Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Safety of Nuclear Power Plant : Dependent Failures

Prof. Wolfgang Kröger

(http://www.riskcenter.ethz.ch, kroeger@ethz.ch)

Present model assumptions

- All failures of a system are due to independent failures at components (“elements”) level
- The failure of an element has no functional influence on other system elements
- The physical effects of an element failure on other elements are marginal
- By adding (redundant) elements the systems failure probability can be reduced to a minimum

These assumptions contradict common experience!

German Nuclear Power Plants

- Failure of starting all four emergency diesels while testing leads to the identification of a dependent failure; the batteries for starting the diesels have been insufficiently maintained (Würgassen).

- A polluted screen in the river water inlet (single failure) lead to a lack of cooling water for the main and auxiliary cooling water pumps (dependent failures of the redundant cooling water supply (Lingen).

- A lighting strike (external event as common cause) lead via the bearing oil supply to the shut down of two main cooling water pumps (Stade).

Definitions

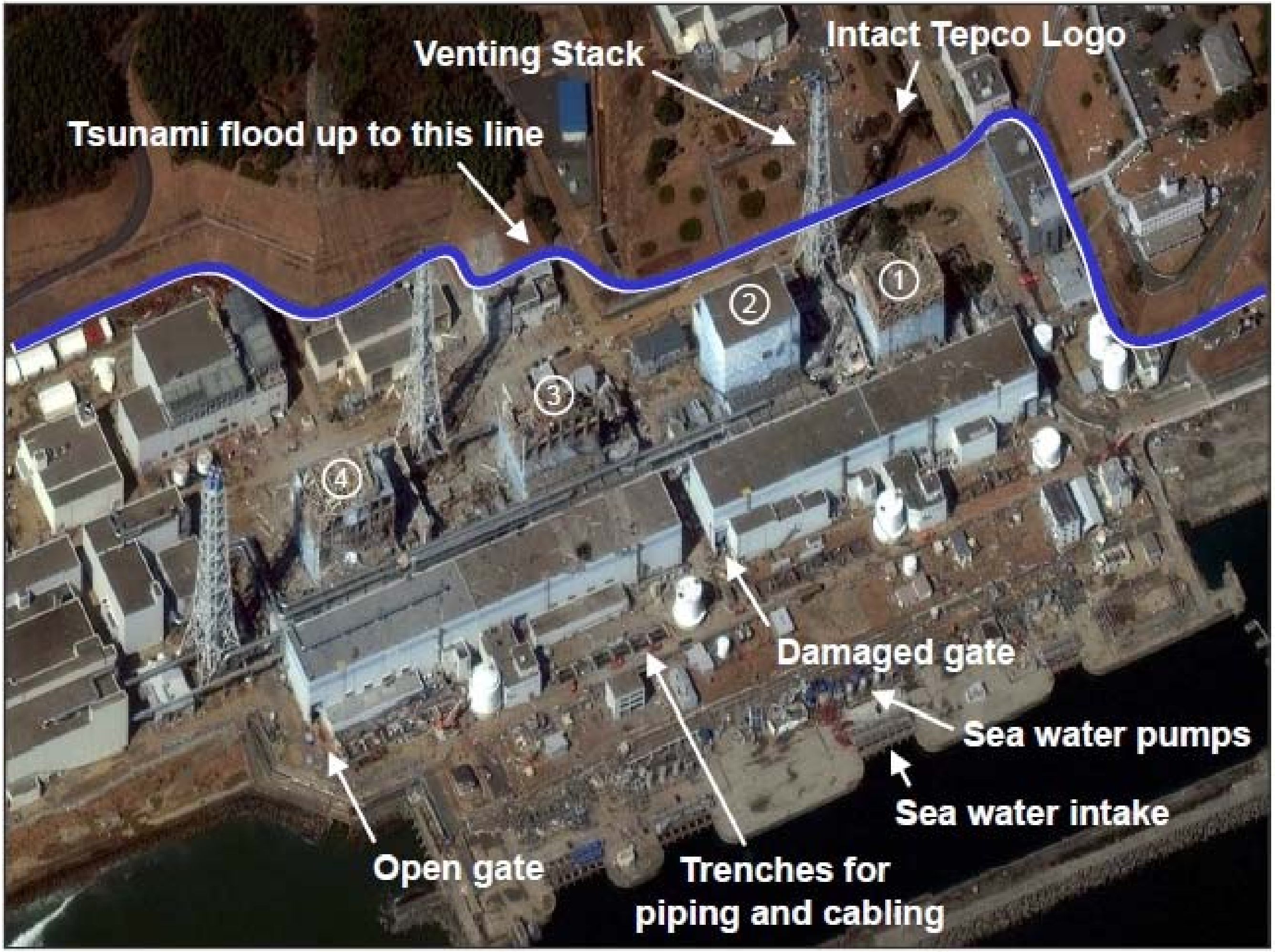
Dependent failure (DF)

Event, of which the occurrence probability cannot be modelled as a product of single occurrence probabilities (mathematical), or

Event, which is caused by any interdependent structures (multiple failure, technical)

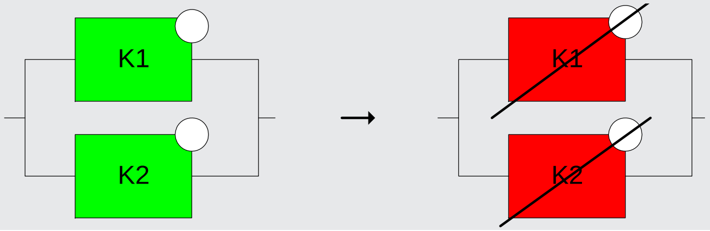
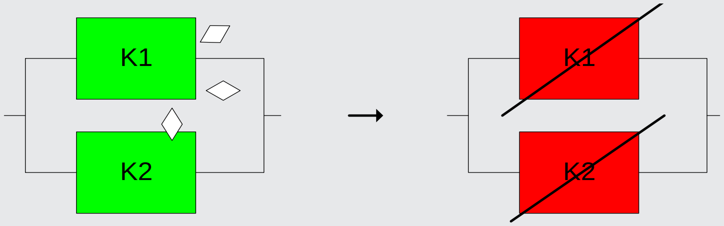
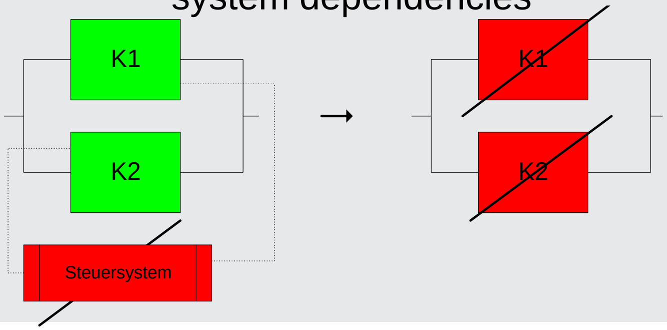
- **CCF** (common cause failure)
  Description of a type of a dependent failure, at which a common single cause triggers several failures occurring (almost) simultaneously
- **CMF** (common mode failure)
  Description for a specific CCF, in which several (system-)units fail in the same way
- **CF** (causal or cascade failures)
  Description for spreading or interdependent failures
- **Common cause initiating events**
  Description for initiating events which can cause several events or event scenarios, e.g. area event such as earthquakes or flooding
- **DF are of paramount important in redundant (parallel) systems.**

Fukushima Dai-ichi : Tsunami Damages



Sources: Janti, Digital Globe, 2011

Causes of DF

Type	Description
common cause  	*m* of *n* system made of *n* identical units. Under certain conditions they all fail at the same time.
cascading failure  	Adjacent units of a redundant group fail due to the influence of the first failure.
system dependencies  	System interconnections lead to dependencies

Transition to the Modeling of DF

Without consideration of existing DF

- uncompleted description of technical systems;
- to optimistic results of safety analysis

Problems:

- Lack of data for highly reliable systems, usually from limited operational experiences (normal operation state, functional testing)
- It is difficult to classify observed events into dependent and independent ones.

Required steps to consider DF

1. Identification of DF in a technical system
2. Qualitative and quantitative consideration of DF within a reasoned framework (model building)
3. Identification of options to prevent/reduce the consequences of DF

Modeling approaches to consider DF

Explicit Methods

- **Event specific models**
  Consideration special consequences from e.g. earthquakes, fire, floods, broken pipes or leakage in the primary loop.
- **Event tree and fault tree analysis**
  Consideration of functional interdependencies (units).
- **Models for the quantification of human actions**
  Consideration of interdependencies between single human actions.
- Examples are interconnecting models in THERP (Technique for Human Rate Error Prediction).

Explicit methods comprise structural and functional interdependencies, they are system-specific but don’t cover safety of systems completely.

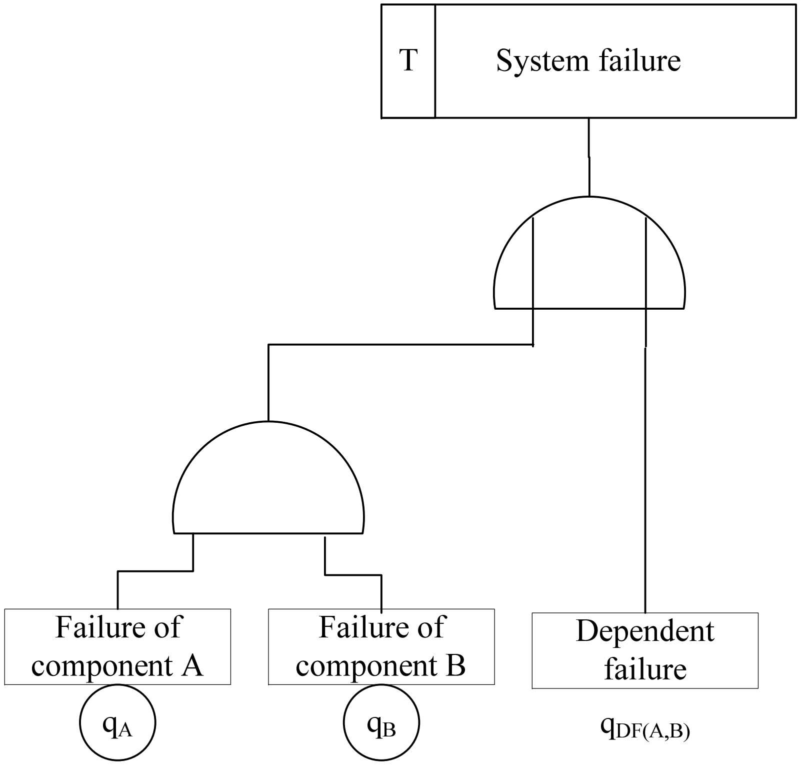
Implicite Method (to consider residuals)

Marshall-Olkin-Model, *b*-Faktor-Model, MGL-Model (Multiple Greek Letter), BFR-Model (Binominal Failure Rate) et al.

General

- In principle, implicit methods can completely cover dependent failures, but great uncertainties arise because the data is based solely on the level of considerate items (CMF).
- Rigorous application bears the danger of insufficient fault tree analyses, e.g. failure of notice or correctly value structural/functional dependencies.

Representation of DF in a fault tree



Modeling (implicit method)

Marshall-Olkin-Model (fundamental modeling)

- **1. System modeling excluding DF**

Example: ‘2 out of 3-system’ with units A, B and C

- System failure, when two units fail: {A, B}, {A, C}, {B, C}
- Probability of system failure: $Q_s = q_a \cdot q_b + q_a \cdot q_c + q_b \cdot q_c - 2\, q_a \cdot q_b\, q_c$

Simplification and notation

- All units failure probabilities are identical: $q_a = q_b = q_c = Q_{k=1}$
  k (k = 1, 2, …, n): Number of involved units in the failure
- Simplification: $\Pr(a \cup b) \approx \Pr(a) + \Pr(b)$

System failure probability of a ‘2 out of 3-system’ excluding DF

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

2. Inclusion of DF in system modeling

Probabilities of failure combinations

- q_{AB}, q_{BC}, q_{AC}
- q_{ABC}

Assumption: equality of all units:

- $q_{AB} = q_{BC} = q_{AC} = \ldots = Q_{k=2}$
- $q_{ABC} = Q_{k=3}$

‘2 out of 3-system’

- Probability of a DF including two units: $3{\cdot}Q_2$
- Combination of three (all) failures: $q_{ABC} = Q_3$.

3. System failure probability

System failure probability Q_s including DF:

Q_s =ΣPr(independent failures) + ΣPr(dependent failures)

‘2 out of 3-system’

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

Failure probability of the units

Q_t is the total failure probability of an element in a group of redundant elements, inclusive of all dependencies. The interrelationship between Q_t and Q_k is asked for:

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

with binominal coefficient

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

Number of failure combinations of an element with (k-1) different elements in a group of (n-1) identical elements.

Group of 3 redundant elements

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

Calculation of Q_k by using relative frequencies

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

n_k: Number of failures with *k* involved elements and the binominal coefficient for the calculation of the combinations with *k* of *n* elements.

Annotation

Ideally the different Q_k can be drawn directly from of observation data. Some models simplify the consideration of DF by making additional assumptions.

One of these models is the ***β*-factor-model**.

β-factor-model

Simplifying assumptions

Failures in a group of redundant elements are either independent or all of the *n* elements fail.

- With $k = 1$, $Q_{k=1}$ is the failure probability of independent failures
- With $k = n$, $Q_{k=n}$ is the failure probability for (totally) dependent failures
- All other failure combination are excluded by definition, so
  $Q_k = 0$ for $n > k > 1$ (for other failure combinations)

For ‘m out of n-system’ it is generally

$$Q_t = Q_1 + Q_n.$$

Definition of the β -factor

$$\beta = \frac{Number\ of\ DF}{Number\ of\ all\ failures} \qquad \beta = \frac{Q_n}{Q_1 + Q_n} = \frac{Q_n}{Q_t}$$

From this it follows directly

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

With $Q_n = Q_t - Q_1$ follows

- $Q_{k=1} = Q_t(1-\beta)$

Finally

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

'2 out of 3-system'

System failure probability $Q_s = 3\cdot Q_1^{\,2} + 3\cdot Q_2 + Q_3$

Changes in the β-factor-model to $Q_s = 3\cdot(1-\beta)^2 \cdot Q_t^2 + \beta \cdot Q_t$

Multiple-Greek-Letter-Model (MGL-Model)

Assumptions identical to the *b*-factor-model, but combinations of failures are possible

Parameter, Definitions	**Example: Group of 3 Redundant Elements**
Q_t: total failure probability of a unit	$Q_t = Q_1 + 2Q_2 + Q_3$
$\alpha = 1$	$\alpha = 1$
β: all *dependent* failure probabilities relating to Q_t	$\beta = \frac{2Q_2 + Q_3}{Q_t} = \frac{2Q_2 + Q_3}{Q_1 + 2Q_2 + Q_3}$
γ: *fraction* of DF probability of a unit, with at least 2 units failing	$\gamma = \frac{Q_3}{2Q_2 + Q_3}$

To consider the MGL-factors the equation for Q_t will be solved for Q_k (k = 1, 2, 3). The resulting terms will be replaced by the parameters β, γ, etc.

Example: Group of 3 Redundant Elements	given: $Q_t = Q_1 + 2Q_2 + Q_3$
$Q_1 = \frac{Q_t - (2Q_2 + Q_3)}{1} = Q_t - (\beta Q_t) = Q_t(1 - \beta)$	$\beta = \frac{2Q_2 + Q_3}{Q_t} = \frac{2Q_2 + Q_3}{Q_1 + 2Q_2 + Q_3}$
$Q_2 = \frac{Q_t - (Q_1 + Q_3)}{2} = \frac{Q_t - \left[Q_t(1-\beta) + \gamma(2Q_2 + Q_3)\right]}{2}$ $= \frac{Q_t - \left[Q_t(1-\beta) + \gamma(\beta Q_t)\right]}{2} = \ldots = \frac{Q_t - \beta(1-\gamma)}{2}$	$\gamma = \frac{Q_3}{2Q_2 + Q_3}$
Q_3 ...	etc.

The results for a redundant group can be generalised by using the notation $\Phi_1 = 1, \Phi_2 = \beta, \Phi_3 = \gamma, \ldots, \Phi_{m+1} = 0$

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

Example: Redundant Group with 3 Elements

$$Q_{k=1}$$
$$= \frac{1}{\binom{3-1}{1-1}} \cdot (\Phi_1) \cdot (1 - \Phi_2) \cdot Q_t$$
$$= 1 \cdot (1 - \beta) \cdot Q_t$$

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

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

Example: Substituting Q_k in the equation "System Failure Probability of a 2 out of 3 System Q_s with DF portion", $Q_s = 3\cdot\ \ + 3\cdot Q_2 + Q_3$, equals

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

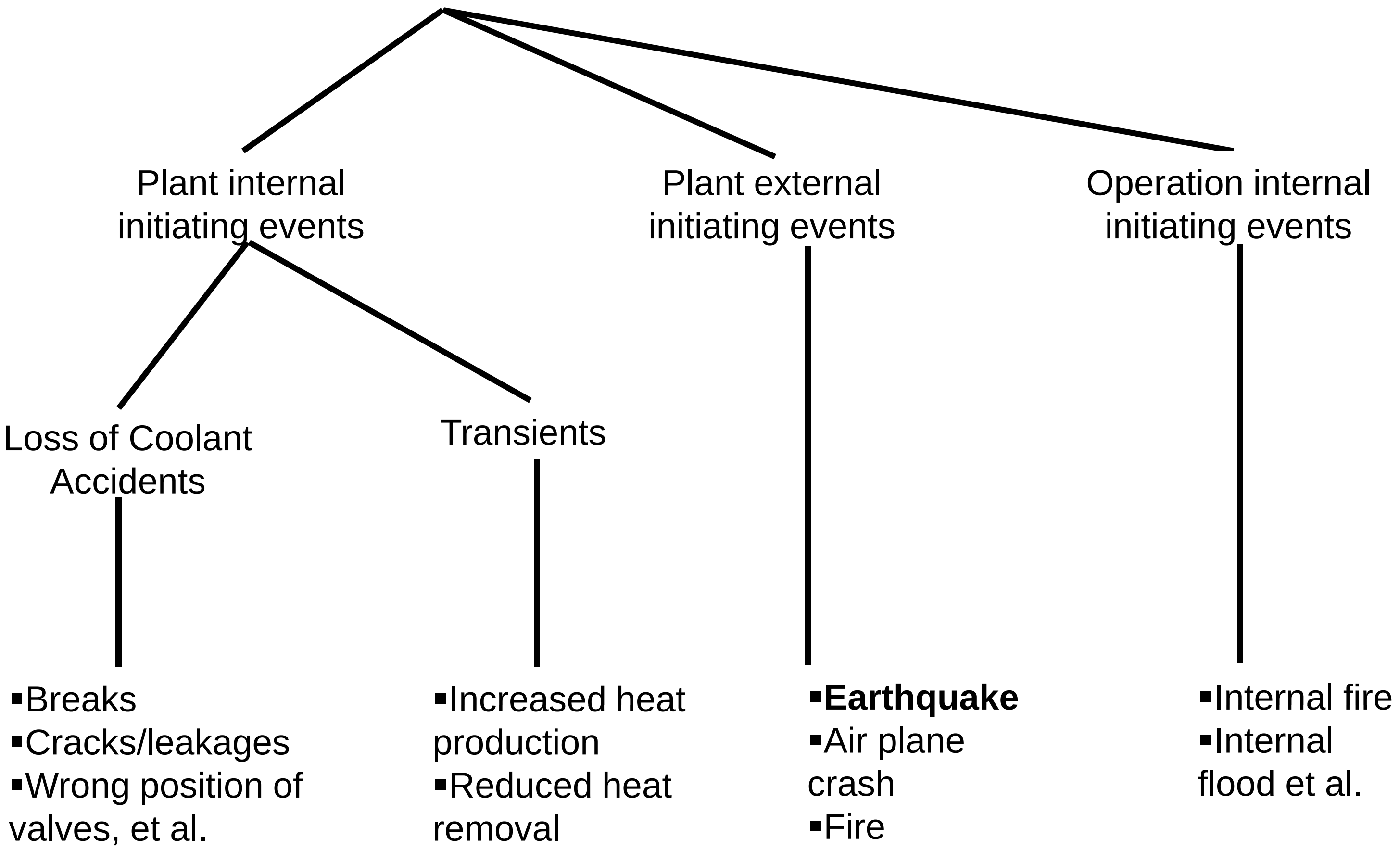
Supposing the MGL-factors are unknown, they can be determined via the respective Q_k (see above: parameters, definitions). The probabilites can be determined via

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

Equating $\gamma = 1$ leads to the result of the β-factor-model. In general, the *b*-factor-model is a special case of the MGL-Model

Common cause initiating event: Seismic Risk Analysis

Classification of initiating events (at plant level, NPP specific)



Plant internal initiating events

- Loss of Coolant Accidents
  - ▪Breaks
  - ▪Cracks/leakages
  - ▪Wrong position of valves, et al.
- Transients
  - ▪Increased heat production
  - ▪Reduced heat removal

Plant external initiating events

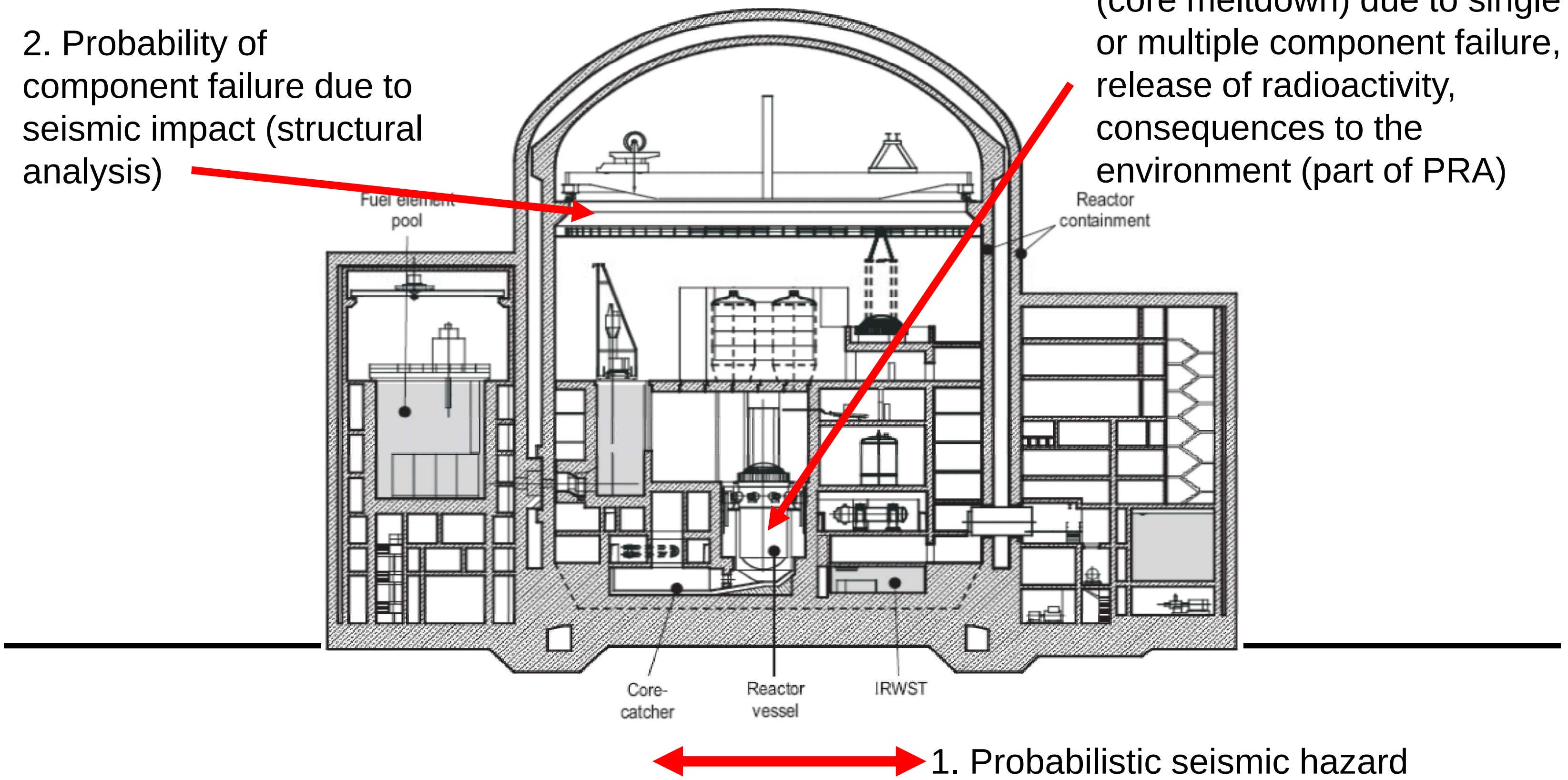
- ▪**Earthquake**
- ▪Air plane crash
- ▪Fire

Operation internal initiating events

- ▪Internal fire
- ▪Internal flood et al.

Seismic Risk Analysis

Seismic risk analysis of NPP’s encompasses the following steps:



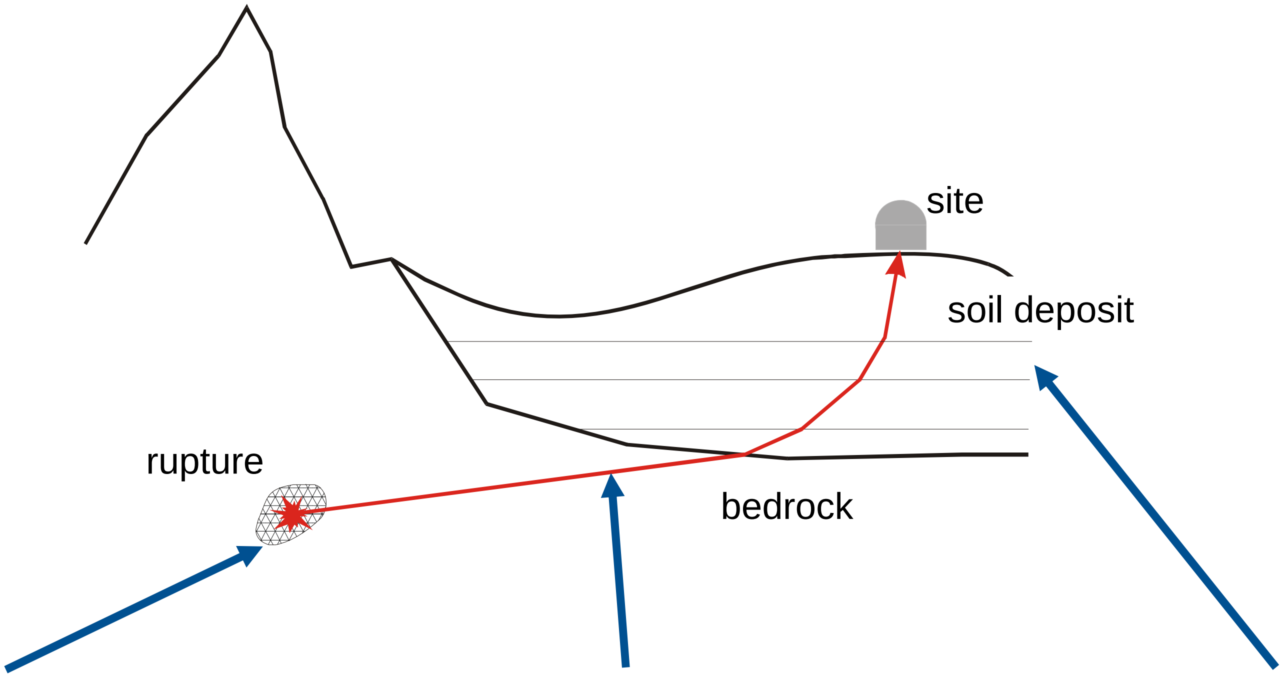
3. Probability of system failure (core meltdown) due to single or multiple component failure, release of radioactivity, consequences to the environment (part of PRA)

2. Probability of component failure due to seismic impact (structural analysis)

1. Probabilistic seismic hazard analysis (PSHA)

Figure from: Landolt-Börnstein VIII - 3 - B: Energy Technologies - Nuclear Energy, 2005, Springer Berlin Heidelberg New York

1. Probabilistic Seismic Hazard Analysis (PSHA) - Elements



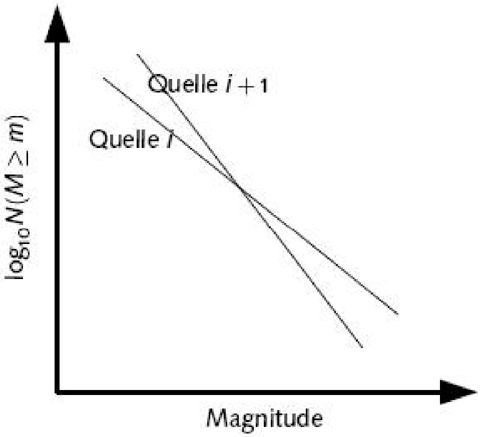
Magnitude-recurrence-relation
(Seismicity of the surrounding area)

Attenuation-relation
(decrease of seismic loads with increasing distance site to source)

Transfer function soil layers
(subsoil effects)

1. Probabilistic Seismic Hazard Analysis (PSHA) - Elements

Magnitude-recurrence-relation

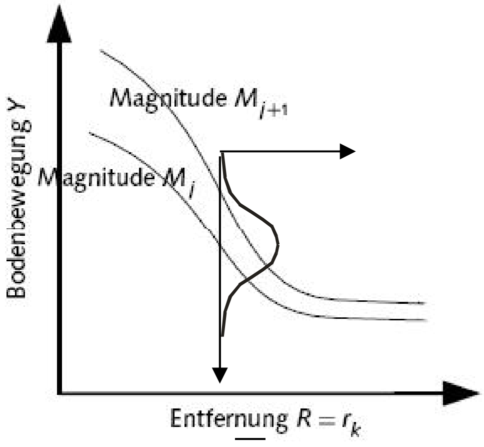


Seismic sources (faults, regions)
Magnitude-recurrence-relation:
e.g.: Gutenberg-Richter

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

M: magnitude (e.g.: M_w, M_s, M_l)
N: number of magnitudes m>=M per year
a, b: regression parameters of the Gutenberg-Richter-law

Attenuation-relation

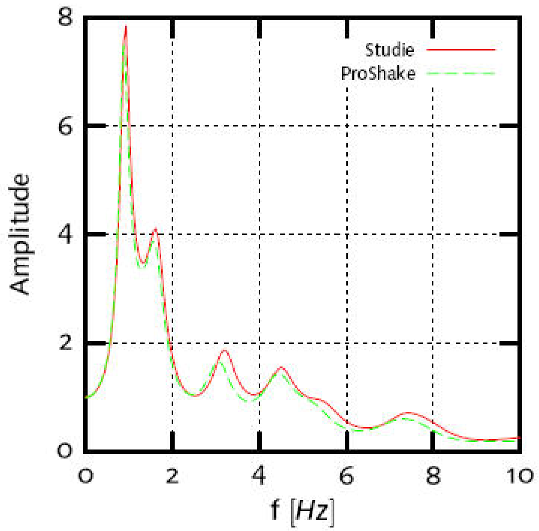


Attenuation relation for spectral accelerations or intensities
e.g.:

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

σ : aleatoric uncertainty
C_n : regression parameters
R: distance site-hypo-/epicentre
ε : coefficient (deviation from mean in s)

Transfer function soil layers



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

-analytical (e. g. frequency domain)
-numerical (e.g. FEM)

1. Probabilistic Seismic Hazard Analysis (PSHA) – Methodical Background

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

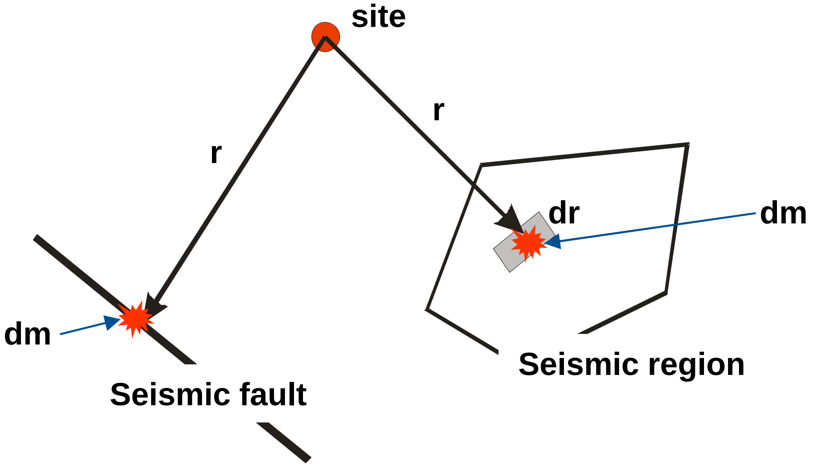
ν : mean annual rate of exceedance of acceleration, intensities etc. S>=s at the site

ν_n: mean annual rate of exceedance of magnitudes M>=m of the seismic source

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

f(r): density function of distance

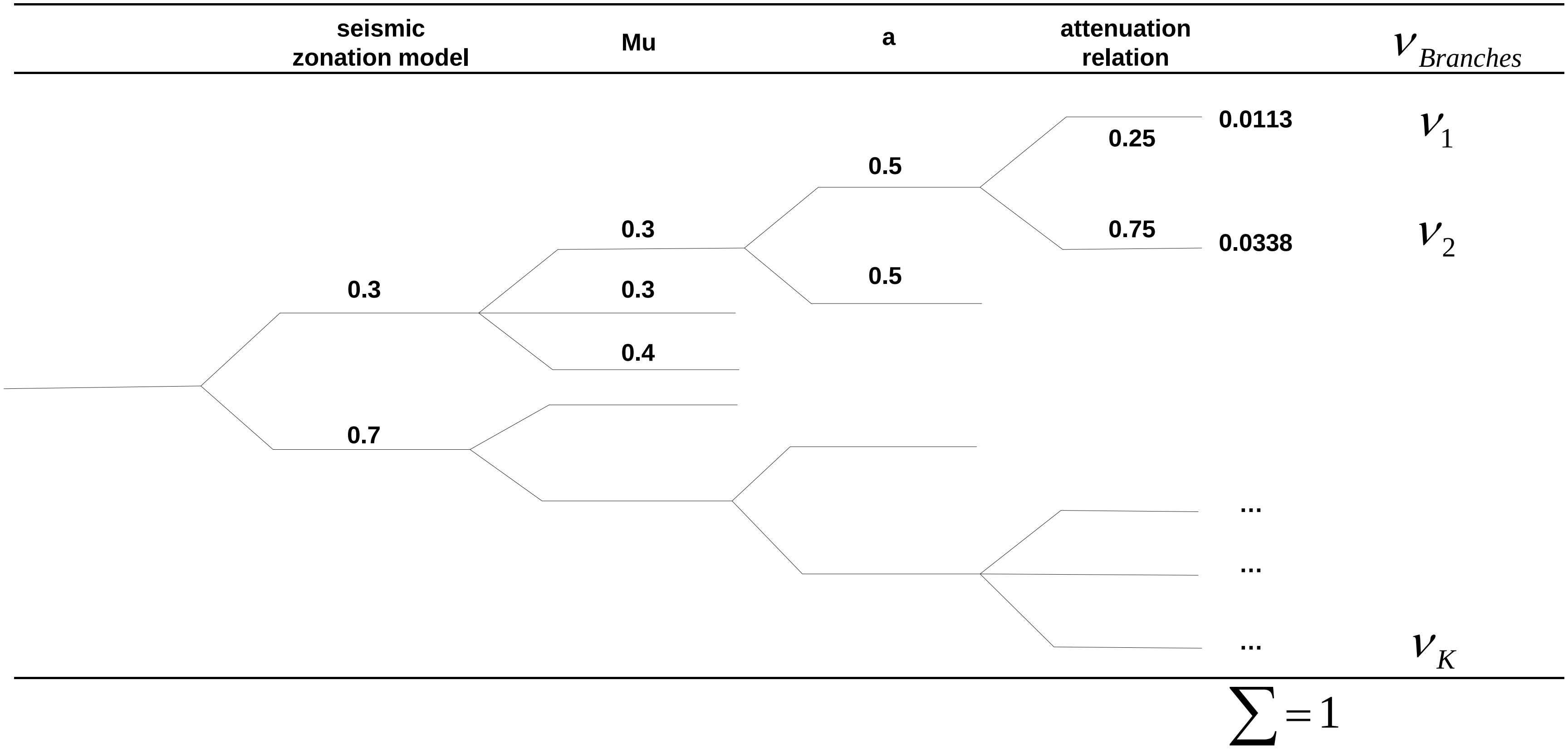
P(S>=s|m,r)=conditional probability of S>=s (attenuation relation)



1. Probabilistic Seismic Hazard Analysis (PSHA) – Logic Tree Approach

epistemic uncertainty: incomplete knowledge (lack of data)

aleatoric uncertainty: inherent randomness of ground motion generation



seismic zonation model | Mu | a | attenuation relation | $\nu_{Branches}$

0.3
0.7

0.3
0.3
0.4

0.5
0.5

0.25
0.75

0.0113 ν_1

0.0338 ν_2

...

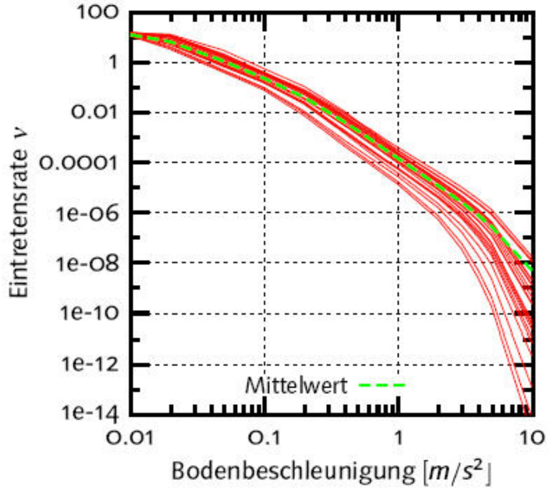
...

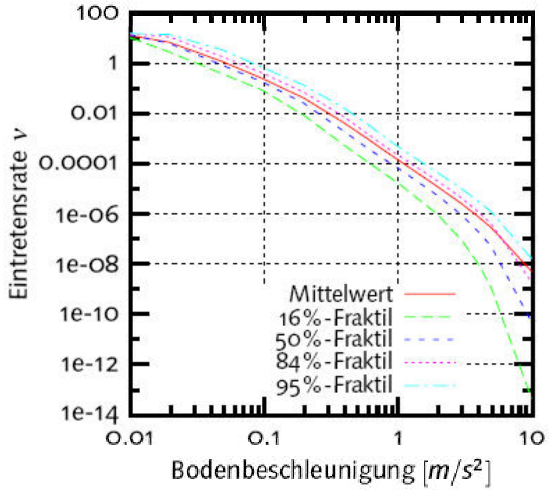
... ν_K

$$\sum = 1$$

1. Probabilistic Seismic Hazard Analysis (PSHA) – Surface Ground Motion

set of hazard curves

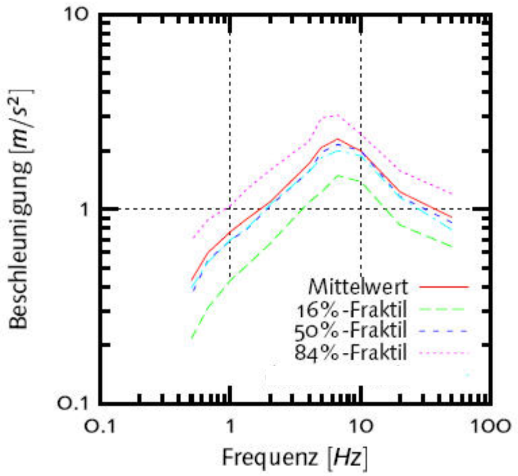


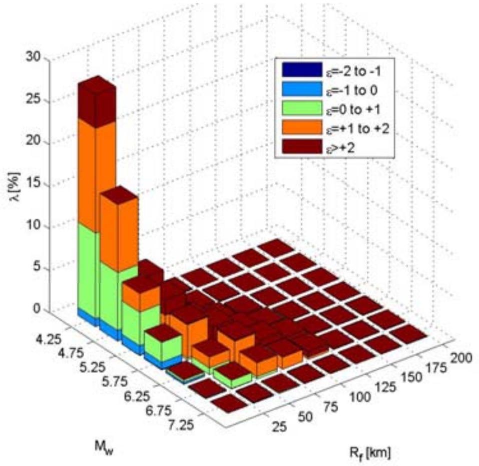


for different frequencies

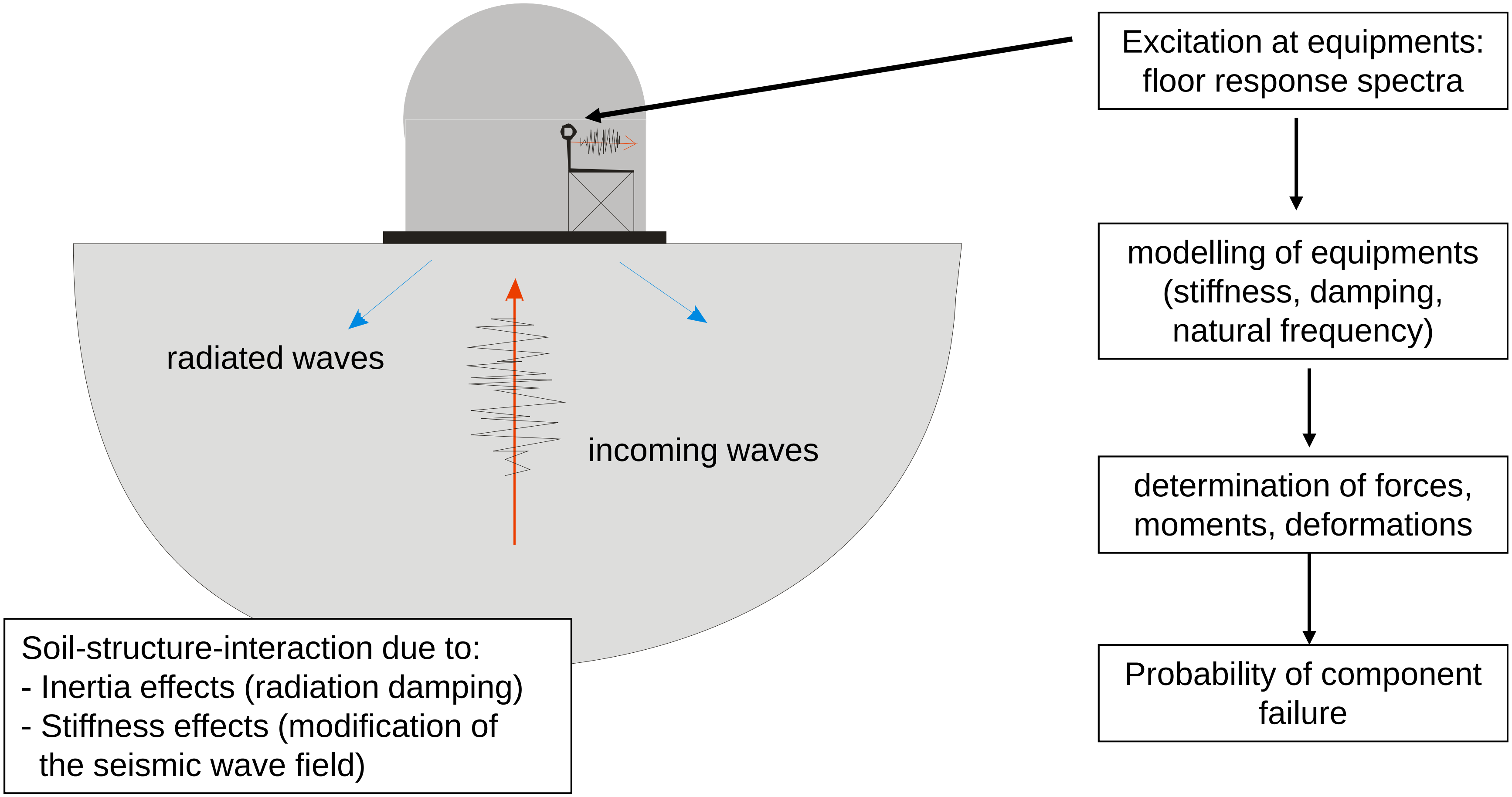
Deaggregation of seismic hazard

response spectra





2. Structural Analysis



Excitation at equipments: floor response spectra

modelling of equipments (stiffness, damping, natural frequency)

determination of forces, moments, deformations

Probability of component failure

radiated waves

incoming waves

Soil-structure-interaction due to:
- Inertia effects (radiation damping)
- Stiffness effects (modification of the seismic wave field)

Result of PSHA: KKL CDF: 4·10^{-6}/y (total) compared to 1,3·10^{-6}/y (total internal)