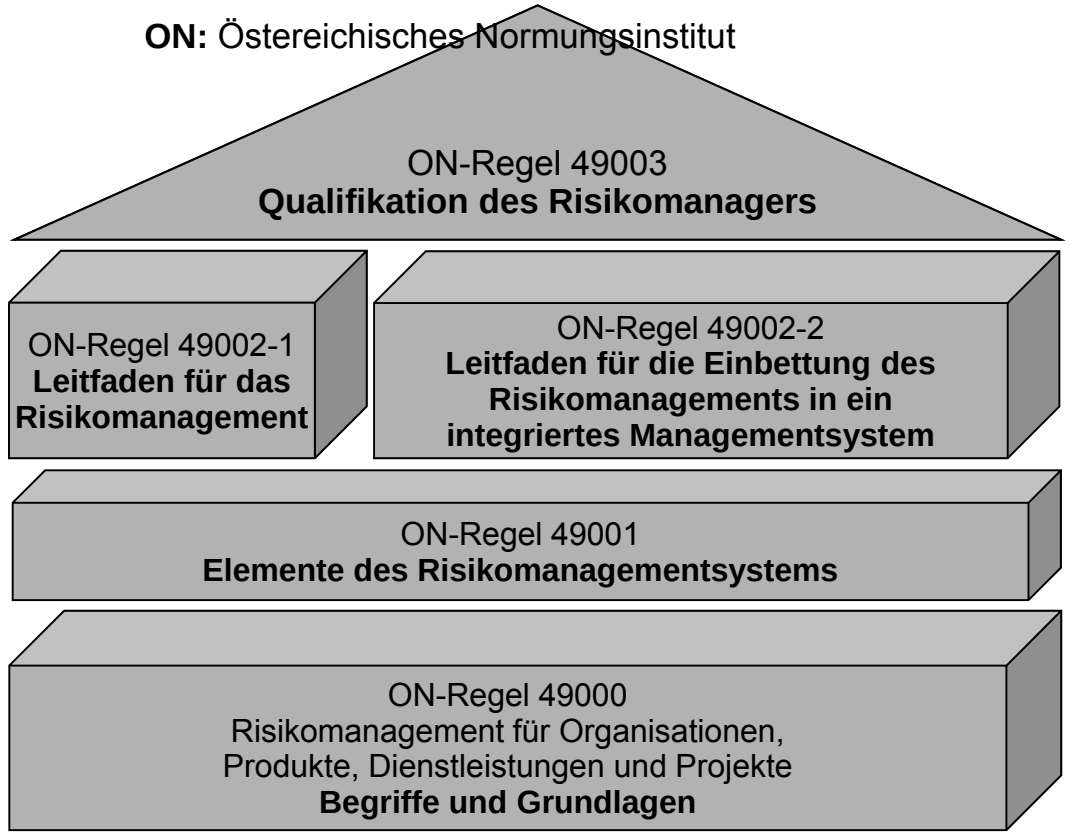
Fehler: Wälle waren nur 7m hoch, Tsunami 13m



http://en.wikipedia.org/wiki/2011_T%C5%8Dhoku_earthquake_and_tsunami

http://en.wikipedia.org/wiki/Fukushima_Daiichi_nuclear_disaster

- Atomenergie ist billig, solange man die Unfälle und die Abfälle nicht betrachtet
  - Unfall Fukushima wegen verkehrter Einschätzung der Natur
  - Unfall Tschernobyl wegen Leichtsinn
  - Müll: Mehrere 1000 Jahre Halbwertszeit
  - Wie den Müll lagern und sichern?
- Schadenshöhe:
  - Tschernobyl: ?? etliche Tote bei der Rettung
  - 1 Mrd. $ bei Kernschmelze in Harrisburg Three Mile Island, 1979, keine Tote
  - Fukushima sicher mehr als 25 Mrd, keine Tote
- Eintrittswahrscheinlichkeit:
  - Deutschland kehrt sich von der Kernenergie ab, weil die Eintrittswahrscheinlichkeit für Unfälle verkehrt eingeschätzt wurde (Kanzlerin Merkel, März 2011)



Quelle: [Wallmüller, E. S.9]

http://www.risknet.de/wissen/grundlagen/risk-management-standards/on-regelwerk-risikomanagement-des-oesterreichischen-normungsinstituts/

Kritikalitätsklassen für Risiken

Kritikalität	***Art des Fehlverhaltens*** (**für Informationssysteme**)
hoch	Fehlverhalten macht sensitive Daten für unberechtigte Personen zugänglich oder verhindert administrative Vorgänge (z. B. Gehaltsauszahlung, Mittelzuweisung) oder führt zu Fehlentscheidungen infolge fehlerhafter Daten
niedrig	Fehlverhalten verhindert Zugang zu Informationen, die regelmäßig benötigt werden
keine	Fehlverhalten beeinträchtigt die zugesicherten Eigenschaften nicht wesentlich

Kritikalität	***Art des Fehlverhaltens*** (**für eingebettete Systeme**)
hoch	Fehlverhalten kann zum Verlust von Menschenleben führen
mittel	Fehlverhalten kann die Gesundheit von Menschen gefährden oder Zerstörung von Sachgütern führen
niedrig	Fehlverhalten kann zur Beschädigung von Sachgütern führen, ohne jedoch Menschen zu gefährden
keine	Fehlverhalten gefährdet weder die Gesundheit von Menschen noch Sachgüter

Quelle: [Balzert, S. 296]

Kritikalitätseinstufung

Beispiel einer projektspezifischen Kritikalitätseinstufung für eine

Realzeitanwendung (z. B. Flugsicherung, fly-by-wire, drive-by-wire)

Kritikalität	***Art des Fehlverhaltens***
hoch	Fehlverhalten, das zu fehlerhaften Positionsangaben der Flugobjekte am Kontrollschirm führen kann
niedrig	Fehlverhalten, das zum Ausfall von Plandaten und damit zu Abflugverzögerungen führen kann
keine	alle übrigen Arten von Fehlverhalten

Maßnahmen zur Abwehr der Auswirkung von Fehlverhalten

Konstruktive Maßnahmen:
Entwicklung von eigensicheren bzw. fehlertoleranten Funktionseinheiten,
Konfigurierung von redundanten oder diversitären Funktionseinheiten (unter diversitär wird in diesem Zusammenhang die Realisierung redundanter Funktionseinheiten durch unterschiedliche Algorithmen oder physische Prinzipien verstanden)

Analytische Maßnahmen:
Durchführung umfangreicher Verifikation und Validation bis zur Zertifikationsreife

Quelle: [Balzert 96]

- Explain the process of risk management
- How are risks analysed? How are they prioritzed?
- Explain the risk reduction formula
- Explain the difference of primary and secondary risk mitigation

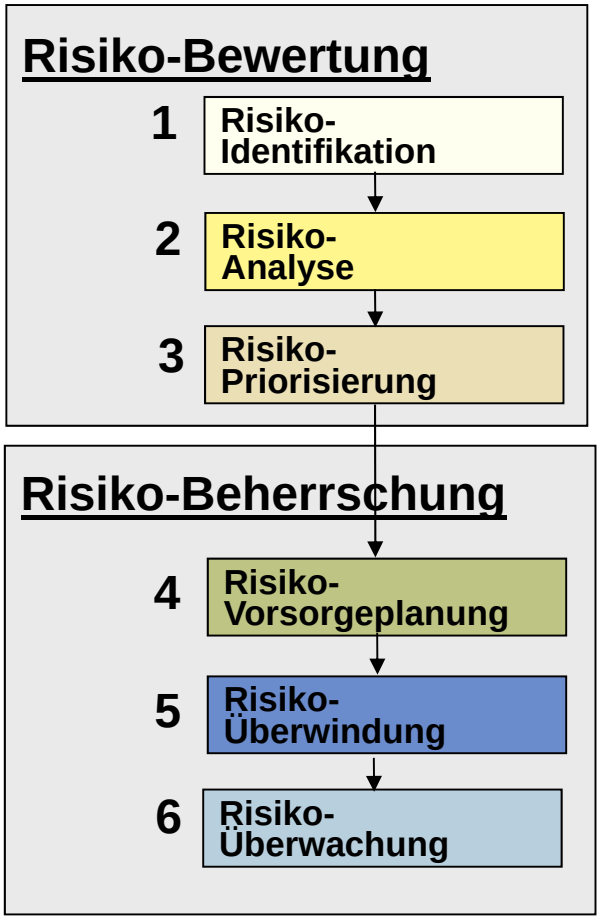
- **Risikohandhabung** gliedert sich in primäre und sekundäre Maßnahmen
- **Primäre Maßnahmen** sind **echte Vorbeugungs-Maßnahmen** zur Behandlung der Risikowahrscheinlichkeit bzw. Risikoeintritts
  - ***Risikovermeidung*** ist kostenintensiv und wird nur praktiziert, wenn bei anderen Vorgehensweisen inakzeptables Gefahrenpotential verbleiben würde.
  - ***Risikoverminderung*** beabsichtigt eine geringe Eintrittswahrscheinlichkeit und/oder einen geringen Schadensumfang im Eintrittsfall.
- **Sekundäre Maßnahmen** sind **Maßnahmen zur Schadensbehandlung** bzw. **Kompensation:**
  - ***Risikostreuung*** bedeutet eine Verteilung der Risiken, z.B. eine Verteilung von Aktien auf unterschiedliche Unternehmen bei Kapitalanlagen.
  - ***Risikoverlagerung (-ausschluss)*** kann durch Vertragsbedingungen, z.B. Verlagerung der Risiken auf Lieferanten, Unterauftragnehmer usw. erreicht werden
  - ***Risikoversicherung*** ist eine sichere aber auch sehr teuere Form der Risikohandhabung (Kosten-/ Nutzenanalyse), u.u. mit Selbstbeteiligung
  - Risiken, für die **Risikovorsorgen** (Rücklagen) bilden sind (bewusst eingegangen)
  - ***Risikoübernahme/Risikoakzeptanz*** heißt, das Unternehmen akzeptiert das

Quelle: [Mayr, S. 176 – 186]

31 2 5 Risikobehandlung

- Risikobehandlung durch die geplanten sekundären Maßnahmen (Gegenmaßnahmen):
  - Initiieren von Notfallmaßnahmen
  - Risikoversicherung: Information von Versicherungen
    Dokumentation von Schäden
  - Risikoverlagerung: Formulierung von Regressansprüchen
- Krisenmanagement
  - Begrenzung von Schäden
  - Wiedergutmachung von Schäden

Schritte des Risikomanagements nach Balzert



Quelle: [Balzert, S. 176 – 185]

31.5 Krisenmanagement, hier bei Entwicklungsrisiken

Entwicklungsrisiken

- Operative Risiken: Planabweichung (Terminverzögerung, Kostensteigerung, Qualitätsmängel)
  - Setze mehr Personal und andere Resourcen ein (Vorsicht, keine Proportionalität!)
  - Delegiere an Unteraufträge
  - Nehme finanziellen Verlust in Kauf und kompensiere im Multiprojektmanagement
  - Nehme nach Gummitwist-Quadrat Reduktion der Leistung in Kauf
  - Spreche mit Kunden

31.3. Primäre Risikobehandlung - Risikoverminderung am Beispiel eines IT-Sicherheitskonzeptes

BSI = Bundesamt für Sicherheit in der Informationstechnik (BSI)

IT-Grundschutzhandbuch

zur Erstellung von IT-Sicherheitskonzepten

http://www.bsi.bund.de

http://www.bsi.bund.de/gshb

Schritte einer IT-Sicherheitskonzeption (Sicherheitsrichtlinie)

1) Ermittlung der **Schutzbedürftigkeit** des Unternehmens (Schadensanalyse)
    1) Möglichen Schaden für das Unternehmen durch Vertraulichkeits- und Integritätsverlust
2) **Bedrohungsanalyse**
    1) Hardware, Software, Datenträger ==> Szenarien durchspielen,
    2) Sicherheitslücken im **Schwachstellenkatalog** beschreiben
    3) **Mis-Use-Diagramme** aufstellen (siehe Softwaretechnogie-II)
    4) **Attacker-Models** erstellen
3) **Risikoanalyse**
    1) Risikoidentifikation: Mängel ermitteln in der Absicherung wie Internetzugänge, Standleitungen usw.
        1) Abschottungen definieren zwischen Unternehmenszweigen bzw. kritischen Bereichen wie Geschäftsführung, Forschungsabteilungen, Buchhaltung oder Personalwesen
    2) Risikofaktoren ermitteln
4) Erstellung des **IT-Sicherheitskonzeptes** als Risikovorsorgeplanung
    1) Bedrohungspotentiale unterteilen in **tragbare** und **nicht tragbare** Risiken
    2) technische und organisatorische **Risiko-Behandlungsmaßnahmen**, die die Risiken auf ein tolerierbares Niveau reduzieren, Auflistung von Restrisiken

2.1 Bedrohungsanalyse: Grundbedrohungen

- a) Verlust der **Verfügbarkeit** (des IT-Systems, von Inf. bzw. Daten)
- b) Verlust der **Integrität** (Modifizierung von Programmen und Daten nur durch Befugte, ordnungsgemäße Verarbeitung und Übertragung)
- c) Verlust der **Vertraulichkeit** (von Informationen/Daten, Programmen, z. B. bei geheimzuhaltenden Verfahren)
- Bedrohungen setzen an Objekten an und können über Objekte Schaden anrichten, also Schutz der Objekte gegen Bedrohungen.

Sicherheitsgrundfunktionen zur Sicherung gegen Grundbedrohungen

- **Identifikation** und **Authentisierung**
- **Rechteverwaltung** und -**prüfung**
- **Beweissicherung** durch Aufzeichung
- **Fehlerüberbrückung** und Gewährleistung der Funktionalität (Verfügbarkeit des Systems oder spezieller Funktionen, z. B. bei Gefährdung von Menschen: Luftverkehr, Kraftwerke, ...)
- **Übertragungssicherung** (Anforderungen an Kommunikationspartner, Übertragungswege, Vorgang der Übertragung, ...)

- Tool zur Analyse des IT-Grundschutzes
  - https://www.bsi.bund.de/DE/Themen/weitereThemen/GSTOOL/gstool_node.html

Objektgruppen, die Risiken auslösen

Infrastruktur		IT-Räume, Aufbewahrungsräume Stromversorgung, Klima, Zutrittskontrolle, Feuerschutz, ...
Materielle Objekte	**Hardware**	Benutzerterminal, wechselbare Speicher Nutzerzugang, ...
	Datenträger	Ur-Versionen, Anwendungs-Software, Sicherungskopien, ...
	Paperware	Bedienungsanleitungen, Betriebsvorschr. für Normalbetrieb und Notfall, Protokoll-ausdruck, Anw.-Ausdruck
Logische Objekte	**Software**	Anw.-Software, Betriebssystem-SW, Zusatz-Software
	Anw.-Daten	Eingabe, Verarbeitung, Speicherung, Ausgabe, Aufbewahrung
	Kommunikation	Dienstleistungsdaten (Nutzer-), Netzsteuerungsdaten
Personelle	**Personen**	betriebsnotwendige Personen.

4 Erstellung IT-Sicherheitskonzept

- Ziel: IT-Sicherheitskonzept mit
  - Ordnung der Maßnahmen mit Prioritäten
  - personeller Verantwortung
  - Zeitplan zur Realisierung der Maßnahmen
  - Hinweisen zur Überprüfung auf Einhaltung der Maßnahmen
  - Zeitpunkt zur Überprüfung des IT-Sicherheitskonzepts

- Schritte zur Erstellung des Sicherheitskonzeptes
  - **a) Auswahl von Maßnahmen**
  - **b) Bewertung der Maßnahmen**
  - **c) Kosten-/Nutzen-Analyse**
  - **d) Restrisikoanalyse**

4a) Maßnahmenbereiche strukturieren sich anhand der Objektgruppen**:**

- **Infrastruktur:** Bauliche und infrastrukturelle Maßnahmen
  (Gelände, Gebäude, Fenster, Türen, Decken, ...)
- **Organisation:** Regelung von Abläufen und Verfahren
  Einsatz eines IT-Sicherheitsbeauftragten
- **Personal:** Schulung, Motivation, Sanktionen, …
- **Hardware/Software:** Identifikation, Authentisierung,Zugriffskontrolle, Beweissi
  Wiederaufbereitung, Übertragungssicherheit
- **Kommunikations-technik:** z. B. Verschlüsselungsverfahren zur Wahrung von Integrität und Vertraulichkeit
  Virenschutz-Software, Firewalls
  Wahl von sicheren Passwörtern
  Verschlüsselung von Datenträgern
  Digitale Signaturen, Digitaler Personalausweis
- **Abstrahlschutz:** gegen missbräuchlichen Gewinn von Informationen
- **Notfallvorsorge:** Wiederherstellung der Betriebsfähigkeit nach Ausfall
- **Versicherungen:** - von Hardware (Elektronik-Sachversicherung), für Datenträg
  - gegen Folgeschäden von Betriebsunterbrechungen

- **4b) Bewertung der Maßnahmen:**
  - Beschreibung des Zusammenwirkens der Maßnahmen mit Ursache-Wirkungsanalyse
  - Überprüfung der Auswirkungen auf den Betrieb des IT-Systems
  - Überprüfung auf Vereinbarkeit mit Vorschriften (A-Recht, Datenschutz)
  - Bewertung der Wirksamkeit der Maßnahmen

- **4c) Kosten / Nutzen-Analyse:**
  - Kosten der Maßnahmen (Risikoreduktionskosten)
  - Verhältnis Kosten/Nutzen (Risikoreduktionsnutzen feststellen)

- **4d) Restrisikoanalyse:**
  - sind die Restrisiken tragbar?
- evtl. zurück zu a)

Referenzen

- Datensicherung

http://www2.ec-kom.de/ec-net/20100804_Flyer_10_Praxistipps_Sicherheit.pdf

- Laptop-Sicherheit
- http://www2.ec-kom.de/ec-net/20100728_WLAN-Sicherheit.pdf
- http://www2.ec-kom.de/ec-net/20100804_Flyer_10_Praxistipps_Sicherheit.pdf
- Umfrage Computer-Spionage
- http://www.ec-net.de/EC-Net/Navigation/root,did=372400.html

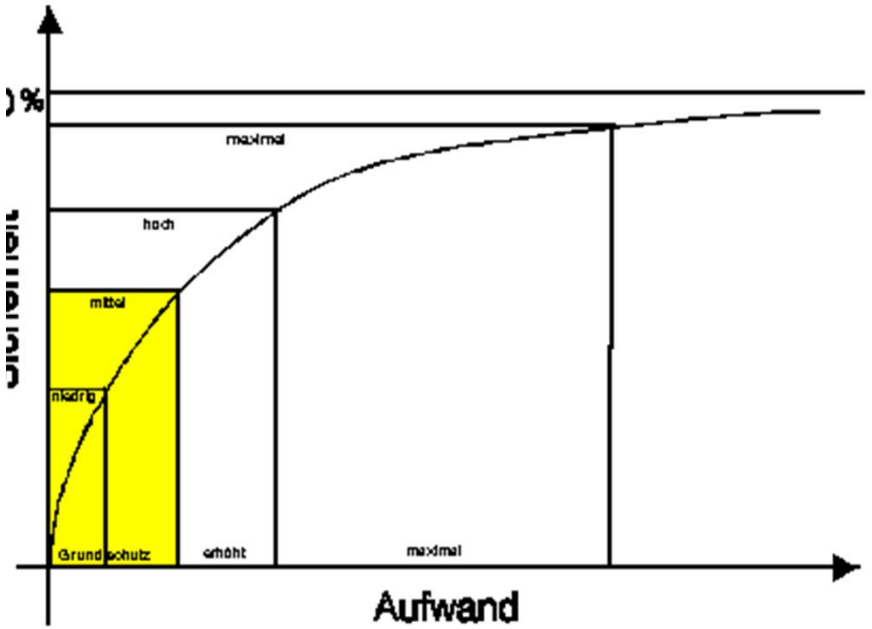
IT-Sicherheitsniveaus laut BSI

Maximal:
Schutz vertraulicher Informationen
Informationen im höchsten Maße korrekt
Zentrale Aufgaben ohne IT-Einsatz nicht durchführbar.
Knappe Reaktionszeiten für kritische Entscheidungen
Ausfallzeiten sind nicht akzeptabel.

Hoch:
Der Schutz in sicherheitskritischen Bereichen stärker
Die verarbeiteten Informationen müssen korrekt sein
Fehler erkennbar und vermeidbar
In zentralen Bereichen laufen zeitkritische Vorgänge
oder es werden dort Massenaufgaben bearbeitet
es können nur kurze Ausfallzeiten toleriert werden.

Mittel:
Kleinere Fehler können toleriert werden, Fehler,
die die Aufgabenerfüllung erheblich beeinträchtigen,
müssen jedoch erkenn- oder vermeidbar sein.
Längere Ausfallzeiten sind nicht zu tolerieren.

Niedrig:
Vertraulichkeit von Informationen ist nicht gefordert.
Fehler können toleriert werden, solange sie die
Erledigung der Aufgaben nicht unmöglich machen;
längere Ausfallzeiten sind jedoch hinnehmbar.



Quelle: http://www.bsi.bund.de/

Datensicherungskonzept

Durch technisches Versagen, versehentliches Löschen oder Manipulation

können gespeicherte Daten unbrauchbar werden bzw. verloren gehen.

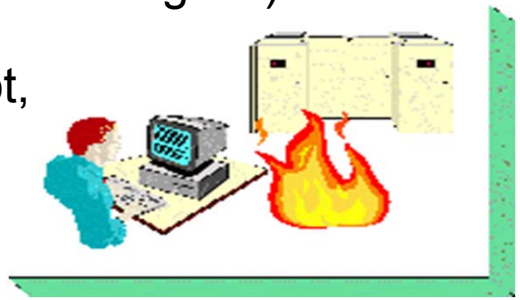
- Entmagnetisierung von magnetischen Datenträgern durch Alterung oder durch ungeeignete Umfeldbedingungen (Temperatur, Luftfeuchte),
- Störung magnetischer Datenträger durch äußere Magnetfelder,
- Zerstörung von Datenträgern durch höhere Gewalt wie Feuer oder Wasser,
- versehentliches Löschen oder Überschreiben von Dateien,
- technisches Versagen von Peripheriespeichern (Headcrash),
- fehlerhafte Datenträger,
- unkontrollierte Veränderungen gespeicherter Daten (Integritätsverlust),
- vorsätzliche Datenzerstörung durch Computer-Viren

Ziel: kurzfristige Wiederaufnahme des IT-Betriebes durch redundanten Datenbestand

Maßnahmen gegen Datenverlust

- Maßnahmebündel für den IT-Grundschutz:
  - Organisation
  - Personal (Verpflichtung, Vertretung, Schulung, Verfahren beim Ausscheiden usw.)
  - Gebäude, Verkabelung,
  - Büroraum (Fenster, Türen, Schlüssel, Zutrittsregelung, Kontrollgänge, . . .)
  - Datenträgerarchiv
- Beispiel Minimaldatensicherungskonzept:
  - **Software**: erworben oder selbst erstellt, einmalig Vollsicherung
  - **Systemdaten**: sind mindestens einmal monatlich mit einer Generation zu sichern.
  - **Anwendungsdaten**: mindestens monatlich Vollsicherung im Drei-Generationen-Prinzip
  - **Protokolldaten**: mindestens monatlich Vollsicherung im Drei-Generationen-Prinzip
- Ergänzende Kontrollfragen:
  - Werden sämtliche Mitarbeiter, auch neu eingestellte, auf ein Datensicherungskonzept oder ersatzweise auf das

(Maßnahmen zur Wiederherstellung der Betriebsfähigkeit)



Phase 1: **Planung der Notfallvorsorge**

- Maßnahmen während des Betriebes (z. B. Rauchverbot, Stromversorgung, Wartung, Datensicherung)
- Notfallpläne (Teile eines Notfallhandbuchs) mit Maßnahmen bei Eintreten eines Notfalls

Phase 2: **Umsetzung der Notfallvorsorgemaßnahmen**

- Ziel: Eintrittswahrscheinlichkeit eines Notfalls verringern sowie zügige und wirtschaftliche Wiederherstellung der Betriebsfähigkeit.

Phase 3: **Durchführung von Notfallübungen**

- Umsetzung der im Notfall-Handbuch aufgeführten Maßnahmen einüben und Steigerung deren Effizienz

Phase 4: **Umsetzung geplanter Maßnahmen nach Eintreten eines Notfalls**

Notfallvorsorge: u. a.:

M 6.1 Erstellung einer Übersicht über Verfügbarkeitsanforderungen
M 6.2 Notfall-Definition, Notfall-Verantwortlicher
M 6.3 Erstellung eines Notfall-Handbuches
M 6.5 Definition des eingeschränkten IT-Betriebs
M 6.6 Untersuchung interner und externer Ausweichmöglichkeiten
M 6.11 Erstellung eines Wiederanlaufplans
M 6.8 Alarmierungsplan
M 6.12 Notfallübungen
M 6.16 Versicherungen
M 6.14 Ersatzbeschaff.-plan

BSI-Sicherheitszertifikat

BSI

Bundesamt für Sicherheit in der Informationstechnik

Sicherheitszertifikat

BSI-ITSEC-9999-2000

Zertifiziertes Produkt: IT Grund
Antragsteller: CoSS [Company of Security Specialists]
Kriterien: ITSEC, Version 1.2
Zertifizierungsanlaß: Antrag auf Zertifizierung vom 01.01.1900
Produkt-Auslieferung: Direktbezug beim Hersteller
Produkttyp: PC-Sicherheitsprodukt
Prüfergebnis: Funktionalität Funktionalitätsklasse F-C2
Evaluationsstufe: E3
Mindeststärke der Mechanismen: mittel

Auflage: Siehe Hinweise und Auflagen im Zertifizierungsreport

Hinweis: Dieses Zertifikat gilt nur in Verbindung mit dem Zertifizierungsreport

Bonn,den
Der Präsident des Bundesamtes für
Sicherheit in der Informationstechnik

Die europäischen Sicherheitskriterien
(**I** nformation **T** echnology **S** ecurity **E** valuation
C riteria **ITSEC**) = Grundlage für die Prüfung
der Vertrauenswürdigkeit von IT-Produkten
(Korrektheit u. Wirksamkeit der Sicherheits-funktionen wie Authentisierung, Zugriffskontrol-le und Übertragungssicherung).
Die Sicherheitsfunktionen wirken gegen folgende **Gefährdungen**:

- **Verlust der Vertraulichkeit**
- **Integrität**
- **Verfügbarkeit**

Der Zertifizierungsreport enthält neben dem Sicherheitszertifikat einen **Bericht**, in dem Details der Prüfung und Zertifizierung veröffent-licht werden.
(Sicherheitseigenschaften des IT-Produkts, abzuwehrende Bedrohungen, Anfor-

(Prüfung und Bewertung der Sicherheit von Informationstechnik)

• Standard **Common Criteria for Information Technology Security Evaluation (CC**
Version 2.0 , 5/1998 unter Beteiligung Deutschlands, Frankreichs, Großbritanniens, Kanadas, der Niederlande und der USA

Version 3.1 , 9/2006

⇨ für die **Bewertung** der Sicherheitseigenschaften der informationstechnischen Produkte und Systeme

• **CC-Dokumentation gegliedert:**

Teil 1: Einführung und allgemeines Modell
Teil 2: Funktionale Sicherheitsanforderungen
Teil 2: Anhang
Teil 3: Anforderungen an die Vertrauenswürdigkeit

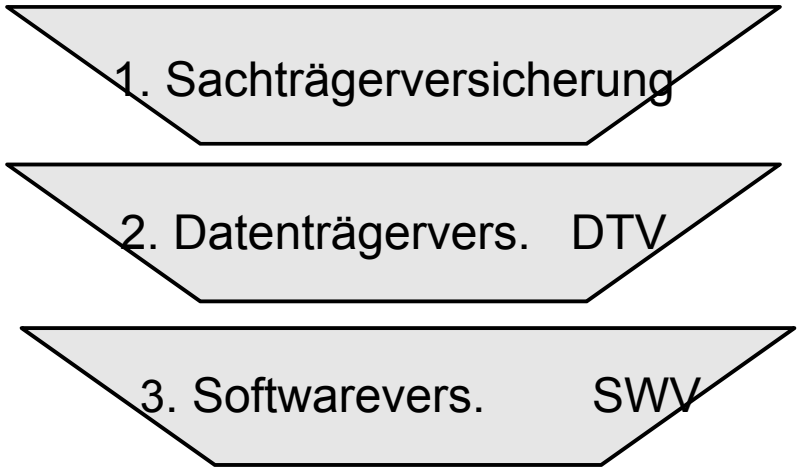
Quelle: http://www.bsi.bund.de/cc/
http://www.commoncriteriaportal.org/cc/

31.3.2 Sekundäre Maßnahmen (Gegenmaßnahmen), hier Risiko-Versicherung

Versicherungsarten (1)

***Elektronikversicherung* am Bsp. einer großen Versicherung** (500 MA, 18 Stand

Versicherungsarten:



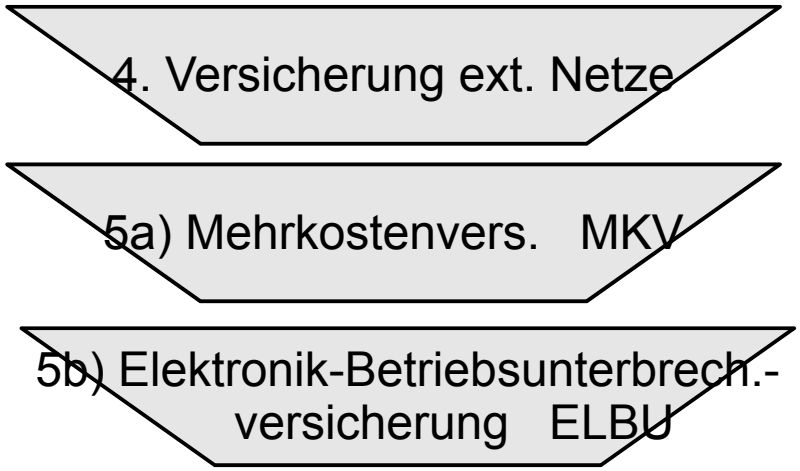
Ersatz zum Nennwert der Anlage (Schaden durch Einwirkung von außen)
Erweiterung: Leihgerät während Reparatur

wie bei 1., ohne “auswechselbare” DT
hier: Materialwert + Rekonstruktion der Date
Progr. ==> versichert ist nur das Nicht-funktionieren der eigenen Datensicherung

Bei Verlust /Veränderung auch ohne Sach-schaden. Bsp.: DFÜ, Bedienfehler, Viren, Manipulation Dritter.
Leistung: Kosten der Wiederherstellung
DT-Versicherung ist in Softwareversicherung enthalten

ABE = Allg. Bedingungen für Elektronikvers.

noch: Elektronikversicherung am Bsp. einer großen Versichung



Mehrkosten für ein Ausweichkonzept (Anmietung, Gebäude, Personal u.a.), max. 1 Jahr

für Folgeschäden
eines sachschadenbedingten Ausfalls
=>wenn Ausweichmaßn. nicht möglich,
für entgangenen Gewinn u. fortl. Kosten