

Risikoanalysen in der IT

Einleitung

Risiken: - Potenzielle Schadensereignisse / Unerwünschtes Ereignis - Technisch
- Finanziell - Physisch - Personell

Risiken: - Erkennen - Bewerten - Massnahmen - Protokollieren / Dokumentieren
- Zukünftige Ereignisse

Risiko-Fragen: - How safe? (Risiko-Analyse, risk estimation) - How safe is safe enough? (Risiko-Beurteilung, risk assessment) - How safe is too safe? (Risiko-Management, risk management)

Messung: - $R = f(F, C)$ *F: Frequency, C: Consequence*

Risikoanalyse / Risikoassessment: Risiken erkennen & bewerten (berechnen, beurteilen)

Ansätze: Klassische Ansätze sind für moderne IT nur bedingt genügend.

Begriffe: - Gefährdung: Potenzielle Schadensquelle - Bedrohung: Alles, was eine Schwachstelle ausnutzen könnte

Begriffe gemäss ISO 73 / 31000: - Risiko: Auswirkung der Unwägbarkeit auf Schutzziele - Auswirkung: Abweichung vom Erwarteten (positiv / negativ) - Welche Gefährdungen gibt es? - Welche Szenarien gibt es? - Welche Auswirkungen hat es? - Unsicherheit (uncertainty): Informationsmangel in Bezug auf ein Ereignis, eine Entwicklung ... , Wahrscheinlichkeit ist ein Mass für Unsicherheit - Wie wahrscheinlich ist es? - Schutzziele (objectives): unterschiedliche Aspekte, relevant auf verschiedenen Ebenen - Welche Ziele gibt es?

Für uns: Häufigkeit und Ausmass unerwünschter Ereignisse

IT: - Probability: Statistische Wahrscheinlichkeit - Likelihood: Geschätzte Wahrscheinlichkeit

Analysen: - Risikoanalyse: $R = (A, C, P)$ - A: Accident (unerwünschtes, zufälliges Ereignis) - C: Consequence (Folge) - P: Häufigkeit (Prob.) von A - Erweiter: $R = (A, B, C, P, U, K)$ - B: C hängt von Barrieren-Wirksamkeit ab - U: A und C enthalten Ungewissheiten - K: U hängt vom Kenntnisstand K ab - Vulnerability-Analyse: $V = (B, C, P, U, K|A)$ - $K|A$: Wissen um Anfälligkeit bestehender Stelle gegen Unfallereignis A - Analyse Systemschwachstelle - Resilience-Analyse: $Re = (B, C, P, U, K|A_i)$ - $K|A_i$: Wissen um Anfälligkeit best. Stelle auf alle Arten von Bedrohungen A_i $i = 1, 2, \dots$ - Einfluss aller Bedrohungen, Mass Widerstandskraft

Anwendung in Praxis: Definition von "Risiko" ist wichtig, Auswahl Risikobeurteilungs-Methoden

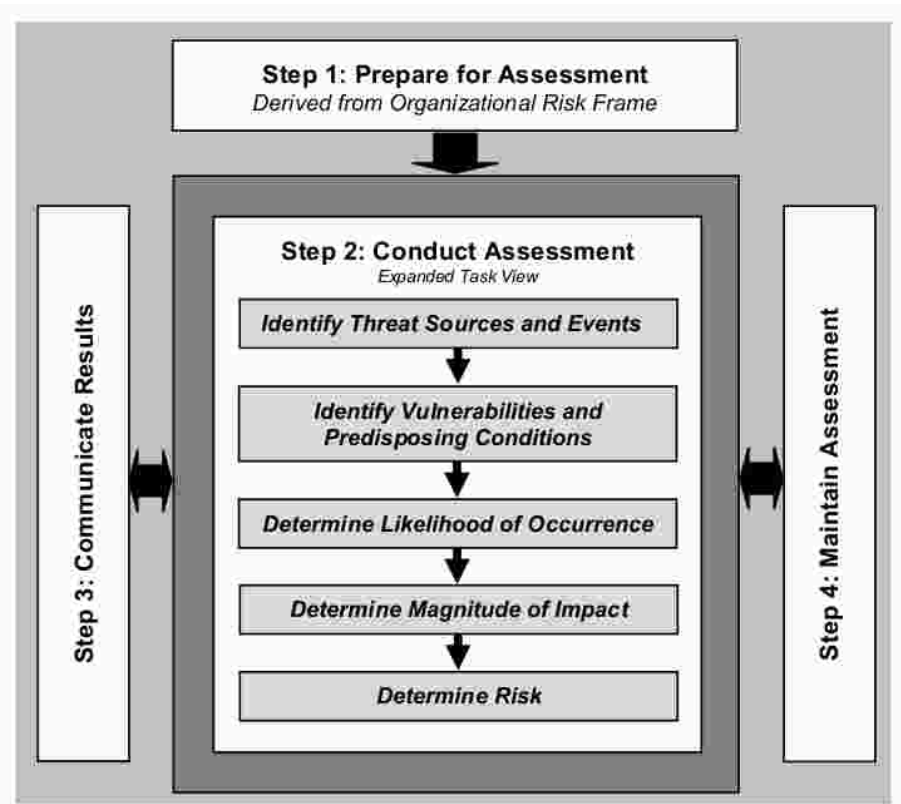


Figure 1:

Risk-Assessment-Prozess

Vulnerabilitätsanalyse

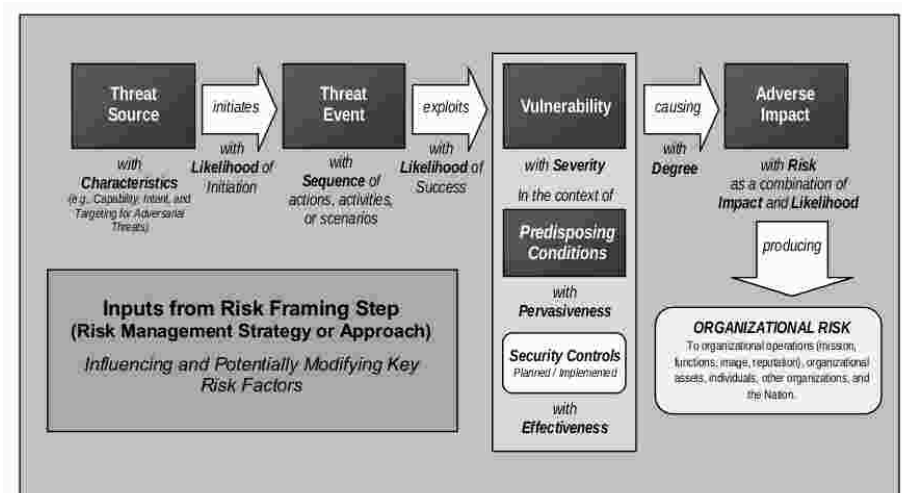


Figure 2:

Management und Entscheidungsprozesse

Probleme Risikoanalytik

- Ergebnisse innerhalb von Monaten Erwarteten
- Systeme veralten schnell, hochdynamisch
- wachsende Bedeutung IT-Systeme
- Hardware-Software-Dualität
- Knappe Ressourcen
- Komplizierte Architekturen / Security

Risikoanalysen in der IT

Übung 01

Risikobegriff

- **Risiko 1: Ausfall eines Kernsystemes**
Ein Kernsystem stürzt unerwartet (ohne bewusste Einflussnahme) ab oder

| | | Entscheidungsebene | | |
|----------------------|-------------------|------------------------------------|--------------------|--------------------|
| | | Operational Control | Management Control | Strategic Planning |
| Entscheidungsfindung | strukturiert | „Best Practice“ | | |
| | semi-strukturiert | etablierte Risiko-Analyse-Methoden | | |
| | un-strukturiert | | | |

Figure 3:

stellt seinen Betrieb ohne zutun von Aussen ein. Durch den Ausfall können wichtige Geschäftsprozesse nicht mehr abgewickelt werden.

- **Risiko 2: Neue gesetzliche Anforderungen**
Durch externe (nicht kontrollierbare) Einflüsse werden neue gesetzliche Rahmenbedingungen geschaffen, welche einen starken Einfluss auf das Kerngeschäft haben. Damit das Kerngeschäft weiterbetrieben werden kann, sind umfangreiche Anpassungen notwendig.
- **Risiko 3: Schliessung einer Betriebsliegenschaft**
Aufgrund unbeeinflussbarer und unerwarteter externer Einflüsse (Feuer, Wasser, etc.) muss eine der Kernbetriebsliegenschaften geschlossen werden. Dadurch wird die Geschäftstätigkeit erheblich beeinträchtigt.
- **Risiko 4: Netzwerkunterbruch**
Durch einen plötzlichen und unvorhersehbaren Unterbruches des Netzwerkes oder eines Netzwerksegmentes können Kernsysteme nicht mehr erreicht werden. Durch den Unterbruch wird die Geschäftstätigkeit erheblich beeinträchtigt.
- **Risiko 5: Datenverlust**
Daten gehen bemerkt oder unbemerkt verloren, beziehungsweise werden von unberechtigten Personen gestohlen oder in irgendeiner Form der Öffentlichkeit zugänglich gemacht.

Lektion 2

Review Übungen 01

ISO 31'000: Auswirkung von Unsicherheit (Mangel an Wissen) auf Ziele - Ziel definieren - Definition Unsicherheiten / Ungewissheiten (gemessen mit

Wahrscheinlichkeiten) - Definition (unterwünschtes) Ereignis (Abweichung vom Ziel: positiv / negativ), pro Ereignis: - Auswirkung + Ausmass

Risikoanalyse

Was wird wirklich erwartet / gebraucht? Aus Methode kann Zahl ermittelt werden, aber Aussagekraft muss von Aussen gegeben werden.

As Low As Reasonable Practicable (ALARP), umgekehrte Pyramide, unterteilt in 3 Bereiche: - Tiefe Einzelrisiken, Massnahmen getroffen -> Inkaufnahme (Pyramide: Unten) - Normen, Standards, Anforderungen, etc. erfüllt -> Inkaufnahme höhere Risiken (Pyramide: Mitte) - Ausgebildet für Risiko VS. "Konsument"-Risiko (Pyramide: Oben)

Methoden

| Methode | Häufigkeit | Ausmass | Auswirkungen | Unsicherheiten | Ursachen |
|----------|------------|------------|--------------|----------------|----------|
| Fishbone | Nein | Nein | Nein | Nein | Ja |
| MLD | Nein | Nein | Nein | Nein | Ja |
| Bow-Tie | Nein | Ja (Prosa) | Indirekt | Nein | Ja |

Nachteile Fishbone, MLD, Bow-Tie: Top-Event wird benötigt

Fishbone-Diagramm (Ishikawa-Diagramm)

Brainstorming-Methode, Beginn mit Top-Event (Unterwünschtes Ereignis, o.ä.), Definition von Auslösern / Ursachen, Bsp: Wie können User zum Datenverlust beitragen? wichtigsten Pfad ankreuzen

Keine Risikoanalyse für Ausmass und Häufigkeit!, Nur Ursachen von Ereignissen darstellen

Master-Logik-Diagramm (MLD)

Beginn mit Top-Event (Unterwünschtes Ereignis), wie kann es zu diesem Datenverlust kommen? Hierarchie von Ursachen, grafisch dargestellte Liste

Keine Risikoanalyse für Ausmass und Häufigkeit!, Nur Ursachen von Ereignissen darstellen

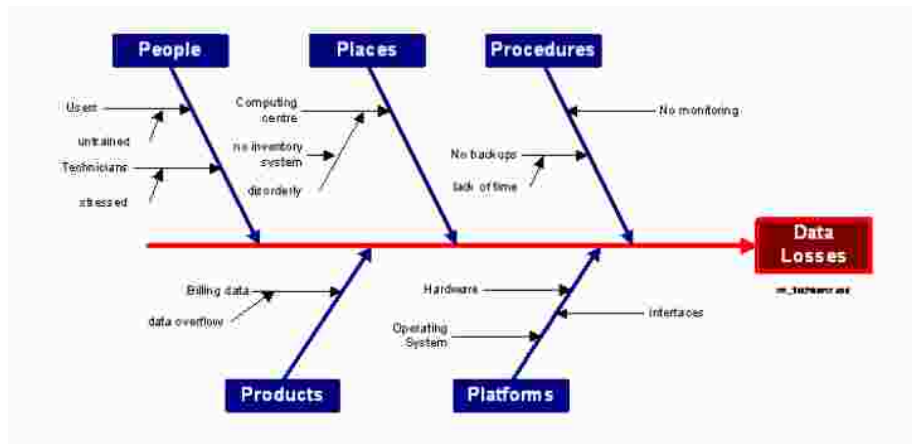


Figure 4:

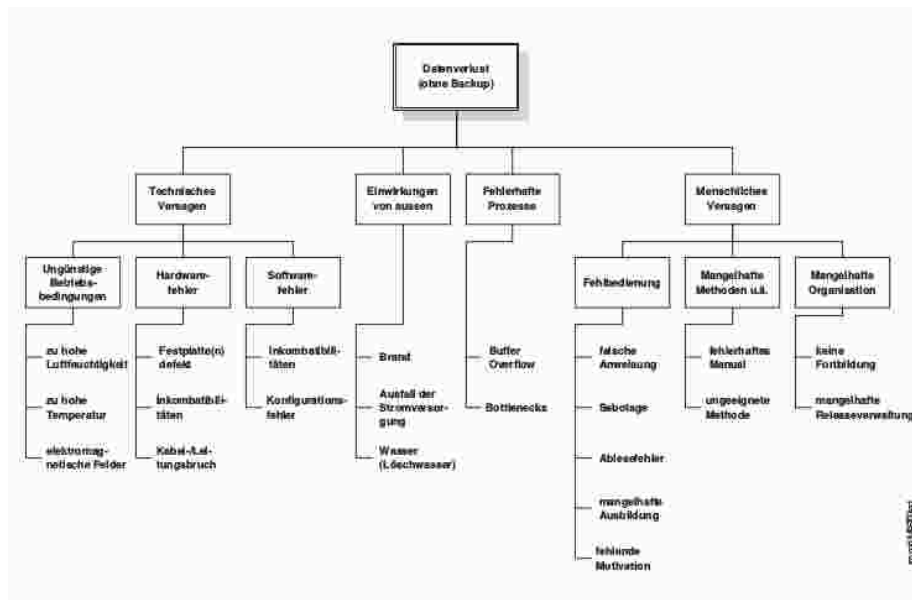


Figure 5:

Bow Tie

Top-Event: Unterwünschtes Ereignis, Ursachen des Ereignisses (Gefährdungen), Schäden der Ereignisse (Konsequenzen), zwischen Ursachen - Ereignis: Präventive Sperren, zwischen Ereignis und Schaden: Schadensminimierende Sperren

Sperren: Mehrere Sperren pro Verbindung möglich

Eskalationsfaktor: Pro Sperre Eskalationsfaktor, Schwächt Wirkung der Sperre, Massnahmen zur Verhinderung der Abschwächung

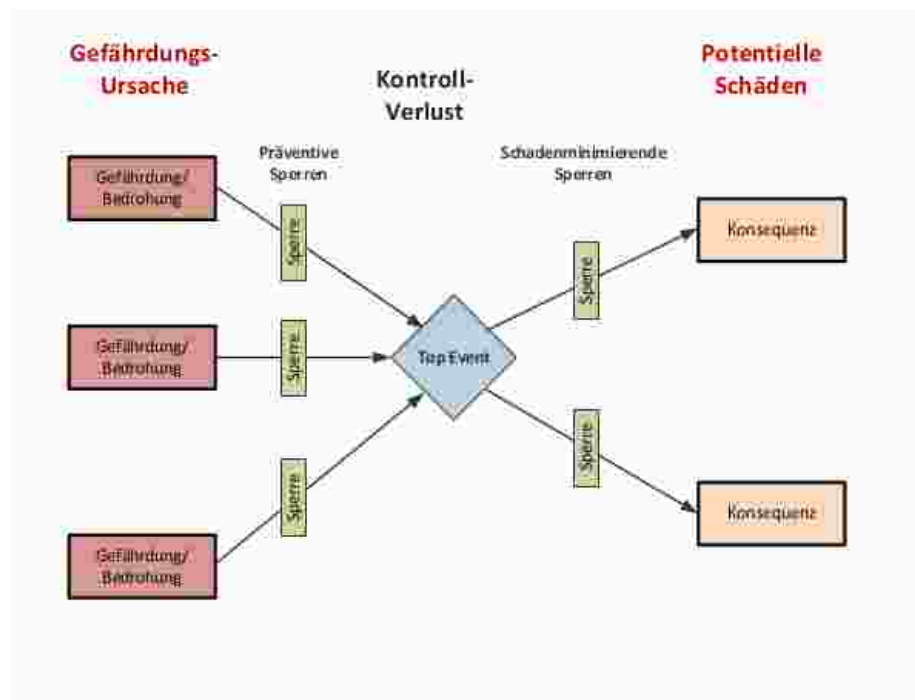


Figure 6:

Frequency/Consequence-Diagramm & Risikomatrix

X-Achse: Ausmass, Y-Achse: Häufigkeit, Häufigkeit und Ausmass pro Top-Events eintragen

Akzeptanzlinie: Bewertung (Was ist noch akzeptabel? unterhalb: gute Risiken, oberhalb: böse Risiken), Wer legt die Linie fest? (Grundsätzlich: Durch Management festgelegt), Festlegung: Evtl. durch Ausschluss best. Ausmasse / Häufigkeiten (z.B. Es dürfen nie Katastrophale Risiken, oder Ausklammerung von Bagatellen), vor der Analyse eintragen / definieren

Verschiebung Punkt: Minimierung Konsequenz oder Häufigkeit oder Beides

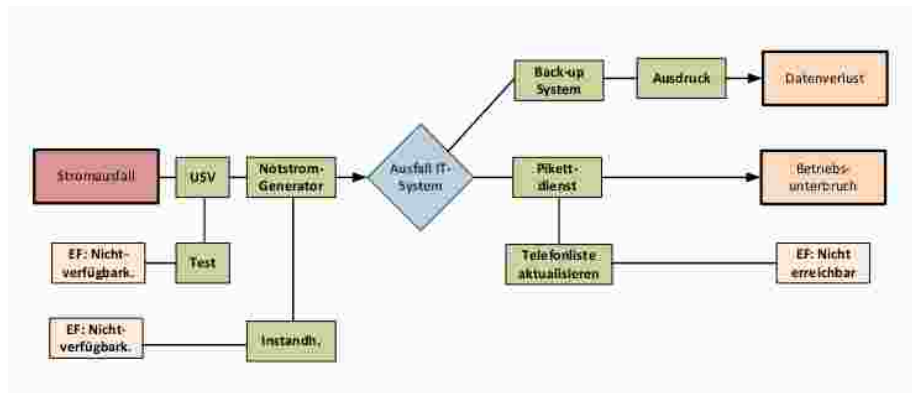


Figure 7:

Lektion 3 & 4

Prüfung

Risikodefinitionen: ISO 31'000, llgemeinere Form und formale (Auswirkungen von Unsicherheiten auf Ziele)

Hilfsmittel: 1 Blatt A4, PC oder Handgeschrieben

Allgemeines

Risiko: Frequency x Consequence (Kosten), C: Worst-Case, F: Gewichtung wie weit man von Worst-Case weg ist, Für Risikoabschätzung: Rahmen für Betrachtung / Auswirkungen angeben

Failure Mode and Effects Analysis (FMEA)

Failure Modes: Ausfallarten

Effects: Konsequenzen

Ziel: Qualitative Untersuchung von Einheiten auf Ausfallarten und deren Auswirkungen auf das übergeordnete Systeme, induktiv

Prozess: PDCA

Gründe für FMEA: - Umsetzung Unternehmensziele (z.B. Null-Fehler-Produkte) - steigende Kundenanforderungen - verschärfte gesetzliche Auflagen

Arbeitschritte

1. Auflistung aller Einheiten (E) (Personen, Computer, ...)
2. Identifizierung aller Ausfallarten für jede der in 1. aufgelisteten E
3. Bestimmung der Auswirkungen jeder Ausfallart auf andere E und Auswertung daraus resultierender Auswirkungen auf das System oder den Systemzustand
4. Klassifizierung nach Gefahr und Auswirkung für die einzelnen Ausfallarten
5. Ermitteln von Vorgehensweisen zur Reduzierung der Ausfallhäufigkeiten und Ausfallauswirkungen (Risikoverminderung)
6. Ausfüllen eines Formblattes, das die Ergebnisse der Arbeitsschritte 1. bis 5. zusammenfassend darstellt.

Ausfallarten

Bestimmung aus Funktionselementen oder Einzelteilen

Auswirkungen

Klassifizierung Systemendzustand und dessen Auswirkung (Klassen 1 -4, sicher - katastrophal)

Klassifizierung der Ausfallwirkung (sehr schwer - sehr gering, Der Ausfall einer Einheit E führt...)

Klassifikation der Häufigkeiten (wahrscheinlich (z.B. $> 1x$ in 10^4 Betriebsstunden) - sehr selten ($< 1x$ in 10^7 Betriebsstunden))

FMEA-Arten und Zusammenhäng

- System-FMEA: Einheiten eines Systemes, Funktionstüchtigkeit
- Konstruktions- / Produkt-FMEA: Einheiten hinsichtlich Erfüllung beschriebener Teilfunktionen
- Prozess-FMA: Tätigkeit / Arbeitsschritt innerhalb einer Arbeitsfolge oder Prozesses

Bewertung

- Kleinstes Risiko: 1
- Mittleres Risiko: 25 (5×5)
- Höchstes Risiko: 100 (10×10)

| Kopie von: _____ | | | | Produkt-/Prozess-Benennung: _____ | | | | | | | | | | Erstellt/Ausgegeben etc.: | | | | | | |
|--|---|---|---|--|-------------------------------------|-------------------------------------|---|----------------------|----|-----|---|-----------------------------------|---------------------|-----------------------------------|----|----|----|----|----|---|
| Kritischer FMEA □ | | | | Prozess FMEA □ | | | | | | | | | | | | | | | | |
| | | | | DERZEITIGER ZUSTAND | | | | | | | | | | VERBESSERTER ZUSTAND | | | | | | |
| System-Merkmal | potenzielle Fehler | pot. Folgen des Fehlers | D | pot. Fehlerursachen | vorge-sehene Prüfmass-nahmen | A | B | E | R | P | Z | empfohlene Abstellmass-nahme | Verantwort-lichkeit | gintroffene Massnahme | A | B | E | R | P | Z |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | |
| Spule wechseln (gem. Ab- weisung xy) | Windungs- zahl zu hoch | Spulenwider- stand zu hoch - Rel. zieht nicht an - Ausfall | - | Zähler für Windungs- zahl setzt aus | Zähler periodisch kalibrieren | 6 | 8 | 8 | 6 | 384 | | Zählgerätee schleichen | W. Erweit. | neuer Zähler + Regelung Nr. | 2 | 8 | 4 | 64 | | |
| Wie könnte etwas noch i. O. sein? | Wie könnte sich das Fehler bekommen? | Was könnte im Fehlerfall passieren? | Warum würde das Fehler die Folge entstehen? | Welche Massnahmen kennt Du? (sicherheitsfähig notwendig?) | Welche Risiko (A, B, E, RPZ)? | Wie weit ist es bis sein müsste? | | | | | Welche Massnahmen wurden realisiert? | Welches Risiko (A, B, E, RPZ)? | | | | | | | | |
| Fehlerbeschreibung | | | | Bewertung | | | | Empfehlung/Kontrolle | | | | Neubewertung | | | | | | | | |

Figure 8:

Struktur

- Spalte 1: Baugruppe / Teil / Prozess / Arbeitsschritte
- Spalte 2: Ausfall- / Fehlerart
- Spalte 3: Fehlerfolgen
- Spalte 4: Control Item D (sicherheitsrelevante, dokumentationspflichtige Einheit)
- Spalte 5: Fehlerursachen (Gliederung z.B. nach 5M: Mensch, Maschine, Material, Methode, Mitwelt)
- Spalte 6: Verhütungs- / Prüfmassnahmen
- Spalte 7: Auftreten A (1-10)
- Spalte 8: Bedeutung B (1-10)
- Spalte 9: Entdeckbarkeit (vor Auslieferung Kunde) E (1-10), Betrachtung von zeitpunkt betrachtete Arbeitsphase (1-10)
- Spalte 10: RPZ = ABE

Kunde: derjenige, bei dem der ungünstigste Fall auftreten kann, K-FMEA: meist Endbenutzer, P-FMEA: letzter Arbeitsschritt, bei dem Fehler zu Störungen der Weiterbearbeitung führen kann

RPZ: Orientierungsgrösse zur Prioritätssetzung, RPZ mit grossem A zuerst

Risikoanalysen in der IT

ISO 27002:2005, COBIT (Control Objectives for IT), Mehari (Méthode Harmonisée de Resques), BSI, US-CERT

Mehari

Einfache Risikoanalyse, Hilfe Erstellung Sicherheitskonzepte, ISO 2700x konform

Lektion 5 & 6

Boolesche Algebra

Für quantitative Risiko- und Zuverlässigkeitsanalysen

Theorie: Zustand (techn. System) als Boolesche Funktion, Gesucht: Vorgehensweise um Ausfallwahrscheinlichkeit zu berechnen, Problem: Übergang in kanonische Darstellung notwendig

Boolesche Variable: L: Zustand erfüllt, O: Zustand nicht erfüllt

Boolesche Operatoren: und, oder

Boolesche Axiome (Schaltalgebra): Kommutativgesetz, Assoziativgesetz, Distributivgesetz, Idempotenzgesetz, Absorptionsgesetz, Komplementärgesetz, Verneinungsgesetz, de-Morgansches Gesetz, Extremalgesetze, Neutralitätsgesetze

Kanonische Darstellung Boolescher Funktionen Disjunktive Normalform (DN): Konjunktionsterm aus einfachen oder negierten Booleschen Variablen

Ausgezeichnete DN (ADN): in jedem Ki kommt jede Variable genau einmal vor (einfach oder negiert), Minterm (MI)

Vorgehensweise: Unvollständige Konjunktionsterme erweitern (Anwendung der Gesetze der Schaltalgebra)

Verfahren Quantifizierung

- Zuverlässigkeitsblockdiagramme
- Minimalschnitte und -pfade
- Funktions- bzw. Wahrheitstabellen
- Fehlerbäume

Einfache Systemmodellierung: Zuverlässigkeitsblockdiagramme

Grafische Darstellung Boolesche Gleichung, Seriensystem, Parallelsystem

- Überlebenswahrscheinlichkeit: $P(X_i = 1) = P(x_i) = p_i$

Systemanalyse

Systemwahrscheinlichkeiten über Erfolgswege ermitteln, Regel (Vereinfachung):
Wenn 0: dann $(1 - x_i)$

Minimalschnitte

Minimalpfade

Quantitative Tests

Teststand: 100 Glühbirnen, 2 Zustände: Funktioniert, Funktioniert Nicht - $t = 0$: Alle sind neu (keine Vorbelastung), WSK Funktionsfähig: $1 - t = \text{unendlich}$, WSK Funktionsfähig: $0 - t = 1$ Woche ($\hat{P} = n/N$) (Dach auf P: laufender Versuch), $P_t(T \leq t_{1w}) = \text{Summe } (i) \Pr(T=t_i)$

$T = \{t_1, t_2, t_3, \dots, t_n\}$, 1 Komponente nacheinander flt aus, Schrittlänge unterschiedlich

- Ausfallrate = $\lambda = n/(N \cdot t_{\text{betrieb}})$ (Bezogen auf Zeit (interval))
- Ausfallwsk: $F(t) = 1 - e^{(-\lambda t)}$, konstante Ausfallrate

MeanTimeToFailure (MTTF): - Konstante Ausfallrate: $1 / \lambda$

Badewannenkurve der Ausfallrate (Zuerst Einführung, dann “Betrieb”: e-Gleichung, dann “End-of-Life”)

Notes / Hints - Wahrscheinlichkeit: Dimensionslose Grösse - Rate: irgendetwas pro zeit - Ausfall: Alles was repariert werden müsste / wurde

Prüfung - Definitionen: Risiko, etc. - Besprochene Methoden (Fishbone, Master-Logik-Diagramm, FMEA, Bow-Tie, Zuverlässigkeitsblockdiagramme, ...): Wie geht das, was kann man damit machen - Berechnung einfacher Blockdiagramme - Ausfallrate ($\lambda = n/(N \cdot t_{\text{betrieb}})$), zeitlich Konstant, Zusammenhänge Badewannenkurve - Ausfallwahrscheinlichkeit ($P = n/N$) - MeanTimeToFailure ($1/\lambda$) - Wahrscheinlichkeit: $F(t) = 1 - e^{(-\lambda t)}$ - Ausfalldichte anschauen (Steigung in einem Punkt) - Einteilung Badewannenkurve

Lektion 7

Ereignisbaumanalyse

Ereignis am Anfang, Entwicklung Konsequenzen / Folgen.

Lektion 8 & 9

Fehlerbaumanalyse

Ausgehend von Ursache (Top-Event, Worst-Case), basierend auf boolescher Algebra, Berechnung: Wahrscheinlichkeit Ausfall Top-Event, Basis: auch Ausfallwahrscheinlichkeiten, Momentaufnahme, keine Berücksichtigung Zeit, keine Schleifen / Loops, für jeden Fehlerbaum: Minimalschnitte anschauen (einfachste und kompakteste Art und Weise Fehlerbaum darzustellen)

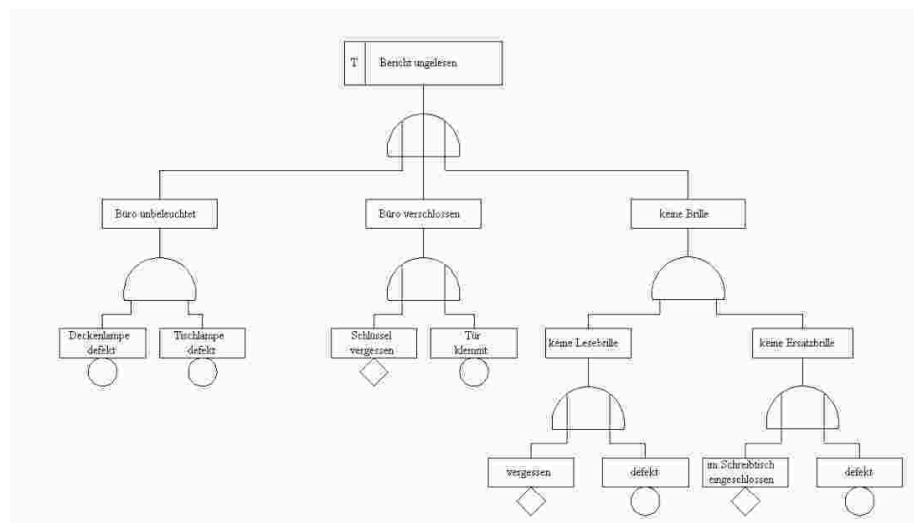


Figure 9:

Problematisik

In komplexen Systemen Fehlerursachen via Brainstorming schwer ermittelbar, hochzuverlässige / einzigartige Systeme: kaum Zuverlässigkeits- / statistische Daten vorhanden

Logische Verknüpfungen: UND, ODER, NICHT, Und (Halb-Kreis ohne Striche innerhalb), Oder (Halb-Kreis mit Strichen innerhalb), Basisereignisse, Gatter

Boolsche Logik im Fehlerbaum

- Grafische Darstellung Boolescher Gleichung
- Zeigt nur Ausfälle / Fehler
- Reihenfolge Ereignis spielt keine Rolle

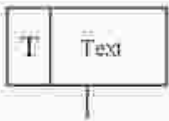

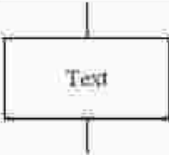



| Symbol | Benennung | Symbol | Benennung |
|---|-----------------------------|---|---|
|  | Bezeichnung des "top event" |  | nicht weiter entwickeltes Ereignis |
|  | Kommentar, Beschreibung |  | Transfer zu einem separaten Fehlerbaum |
|  | Basisereignis |  | Transfer von einem separaten Fehlerbaum |

Figure 10:

- Zeitlos
- Quantitativ
- Korrekte Berechnung nur via Boolesche Algebra

Berechnung

Einsetzen Ausfallwsk in Basisereignisse, Verwendung Kanonische Darstellung für Berechnung, Und-Verknüpfung = Multiplikation, Oder-Verknüpfung = Addition - Multiplikation (Multiplikation kann bei kleinen WSK 10^{-3} weggelassen werden.). Wenn alle Ereignisse nur 1 x: gut, sonst Berechnung via boolesche Algebra oder Programm

Regeln

1. Kleine WSK: Oder-Verknüpfungen einfach addieren, ohne Subtraktion
2. Genaue Berechnung nur möglich, wenn jedes Basisereignis nur 1 x vorkommt
3. Wenn Minimalschnitte von Fehlerbäumen gleich \rightarrow Wahrscheinlichkeit auch gleich

ZBD

Zeigt Funktionieren System, grafische Darstellung B.A.

Vom Fehlerbaum zu Minimal-Schnitten

- Beginn bei Top-Event
- UND: Alle Eingänge nebeneinander
- ODER: Alle Eingänge untereinander
 - Pro Eingang: Neue Zeile, Rest bleibt erhalten
- Hinweis Zeile: Idempotenzgesetz
- Hinweis Spalte: Absorptionsgesetz

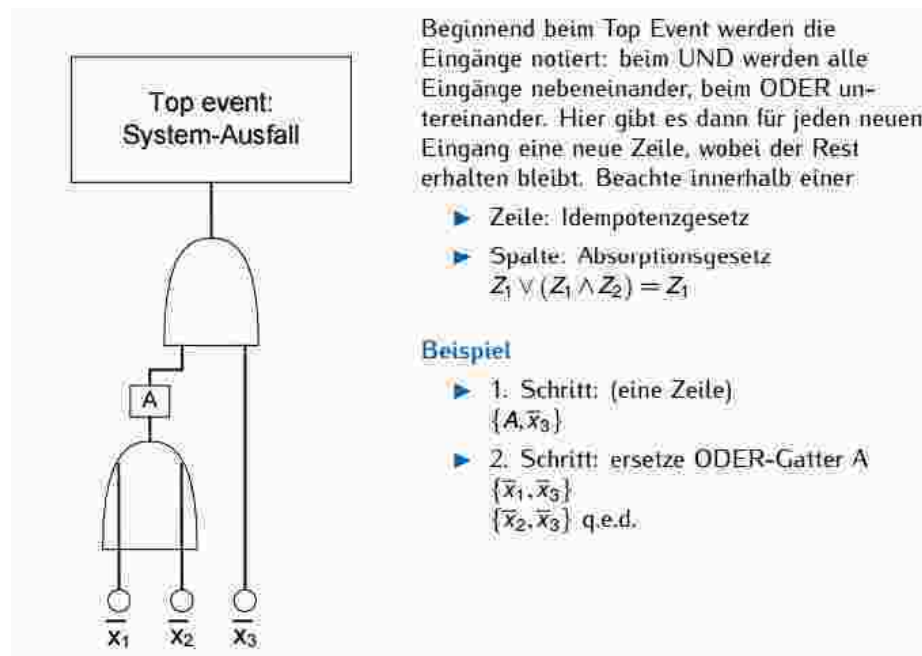


Figure 11:

Importanz-Analysen

Wichtigkeit einzelner Systemeinheiten kennen / beachten, Beitrag für Systemzuverlässigkeit: Importanz-Analysen - Zuverlässigkeit System bestimmt durch: - Merkmale seiner Einheit - Anordnung der Einheiten - Zuverlässigkeitskenngrößen

der Einheiten - Wichtigkeit (je nach Problemstellung anders definiert) - Je nach Datenbasis unterschiedliche Methoden

Problemkreise

- Verbesserung einzelner Einheit, beste auswirkung auf System (Systemoptimierung)
- Einheit i löst den Systemausfall aus, Systemausfall korrespondiert mit Zeitpunkt Ausfall i
- Fehlererkennung / -diagnose Reihenfolge zu reparierenden Einheiten bedeutungsvoll (Optimierung Instandhaltung)

Strukturelle Importanz

Ansatz

- Jede Einheit i weist Zustand $x_i = 0$ (ausgefallen) oder $x_i = 1$ (intakt) auf.
- Systemfunktion $\phi(x)$, besteht aus Einheiten x_i , System: Zustand 0 oder 1
- Zustandsvektor x : Realisierung Einheiten-Zustände in System
- Anzahl Kombinationen: 2^n unterschiedliche Zustandsvektoren

Beispiel: Serien-Parallelsystem

Marginale Importanz

WSK, dass sich System in Zustand befindet, in dem der Betrieb kritisch ist, partielle Ableitung der Systemausfallwsk $F(q)$ in Bezug auf eine zu untersuchende Komponente q

Diagnostische Importanz (Fusel-Wesley)

Am meisten verwendet, Bruch: Nenner: Ausfall-WSK Top-Event, Zähler: Ausfall-WSK Komponente i - Wie viel trägt Ausfall-WSK einer Komponente zur Gesamtausfall-WSK bei. Wenn i mehrfach: Minimalschnitte betrachten: Nenner: Ausfall-WSK Top-Event, Zähler: Summe aller Minimalschnitte (Pro Minimalschnitt: Produkt der Ausfall-WSK der einzelnen Komponenten) mit Komponente i

Ansatz (Forts.)

- Ein System fällt aus ($\phi(0_i; \underline{x}) = 0$), falls Einheit i ausfällt ($x_i = 0$), und es bleibt intakt ($\phi(1_i; \underline{x}) = 1$), falls i intakt ist ($x_i = 1$). Damit bestimmt der Zustand der Einheit i den Systemzustand. Damit gilt die **Bedingung** der Gl. 1:

$$\phi(1_i; \underline{x}) - \phi(0_i; \underline{x}) = 1, \text{ „ist wahr“} \quad (1)$$

- Gibt man den Zustand der Einheit i vor, dann reduziert sich die Anzahl der Vektoren auf 2^{n-1}
- Vektoren, die die Bedingung erfüllen, nennt man kritische Vektoren.
- Die Strukturelle Importanz ist definiert als der Quotient aus der Anzahl der kritischen Vektoren der Einheit i und der Gesamtanzahl aller Vektoren. Die relative Wichtigkeit einer Einheit i für das Funktionieren des Gesamtsystems ist damit

$$I_{\phi(i)} = \frac{1}{2^{n-1}} \cdot n_{\phi(i)}, \text{ wobei}$$

- 2^{n-1} : Anzahl möglicher Vektoren
- $n_{\phi(i)}$: Anzahl der kritischen Vektoren der Einheit i

Figure 12:

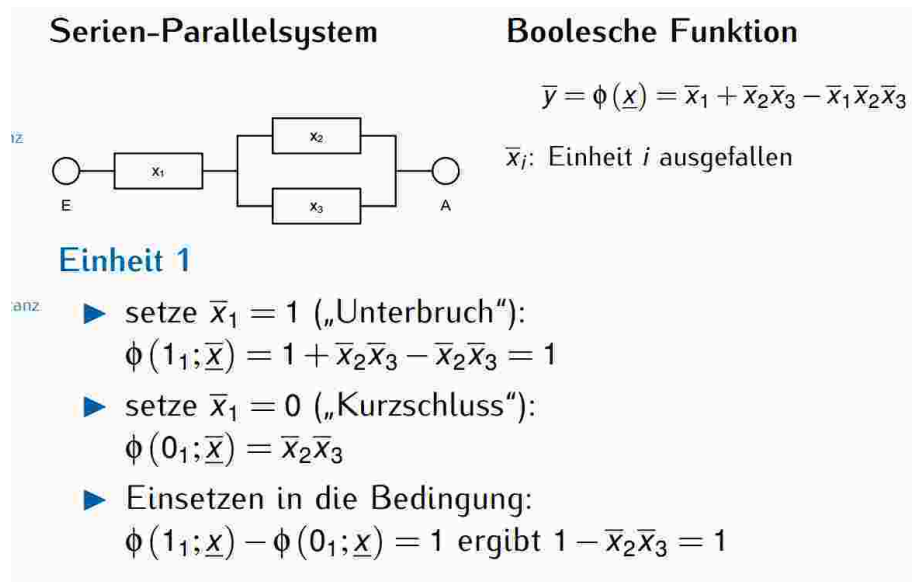


Figure 13:

Beispiel (Forts.)

Frage: Welche Zustände erfüllen die Bedingung $1 - \bar{x}_2\bar{x}_3 = 1$?

► Zustandstabelle

| $\bar{x}_2 =$ | $\bar{x}_3 =$ | resultierender Zustand aus $1 - \bar{x}_2\bar{x}_3 = ?$ |
|---------------|---------------|---|
| 0 | 0 | 1 |
| 0 | 1 | 1 |
| 1 | 0 | 1 |
| 1 | 1 | 0 |

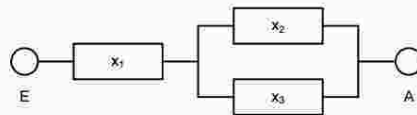
- drei kritische Vektoren erfüllen die Gl. 1, d.h. $n_{\phi(1)} = 3$
- damit ist die strukturelle Importanz der Einheit 1

$$I_{\phi(1)} = \frac{1}{2^{n-1}} \cdot n_{\phi(1)} = \frac{1}{2^{3-1}} \cdot 3 = \frac{3}{4}$$

Figure 14:

Ansatz

Serien-Parallelsystem



System-Ausfallwahrscheinlichkeitsfunktion

$$F(q) = q_1 + q_2 q_3 - q_1 q_2 q_3$$

partielle Ableitung

$$\begin{aligned} \triangleright I_m(1) &= \frac{\partial F(q)}{\partial q_1} = 1 - q_2 q_3 \\ \triangleright I_m(2) &= \frac{\partial F(q)}{\partial q_2} = q_3 - q_1 q_3 \\ \triangleright I_m(3) &= \frac{\partial F(q)}{\partial q_3} = q_2 - q_1 q_2 \end{aligned}$$

Differenz

$$\begin{aligned} \triangleright I_m(1) &= F(q_1 = 1; F(q)) - F(q_1 = 0; F(q)) = \\ &= 1 + q_2 q_3 - 1 \cdot q_2 q_3 - (0 + q_2 q_3 - 0) = \\ &= 1 - q_2 q_3 \\ \triangleright I_m(2) &= q_1 + q_3 - q_1 q_3 - (q_1 + 0 - 0) = \\ &= q_3 - q_1 q_3 \\ \triangleright I_m(3) &= q_2 - q_1 q_2 \end{aligned}$$

Resultat: Nach dem Einsetzen der Ausfallwahrscheinlichkeiten q_i folgt die wichtigste Einheit (größte Importanz). Im Beispiel ist dies immer die Komponente 1.

Figure 15:

Ansatz

Es gibt zwei Ansätze zur Berechnung der diagnostischen Importanz (Fussell-Vesely-Importanz)

- Wahrscheinlichkeit, die Komponente i zum Systemausfall beiträgt (Importanz des Basisereignisses q_i), und damit in den Minimalschnitten vorkommt:

$$I_{d, BE}(i) = \frac{F_i(q)}{F(q)}$$

- Wahrscheinlichkeit, die der einzelne Minimalschnitt σ_i zum Systemausfall beiträgt (Importanz des Minimalschnittes σ_i):

$$I_{d, \sigma_i}(i) = \frac{F_{\sigma_i}(q)}{F(q)}$$

Anmerkungen

- Der Systemausfall ist im Zeitintervall $[0; t]$ aufgetreten.
- Die Ausfallwahrscheinlichkeiten sind somit (auch) zeitabhängig verteilt, z.B. $q_i = q_i(t) = 1 - e^{-\lambda_i \cdot t}$

Figure 16:

Erläuterung zu $I_{d,\sigma_i}(i) = \frac{F_{\sigma_i}(q)}{F(q)}$

- ▶ $F_{\sigma_i}(q)$: Systemfunktion aller Minimalschnitte, die i enthalten, d.h.

$$- F_{\sigma_i}(q) = Pr \left(\bigvee_{j=1}^n \left[\bigwedge_{c_{ij}} \bar{x}_c \right] \right)$$

- ▶ n : Anzahl der Minimalschnitte, die i enthalten
- ▶ C_{ij} -ter Minimalschnitt, der i enthält
- ▶ $F(q)$ Ausfallwahrscheinlichkeit des Systems

Berechnungsbeispiel: aus einer System-Analyse ergeben sich zwei Minimalschnitte, die Komponente 1 enthalten: $\sigma_1 = \{\bar{x}_1; \bar{x}_2\}; \sigma_2 = \{\bar{x}_1; \bar{x}_3\}$.

- ▶ exakt: $F_{\sigma_1}(q) = q_1 q_2 + q_1 q_3 - q_1 q_2 q_3$
(nach Anwendung des Idempotenzgesetzes)
- ▶ näherungsweise: $F_{\sigma_1}(q) \approx q_1 q_2 + q_1 q_3$

Figure 17:

Hints mündliche Prüfung

- Fehlerbäume
- Fehlerbaum aus ZBD ableiten + berechnen, Was muss man bei der Berechnung beachten?
- Importanz-Analyse (Was kann man damit machen?)
- Analyse eines Datenblattes

Lektion 10 & 11

Markov-Modelle

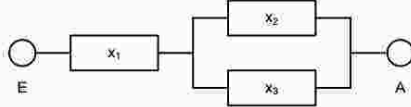
Gedächtnisfrei / -los, mit Loops, absorbierende Zustände (kein Weg zurück / weiter), Ausfall: $F(t) = 1 - e^{-(\lambda t)}$, nur für konstante Ausfallraten, Allgemeine Sicht von allem was wir bisher angeschaut haben. Einsatzgebiet: Entwurf Rechner, Platinen, Cloud

Allgemeines

- Nur für nicht-instandsetzbare Einheiten

Beispiel

Serien-Parallelsystem



System- Ausfallwahrscheinlichkeitsfunktion

$$F(\underline{q}) = q_1 + q_2 q_3 - q_1 q_2 q_3 \text{ mit}$$

Minimalschnitte: $\{\bar{x}_1\}; \{\bar{x}_2; \bar{x}_3\}$.

Importanzen $I_{d,BE}$

$$\blacktriangleright I_{d,BE}(1) = \frac{F_1(\underline{q})}{F(\underline{q})} = \frac{q_1}{q_1 + q_2 q_3 - q_1 q_2 q_3}$$

$$\blacktriangleright I_{d,BE}(2) = \frac{F_2(\underline{q})}{F(\underline{q})} = \frac{q_2 q_3}{q_1 + q_2 q_3 - q_1 q_2 q_3}$$

$$\blacktriangleright I_{d,BE}(3) \text{ entspricht } I_{d,BE}(2)$$

Resultat: Nach dem Einsetzen der Ausfallwahrscheinlichkeiten q_i folgt die wichtigste Einheit (größte Importanz)

Unterschiede: $I_{d,BE}$ berücksichtigt im Zähler alle Minimalschnitte, die die interessierende Komponente i enthalten (siehe auch Tool LOGAN). $I_{d,\sigma}$ berücksichtigt den einzelnen Minimalschnitt.

Figure 18:

- Instandsetzung beeinflusst Verfügbarkeit wesentlich, es gibt Schleifen

Ablauf

1. Diagramm erstellen
2. Gleichungssystem aufstellen

Abhängige Ausfälle

- Bestehen oft aus Standardkomponenten
- Verwenden häufig Standardsoftware
- Werden häufig von wenigen Personen betrieben / instand gehalten
- Sind mit Aussenwelt vernetzt.