Risikoanalysen in der IT
Risiko: Potenzielles Schadensereigniss / Unerwünschtes Ereignis (Technisch, Finanziell, Physisch, Personell), Risiken: Erkennen, Bewerten, Massnahmen, Protokollieren / Dokumentieren, Zukünftige Ereignisse – **Fragen:** How Save? (Analyse, estimation), How safe is enough? (Beurteiliung, assessment), How safe is too safe (Management), **Messung:** R = f(F,C) F: Frequency, C: Consequence – **Begriffe (Normal):** Gefährdung: Potenzielle Schadensquelle, Bedrohung: Alles was Schwachstelle ausnutzen kann – **Begriffe (ISO 31000):** Risiko: Auswirkung der Unabwägbarkeit auf Schutzziele, Auswirkung: Abweichung vom Erwarteten (positiv / negativ) – Welche Gefährdungen / Szenarien / Auswirkungen gibt es?, Unsicherheit: 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? | **IT**: Probability: Statistische Wahrscheinlichkeit, Likelihood: Geschätzte Wahrscheinlichkeit | **Analysen:** Risikoanalyse: R= (A,C,P) oder (A,B,C,P,U,K) – A: Accident, C: Consequence, P; Probability, B: C hängt von Barrieren-Wirksamkeit ab, U: A und C enthalten Ungewissheiten, K: U hängt von Kenntnisstand K ab - Vulnerability-Analyse: V = (B,C,P,U,K|A), K|A: Wissen Anfälligkeit best. Stelle gegen A, Analyse Systemschwachstelle – Resilence-Analyse: Re = (B,C,P,U,K|Ai) K|Ai: Wissen Anfälligkeit best. Stelle gegen alle Arten von Bedrohungen, Mass Widerstandskraft | **Risikoanalytik Probleme:** Wenig Zeit, Schnelle Systementwicklung, Bedeutung IT, Knappe Ressourcen, Komplexität | **Risikoanalyse:** Ziele definieren, Def. Unsicherheiten / Ungewissheiten (gemessen mit WSK), Definition unterswünschte Ereignis (Abweichung vom Ziel), Auswirkung + Ausmass – As Low As Reasonable Practicable - Umgekehrte Pyramide, Unten: Tiefe Einzelrisiken, Massnahmen getroffen, Inkaufnahme, Mitte: Normen, Standards, Anforderungen erfüllt, Inkaufnahme höhere Risiken, Oben: Risiko vs "Konsument"-Risiko

Methoden:
Fishbone: Häufigkeit: Nein, Ausmass: Nein, Auswirkungen: Nein, Unsicherheiten: Nein, Ursachen: Ja – Fishbone / Ishikawa, Brainstorming, Def. Auslöser / Ursachen
Master Logic Diagramm: Häufigkeit: Nein, Ausmass: Nein, Auswirkungen: Nein, Unsicherheiten: Nein, Ursachen: Ja – Ursachen / Auswirkungen Ereignis, Hierarchie von Ursachen, grafisch dargestellte Liste
Bow-Tie: Häufigkeiten: Nein, Ausmass: Prosa, Auswirkungen: Indirekt, Unsicherheiten: Nein, Ursachen: Ja, Ursachen / Auswirkungen, Ursachen – Ereignis: Präventive Spärren, Ereignis – Schaden: Schadensmindernde Sperren, Mehrere Sperren pro Verbindung, Eskalationsfaktor: Pro Sperre EF, Schwächt Wirkung Sperre, Massnahmen zur Verhinderung Abschwächung
Frequency / Consequence-Diagramm & Risikomatrix: X-Achse: Ausmass, Y-Achse: Häufigkeit, Häufigkeit / Ausmass pro Top-Event eintragen, Akzeptanzlinie: Bewertung (Was ist noch akzeptabel?) unterhalb: gute Risiken, oberhalb: schlechte R, Linie durch Mgmt / Auftraggeber festgelegt, evtl. Ausschluss best. Ausmasse / Häufigkeiten – Verschiebung Punkte
Fishbone, Bow-Tie, MLD: Top-Event wird benötigt.
Failure Mode and Effects Analysis (FMEA): Ausfallarten / Konsequenzen, Qualitative Untersuchung von Einheiten auf Ausfallarten und deren Auswirkungen auf übergeordnetes System, induktiv, Prozess: PDCA, Gründe FMEA: Umsetzung Unternehmensziele (Null-Fehler-Produkte), steigende Kunden-Req., verschärfte gesetzl. Auflagen, Einsatz über gesamten Entwicklungsprozess, meist in Risiko- / Qualitätsmanagement Fertigungsindustrie – Ablauf: 1. Ablauf alle Einheiten (E), 2. Identifizierung Ausfallarten für jede E., 3. Bestimmung Auswirkungen jeder Ausfallart auf andere E und Auswertung Auswirkung auf System / Systemzustand, 4. Klassifizierung nach Gefahr pro Ausfallart, 5. Ermittlung Vorgehensweise Reduktion Ausfallhäufigkeit / - wirkung, 6. Ausfüllen Formelblatt – Arten: System-, Konstruktions-, Produkt-, Prozess-FMEA – Spalten: 1. Baugruppe/Teil/Prozess/Schritt, 2. Ausfallart (Entwicklung und Gebrauch), 3. Fehlerfolgen (Worst Case), 4. Control Item D (Sicherheitsrelevant: J/N), 5. Fehlerursachen (Mensch, Maschine, Material, Methode, Mitwelt), 6. Verhütungs- / Prüfmassnahmen, 7. Auftreten (1-10), 8. Bedeutung (1-10), 9. Entdeckbarkeit (1-10) vor Auslieferung an Kunde, ausgehend von betrachteten Arbeitsphase, E > 1 (Fehler erst mind. Im übernächsten Arbeitsschritt entdeckt), E = 0 (Design-Fehler, Entdeckt bei internem Kunden, Fertigungsfehler), E = 10 (Entdeckt bei externem Kunden, Lebensdauerursachen), 10. Risikoprioritätszahl RPZ (= A*B*E) RPZmin = 1, mittel = 125, max = 1000, Orientierungsgrösse, RPZ mit grossem A vorrangig bearbeiten, A >= 8, b >= 8: intensive Betrachtung - Kunde: derjenige bei dem der ungünstigste Fall auftreten kann (K-FMEA: meist Endbenutzer Produkt – P-FMEA: letzter Arbeitschritt, bei dem der Fehler zu Störungen führen kann)

ZuverlässigkeitskenngrössenSchätzung:
WSK / Probability (Pr): Dimensionslose Grösse zwischen 0 und 1 (Basis: Axiomsystem Kolmogoroff), klassisch: frequentistisch: relative Häufigkeit (bzw. %), subjektiv: Grad Erwartung / Vertrauen eines individuums – **Häufigkeit:** absolut: Anzahl eingeroffener Ereignisse n, relativ: bezogen auf ein Ereignis ^p =n/N (^= Schätzer), bezogen auf Zeit: Rate, Frequenz – Frequenz: akt. Veränderung Grösse in Einheiten zur veränderung einer anderen Grösse (z.B. Zeit), ^lambda = ^p/delta t – **Lebensdauer:** T, **AusfallWSK** F(T): Anz. Der bis zum Zeitpunkt t ausgefallenen Einheiten bezogen auf Anzahl zu t = 0 funktionsfähigen Einheiten F(t) = Pr(T <= t) (% Anteil der bis zur Zeit t ausgefallenen Einheiten), Randbedingungen: Pr 0: t= 0, 1: t= unendlich – ÜberlebensWSK: Reliability, R(t) = Pr(T > t) = 1 – Pr(T <= 1) = 1 – F(T) | es gilt: R(t=0) = 1, R(t=unendlich) = 0 (% Anteil der bis zur Zeit t funktionierenden Einheiten)
Evt. Weiter Ab Slide 14 (Grundlagen Zuverlässigkeitsanalyse)
Badewannenkurve: Verlauf Ausfallrate, 3 Phasen: sinkend (Frühausfälle, Optimierungsphase), konstant (zufällige ausfälle), steigend (Verschleiss, Alter) – **Mean Time To Failure (mittlere Lebensdauer):** MTFF = t_betriebszeit / n_GesamtzahlAusfälleBeobachtungszeitraum, entspricht Kehrwert Ausfallrate lambda_konstant = 1/MTFF, nur bei nicht instandsetzbaren Einheiten – **Mean Time Between Failures** (mitt. Ausfallabstand), nur bei konstanter Ausfallrate, entspricht Kehrwert Ausfallrate, nur bei instandsetzbaren E.,

Zuverlässigkeitsblockdiagramme:
Zeigt Funktionieren eines Systems, grafische Darstellung Boolsche Gleichung, Seriensystem, Parallelsystem, hat Eingang E und Ausgang A, Berechnung System-Zustandswahrscheinlichkeit (Ausfall- / Überlebenswsk) – **Serie**: System funktioniert wenn beide Komponenten funktionieren, fällt aus wenn eine ausfällt – **Parallel**: System funktioniert wenn eine Komp. Ausfälle, fällt aus wenn beide ausfallen – Boole: 1: Komp funktioniert, 0: funktioniert nicht – **Überlebenswsk**: P(Xi = 1) = P(xi) = pi – Ausfallwsk: P(Xi = 0) = P(nicht xi) = qi – pi + qi = 1 bzw. Pi = 1-qi

- System-Überlebenswahrsch.:

$$\begin{aligned} R_S &= P(X_S) = P(x_1 \wedge x_2) \\ &= p_1 \cdot p_2 \\ &= (1-q_1)\cdot(1-q_2) \\ &= 1 - q_1 - q_2 + q_1 \cdot q_2 \end{aligned}$$

- System-Ausfallwsk:

$$\begin{aligned} F_P &= P(\overline{X}_P) = P(\overline{x}_1 \wedge \overline{x}_2) \\ &= q_1 \cdot q_2 \\ &= (1-p_1)\cdot(1-p_2) \\ &= 1 - p_1 - p_2 + p_1 \cdot p_2 \end{aligned}$$

- System-Ausfallwahrsch.:

$$\begin{aligned} F_S &= P(\overline{X}_S) = P(\overline{x}_1 \vee \overline{x}_2) \\ &= P(\overline{x}_1) + P(\overline{x}_2) - P(\overline{x}_1 \wedge \overline{x}_2) \\ &= q_1 + q_2 - q_1 \cdot q_2 \\ &\equiv 1 - p_1 \cdot p_2 = 1 - R_S \end{aligned}$$

- System-Überlebenswahrsch.:

$$\begin{aligned} R_P &= P(X_P) = P(x_1 \vee x_2) \\ &= P(x_1) + P(x_2) - P(x_1 \wedge x_2) \\ &= p_1 + p_2 - p_1 \cdot p_2 \\ &\equiv 1 - q_1 \cdot q_2 = 1 - F_P \end{aligned}$$

Seriensystem
$W_1 = \{x_1, x_2\}$

W_i	x_1	x_2
W_1	1	1

$S = x_1 \cdot x_2$
$R = p_1 \cdot p_2$

Parallelsystem
$W_1 = \{x_1\}, W_2 = \{x_2\}, W_3 = \{x_1, x_2\}$

W_i	x_1	x_2
W_1	1	0
W_2	0	1
W_3	1	1

$S = x_1(1-x_2) + (1-x_1)x_2 + x_1x_2 = \cdots = x_1 + x_2 - x_1x_2$
$R = p_1 + p_2 - p_1p_2$

Minimalschnitt: kleinste Menge ausgefallener Komponenten, die den Weg vom E zu A versperren, kleinOmegai = {nicht x1, nicht x2,..} **Minimalpfad**: Kleinste Menge funktionierender K, die Weg von E nach A offen hält phij = {x1, x2,...}

Boolsche Algebra
Modell: Zustand technisches System, Gesucht: Vorgehensweise Berechnung AusfallWSK, Problem: Übergang von Boolesche in kanonische Darstellung notwendig, Verfahren Quanitifzierung: ZBD, Minimalschnitte / -pfade, Funktions- / Wahrheitstabellen, Fehlerbäume – Problem 1: X = xi zur WSK P(X = xi), Problem 2: ODER, P(A U B) = P(A)+P(B) – P(A n B), P(A U B) != P(A) +r(B)

Boolesche Variable

$$X = \begin{cases} L & : \text{Zustand erfüllt} \\ O & : \text{Zustand } \textit{nicht} \text{ erfüllt} \end{cases}$$

Boolesche Operatoren

- UND: $\wedge$, $\cap$ (**Anm.:** Wird in Funktionen oft weggelassen, z. B. $X \wedge Y \equiv X$
- ODER: $\vee$, $\cup$

Boolesche Axiome (Schaltalgebra)

symbolisch	Beschreibung	symbolisch	Beschreibung
$X \wedge Y = Y \wedge X$ $X \vee Y = Y \vee X$	kommutative Gesetze	$\overline{\overline{X}} = X$ $\overline{O} = 1; \overline{L} = 0$	Verneinungsgese
$X \wedge Y \wedge Z = (X \wedge Y) \wedge Z$ $X \vee Y \vee Z = (X \vee Y) \vee Z$	assoziative Gesetze	$\overline{(X \wedge Y)} = \overline{X} \vee \overline{Y}$ $\overline{(X \vee Y)} = \overline{X} \wedge \overline{Y}$	de-Morgansches Gesetz
$X \wedge (Y \vee Z) = (X \wedge Y) \vee (X \wedge Z)$ $X \vee (Y \wedge Z) = (X \vee Y) \wedge (X \vee Z)$	distributive Gesetze	$O \wedge X = O$ $L \vee X = L$	Extremalgesetze
$X \wedge X = X$ $X \vee X = X$	Idempotenzgesetze	$L \wedge X = X$ $O \vee X = X$	Neutralitätsgese
$X \wedge (X \vee Y) = X$ $X \vee (X \wedge Y) = X$	Absorptionsgesetze	$X \vee (\overline{X} \wedge Y) = X \vee Y$ $X \wedge (\overline{X} \vee Y) = X \wedge Y$	
$X \wedge \overline{X} = O$ $X \vee \overline{X} = L$	Komplementärgesetze		

Ausfallrate = ^lambda = n/(N*tbetrieb) (Bezogen auf Zeit (interval)) Ausfallwsk: F(t) = 1-e^(-lambda t), konstante Ausfalli
Ausfallwahrscheinlichkeit (P = n/N)
MeanTimeToFialure (1/x)
Wahrscheinlichkeit: F(t) = 1-e^(-lambda t)
Emp. Ausfalldichte ^f(t) = Anz. Der im intervall t, t+delta T ausgefallenen Einheiten / n
Emp. Ausfallrate ^lambda(t) = "" / Anz. Zur Zeit t funktionsfähig Elmenten * delta t

Kanonische Darstellung Boolescher Funktionen

- **Disjunktive Normalform (DN)**
  $K_0 \vee K_1 \vee \cdots \vee K_{n-1} = \bigvee_{i=0}^{n-1} K_i$
  K_i : Konjunktionsterm, z.B. $x \wedge y$ aus einfachen oder negierten Booleschen Variablen
  Beispiel: Exklusiv-ODER
  $f(x_0, x_1) = (x_0 \wedge \overline{x}_1) \vee (\overline{x}_0 \wedge x_1)$
- **Ausgezeichnete DN (ADN):** in jedem K_i kommt jede Variable genau einmal vor (einfach oder negiert). Eine solche Konjunktion wird Minterm MI genannt.

  Vorgehensweise: „Unvollständige" Konjunktionsterme K_i mit „1 ": $X \vee \overline{X} = L$ erweitern

$$\begin{aligned} x_0 \vee \overline{x}_1 &= x_0(x_1 \vee \overline{x}_1) \vee \overline{x}_1(x_0 \vee \overline{x}_0) \\ &= x_0x_1 \vee x_0\overline{x}_1 \vee x_0\overline{x}_1 \vee \overline{x}_0\overline{x}_1 \quad |\text{Idempotenzgesetz} \\ &= x_0x_1 \vee x_0\overline{x}_1 \vee \overline{x}_0\overline{x}_1 \end{aligned}$$

Vertiefung des Beispiels $x_0 \vee \overline{x}_1$

- ADN des Beispiels (s.o.): $x_0 \vee \overline{x}_1 = x_0x_1 \vee x_0\overline{x}_1 \vee \overline{x}_0\overline{x}_1$
- Diese ADN enhält drei Minterme MI
  $MI_1 = x_0x_1$; $MI_2 = x_0\overline{x}_1$; $MI_3 = \overline{x}_0\overline{x}_1$
- Scheinbar bleibt das „Summenproblem" mit den ODER-Verknüpfungen. **Aber:** Eine paarweise Verknüpfung von Mintermen ergibt null, d.h.

$$\begin{aligned} MI_1 \wedge MI_2 &= x_0x_0x_1\overline{x}_1 = 0 \\ MI_1 \wedge MI_3 &= x_0\overline{x}_0x_1\overline{x}_1 = 0 \\ MI_2 \wedge MI_3 &= x_0\overline{x}_0\overline{x}_1\overline{x}_1 = 0 \end{aligned}$$

- Damit wird der Übergang zu Wahrscheinlichkeiten möglich:

$$x_0 \vee \overline{x}_1 = x_0x_1 \vee x_0\overline{x}_1 \vee \overline{x}_0\overline{x}_1 = x_0x_1 + x_0\overline{x}_1 + \overline{x}_0\overline{x}_1$$
$$\Rightarrow P(x_0 \vee \overline{x}_1) = P(x_0)P(x_1) + P(x_0)\overline{x}_1 + P(\overline{x}_0)P(\overline{x}_1)$$