

Grundlagen der technischen Risikoanalytik

Methodik der probabilistischen/quantitativen Risikoanalyse



Inhalt

- Vorgehensweise
- Analyseschwerpunkte, Szenarienanalyse
- Ergebnisdarstellung
- Unsicherheiten

Probabilistische Risikoanalyse

- Man unterstellt das Auftreten von Störfallauslösern und Versagen von störfallbeherrschenden Einrichtungen bzw. Massnahmen.
- Man modelliert das technische System und bestimmt Szenarien mit zugehörigen Eintrittshäufigkeiten und Anlagezuständen.
- Man modelliert für die postulierten Szenarien ausgelöste physikalische Phänomene und schätzt die verursachten Schäden ab – innerhalb und ausserhalb der Anlage.
- Das Risiko des betrachteten Systems ergibt sich beispielsweise aus der Summe der Produkte von realistisch bestimmten Schadensumfängen x und Häufigkeiten $h(x)$: $R = x_1 \cdot h(x_1) + x_2 \cdot h(x_2) + \dots$
für eine Menge möglicher auslösender Ereignisse und Ereignisketten (Szenarien), die einander ausschliessen müssen.

Betrachtungsweisen

Deterministisch (postulierend)

- Ereignisse durch Wirkungsketten durchgängig vorbestimmt (Kausalität).
- Analyse der Wirkung angenommener Ursachen.

Statistisch (rückschauend)

- Erfahrungsgesetze ableitbar aus grosser Anzahl von gleichen Ereignissen.
- Übertragung direkt nutzbarer Beobachtung auf System / Ereignisebene.

Probabilistisch (prognostisch)

- Ereignisse und Ereignisketten im Voraus identifizierbar und durch Eintrittswahrscheinlichkeiten bestimmbar.
- Nutzung von Beobachtungen auf der Ebene von Komponenten (Axiomsystem von Kolmogoroff).

Begriffe zur probabilistischen Risikoanalyse

Ereignisse (Beispiele):

- Pumpe fällt innerhalb eines vorgegebenen Zeitraumes aus
- Windgeschwindigkeit überschreitet innerhalb eines vorgegebenen Zeitraumes einen bestimmten Wert,
- eine Vielzahl von Vorkommnissen löst eine physikalische Reaktion aus usw.

Wahrscheinlichkeiten:

- Klassisch (Laplace): Wahrscheinlichkeit als Zahl der Fälle, in denen ein Ereignis eintritt, dividiert durch die Zahl aller möglichen Fälle (Wahrscheinlichkeit als relative Häufigkeit).
- Frequentistisch (Mises): Wahrscheinlichkeit als Grenzwert der relativen Häufigkeit, mit der ein Ereignis bei (unendlich) vielen Wiederholungen unter gleichen Bedingungen eintritt.
- Subjektiv: Wahrscheinlichkeit als Grad der Erwartung oder des Vertrauens eines Individuums in die Aussage, dass ein mögliches Ereignis eintritt, ein umschriebener Sachverhalt zutrifft, usw.

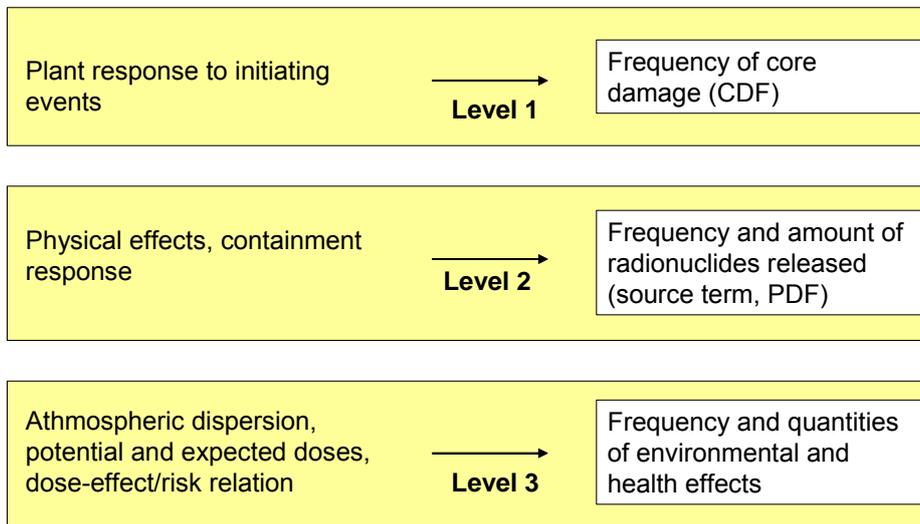
Frequenz:

- Zeitbezogene Häufigkeit (z.B. Anzahl pro Jahr)

PRA indicators

- Core damage frequency (**CDF**): „Expected number of events per calendar year that occur during power operation resulting in uncovering or heat up of the reactor core and leading to significant release of radioactive material from the core“ [ENSI-A05]
- KKL (Kernkraftwerk Leibstadt) defines Core Damages as:
 - Temperature of the cladding $\geq 1500^{\circ}\text{K}$
 - Cladding oxidation $\geq 17\%$

Structure and "Levels" of a PRA for Nuclear Power Plants



Auslösende Ereignisse

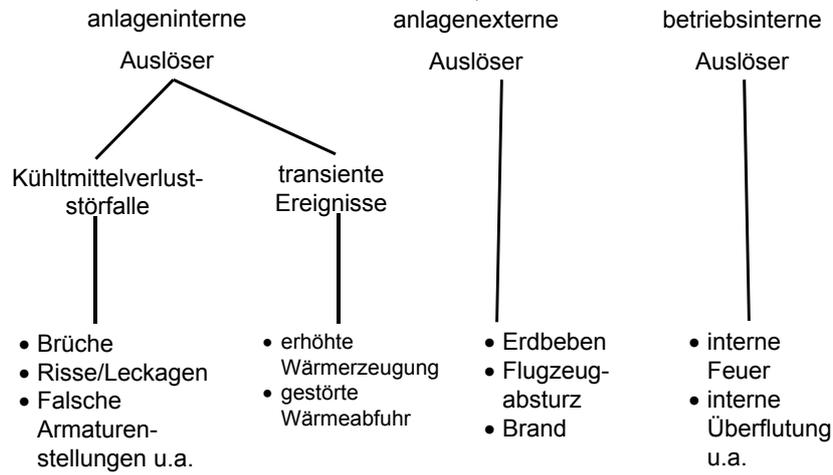
Definition:

- Ein auslösender Ereignis liegt dann vor, wenn ein Zwischenfall eintritt, bei dem eine automatische oder vom Operateur ausgehende Aktion notwendig wird, um die Anlage in einen sicheren Gleichgewichtszustand zu bringen; ohne diese Aktion könnte es zu einer Beschädigung des Kerns kommen.

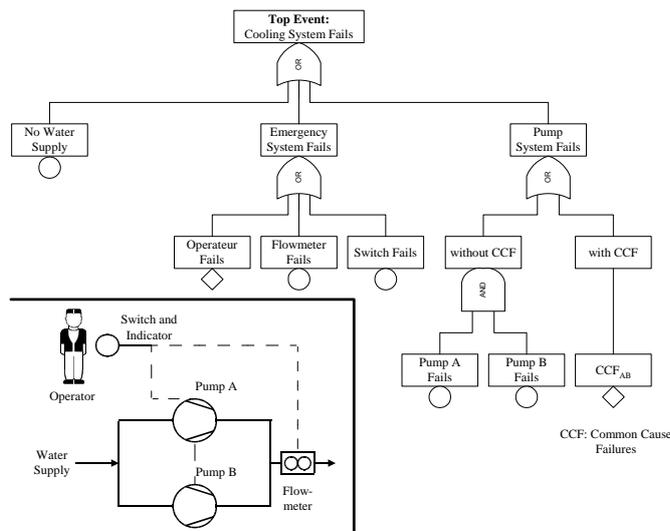
Aufgabe innerhalb einer Level-1-PRA sind:

1. Die Identifikation von auslösenden Ereignissen,
2. ihre Einteilung in Kategorien und
3. die Abschätzung ihrer Häufigkeiten.

Unterteilung

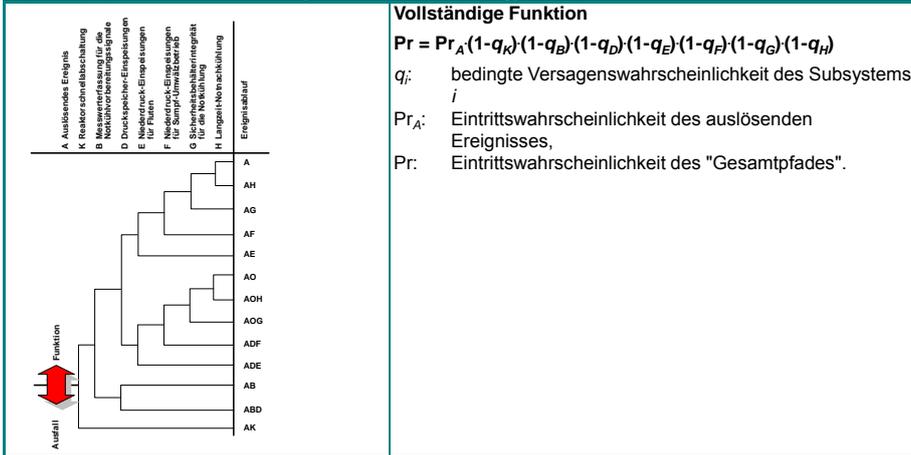


Flow Chart and its Fault Tree Representation (simplified example)

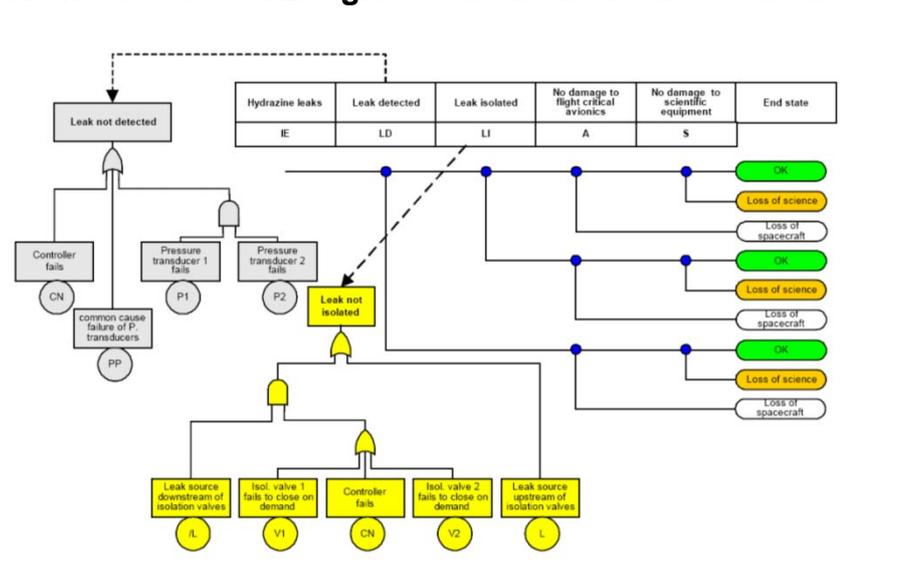


Anwendung Ereignisbaum in der Kernenergie

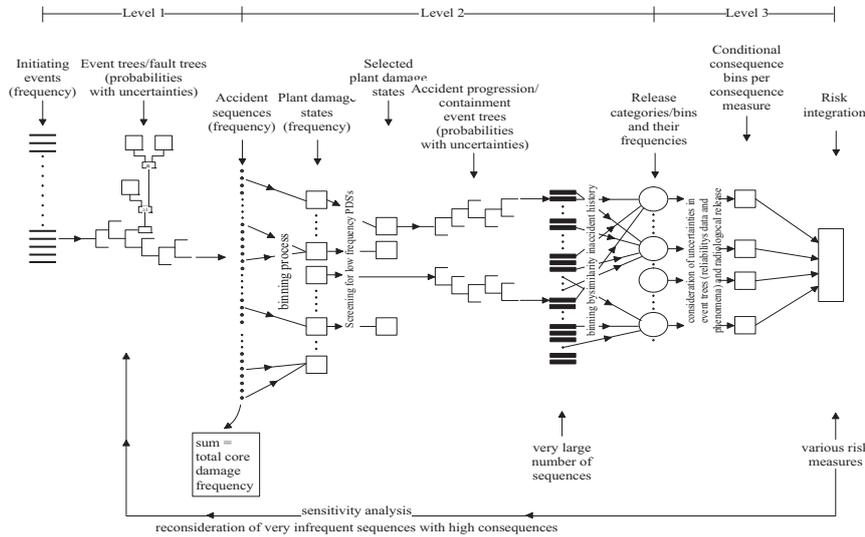
"Grosses Leck in der Hauptkühlmittelleitung" eines KKW



Kombination von Ereignisbäumen und Fehlerbäumen



Überblick über die PRA Methodik



Characterisation of a full PRA (Example KKL)

- More than 100 initiating events (power operation + shut down states) and event trees, more than 1'000 system fault trees, more than 10'000 components
- Accident sequences added to a total core damage frequency (CDF); combined use of fault tree and event tree techniques
- More than 10'000 sequences ($\geq 10^{-10} \text{ a}^{-1}$) binned into 20 plant damage states (PDS)
- 15 to 20 release categories and 10 to 15 damage indicators per release category formed
- Source term analysis: simulation of dominating accident sequences
- Living PSA (revision of models every 10 a, update of plant specific data every 5 years)

Informationsbedarf

Häufigkeit auslösender Ereignisse

- Generische Daten (Veröffentlichungen)
- Anlagespezifische Erfahrung

Systemantwort / Systemzuverlässigkeit

- Zuverlässigkeitskennndaten von einzelnen Komponenten
- Menschliche Zuverlässigkeit (Operator-Unterlassungsfehler)
- Common Cause Fehlermechanismen / Dateien

Erneuerungsprozesse / Instandhaltung

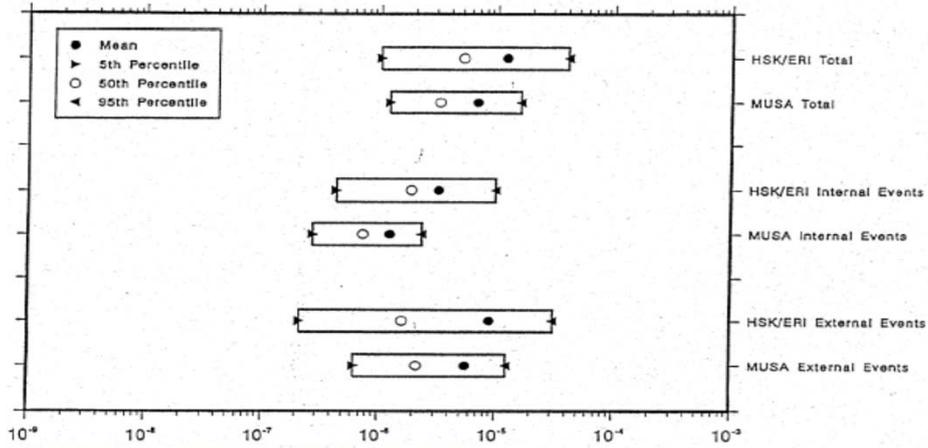
Aktuelle Anlage/Systembeschreibung, Handbücher

GRS-Results Level 1 PRA, German NPP GKN-II, Full Power

Initiating Events	System damage state	Core damage state
Loss of main feed water	26%	<5%
Loss of main heat sink	20%	<5%
Loss of preferred power	17%	10%
Very small primary leaks	16%	53%
SBLOCA via stuck-open SRV	5%	15%
Steam generator tube rupture	4%	7%
Total expected frequency of system damage state without AM: 8.5×10^{-6} /year		
Total expected frequency of core damage state with AM: 2.5×10^{-6} /year		

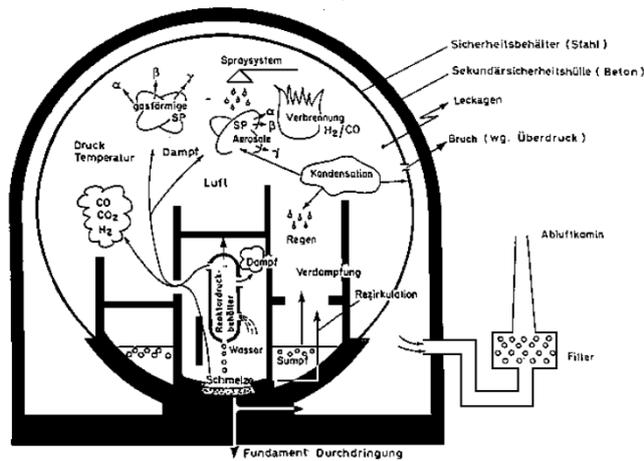
--	Expected frequency of system damage state / year	Expected frequency of core damage state / year
Mean	8.5×10^{-6}	2.5×10^{-6}
5% Fractile	1.6×10^{-6}	4.4×10^{-7}
50% Fractile (median)	4.6×10^{-6}	1.5×10^{-6}
95% Fractile	2.1×10^{-5}	7.3×10^{-6}
„Point Value“**	5.0×10^{-6}	1.7×10^{-6}

Level 1 PRA results for KKM in comparison (“peer review”)

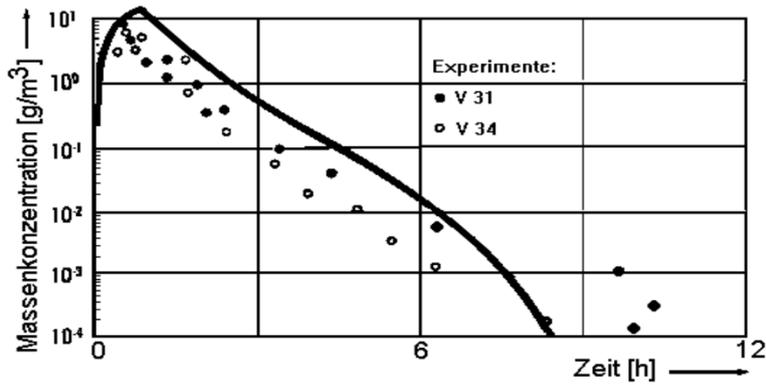


MUSA: Mühleberg Safety Analysis
HSK: Hauptabteilung für Sicherheit von Kernanlagen
ERI: Energy Research, Inc.

Level 2: Phänomene im Sicherheitsbehälter und prinzipielle Freisetzungspfade

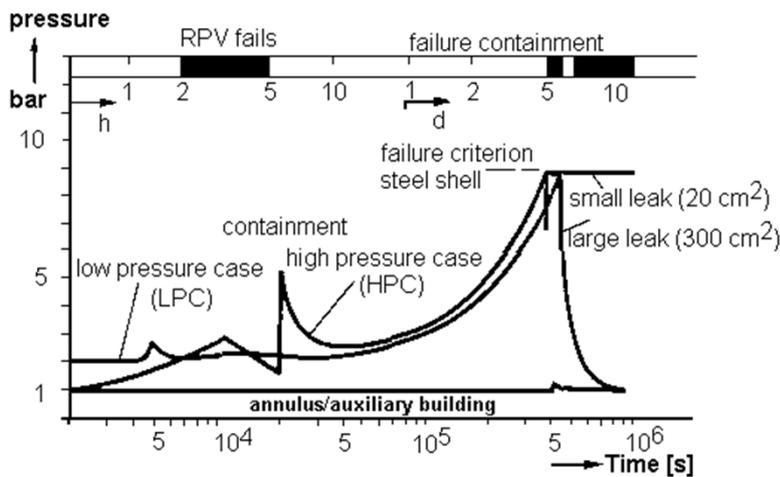


Aerosolkonzentration in Unfallatmosphäre als Funktion der Zeit



Vergleich der berechneten luftgetragenen, zeitabhängigen Aerosolkonzentrationen (Versuchsergebnisse)

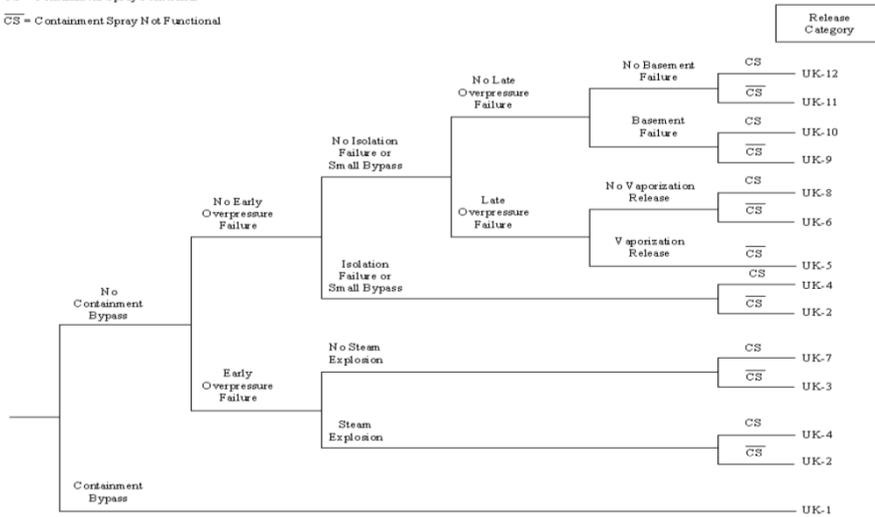
Druckverlauf im Containment nach einem Kernschmelzunfall (II)



Simplified Event Tree for Source Term Characterisation

CS = Containment Spray Functional

\overline{CS} = Containment Spray Not Functional

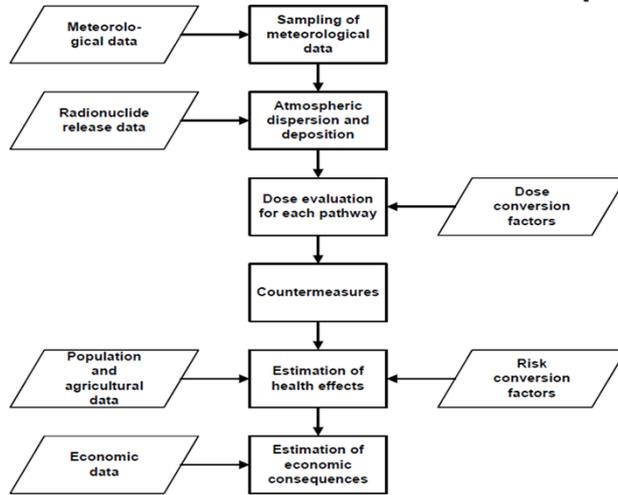


Der Quellterm

- Die Isotopenzusammensetzung und jeweilige Menge, die Wärmemenge in der Schadstoffphase, das Zeitprofil und die Freisetzungshöhe beschreiben den Quellterm.
- Der Quellterm ist aufgeschlüsselt nach Unfallsequenzen mit zugehöriger Eintrittshäufigkeit (Beispiel nachfolgend).

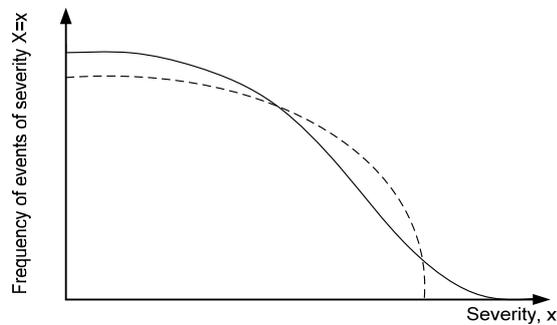
Quellterm	Zeit vor Freisetzung [h]	Dauer der Freisetzung [h]	Freigesetzte Energie [MW]	Freisetzungshöhe [m]	Zeit zur Alarmierung [h]	Freigesetzter Anteil							
						Xe-Kr	Org-I	I	Cs-Rb	Te-Sb	Ba-Sr, Ru	La	
QT1	2.0 3.0	1.0 5.0	2.0 0.2	10 10	1.0 -	1.0 -	0.001 -	0.1 -	0.1 -	0.05 0.05	0 0	0 0.001	
QT2	2.0	1.0	0	10	1.0	1.0	0.001	0.1	0.1	0.1	0.01	0.001	
QT3	2.0	1.0	0	10	1.0	0.1	0.00001	0.001	0.001	0.001	0.0001	0.00001	
QT4	2.0 3.0 5.0	1.0 1.0 1.0	0 0 0	10 10 10	1.0 - -	1.0 - -	0.00033 0.00033 0.00033	0.033 0.033 0.033	0.033 0.033 0.033	0.033 0.033 0.033	0.0033 0.0033 0.0033	0.00033 0.00033 0.00033	
QT5	2.0	24.0	0	10	1.0	1.0	0.001	0.1	0.1	0.1	0.01	0.001	

Elements of Probabilistic Consequence Assessment (PSA Level 3)



Risikodarstellung

- Risiko : $f(\text{Eintrittshäufigkeit, Konsequenzen})$
- Häufigkeits - Ausmass (F/C) – Diagrammen (Histogramm), meist doppelt logarithmisch



Wie kommen die probabilistischen Kurven zustande?

- Ausgangspunkt bildet eine begrenzte Anzahl von Quelltermen, die Unfallsequenzen mit ähnlichem Freisetzungsscharakter konservativ bündeln sowie die zugehörigen Eintrittshäufigkeiten zurodnen.
- Modellierung der Ausbreitung, Exposition und Wirkung durch Gewichtung der Beeinflussungsfaktoren anhand ihrer bedingten Wahrscheinlichkeiten gegeben eine Freisetzung:
 - **Windrichtung** und die daraus resultierende betroffene **Bevölkerungsverteilung** durch Aufteilung der Windrose in Sektoren.
 - **Windstärke** und **atmosphärische Schichtung** bestimmen die Verteilung der Schadstoffe (instabile Schichtung -> gute Verdünnung).
 - **Niederschlag** und damit einhergehende lokale Deposition.
 - Zusammenfassen der Konsequenzen **aller** Freisetzungsklassen und Ordnen nach zunehmender Schwere; Auftragen zugehöriger Häufigkeiten.

Beispiel: Anzahl Tote durch Tornados in den USA in den Jahren 1938 bis 1977

- Kumulierte Häufigkeiten als Basis für F-C-Diagramme
- Vorgehensweise zur Erstellung eines F-C-Summen-Diagramms (CCDF)

$$F(N \geq n) = \sum_{i=1}^k F(N=n_i)$$

Anzahl Todesopfer: n_i	Anzahl Tornados mit n_i Todesopfern: $F(N=n_i)$	kumulative Häufigkeit: $F(N=n_i)$	kumulative Häufigkeit pro Jahr: $F(N=n_i)/40$
10	5	79	1.975
11	4	74	1.850
12	3	70	1.750
...
250	1	3	0.075
270	1	2	0.050
323	1	1	0.025

Unsicherheiten

Risikoanalytik bedeutet die Modellierung und Simulation von Realität mit einer Vielzahl von Daten und Annahmen

Damit ist Risikoanalyse auch immer ein Umgang mit Unsicherheiten.

generelle Massnahmen

Anlagenbegehungen, Gespräche vor Ort, Review, Plausibilitätsabgleiche.

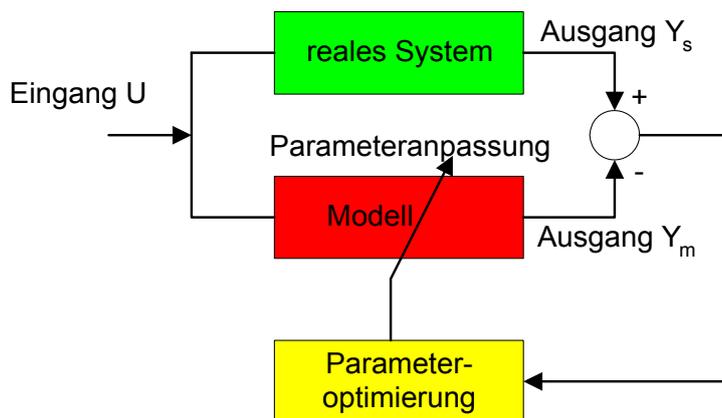
Arten von Unsicherheiten

Strukturunsicherheiten

aus unvollständigem Verständnis der Funktionsweise eines Systems

Massnahme: Modellvalidierung (Vergleich "Modell" - "Realität").

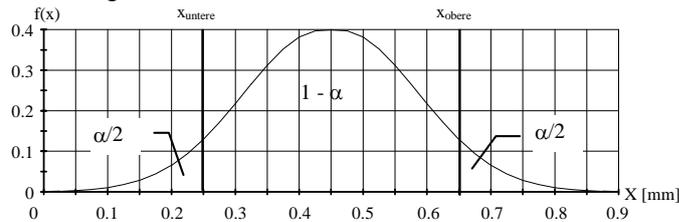
Parameterunsicherheiten: aus ungenauer Kenntnis von Einflussgrössen



Massnahmen: Identifikationsverfahren, Messungen.

Parameterunsicherheiten lassen sich im Rahmen einer Statistik durch Angabe eines **Vertrauensbereiches** angeben.

Ein Vertrauensintervall ist ein Bereich, das den unbekanntem Wert eines zu schätzenden Parameters mit einer vorgegebenen Wahrscheinlichkeit $1 - \alpha$ überdeckt. Je grösser das Intervall (bei vorgegebenem α) ist, desto grösser ist die Streuung.

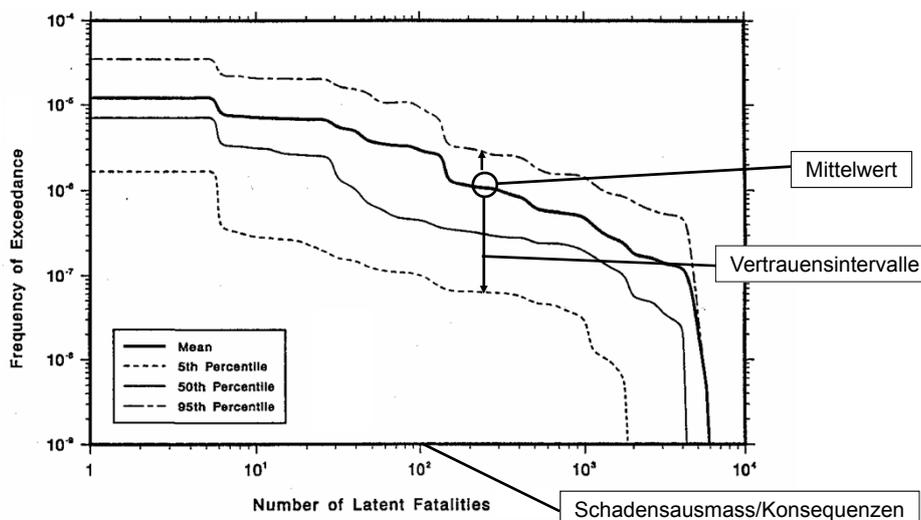


Zweiseitiges Vertrauensintervalle (Normalverteilung)

Modellvoraussetzungen: Modelle sind nur unter bestimmten Voraussetzungen aussagekräftig.

Massnahme: Prüfung auf Plausibilität der Ergebnisse.

Ergebnisdarstellung



Grenzen, Unsicherheiten

- Vollständigkeit des Spektrums auslösender Ereignisse und identifizierter Ereignisketten mathematisch nicht nachweisbar
- Komponenten-Ausfallwahrscheinlichkeit über konstante Ausfallrate beschrieben (keine Verschleissausfälle)
- Human Factors: „Errors of commission“ oft unberücksichtigt
- „Hot issues“: Erfassung
 - aller relevanten Anlagezustände (inkl. Stillstand)
 - bössartiger Attacken (cyber, innere Sabotage)
 - terroristischer Angriffe
- Datenunsicherheiten berücksichtigt und auf CDF Ebene fortgepflanzt