# Grundlagen der technischen Risikoanalytik

## Spezielle Problematiken

ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich
DMAVT
Departement Maschinenbau & Verfahrenstechnik
Department of Mechanical & Process Engineering

## Inhalt

- Abhängige Ausfälle (Bisherige Modellannahmen, Beispiele, Definitionen)
- Übergang zur Modellierung von abhängigen Ausfällen
- Modellbildung (explizite und implizite Methoden)
- Einbezug Naturgefahren (Erdbeben)

## Abhängige Ausfälle

### Bisherige Modellannahmen

Alle Ausfälle in einem System sind voneinander unabhängig, d.h.:

- der Ausfall einer Einheit hat keinen funktionalen Einfluss auf andere Systemeinheiten,
- die physikalischen Auswirkungen des Ausfalls einer Einheit sind für andere Einheiten unbedeutend,
- durch Hinzufügen weiterer (redundanter) Komponenten lässt sich eine beliebig kleine Systemversagenswahrscheinlichkeit erreichen.

**Diese Annahmen widersprechen bereits alltäglicher Erfahrung.**





## Beispiele zu abhängigen Ausfällen: Notstromversorgung

Das Rechenzentrum einer Grossbank verfügt über eine hochredundante Notstromversorgung. Dazu dienen 4 Notsromdiesel (NSD), wobei ein NSD für den Notbetrieb der Zentrale über zwei Tage ausreicht. Fällt ein NSD aus, so wird der nächste gestartet (stand-by-Betrieb). Annahmen:

Operateur

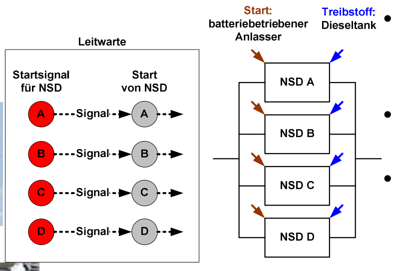



*Bild*: www.cammisawipf.com

- Ein NSD wird von einem Operateur von einer Leitwarte aus gestartet.
- Jeder NSD verfügt über eine eigene Ansteuerung.
- Jeder NSD verfügt über einen Anlasser, eine Batterie und einen Tank.
- Wartung und Betankung aller NSD erfolgt in einem Vorgang.

:

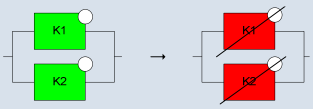
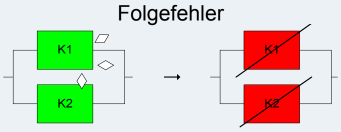
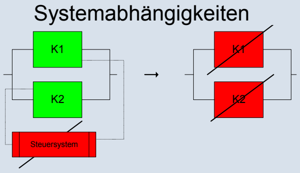
## Definitionen

**Abhängiger Ausfall (dependent failure, DF)**

- Ereignis, dessen **Eintrittswahrscheinlichkeit nicht als Produkt** aus einzelnen Ereigniseintrittswahrscheinlichkeiten darstellbar ist (mathematisch), oder
- Ereignisse, die durch **irgendwelche voneinander abhängigen Strukturen** hervorgerufen werden („Mehrfachausfälle“, technisch)
  - **CCF (common cause failure)**
    Bestimmte Art eines abhängigen Ausfalls, wobei aus einer einzigen gemeinsamen Ursache (fast) gleichzeitig mehrere Ausfälle entstehen
  - **CMF (common mode failure)**
    Ausdruck für bestimmte CCF, in denen mehrere (System-)Bestandteile durch dieselbe Art und Weise ausfallen
  - **CF (causal or cascade failures)**
    Bezeichnung für sich ausbreitende Ausfälle.
  - **Common cause initiating events**
    Bezeichnung für (z.B. „flächig wirkende“) Startereignisse, die mehrere Ereignisse bzw. Ereignisszenarien auslösen können.
- DF können nur innerhalb redundanter Systeme (Parallelsysteme) eine Rolle spielen.



## Ursachen von DF

| Typ | Beschreibung |
|---|---|
| gemeinsame Ursache   | System aus n identischen Einheiten. Unter bestimmten Rahmenbedingungen fallen diese gemeinsam und quasi-gleichzeitig aus. |
| Folgefehler   | Benachbarte Einheiten einer Redundanzgruppe fallen durch die Auswirkungen des Ausfalls der ersten Einheit ebenfalls aus. |
| Systemabhängigkeiten   | Die Systemvernetzung führt zu funktionellen Abhängigkeiten. |

ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

DMAVT
Departement Maschinenbau & Verfahrenstechnik
Department of Mechanical & Process Engineering

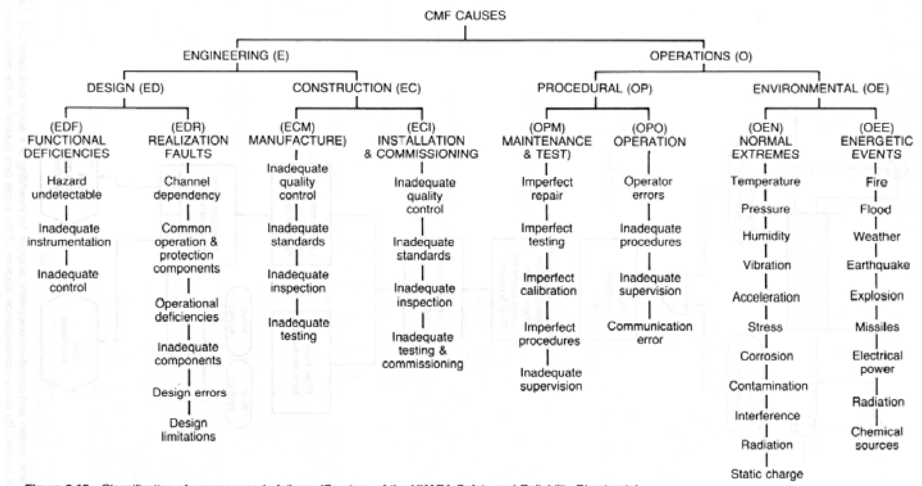



***Figure 9.15*** *Classification of common mode failures (Courtesy of the UKAEA Safety and Reliability Directorate)*

Quelle: Lees F.P., *Loss Prevention in the Process Industries*. Oxford: Butterworth-Heinemann, 1996



ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

DMAVT
Departement Maschinenbau & Verfahrenstechnik
Department of Mechanical & Process Engineering

# Übergang zur Modellierung von DF

**Ohne DF-Berücksichtigung**

- wird ein technisches System unvollständig beschrieben;
- werden Sicherheitsanalysen in ihren Ergebnissen zu optimistisch.

**Problematiken**

- Datenmangel, Betriebserfahrungen (Normalbetrieb, Funktionsprüfungen) müssen oft als Quellen herangezogen werden.
- Beobachtete Ereignisse zum Teil schwierig zu klassifizieren.

**Arbeitsschritte zur Berücksichtigung von DF**

1. Identifizieren möglicher DF in einem technischem System.
2. Qualitative und quantitative Berücksichtigung von DF innerhalb eines logischen Rahmens (Modellbildung).
3. Möglichkeiten zur Vermeidung oder Verringerung der Auswirkungen von DF.

## Modellierungsansätze

**Explizite Methoden**

- **Ereignisspezifische Modelle**
  berücksichtigen z.B. der Einwirkungen von Erdbeben, Brand, externe oder interne Überflutung etc.
- **Ereignisbaum- und Fehlerbaumanalyse**
  berücksichtigen funktioneller Abhängigkeiten unter gemeinsamen Einheiten.
- **Modelle zur Quantifizierung von Personalhandlungen**
  berücksichtigen Abhängigkeiten bei Handlungen mehrer Personen, z.B. Kopplungsmodelle in THERP (Technique for Human Rate Error Prediction).

Explizite Methoden erfassen strukturelle/funktionelle Abhängigkeiten, sind somit anlagen- und situationsspezifisch, aber nicht mit Sicherheit vollständig.





## Modellierungsansätze (Forts.)

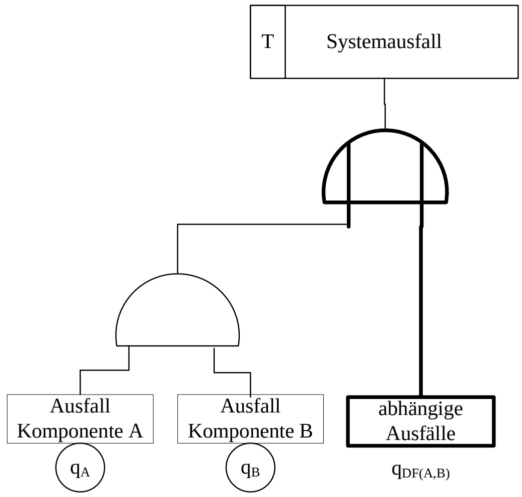
**Implizite Methoden (zur Erfassung von Restanteilen)**

Marshall-Olkin-Modell, $\beta$-Faktor-Modell, MGL-Modell (Multiple Greek Letter), BFR-Modell (Binominal Failure Rate) u.a.

**Generell**

- Implizite Methoden erfassen abhängige Ausfälle im Prinzip vollständig; Anwendung aufgrund der Datenlage aber nur auf Ebene der Betrachtungseinheiten (CMF) möglich und mit grossen Unsicherheiten behaftet.
- Rigorose Anwendung birgt Gefahr in sich, Fehlerbaumanalysen nicht detailliert genug durchzuführen und somit strukturelle/funktionelle Abhängigkeiten zu übersehen bzw. zu unterschätzen.

# Modellbildung (explizite Methoden)








# Modellbildung (implizite Methoden)

**Marshall-Olkin-Modell (Basismodellierung)**

**1. Systemmodellierung ohne DF-Anteil**

**Beispiel**: 2v3-System mit den Einheiten A, B und C

- Systemausfall, wenn zwei Einheiten ausfallen: {A, B}, {A, C}, {B, C}
- Systemausfallwahrscheinlichkeit $Q_s = q_a \cdot q_b + q_a \cdot q_c + q_b \cdot q_c - 2\, q_a \cdot q_b\, q_c$

**Vereinfachungen und Schreibweisen**

- Alle Einheiten (Ausfallwahrscheinlichkeiten) sind gleich: $q_a = q_b = q_c = Q_{k=1}$
  $k$ ($k$ = 1, 2, ..., $n$): Anzahl der am jeweiligen Ausfall beteiligten Einheiten
- Näherung $\Pr(a \cup b) \approx \Pr(a) + \Pr(b)$

- **Systemausfallwahrscheinlichkeit des 2v3-Systems ohne DF-Anteil**

$$\boxed{Q_s = q_a \cdot q_b + q_a \cdot q_c + q_b \cdot q_c = 3 \cdot Q_1^2}$$

**Einbezug des DF-Anteils**

Wahrscheinlichkeiten der Ausfallkombinationen

$q_{AB}$, $q_{BC}$, $q_{AC}$ etc.

$q_{ABC}$, $q_{ABD}$ etc.

Annahme: Gleichheit aller Einheiten:

$q_{AB} = q_{BC} = q_{AC} = \ldots = Q_{k=2}$

$q_{ABC} = q_{ABD} = \ldots = Q_{k=3}$.

**2v3-System**

- Wahrscheinlichkeit des DF-Ausfalls mit zwei beteiligten Einheiten: $3 \cdot Q_2$
- Kombination dreier (aller) Ausfälle $q_{ABC} = Q_3$.

**Systemausfallwahrscheinlichkeit $Q_s$ mit DF-Anteil**

$Q_s =$ ΣPr(unabhängige Ausfälle) + ΣPr(abhängige Ausfälle)

**2v3-System**

$Q_s = 3 \cdot Q_1^2 + 3 \cdot Q_2 + Q_3$.





**Ausfallwahrscheinlichkeit der Einheiten**

$Q_t$ ist die totale Ausfallwahrscheinlichkeit einer Einheit in einer Redundanzgruppe einschliesslich aller Abhängigkeiten. Zur einfacheren Datenermittlung wird ein Zusammenhang zwischen $Q_t$ und $Q_k$ gesucht:

$$Q_t = \sum_{k=1}^{n} \binom{n-1}{k-1} \cdot Q_k$$

mit Binominalterm

$$\binom{n-1}{k-1} \equiv \frac{(n-1)!}{(n-k)! \cdot (k-1)!}$$

Anzahl der Ausfallkombinationen einer Einheit mit ($k$-1) anderen Einheiten in einer Gruppe $n$ - 1 weiterer gleicher Einheiten.

**3er-Redundanzgruppe**

$$Q_t = \binom{3-1}{1-1} \cdot Q_1 + \binom{3-1}{2-1} \cdot Q_2 + \binom{3-1}{3-1} \cdot Q_3 = Q_1 + 2 \cdot Q_2 + Q_3$$

## Bestimmung von $Q_k$ über relative Häufigkeiten

$$Q_k = \frac{n_k}{\binom{n}{k}}$$

$n_k$: als Anzahl der Ausfälle mit $k$ beteiligten Einheiten und dem Binominalterm zur Ermittlung der Anzahl der Kombinationen mit $k$ von $n$ Einheiten.

**Anmerkung:**
Idealerweise liessen sich die verschiedenen $Q_k$ direkt aus Beobachtungsdaten gewinnen. Einige Modelle vereinfachen die Berücksichtigung von DF unter Zuhilfenahme zusätzlicher Annahmen. Ein solches Modell ist das **$\beta$-Faktor-Modell**.





## $\beta$-Faktor-Modell

**vereinfachende Annahme**

Ausfälle in einer Redundanzgruppe sind entweder unabhängig, oder es fallen immer alle $n$ Einheitenaus:

- *mit* $k = 1$ ist $Q_{k=1}$ die Ausfallwahrscheinlichkeit bei unabhängigem Ausfall
- *mit* $k = n$ ist $Q_{k=n}$ die Ausfallwahrscheinlichkeit für (total) abhängige Ausfälle
- Ausfallwahrscheinlichkeit $Q_k = 0$ für $n > k > 1$

**Generell gilt für *mvn*-Systeme**

$$Q_t = Q_1 + Q_n.$$

**Definition $\beta$-Faktor**

$$\beta = \frac{\text{Anzahl DF-Ausfälle}}{\text{Anzahl Gesamtausfälle}} \quad \text{bzw.} \quad \beta = \frac{Q_n}{Q_1 + Q_n} = \frac{Q_n}{Q_t}$$

## Daraus folgt direkt

- $\beta \cdot Q_t = Q_{k=n}$
- $\beta \cdot (Q_1 + Q_n) = Q_{k=n}$

mit einsetzen von $Q_n = Q_t - Q_1$ folgt
$Q_{k=1} = Q_t(1-\beta)$ und damit

$$Q_k = \begin{cases} (1-\beta)\cdot Q_t & k = 1 \\ 0 & m > k > 1 \\ \beta \cdot Q_t & k = n \end{cases}$$

**2v3-System**
Systemausfallwahrscheinlichkeit $Q_s = 3 \cdot Q_1^2 + 3 \cdot Q_2 + Q_3$

wird im β-Faktor-Modell zu $Q_s = 3 \cdot (1-\beta)^2 \cdot Q_t^2 + \beta \cdot Q_t$





## Diskussion des β-Faktor-Modells

| *β*-Faktor-Modell: | |
|---|---|
| **Vorteile** | **Nachteile** |
| leichte Anwendbarkeit | zu konservativ bei gleichzeitigem Ausfall vom mehr als zwei redundanten Einheiten. |
| *β*-Parameter relativ leicht aus Betriebserfahrungen bestimmbar | Ergebnisse sind bei Redundanzgruppen *n* > 2 zu konservativ |
| | Gefahr der pauschalen Anwendung |

# Multiple-Greek-Letter-Modell (MGL-Modell)*

Annahmen identisch zum *b*-Faktor-Modell, jedoch sind alle Kombinationen von Ausfällen zugelassen.

| Parameter, Definitionen | Beispiel: 3er-Redundanzgruppe |
|---|---|
| $Q_t$: totale Ausfallwahrscheinlichkeit einer Einheit | $Q_t = Q_1 + 2Q_2 + Q_3$ |
| $\alpha = 1$ | $\alpha = 1$ |
| $\beta$: alle *abhängigen* Ausfallwahrscheinlichkeiten bezogen auf $Q_t$ | $\beta = \frac{2Q_2 + Q_3}{Q_t} = \frac{2Q_2 + Q_3}{Q_1 + 2Q_2 + Q_3}$ |
| $\gamma$: *Bruchteil* der DF-Ausfallwahrscheinlichkeit der Einheiten, bei dem *mindestens zwei* weitere Einheiten ausfallen | $\gamma = \frac{Q_3}{2Q_2 + Q_3}$ |

* zur Information, kein Prüfungsstoff





Zur Berücksichtigung der MGL-Faktoren wird die Gleichung für $Q_t$ schrittweise nach $Q_k$ ($k$ = 1, 2, 3) aufgelöst. In die dadurch entstehenden Terme werden, entsprechend aufgelöst, die Parameter $\beta$, $\gamma$, etc. eingesetzt.

| Beispiel: 3-er Redundanzgruppe | bekannt, gegeben: $Q_t = Q_1 + 2Q_2 + Q_3$ |
|---|---|
| $Q_1 = \frac{Q_t - (2Q_2 + Q_3)}{1} = Q_t - (\beta Q_t) = Q_t(1-\beta)$ | $\beta = \frac{2Q_2 + Q_3}{Q_t} = \frac{2Q_2 + Q_3}{Q_1 + 2Q_2 + Q_3}$ |
| $Q_2 = \frac{Q_t - (Q_1 + Q_3)}{2} = \frac{Q_t - [Q_t(1-\beta) + \gamma(2Q_2 + Q_3)]}{2} = \frac{Q_t - [Q_t(1-\beta) + \gamma(\beta Q_t)]}{2} = \ldots = \frac{Q_t - \beta(1-\gamma)}{2}$ | $\gamma = \frac{Q_3}{2Q_2 + Q_3}$ |
| $Q_3$ ... | etc. |

Die Ergebnisse lassen sich für Redundanzgruppen mit Hilfe der Notation $\Phi_1 = 1,\ \Phi_2 = \beta,\ \Phi_3 = \gamma,\ \dots, \Phi_{m+1} = 0$ verallgemeinern

$$Q_k = \frac{1}{\binom{n-1}{k-1}} \cdot \left( \prod_{i=1}^{k} \Phi_i \right) \cdot (1 - \Phi_{k+1}) \cdot Q_t$$

**Beispiel: Anwendungsbeispiel 3-er Redundanzgruppe**

| | | |
|---|---|---|
| $Q_{k=1} = \frac{1}{\binom{3-1}{1-1}} \cdot (\Phi_1) \cdot (1-\Phi_2) \cdot Q_t = 1 \cdot (1-\beta) \cdot Q_t$ | $Q_{k=2} = \frac{1}{\binom{3-1}{2-1}} \cdot (\Phi_1 \cdot \Phi_2) \cdot (1-\Phi_3) \cdot Q_t = \frac{1}{2} \cdot 1 \cdot \beta \cdot (1-\gamma) \cdot Q_t$ | $Q_{k=3} = \frac{1}{\binom{3-1}{3-1}} \cdot (\Phi_1 \cdot \Phi_2 \cdot \Phi_3) \cdot (1-\Phi_4) \cdot Q_t = 1 \cdot \beta \cdot \gamma \cdot (1-0) \cdot Q_t$ |



**Beispiel:** Einsetzen der $Q_k$ in die Gleichung "Systemausfallwahrscheinlichkeit des 2v3-Systems $Q_s$ mit DF-Anteil" $Q_s = 3 \cdot Q_1^2 + 3 \cdot Q_2 + Q_3$ ergibt

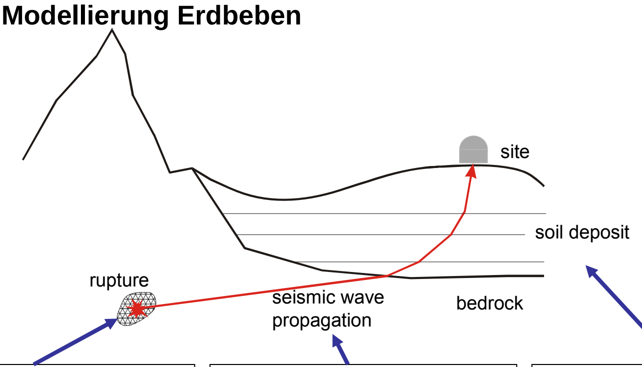
$$\boxed{Q_s = 3(1-\beta)^2 Q_t^2 + \frac{3}{2}\beta(1-\gamma)Q_t + \beta\gamma Q_t}$$

Falls die MGL-Faktoren nicht bekannt sind, lassen sie sich über die jeweiligen $Q_k$ er-mitteln (s.o. unter Parameter, Definitionen). Die Bestimmung der Wahrscheinlich-keiten erfolgt über

$$Q_k = \frac{n_k}{\binom{n}{k}}$$

Mit $\gamma = 1$ folgt as Ergebnis des $\beta$-Faktor-Modells. Allgemein gilt, dass das $\beta$-Faktor-Modell ein Spezialfall des MGL-Modells ist.

## Einbezug flächig wirkender Ereignisse (common cause initiating events): Modellierung Erdbeben




Seismic sources (faults, regions)
Magnitude-recurrence-relation:
e.g.: Gutenberg-Richter

$$\log N(m \geq M) = a - bM$$

M: magnitude (e.g.: $M_w$, $M_s$, $M_l$)
N: number of magnitudes m≥M per year
a, b: regression parameters

Attenuation relation for spectral accelerations or intensities
e.g.:

$$\log S_a = C_1 + C_2 M + C_3 \log(R) + \varepsilon\sigma$$

$\sigma$: aleatoric uncertainty
$C_n$: regression parameters
R: distance site-hypo-/epicentre
$\varepsilon$: coefficient

Site response:
damping or amplification of seismic waves due to soft soil layers

-analytical (frequency domain, RVT)
-numerical (FEM, BEM, FDM)





## Integration der seismischen Quellen

application of the total probability theorem: $\nu(S \geq s) = \sum_n \nu_n \iint f(m) f(r) P(S \geq s \mid m, r) dm dr$

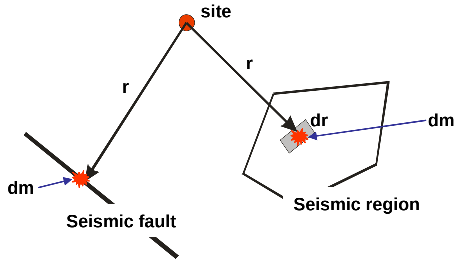
$\nu$ : mean annual rate of occurence of acceleration, intensities etc. S ≥ s at the site

$\nu_n$ : mean annual rate of occurence of magnitudes M ≥ m of the seismic source

f(m): density function of magnitude (magnitude-recurrence relation)

f(r): density function of distance

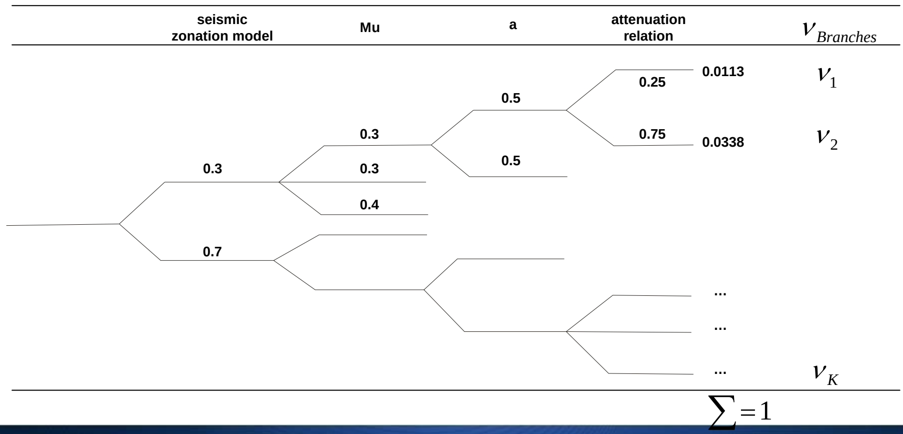
P(S ≥ s|m,r)=conditional probability of S ≥ s (attenuation relation)



## Entscheidungsbaum zur Erfassung der epistemischen Unsicherheiten

epistemic uncertainty: incomplete knowledge (lack of data)

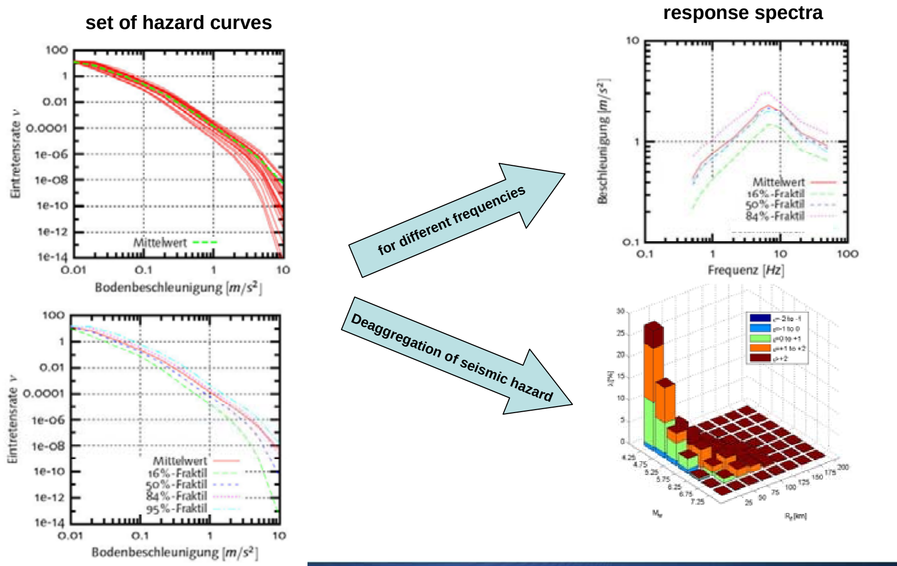
aleatoric uncertainty: inherent randomness of ground motion generation








## Ableitung der Antwortspektren und representative Ereignisse



## Anwendung der Erdbebeneinwirkung auf Bauwerke und deren Anlagen