Lernkärtchen für Risikoanalyse
Prof. W. Kröger
1. Teil

Frühling 2006

Erstellt durch
Eveline Minder

Welches sind mögliche Fragestellungen in der Risikoanalytik?

-Warum soll man sich damit auseinandersetzen?

-In welchem Rahmen? Mit welchem Ziel?
- -was
- -mit welchen Methoden?
- -wie Gefährdungen erkennen, Ursachen ermitteln?
- -wie externe Auswirkungen abschätzen?
- -wie Plausibilitätsprüfung/Beurteilung durchführen?
- -Interpretation, Beurteilung der Ergebnisse? Optimierungsmöglichkeiten?
- -welches Risiko ist niedrig genug?

-Welche rechtliche Vorgaben sind vorhanden?

Welche zwei Arten von Risiko gibt es?
Was sind allgemein die Aufgabenstellungen der Risikoanalytik? Worauf konzentriert man sich und was sollte man beachten?

Risiko:
-das tatsächliche (mathematisch. gefasste)
-das wahrgenommene (subjektiv empfundene)

Aufgabenstellungen: -Ermittlung (Analyse)
-Beurteilung (Bewertung)
-Handhabung (Management)
von Gefahren und Risiken mit naturwiss./ingenieurwiss. Methoden ->
Konzentration auf das mathem. gefasste Risiko (berechnet)

Beachtung von:
-Nachprüfbarkeit
-Unabhängigkeit des Analytikers
-sachgerechte Anwendung einer Methode (logisch!)
-Angabe von Unsicherheiten

Was ist die Definition von Risiko?
Wie wird es berechnet?
Wie gewichtet?

Definition:
Mass für die Grösse einer Gefährdung. Funktion der Häufigkeit (F) und des Schadenausmasses (C)
Die zwei Elemente des Risikos: Schaden und Häufigkeit

Berechnung:
Risiko = f(F,C) = $\sum$Fi * Ci (bei mehreren Ereignissen)
(Nachteil: grosse Schäden werden über kl. Häufigkeit „weggerechnet“)

Gewichtung (Aversion – d.h.?):
ab Schwellenwert a, Gewichtung mit Koeff.α (zw.1,2 und 2)
Risiko = F*C (A< ai)
Risiko = F*C^α (A>ai)
Bei Infrastrukturen: zusätzliche Berücksichtigung der Häufigkeit einer Unterbrechung des Services + Folgen für Betroffene.

Welche verschiedenen Arten von mathematisch. gefasstem Risiko gibt es?

-Statistisches Risiko: aufgrund von vorliegenden Daten
- Erfahrungsgesetze aus vielen gleichen Eregnissen ableitbar
- Übertragung von Beobachtung auf System/Ereignisebene

-Wahres Risiko: aufgrund vollständiger Daten -> erst nach unendlich langer Beobachtung -> praktisch: unmöglich

-Prognostisches Risiko:aufgrund von Störfallszenarien und Modelle (z.B. Fehlerbaumanalyse):
-Ereignisse durch Eintrittswahrsch. bestimmbar
-Beobacht. auf Komponentenebene

-Grenzrisiko: grösstes noch vertretbares Risiko

-Restrisiko: Deskriptiv: nach allen Sicherheitsmassnahmen verbleibendes Risiko (bewusst akzeptiertes Risiko; falsch beurteiltes Risiko; nicht erkannte Gefahren)
Normativ: erlaubtes Risiko (Akzeptabilitätsbeurteilungen)

Was bedeutet „Schaden“?

Allg.: negative Folgen eines unerwünschten Ereignisses oder Beeinträchtigung eines Schutzgutes.

I.e.S.: Schwächung/Schädigung der Zuverlässigkeit, Sicherheit oder Tauglichkeit der materiellen Substanz der Betrachtungseinheit.

Beachte: Schadensgrössen sind nicht immer eindeutig definiert. Bsp.: Zählung Schwerverletzter nach einem Unfall.

Was bedeutet Häufigkeit?
Welche verschiedene Arten von Häufigkeit gibt es?

-Häufigkeit: Anzahl

-rel.Häufigkeit: Anzahl pro mögliche Fälle: F = n/N

-Rate: momentane Veränderung einer Grösse in (üblicherweise) Zeiteinheit. Empirisch: art Durchschnittsbildung über ein Zeitintervall.

-Frequenz: zeitbezogene Häufigkeit

-Wahrscheinlichkeit: dimensionslose Grösse zwischen 0 und 1. (Axiomsystem von Kolmogoroff)

Was ist der Unterschied zwischen Gefahr und Gefährdung?

Gefahr: Zustand, Umstand oder Vorgang aus dem Schaden entstehen kann. Bsp.: eine Tankfüllung Benzin, ein Messer.

Gefährdung: Konkretisierung einer Gefahr auf Personen oder Sachen. Ein „spezifiziertes Potential“ nach Art, Grösse und Richtung.

Was bedeutet Sicherheit? Was bedeutet Schutz?

Sicherheit: Nichtvorhandensein von Gefahren.
subjektiv: empfundene Gewissheit, geschützt zu sein
inhärent: Eigenschaft die eine Gefahr zwingend auf ein akzeptierbares Mass limitiert.

Schutz: Kontrolle/Isolation einer Gefährdung (aktiv) oder deren Abwehr (passiv)

Wie sieht der Ablauf einer Risikoanalyse aus? (allgemein, schematisch)
(s. S.32 1.Folienteil)

Was gehört zur Analysevorbereitung?

-Klärung der Methodik, Vorgehensweise, Ressourcenrahmens
(Fragestellung, Gefahrenermittlung, Ereignisabläufe und – häufigkeiten)

-Definition der Schutzziele
(Personen, Umgebungs- und Sachwertschutz + Risikozielvorgaben)

-Festlegung Analyseobjekts (Dokumentation + Systemgrenzen, ev. LCA)

-Festlegung Systemzustände und –arten (Normalbetrieb, Störfälle, Stilllegung, … + Produktion, Transport, Lagerung)

-Festlegung Analysetiefe (Abschneidekriterium bestimmen, d.h. Grenze der Eintrittshäufigkeit bis zu welcher Abläufe verfolgt werden)

-Festlegung zu berücksichtigender Einwirkungen:
im System: techn. oder menschl. Versagen
von aussen: natürliche oder zivilisationsbedingte Ursachen

Welche Beziehung besteht zwischen „Risikoanalyse“ und „Risikomanagement“?

Das **Risikomanagement** (Überbegriff) beinhaltet:

-Risikobewertung: -**Risikoanalyse** + Risikoevaluation

-Risikobehandlung: -vermeidung
-optimierung
-verlagerung
-„behaltung“ (ähnlich wie Akzeptanz)

-Risikoakzeptanz

-Risikokommunikation

Welche Basismethoden der Risikoanalytik gibt es?

-Screening-Methoden:
Checklisten, Master Logic Diagramm, Fishbone-Diagramm
(Brainstorming-mässig – so nach gesundem Menschenverstand)

-Semiformale Mehoden:
Hazard and Operability Study (HAZOP),
Failure Mode and Effects Analysis (FMEA),
Zurich Hazard Analysis (ZHA)

-Formale Methoden: Ereignisbaum, Fehlerbaum

Was sind die Ziele und Gründe für eine „Hazard and Operability Study“ (HAZOP)?
Wo wird sie angewendet?

Ziele: -qualitative Untersuchung von Prozessen in einem System. D.h. Erkennung von Gefahren in und ausserhalb des Systems und Ursachen von betrieblichen Störungen.

Gründe: verschärfte Auflagen.

Anwendungsbereich:
allg. verfahrenstechnische Systeme (kontinuierliche Produktion oder diskontinuierliche Prozesse)

Welches sind die Arbeitsschritte einer HAZOP und was beinhalten sie?

1. Festlegung von Leitwörtern (kein, gering, höher, anders,…) und Prozessvariablen (z.B. Massenstrom, Korrosionsprodukte, Betriebszustand,…)

2. Zusammensetzung des Teams (Vorsitzender, Experten, 5-7-Personen)

3. Beschaffung von Anlageinformationen (z.B. Konstruktionszeichnungen, Rohrleitungsschemata, Betriebsvorschriften,… - durch Begehungen überprüfen)

4. Dokumentation der Ergebnisse (Eintrag in Tabelle)

Tabelle einer HAZOP:
Leitwort/Abweichung/mögliche Ursachen/Folgen/erforderliche Handlung
(Bsp. s. S.12 2. Folienteil)

Was sind die Ziele und einer der Gründe einer „Failure Mode and Effects Analysis“ (FMEA)?

Ziele:
-qualitative Untersuchung von Einheiten bezüglich Ausfallarten und Auswirkungen auf das übergeordnete System. (wie der Name sagt: Ausfalleffektanalyse, Fehlermöglichkeits- und Fehlereinflussanalyse)
- Umsetzung von Unternehmenszielen (Null-Fehler-Produkte) und steigende Kundenanforderungen
- Verschärfte gesetzliche Auflagen (z.B. innerhalb der schweizerischen Störfallverordnung)

Grund:
80% aller Fehler beruhen auf Schwachstellen im Design (d.h. Entwicklung und Konstruktion von Einheiten), viele sind Wiederholungsfehler.

Welches sind die ersten 3 Arbeitsschritte einer FMEA und was beinhalten sie?

1. Auflistung möglicher Ausfallarten (aller Einheiten): Funktionselemente (schliessen, öffnen, geschlossen bleiben,…) und Ausfallarten (fällt offen/geschlossen aus, schliesst nur teilweise….)

2. Identifizierung aller Ausfallmöglichkeiten (für jede Einheit): alle Funktionselemente anschauen

3. Bestimmung der Auswirkungen auf angrenzende Einheiten und Auswertung der Folgen: Klassifikation des **Systemzustandes** und seiner Auswirkungen (z.B. Klasse 1, **sicher**, unverändert / Klasse 3, **kritisch**, Vollausfall /…)

Was sind die Schritte 4 – 6 einer FMEA und was beinhalten sie?

4. Klassifizierung der Gefahr und **Auswirkung** (Klasse 1, **sehr schwer**, schwere System- und Personenschäden / …)

5. Ermittlung der Vorgehensweisen zur Risikoverminderung, Klassifizierung von Ereignishäufigkeiten (Klasse wahrscheinlich, >1x Versagen in 10^4 Betriebsstunden,…)

6. Ausfüllen eines Formblattes (Tabelle:
Nr / Einheit / Ausfallarten / Häufigkeit / Ausfallerkennung / Massnahmen / Auswirkungen auf angrenzende Einheiten / Bemerkungen / Systemzustand (Spalte 4 -7 beziehen sich auf Spalte 3)
(s. S.20 2. Folienteil)

Was ist die Aufgabenstellung und das Ziel einer „Zurich“ Hazard Analysis (ZHA)?
Welchen Vorteil hat sie bezüglich der HAZOP und der FMEA?

Aufgabenstellung:
vereinfachte qualitative und semiqualitative Analyse einer Betrachtungseinheit.

Ziel:
Ermittlung eines Risikoprofils

Arbeittsschritte: -Systemgrenze
-Unterlagen
-Expertenteam
-Gefahrenidentifikation
-Risikoabschätzung
-Massnahmen

Vorteil: nicht nur einen einzelnen Ausfall betrachtbar, sondern auch Verkettungen.

Was sind Ziele einer Ereignisablaufanalyse (Ereignisbaum / „Event tree analysis“)?

Ziele:
Erfassen der Ereignisabläufe in einem System. Ausgehend von einem auslösenden Ereignis erfolgen Reaktionen in nachfolgenden Subsystemen.
-graphische Darstellung des Ineinandergreifen von Ereignissen (Prinzipieller Aufbau eines Ereignisbaums: s. S.33 2. Folienteil)
- Ermittlung von Zuständen mit einer gewissen Ursache
-Berechnung der Eintrittshäufigkeiten der Systemzustände

Merke: ET ist auch anwendbar auf menschliche Handlungen, physikalisch/chemische und andere Ereignisse mit binärem Charakter.

Welches sind die Arbeitsschritte einer quantitativen Ereignisablaufanalysse?

1. Auflisten aller auslösenden Ereignisse

2. Identifizierung der direkten (funktionellen) Systemantworten

3. Zusammenfügen der auslösenden Ereignisse mit allen Systemantworten

4. Bestimmung von Ereignisketten: am Ende jeder Kette: Beschreibung der Auswirkungen

5. Zuweisung von Eintrittshäufigkeit [a^-1] für das auslösende Ereignis und „bedingten“ Wahrscheinlichkeiten für Funktion/Ausfall

6. Berechnung der Eintrittshäufigkeit der Endzustände des Gesamtsystems.

Was ist zu beachten bei dem Rechnen mit den Wahrscheinlichkeiten innerhalb eines Ereignisbaumes?

- Die Summe über alle „Kettenwahrscheinlichkeiten“ = die des auslösenden Ereignisses

-Die Eintrittswahrscheinlichkeit am Ende einer Kette berechnet sich aus dem Produkt aller vorhergehenden Ereignissen (samt auslösendes Ereignis) s. S.36 2. Folienteil

-Die Wahrscheinlichkeit eines bestimmten Ausmasses ist die Summe der Ketten mit demselben Endergebnis. (Wenn z.B. zwei Ketten zu Feuergrösse „klein“ gelangen -> Beträge adieren.)

Wozu ist eine Ereignisablaufanalyse geeignet?
Was ist dazu nötig?
Was ist zu beachten?

Eignung:
-für grössere Anlagen
-mit aktiven/passiven Sicherheitseinrichtungen
-ungewissen physikalisch-chemischen Zuständen
-für alle Arten technischer Systeme

Notwendigkeit:
-Praktische Erfahrungen + vorausgehende Systemuntersuchungen

Zu beachten:
-> auch EB gibt keine Garantie
-> Review der Ergebnisse gehört zu vollständiger Analyse

Wann ist eine Fault Tree Analysis (FTA) / Fehlerbaumanalyse nötig?
Worin besteht ihren Ansatz und welches sind die Ziele?

-wenn sich komplexe oder „neuartige“ Systeme nicht mehr als „black box“ analysieren lassen, wenn direkt nutzbare Erfahrungen nicht vorliegen.
-Lösungsansatz (deduktives Vorgehen): Zerlegung in Systemkomponenten, deren Eigenschaften eher bekannt sind und somit ihre logischen und funktionellen Verknüpfungen modellierbar werden. Ausgangssituation: definierter Systemzustand („top event“ als Systemausfall) -> Aufschlüsselung „top down“ über Zwischenzustände bis zum Basisereignis (Komponentenausfall).

-Ziele:
-Identifizierung von Ausfallkombinationen (Ursachen) und deren Basisereignisse, welche zu einem „top event“ führen können
-Ermittlung der Eintrittswahrscheinlichkeit von Ausfallkombinationen und des „top events“, (aus Ausfallwahrscheinlichkeiten der Basisereignisse)

Welches sind die Arbeitsschritte der FTA? Was beinhalten sie?

1.Festlegung des „top events“ (Ausfall eines Systems oder best. Funktion)

2.Identifizierung aller Ereigniskombinationen (logische Verknüpfungen UND, ODER, NICHT) die zum „top event“ führen und zugehörige Basisereignisse.

3.Ermittlung von Eintrittswahrscheinlichkeiten (die Ausfallswahrscheinlichkeit und die Ausfallsrate sind zwei von mehreren Zuverlässigkeitskenngrössen (ZKG))

4.Systemmodellierung und Berechnung der Eintrittswahrscheinlichkeit. von Verzweigungen und des „top events“ (techn. und logische Verbindung von Betrachtungseinheiten (BE), d.h. Komponenten. Jede BE kann zwei Zustände annehmen.

5.Analyse der dominierenden Ereigniskombinationen und –beiträge, Vorschläge zur Optimierung

Welche Informationen braucht es für eine FTA?

-relevante Ausfallarten

-relevante Einflussgrössen, z.B. Instandhaltungsmassnahmen, Umwelteinwirkungen

-Zuverlässigkeitskenngrössen (ZKG) (Ausfallwahrscheinlichkeiten)

-Definition des Betriebszustandes und der Systemgrenze der Anlage

Was sind Problematiken bzgl. FTA?

-allg. Datenmangel, v.a. bei ZKG für Spezialanfertigungen in der Kernenergie, für Komponenten unter wechselnden Betriebsbedingungen in der Chemie, für anhängige Ausfälle,…

-Verfügbarkeit von Daten ist Brachenspezifisch (Chemie: wenig Datenquellen)

Was sind Vor- und Nachteile der FTA?

Vorteile:
-gute Modellierung von mechanischer, dualer Vorgänge
-Betrachtung des Zusammenwirkens mehrer Ausfälle auf Komponentenebene möglich. Berechnung bedingter Wahrscheinlichkeiten
-bei genügend Daten -> Quantifizierung möglich
-breite Einsatzmöglichkeiten – Systemoptimierung eingeschlossen

Nachteile:
-schwere Modellierung von zeitabhängigen dynamischen Änderungen wegen „statischer“ Systembeschreibung
-viele Verzweigungen werden unüberschaubar -> Beschränkung aufs Wesentliche
-Eintrittswahrscheinlichkeiten sind z.T. schwer zu ermitteln + unsicher.

Was versteht man unter „Minimalschnitte“ (Cut Sets) bzw. „Minimalpfade“(Path Sets)?

Minimalschnitte (Cut Sets):
kleinste Menge ausgefallener Einheiten, die den Weg vom „Eingang“ zum „Ausgang“ versperrt. (Bsp. s. S. 56 2. Folienteil)

Minimalpfade (Path Sets):
kleinste Menge (funktionierender) Einheiten, die einen Weg vom „Eingang“ zum „Ausgang“ offen hält.

Was sind die Unterschiede zwischen dem Fehlerbaum und dem Ereignisbaum?

Fehlerbaum	**Ereignisbaum**
Deduktive Logik („abwärts“)	Induktive Logik („vorwärts“)
Logische Beziehungen zwischen Ereignissen	Beziehungen nebeneinander gestellter Ereignisse (bedingte Wahrscheinlichkeit)
Einzelne Kette von Ereignissen -> keine technische Bedeutung	Jede Kette hat systemtechnische Bedeutung
„Top event“ legt Systemzustand nicht zwingend fest (meist aber Systemausfall)	Systemzustand wird am Ende einer Kette definiert
	Einsicht in den Beitrag verschiedener Ausfallarten
Statische Betrachtungsweise	Berücksichtigung dynamischer Prozesse begrenzt möglich

Was sind Eigenschaften eines Zuverlässigkeitsblockdiagramm (ZBD)?
Welche Arten von Basissystemen gibt es?

Ein ZBD hat:
-einen Eingang E
-einen Ausgang A
-ein Weg von E nach A (Funktion des Systems)
-alle Einheiten funktionierend

Basissysteme:

Seriensystem / Parallelsystem

Wichtige Bezeichnungen und Grundlagen der „Systemanalyse“?

Bezeichnungen:
-xi: Einheit (Komponente i) weist „Funktion“ auf: (xi = 1)
-xi^-:Einheit weist „Ausfall“ auf ($xi^- = 0$)
-S,(S^-): Boolesche Systemfunktion „Funktion“ („Ausfall“)
-pi (qi): Überlebens- (Ausfallswahrscheinlichkeit) der Einheit i
-R (F): Überlebens- (Ausfallswahrscheinlichkeit) des Systems
-entsprechendes für pi(t), qi(t), R(t), F(t)

wichtige Grundlagen:
- R+F = 1
-p+q = 1
-Idempotenzgesetz: $A \wedge A = A$; $A \vee A = A$
-$xi = 1 - xi^-$

Unterschied Seriensystem, Parallelsystem?
R?
R(t), F(t)?

Seriensystem	**Parallelsystem**
Funktioniert, wenn alle Einheiten funktionieren (Zustand 1)	Fällt aus, wenn alle Einheiten ausfallen (Zustand 0)
$R = p1*p2$	$R = p1+p2 - p1*p2$ (Ereignisse des Überlebens x1 v x2 schliessen sich nicht gegenseitig aus; sie sind voneinander unabhängig)
$R(t) = \Pi\ pi(t)$ $F(t) = 1 - \Pi\ pi(t)$	$R(t) = 1 - \Pi\ qi(t)$ $F(t) = \Pi\ qi(t)$

Es gilt: $q = 1 - p$

$p = 1 - q$

Wie berechnet man die Zuverlässigkeit z.B. einer Brückenschaltung?

-**Funktionstabelle** aufschreiben:
4 Kästchen -> alle Möglichkeiten aufschreiben

-**Zuverlässigkeit**: s (x_) = Summe aller möglichen Kombinationen (jede Kombination als Produkt der Zustände -> x = Funktion, (1-x) = Versagen)

-Annahme p=0.9 -> **Ergebnis**: R=3p^2-2p^3=0.972 (wie geht das genau??)

Wozu braucht man Schaltalgebra? Was beinhaltet sie?

Die Schaltalgebra ist der Ausgangspunkt des Boolschen Modells, welches die Zusammenhänge und Verknüpfungen von Systembestandteilen beschreibt. Dies geschieht in Form von Boolschen Funktionen und zweiwertigen Variablen. Für das Rechnen gelten die Regeln der Boolschen Algebra. (s. S. 11 3. Folienteil)

Schaltalgebra:
-Variablen x, y können Werte 0 und 1 annehmen.
-Operationen: UND, ODER, NICHT -> in Wahrheitstafeln aufgeführt (s. S. 10 3. Folienteil)
-Zeit ist nicht explizit enthalten.

Markoffsche Zuverlässigkeitsmodellierung -> s. S. 14-24 3.Folienteil
(ist nicht so schwierig wie's aussieht… Frage: ist es wichtig??)

Was ist MTTR und MTTF?

MTTR: Mean Time to repair: $\mu=1/MTTR$
(Witz: MTTR kann man aus Erfahrung abschätzen -> daraus hat man μ, welches man in die DGL von Markoff einsetzen kann)

MTTF: Mean Time to failure:$\lambda=1/MTTF$

Wozu Bayes-Statistik? Was ist das?

-> als Erweiterung der „klassischen“ Statistik, weil dort
-anlagespezifische Daten selten + aufwendige Evaluation
-generische Daten selten, veraltet + „unsauber“
-„expert judgement“ ist subjektiv

Bayes:
Prioriwissen + Likelihoodwissen = Posterioriwissen

Ansatz:
$\Theta i = \Theta + \varepsilon i$
-> i-ter Parameter der Stichprobeni bis n =
„idealer“ Parameter, z.B. „wahrer Mittelwert“ + Fehlerteil

Parameter sind nicht konstant (klassische Statistik) sondern verteilt.
(d.h.??)
(Ein Bsp. zur konkreten Berechnung s. S.30+31 3.Folienteil)

Welche spezielle Problematiken gibt es in der Risikoanalytik?

-Humanfaktoren (Arten, Gutwilligkeit vs. Böswilligkeit (in der VL wird immer von Gutwilligkeit ausgegangen), Modellierung menschlicher Zuverlässigkeit)
Zahlen: 80-90% in der Chemie
60-80% in der Luftfahrt
~20% interne und externe Auslöser in der Kernkraft
50-70% interne Auslöser in der Kernkraft
-> menschliches Versagen „beinhaltet“ oder darauf zurück zu führen-

-Abhängige Ausfälle (Kategorisierung, Modellierungsansätze, Einbezug von Naturgefahren)

Wie kann menschliches Versagen dargestellt werden?

Mit einer Human Reliability Analysis (HRA -> Ereignisbaum, Binärabfrage)

-> Mensch als „Funktionselement“ innerhalb einer Fehlerbaum- oder Ereignisablaufanalyse zur Erfassung der Wechselwirkungen „Mensch-System“. Menschliches Versagen = Komponentenversagen.

Voraussetzungen:

-Kenntnis des Systems und der Handlungen
- Einbezug zusätzlicher Faktoren wie Personal- und Handlungskopplungen,…

Wie sieht der Ablauf einer HRA aus? Arbeitsschritte?

1.Analyse der nötigen Handlungen und Aufgaben: Informationen und Übermittlung, Anfang und Ende einer Aufgabe, Klassifikation

2.Analyse des Einflusses der Handlungen auf die Systemsicherheit (Auswahl der wesentlichen Handlungen)

3.Quantifizierung des Verhaltens
Methoden zur Ermittlung von Irrtumswahrscheinlichkeiten:
-THERP: Aufschlüsselung in Unteraufgaben bis Schätzwerte verfügbar + Zeiteinfluss
-AIPA: Zeitabhängigkeit: Verhalten als Verhältnis von benötigter und verfügbarer Zeit (Zeit hilft)
-SLIM: Expertengestützt: Bewertung von Handlungen. Anhand von Erfahrungswerten Kalibrierung der Expertenmeinungen.

4.Erstellung eines Fehlerbaums oder Ereignisbaum (Bsp. s. S. 9+10 4.Folienteil)

Welches sind
-der methodische Ansatz des Accident Initiation and Progression Analysis (AIPA-Modell)?
-die Modellgleichung?

Ansatz (d.h. Annahmen -> zeigen schon wie gut das Modell ist):
-Personal reagiert nicht sofort
-bei genügend Zeit wird Personal Ereignis nicht verschlechtern
-falls erste Handlung nicht reicht, werden weitere Massnahmen getroffen
Gleichung:
Pr (OF) = exp (-t / MTOR) >= 1-Pr(S)

Pr(OF): Wahrsch. des Ausbleibens der richtigen Handlung
t: verfügbare Zeit (berechenbar)
MTOR: für Handlung benötigte Zeit (mean time to a correct operator response – Zeit in der 63% Handlung richtig durchführen)
MTOR +10%, falls Stress höher als normal
Pr(S) obere Schranke der Erfolgswahrsch. einer Handlung (0.99-0.9999)
(Bsp. einer Anwendung s. S. 15 4.Folienteil)

-> AIPA: einfache Anwendbarkeit, Randbedingungen: 10^-4<Pr(OF)<1

Welches sind die ersten 2 Arbeitsschritte der Success Likelihood Index Methodology (SLIM)?

1.Beschreibung, Definition der „Handlungen“ (Gespräch mit Experten und Personal)

2.Bestimmung der PSF (Performance Shaping Factor = Faktoren welche die Durchführbarkeit einer Handlung bestimmen)
-> Bewertung und –Gewichtung (Befragung von Betriebsmannschaften)
-> wichtig für Irrtumswahrsch.abschätzung (FLI).

Für Bewertung der Verfahrensführung (wie werden Anlagevorschriften durchgeführt): Rangliste mit Skalierung von 0-10
Für Gewichtung der Schnittstelle Mensch-Maschine (wie wird die Handlung überprüft???): Rangliste mit Skalierung von 0-4
(genaue Tabellen s. S. 18 +19 4. Folienteil)

Welches sind Schritte 3 und 4?

3.Gruppierung der Handlungen: Zusammenfassung der Gewichtungen:
FLI (Failure Likelihood Index, d.h. die relative Irrtumswahrsch.)

$FLI = \sum wk * rk$
k = PSF (k01,…,n); wk: Gewichtung; rk: Bewertung; (w, r gemittelt)

4.Kalibrierung und Umwandlung des SLI in Irrtumswahrscheinlichkeiten (Human Error Probabilities, HEP, d.h Fehlerwahrscheinlichkeiten)-> mit Erfahrungswerten quantifizieren.

$\log (HEP) = a * FLI + b$
a: Steigung (aus Erfahrung); b: Achsenabschnitt

Was sind Kernfragen zu SLIM?

-Wie sollen Experten zu Rate gezogen werden? Einzeln, als Gruppe?

-Wie Gruppenprozess strukturieren?
Wann Gewichtungen und Zusammenfassungen vornehmen?

-Wie Handlungen gruppieren? Wie Schwankungen in Expertenbeurteilungen berücksichtigen?

-Wahl der PSF wenn Abhängigkeiten oder Korrelationen Rangfolgen stören(???)?

-Wie Unsicherheiten aus Kalibrierung und Umwandlung minimal behalten?

Was ist das Fazit aus der Problematik „Human Facctors“?

-Mensch beeinflusst Zuverlässigkeit technischer Systeme erheblich

-Mit HRA Handlungen modellier- und quantifizierbar (aber unsicher)

-HRA ist nur Teilgebiet von Human Factors

-Analysen realistischer, aber umfangreicher und komplexer

-„Methoden“ sind (k)ein Ersatz für Erfahrungen (??? hat sich da ein Fehler in die Folien eingeschlichen? S.23 -> ich würde sagen: kein)

Warum sind abhängige Ausfälle eine spezielle Problematik?

Weil bisherige Modellannahmen alle Ausfälle als voneinander unabhängig betrachtet haben, d.h. der Ausfall einer Einheit hat keinen funktionalen oder physikalischen Einfluss auf andere Einheiten.

-> dies widerspricht der alltäglichen Erfahrung

Bsp. von abhängigen Ausfällen: **Notstromversorgung**: obwohl hochredundant – es stehen alle Tanke im selben Raum, sie werden von 1 Operateur gewartet (Brechung der Redundanz)

Anderes Bsp.: **Kernkraftwerke**

Was ist ein Abhängiger Ausfall (dependent failure, DF)?

Was sind mehrfach zusammenhängende Ausfälle (multiple related failures, MRF)?

Abhängiger Ausfall:
-Ereignis, dessen Eintrittswahrscheinlichkeit nicht als Produkt einzelner Eintrittswahrscheinlichkeiten darstellbar ist.
(DF spielen nur innerhalb redundanter Systeme (Parallelsysteme) eine Rolle)

Mehrfach zusammenhängende Ausfälle:
Ereignisse, die durch irgendwelche voneinander abhängigen Strukturen hervorgerufen werden:
-CCF (common cause failure) -> aus gemeinsamen Ursache mehrere Ausfälle (z.B. Überflutung)
-CMF(common mode failure) ->wie oben, wenn mehrere Bestandteile auf dieselbe Art ausfallen.
-CF(causal or cascade failures) ->sich ausbreitende Ausfälle
-Common cause initiating events -> Startereignisse, die Ereignisszenarien auslösen können

Welche Typen von Ursachen von DF gibt es?

-gemeinsame Ursache -> n identische Einheiten fallen gleichzeitig und gemeinsam aus.

-Folgefehler -> benachbarte Einheiten einer Redundanzgruppe fallen durch die Auswirkungen des ersten Ausfalls ebenfalls aus.

-Systemabhängigkeiten -> die Systemvernetzung führt zu Abhängigkeiten (Steuersystem fällt aus)

Vorteile einer Modellierung von DF?
Problematiken?
Arbeitsschritte?

Vorteile:
-vollständigere Beschreibung eines Systems
-nicht zu optimistische Ergebnisse

Problematiken:
-wenig Daten (aus Betriebserfahrung)
-Schwierigkeit zu klassifizieren führt zu Schwankungen der quantitativen Aussagen.

Arbeitsschritte:
1.Identifizieren von DF in technischem System.
2.Qualitative und quantitative Berücksichtigung von DF in logischem Rahmen (Modellbildung mit Modellierungsansätze (s. nächstes Kärtchen))
3.Möglichkeiten zur Vermeidung/Verringerung der Auswirkungen durch DF.

Welche expliziten Modellierungsansätze gibt es?

-Ereignisspezifische Modelle
z.B. für Erdbebe, Brand, Überflutung, Rohrleitungsbruch,…

-Ereignisbaum- und Fehlerbaumanalyse
für funktionelle Abhängigkeiten von gemeinsamen Einheiten

-Modelle zur Quantifizierung von Personalhandlungen
für Abhängigkeiten zwischen Personenhandlungen. Z.B. Kopplungsmodelle in THERP

-> explizite Methoden erfassen strukturelle/funktionelle Abhängigkeiten, sind anlagenspezifisch und nicht sicher vollständig.

Welche impliziten Ansätze (Methoden)?
Was ist generell zu impliziten Methoden zu sagen?

-Marshall-Olkin-Modell
-β-Faktor-Modell
-MGL-Modell (Multiple Greek Letter)
-BFR-Modell (Binominal Failure Rate)

Generell:
-sie sind zur Erfassung von Restanteilen gemacht (d.h.?)
-erfassen DF vollständig, aber wegen Datenbasis nur auf Ebene der Betrachtungseinheiten möglich (d.h.?)
-grosse Unsicherheiten
-Gefahr in Fehlerbaumanalyse Abhängigkeiten zu übersehen /zu unterschätzen

Welches sind die 4 Arbeitsschritte des Marshall-Olkin-Modells?

1.Systemmodellierung ohne DF-Anteil

2.Einbezug des DF-Anteils

3.Systemausfallwahrscheinlichkeit

4.Ausfallwahrscheinlichkeit der Einheiten

(Genaueres hierzu auf S. 14-18, 4. Folienteil)

Welche vereinfachenden Annahmen macht das β-Faktor-Modell?

Definition des β-Faktors?

Ausfälle in einer Redundanzgruppe sind entweder unabhängig oder es fallen immer alle n Einheiten aus.

Definition β-Faktor:

β = Anzahl DF-Ausfälle / Anzahl Gesamtausfälle

bzw. $\beta = Qn / (Q1 + Qn) = Qn / Qt$,

Qn: Kombination von n Ausfällen
Q1: Ein Ausfall
Qt: tot. Ausfallswahrscheinlichkeit einer Einheit in einer Redundanzgruppe

Was sind Vor- und Nachteile des β-Faktor-Modells?

Vorteile	**Nachteile**
Leichte Anwendbarkeit	Zu konservativ bei gleichzeitigem Ausfall von mehr als zwei redundanten Einheiten
β-Parameter relativ leicht aus Betriebserfahrungen bestimmbar	Ergebnisse sind bei Redundanzgruppen > 2 zu konservativ
	Gefahr der pauschalen Anwendung

Dem letzten Nachteil begegnet man, indem man ein MGL-Modell anwendet. Dort sind die Annahmen identisch zum β-Faktor-Modell, aber alle Kombinationen von Ausfällen sind zugelassen (Genaueres dazu s. S. 22 – 25, 4 Folienteil).

Mögliche Prüfungsfragen: