Inclusions of common cause failures and geographically distributed events (seismic hazard analysis)

- Dependent failures.
- Definitions.
- Modeling approaches: Explicit method – inclusion of DF in Fault Trees.
- Modeling approaches: Implicit methods.
- Marshall-Olkin-Model (fundamental modeling).
- β-Factor-Model.
- Multiple-Greek-Letter-Model (MGL-Model).

Dependent failures

Source: [1]

Model assumptions up to now

All failures of a system are due to independent failures at components (‘elements’) level, i.e.

- 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 to the system the failure probability can be reduced as you like.

These assumptions contradict common experience!

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).

DF can be classified in the following categories:

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 (cascading failures)
Description for spreading of 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.

- Note: DF are only important in redundant (parallel) systems.

Example of a well-known accident resulting from a common cause failure

The fire at the Browns Ferry nuclear power plant Decatur, Alabama, March 22, 1975.

The fire started when two of the operators used a candle to check for air leaks between the cable room and one of the reactor buildings, which was kept at a negative air pressure.

The candle’s flame was drawn out along the conduit and the urethane seal used where the cables penetrate the wall caught fire. The fire continued until the insulation of about 2000 cables was damaged.

Among these were all the cables to the automatic emergency shutdown (ESD) systems and also the cables to all the ‘manually’ operated valves, apart from four relief valves.

With these four valves it was possible to close down the reactor so that a nuclear meltdown was avoided.

This accident resulted in new instructions requiring that the cables to the different emergency shutdown systems be put in separate conduits and prohibit the use of combustible filling (e.g. urethane foam).

Modeling Approaches to Consider DF

Explicit Methods

- **Event specific models**

Consideration special consequences from e.g. earthquakes, fire, floods, broken pipes or leakages in general.

- **Event tree and fault tree analysis**

Consideration of functional interdependencies (units).

- **Models for the quantification of human actions**

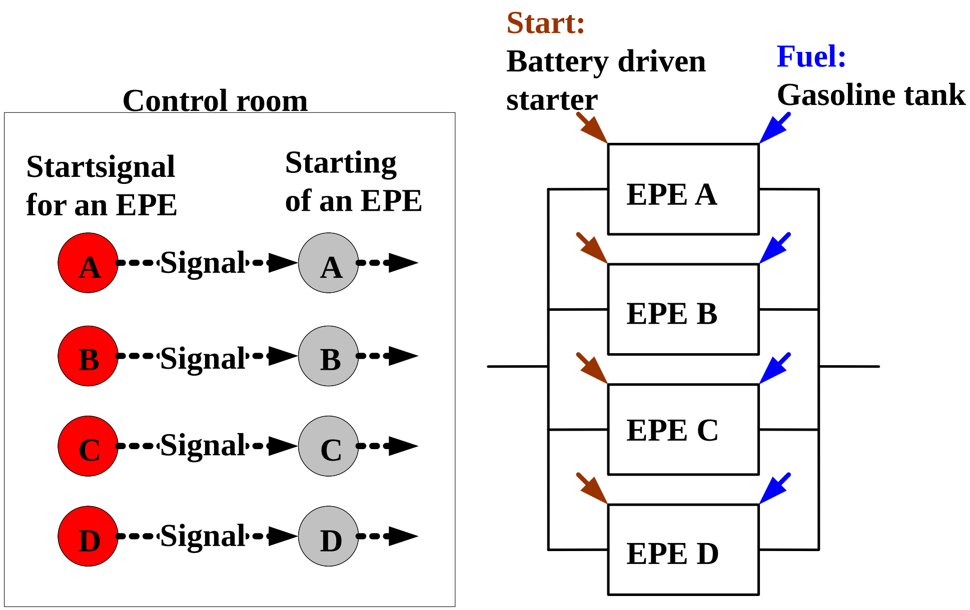
Consideration of interdependencies between single human actions such as coupling models in THERP.

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

Example of dependent failure identification: Emergency power supply

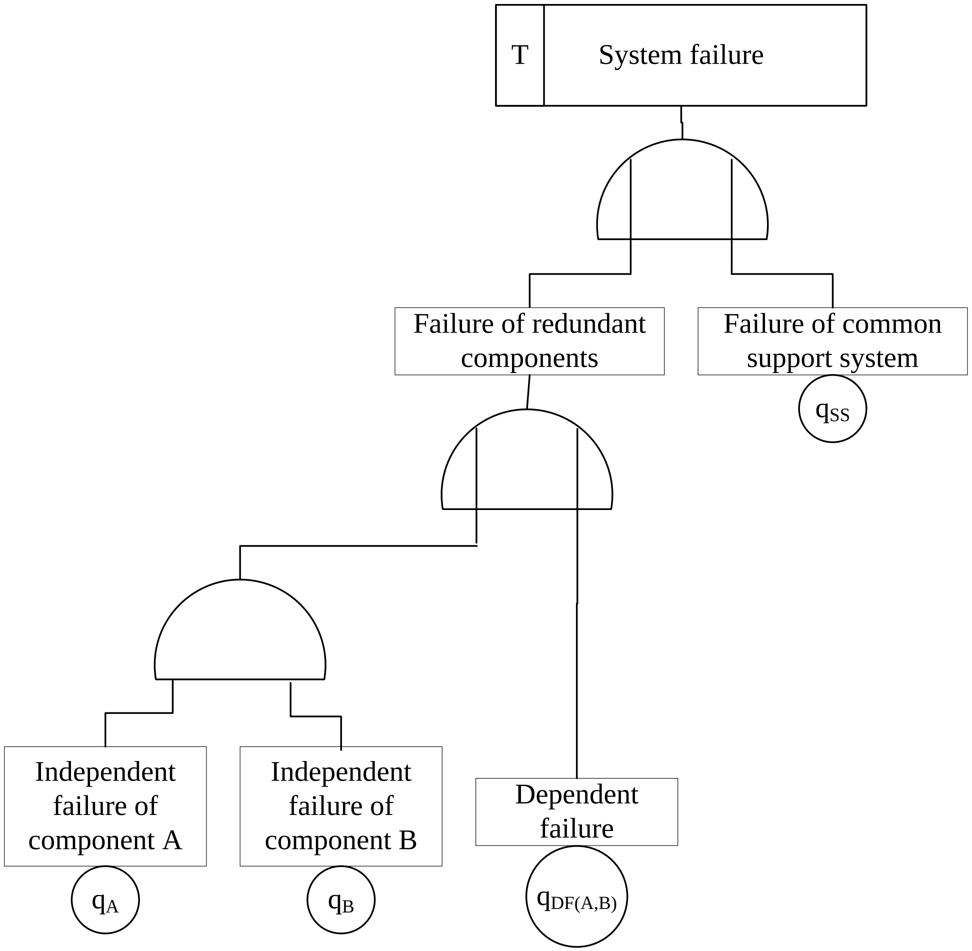
A data processing service centre of a major bank has a largely redundant emergency power supply. Four emergency power engines (EPE) are installed, one engine guarantees the operability of the centre for two days. If one engine fails, the next will be started (stand-by operation). Further in formation about the system:

Operator



- EPE are started by an operator in the control room.
- Each EPE has its own control device.
- Each EPE has its own starter, battery and tank.
- All EPE are maintained and fuelled in one process.

Modelling approaches: Explicit method – inclusion of DF in Fault Trees



Implicit Methods (to consider residual DF – fractions)

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

General

• In principle, implicit methods can completely cover dependent failures, but large uncertainties arise because of insufficient data and data solely based on the level of considered items (CMF).

• Rigorous application bears the danger of insufficient system (e.g. fault tree) analyses, e.g. failure to notice structural/functional dependencies.

Modeling approaches: Implicit methods

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

- *Failure probabilities for all units are identical:* $q_a = q_b = q_c = Q_{k=1}$

k (k = 1, 2, …, n): Number of units involved 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

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

2. Inclusion of DF

Probabilities of failure combinations

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

Assumption: equality of all units:

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

Example: '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:

$Q_s = \Sigma \Pr(\text{independent failures}) + \Sigma \Pr(\text{dependent failures})$

'2-out-of-3-system':

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

4. 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 coefficients:

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

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, such as 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:

$$\beta \cdot Q_t = Q_{k=n}$$

$$\beta \cdot \left(Q_1 + Q_n \right) = Q_{k=n}$$

With $Q_n = Q_t - Q_1$ follows:

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

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 b-factor-model: $Q_s = 3 \cdot (1-\beta)^2 \cdot Q_t^2 + \beta \cdot Q_t$

Discussion of the β-Factor-Model

Advantages	**Disadvantages**
Easy to apply.	Too conservative in the case of simultaneous failures of more than two units.
b-parameter can be determined relatively easily by operational experiences.	Results are too conservative if there are more than two groups of redundancies (n>2).
	Danger of too general application avoiding thorough system analysis with regard to functional dependencies.

Multiple-Greek-Letter-Model (MGL-Model)[1]

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	$Q_t = Q_1 + 2Q_2 + Q_3$
a	single failures	a = 1
b	all *dependent* failure probabilities relating to Q_t	$\beta = \frac{2Q_2 + Q_3}{Q_t} = \frac{2Q_2 + Q_3}{Q_1 + 2Q_2 + Q_3}$
g	*fraction* of DF probability of a unit, with *at least* 2 units failing	$\gamma = \frac{Q_3}{2Q_2 + Q_3}$

[1] Further information, not part of the examinations.

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 *b*, *g*, etc.

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

The results for a redundant group can be generalized 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", $Q_s = 3\cdot Q_1^2 + 3\cdot Q_2 + Q_3$, equals:

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

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

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

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

References

1. Amendola, A. *Classification of Multiple Related Failures: Advanced Seminar on Common Cause Failure Analysis in PSA*. in *Ispra Courses on Reliability and Risk Analysis*. 1989. Ispra: Kluwer Academic Publishers.
2. Marvin Rausand, Arnljot Hoyland, System Reliability Theory, Wiley, 2004.

Seismic Risk Analysis

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

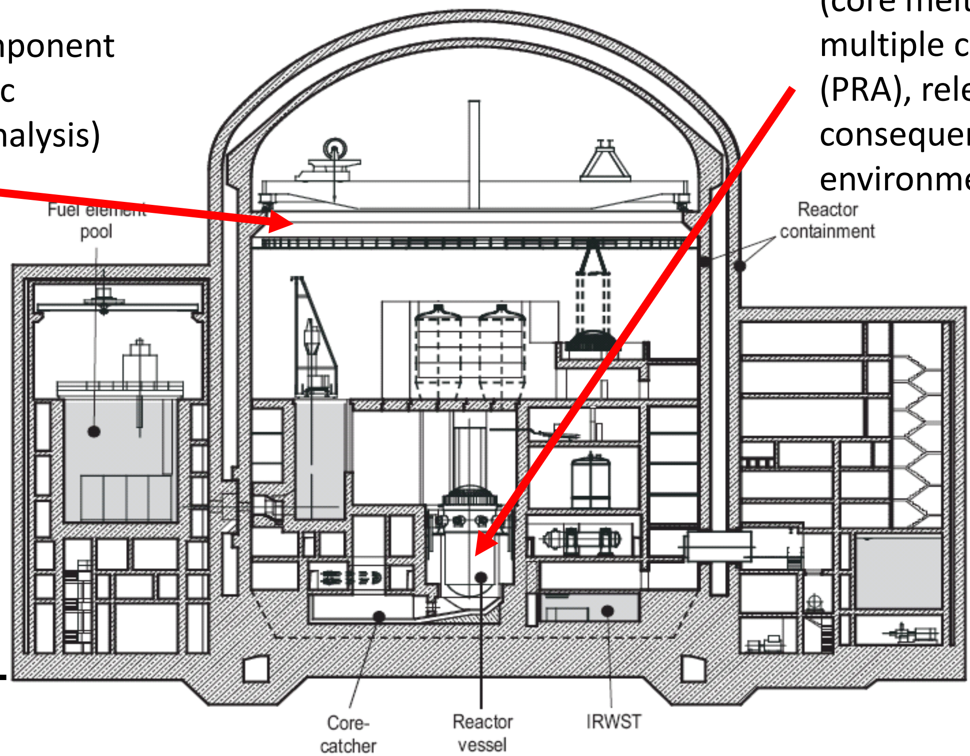
- Plant internal initiating events
  - Loss of Coolant Accidents
    - Breaks
    - Cracks/leakages
    - Wrong position of valves, et al.
  - Transients
    - Increased heat production
    - Reduced heat removal
- Plant external initiating events
  - **Earthquake**
  - Air plane crash
  - Fire
- Operation internal initiating events
  - Internal fire
  - Internal flood et al.

Seismic Risk Analysis

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

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

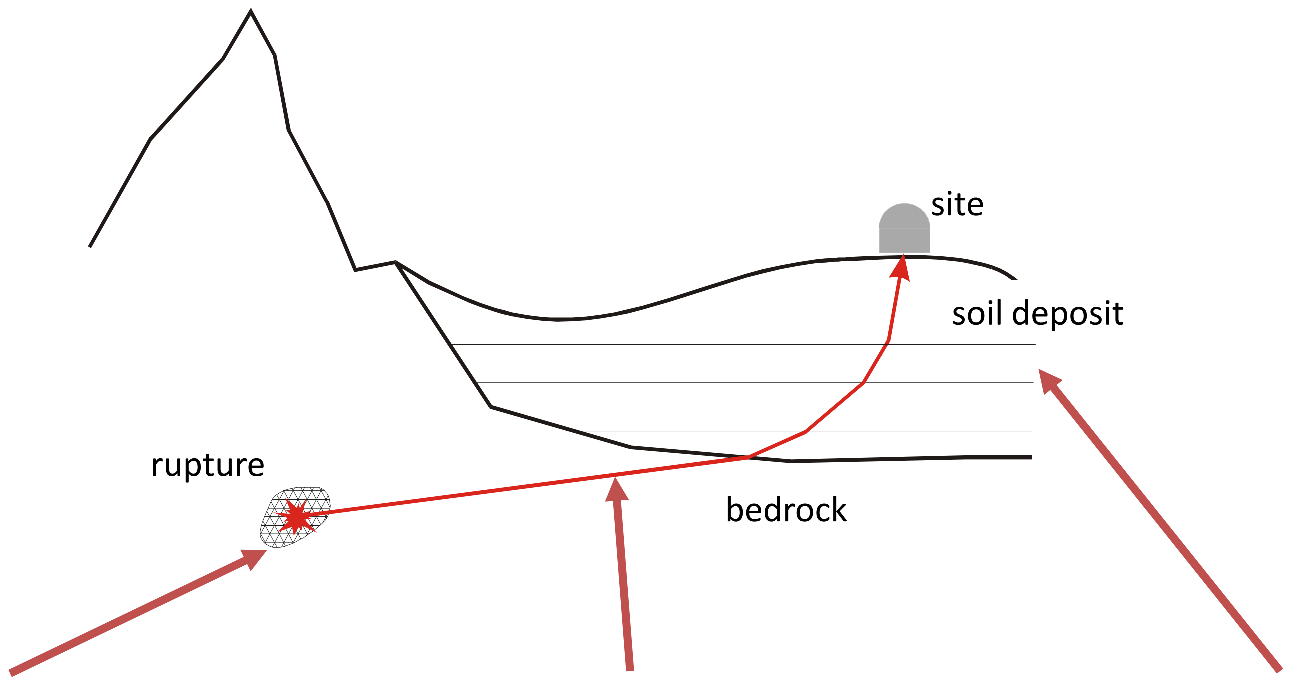
3. Probability of system failure (core meltdown) due to single or multiple component failure (PRA), release of radioactivity, consequences to the environment



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



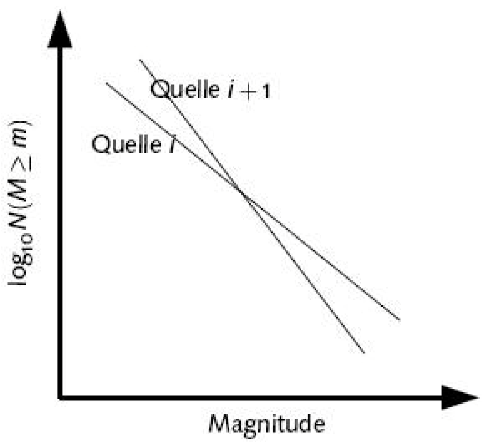
Magnitude-recurrence-relation (Seismicity of the surrounding area)

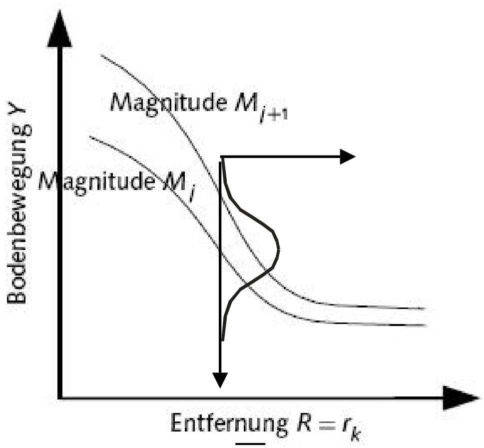
Attenuation-relation (decrease of seismic loads with increasing distance site to source)

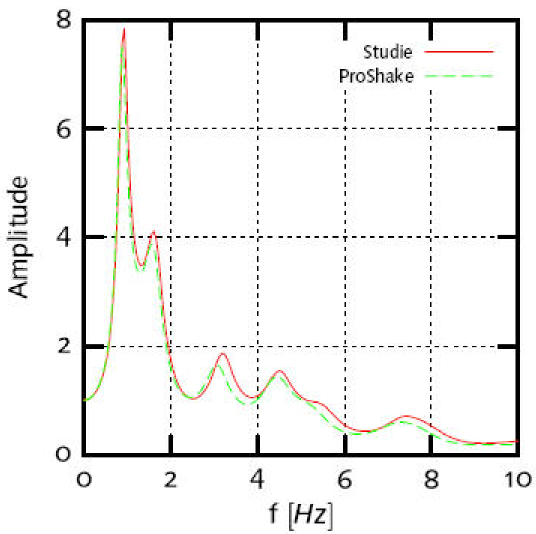
Transfer function soil layers (subsoil effects)

1. Probabilistic Seismic Hazard Analysis (PSHA) - Elements

Magnitude-recurrence-relation	Attenuation-relation	Transfer function soil layers







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 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)

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: $$\nu(S \geq s) = \sum_n \nu_n \iint f(m) f(r) P(S \geq s \mid m, r) dmdr$$

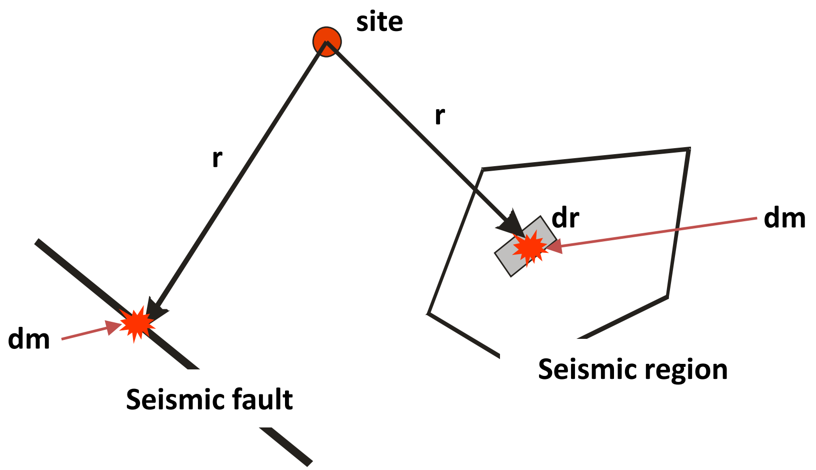
ν : mean annual rate of exceedance of acceleration, intensities etc. S>=s at the site

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

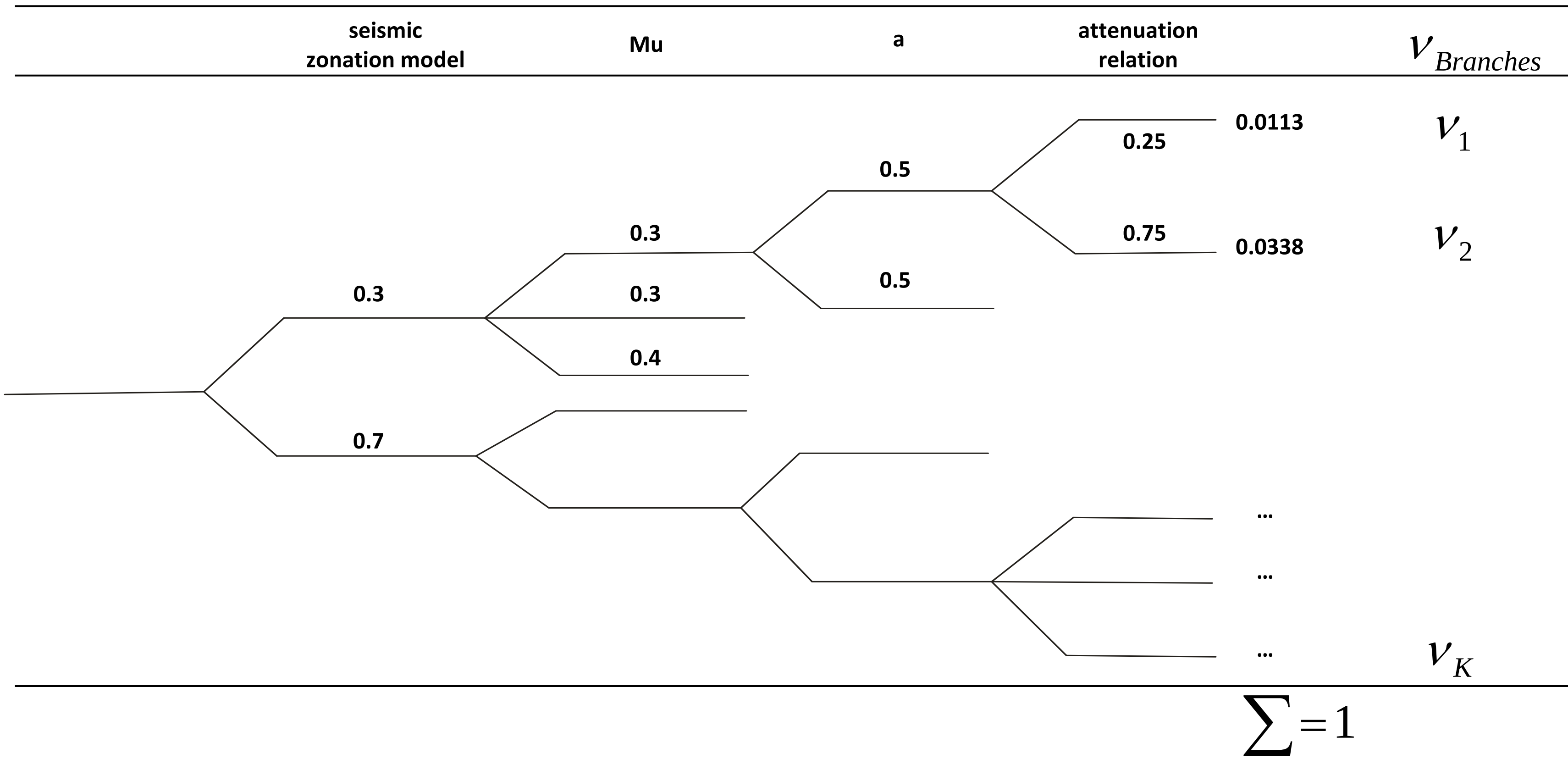
P(S>=s|m,r)=conditional probability of S>=s (attenuation relation)



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

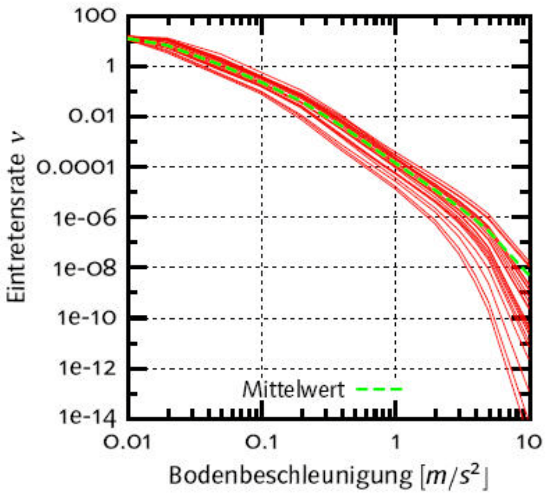
epistemic uncertainty: incomplete knowledge (lack of data)

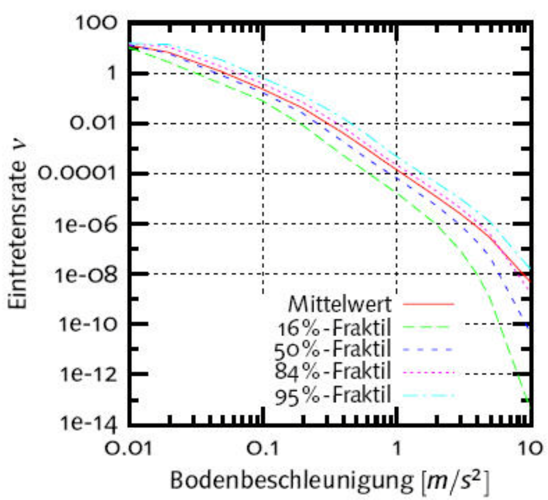
aleatoric uncertainty: inherent randomness of ground motion generation

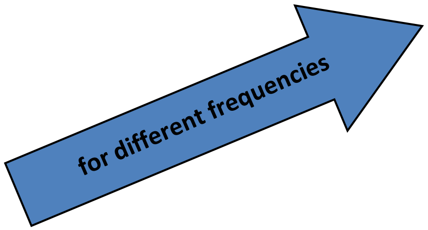


1. Probabilistic Seismic Hazard Analysis (PSHA) – Surface Ground Motion

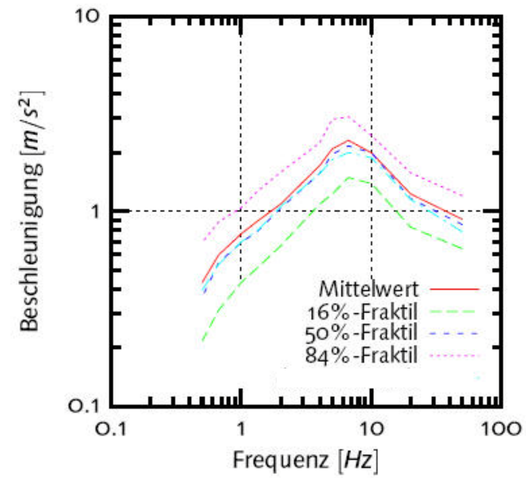
set of hazard curves

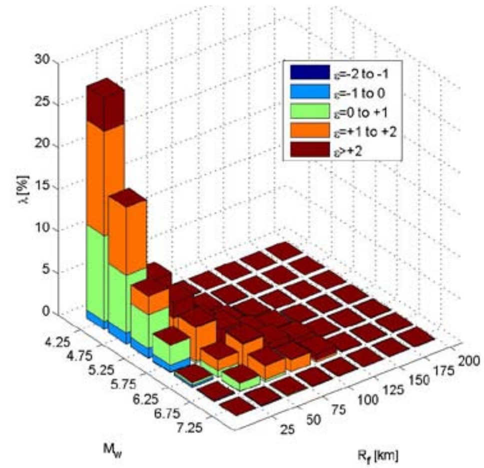




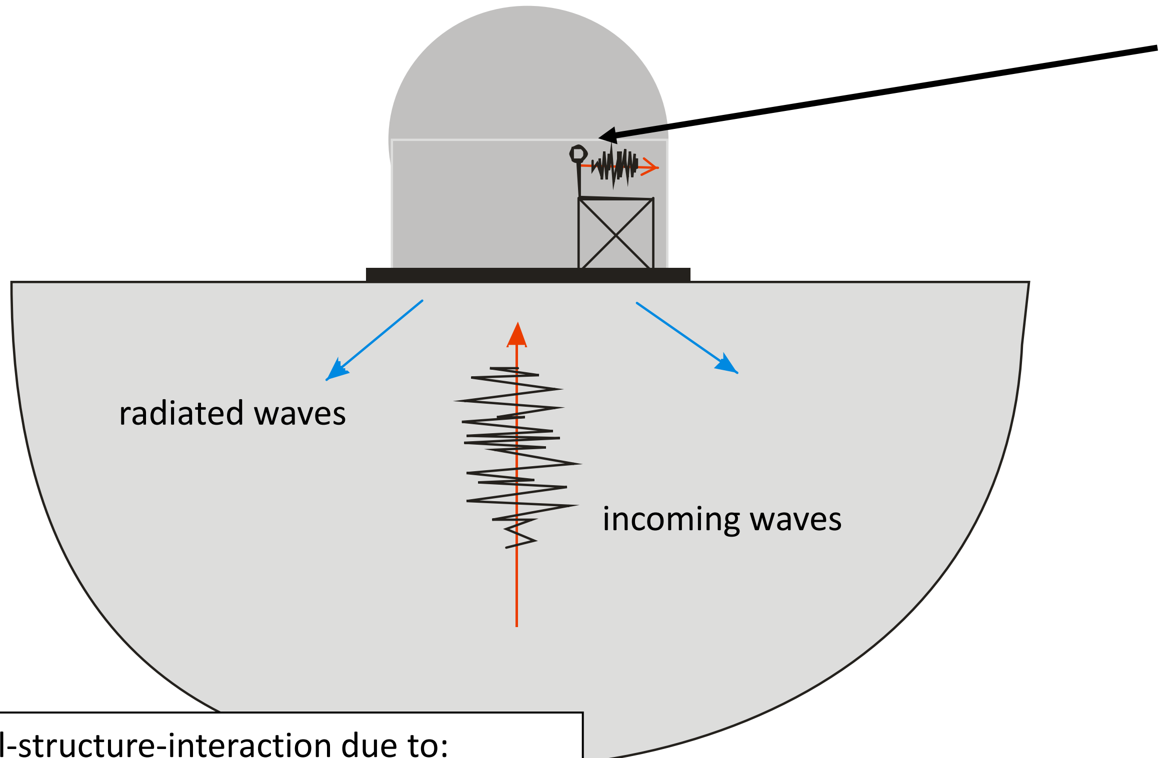


response spectra





2. Structural Analysis



Excitation at equipments: floor response spectra

↓

modelling of equipments (stiffness, damping, natural frequency)

↓

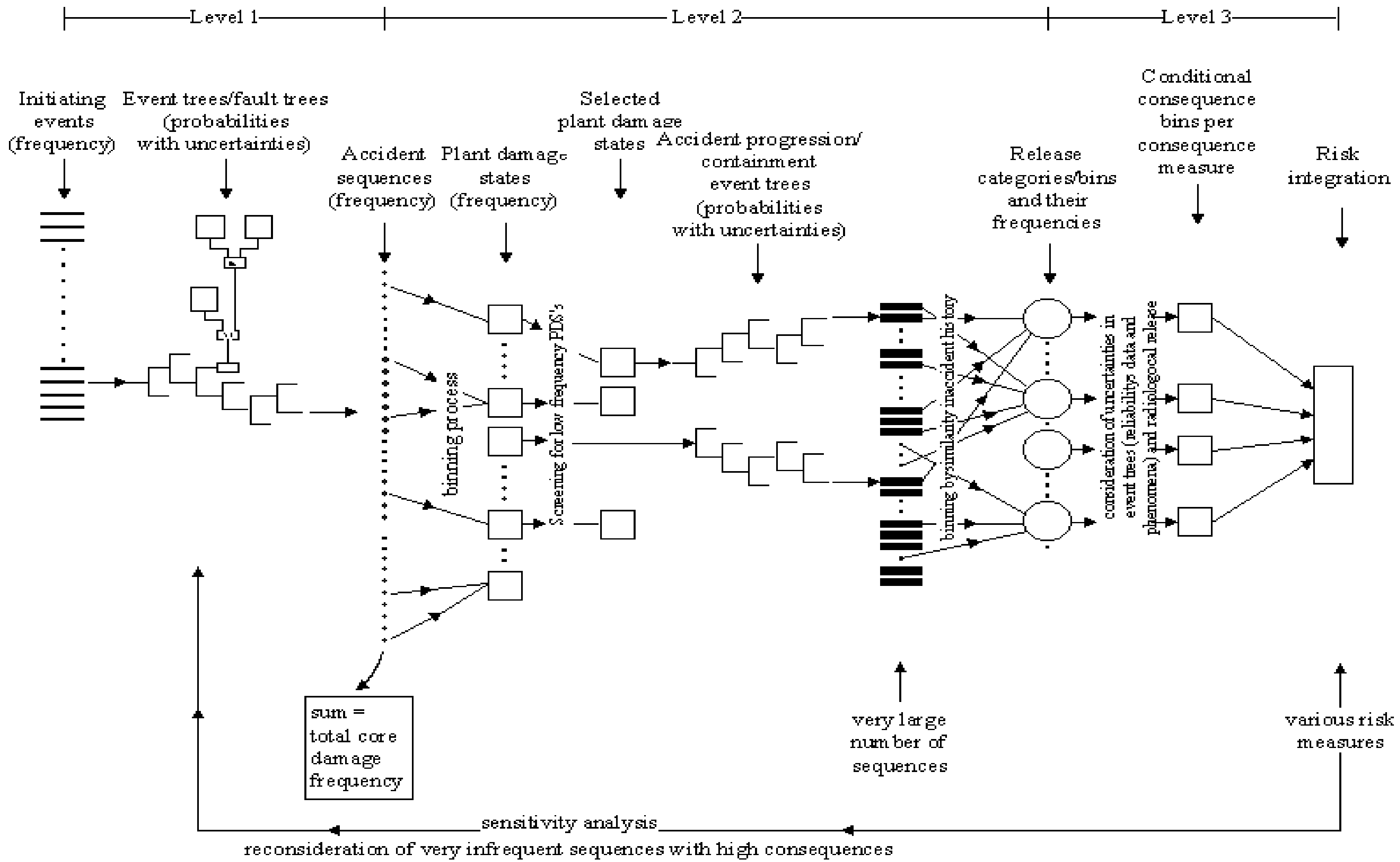
determination of forces, moments, deformations

↓

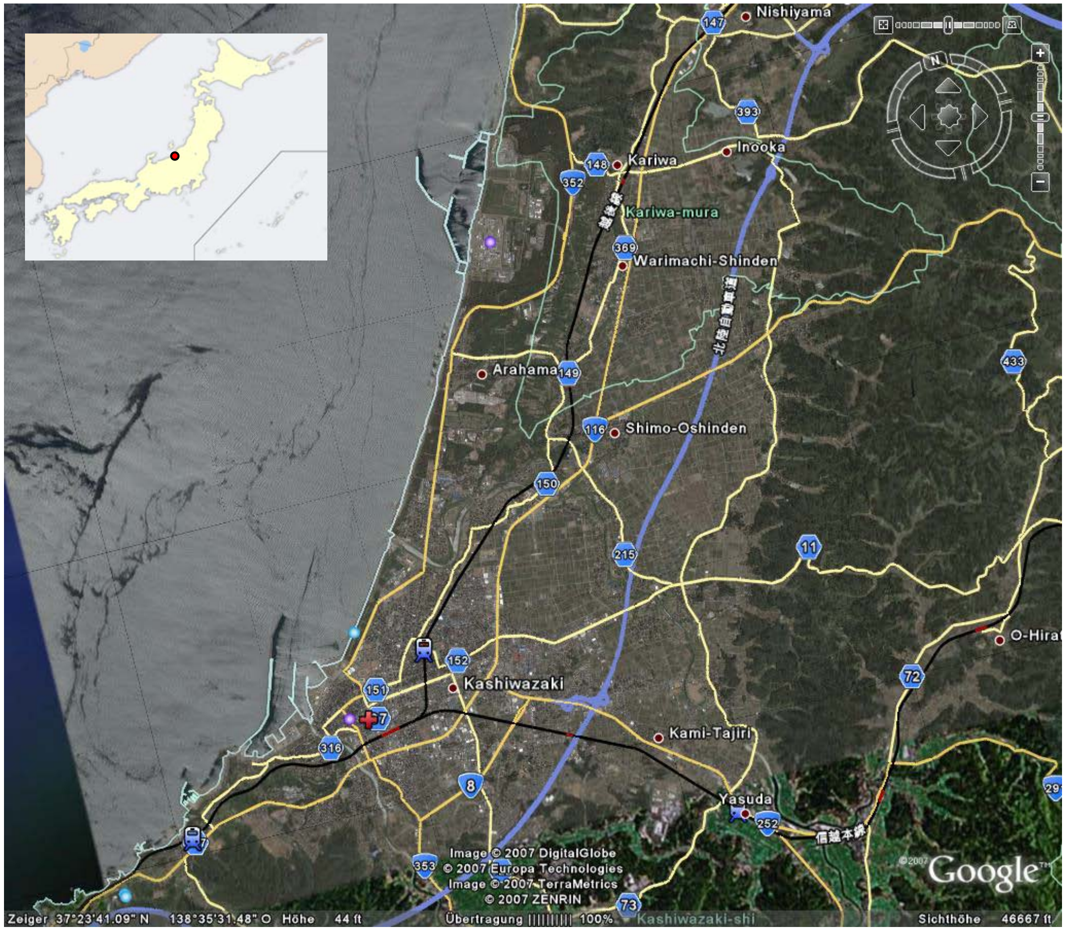
Probability of component failure

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

3. PRA - Overview of PRA methodology



Example (System):

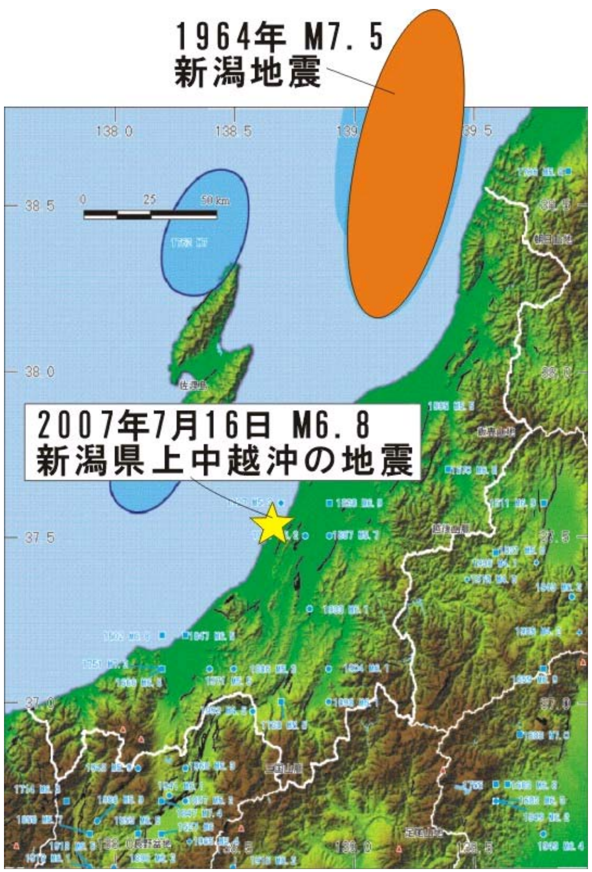


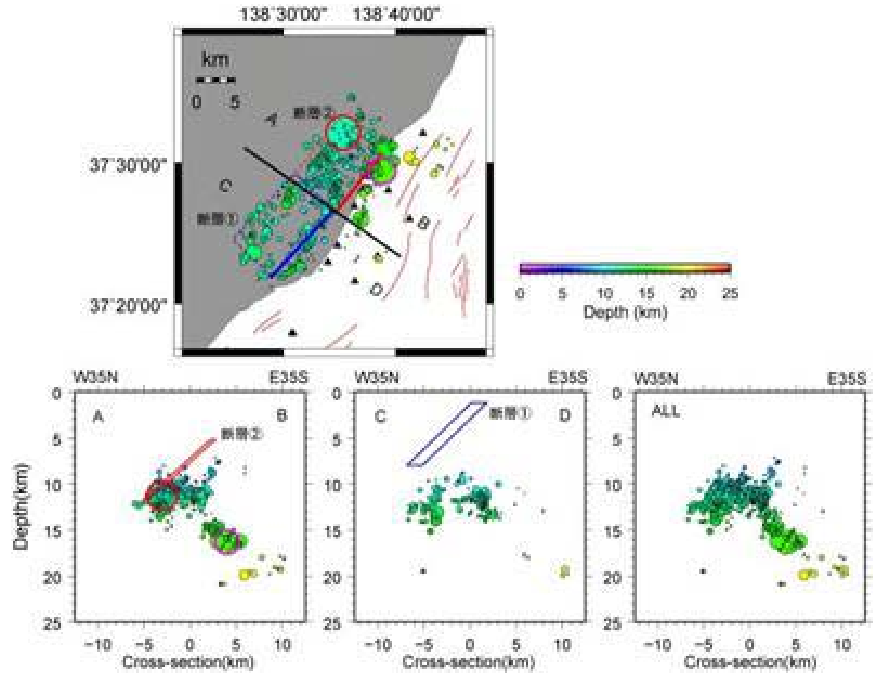
NPP Kashiwazaki-Kariwa

- 7 Units.
- Total power 8212 MW.
- BWR/ABWR.
- Units 1,5,6 for planned outage.
- Units 3,4,7 in operation.
- Unit 2 in start up.

Example (Earthquake Event):

M_{JMA}=6.8 Earthquake, 2007/7/16





Recorded and design pga [cm/s^2]

	Records			Design Earthquake		
Plant	NS	EW	UD	NS	EW	UD
1	311	680	408	274	273	235
5	277	442	205	249	254	235
6	271	322	488	263	263	235

Example (Damages):

General
- Automatically shutdown.
- All plants behaved in a safe manner before, during and after the earthquake.
- No damages to safety related structures, components, systems.

Fire
- Fire in a transformer of of Unit 3, problems with fire fighting.

Seismicity
- Need for reavaluation, detailed geophysical investigations.

Off-Site Power
- No loss of off-site power.

Common cause failures
- Identical failures of light fixtures.
- Damage to ducts (settlement and soil failure, separate foundations).

Seismic System Interaction
- Minor damages due to good housekeeping and maintenance practice.

Soil failure
- Many problems at the NPP were induced by large soil deformations.

Anchorage failure
- Limited number of anchorage failures (transformers, water tanks), no safety equipment failed.

Operational Safety Management
- Management was successful with respect to the reactor safety system.

according to: IAEA Mission Report, PRELIMINARY FINDINGS AND LESSONS LEARNED FROM THE 16 JULY 2007 EARTHQUAKE AT KASHIWAZAKI-KARIWA NPP

Radiation releases

•very minor radioactive releases

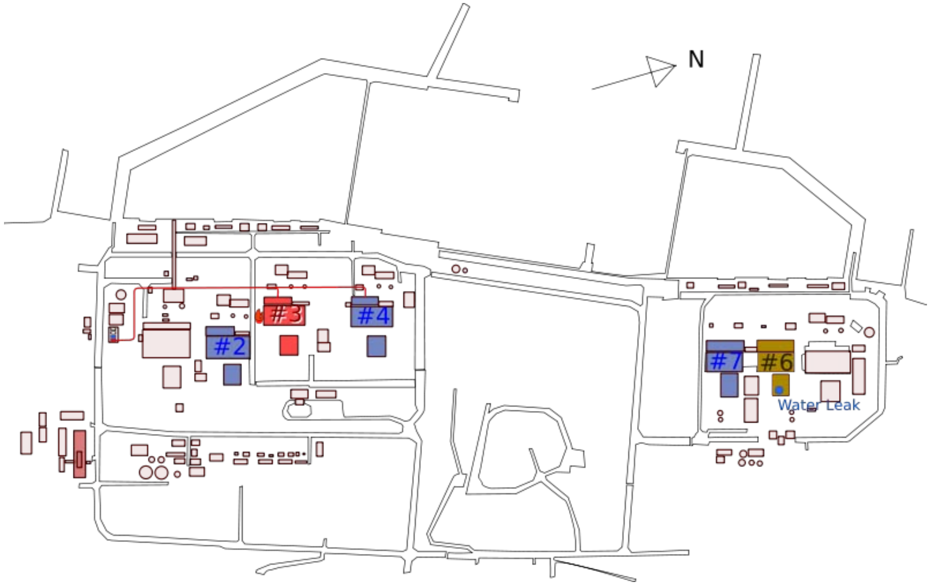
•0.6 liters of slightly radioactive water leaked from the third floor of the Unit 6 reactor building

•0.9 liters of slightly radioactive water leaked from the inner third floor of the Unit 6 reactor building

•From unit 6, 1.3 cubic meters of water from the spent fuel pool leaked from the pool, and flowed into through a drainage pipe, ultimately into the Sea of Japan.

•On Wednesday June 18, at Unit 7, radioactive Iodine was found leaking from an exhaust pipe by a government inspector, the leak began between Tuesday and Wednesday and was confirmed to have stopped by Thursday night.

•About 400 drums containing low-level nuclear waste stored at the plant were knocked over by the aftershock, 40 losing their lids.



according to: IAEA Mission Report, PRELIMINARY FINDINGS AND LESSONS LEARNED FROM THE 16 JULY 2007 EARTHQUAKE AT KASHIWAZAKI-KARIWA NPP and http://en.wikipedia.org/wiki/Kashiwazaki-Kariwa_Nuclear_Power_Plant

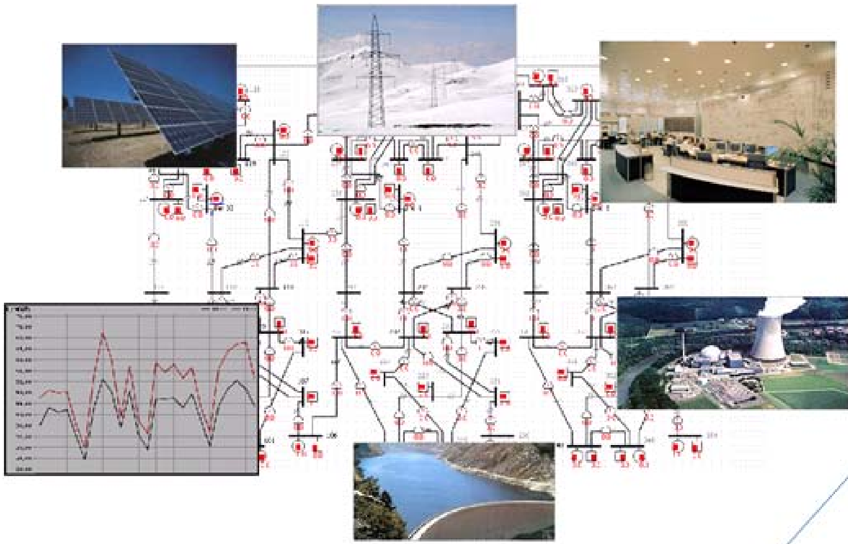
Advanced Methods for Complex Systems' Modeling and Simulation I:

Network theory for the vulnerability analysis of infrastructure systems

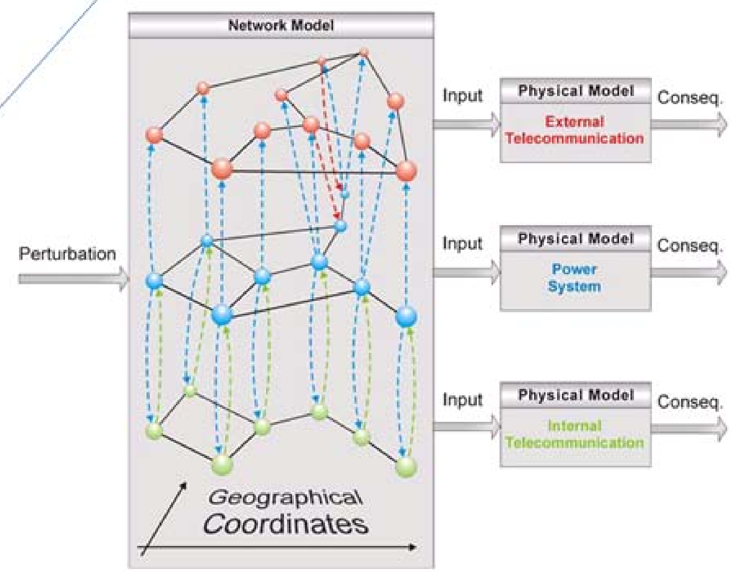
Lecture contents:

1. Introduction and problem description
2. Basic network characteristics
3. Static network vulnerability analysis
   (random failure and attack tolerance)
4. Cascading failures within infrastructure systems

Real Networks



Network Models



Introduction and Problem Description (I)

- Infrastructure systems provide essential goods and services to the industrialised society including transport, water, communication and energy.
- A disruption or malfunction often has a significant economical impact and potentially propagates to other systems due to mutual interdependencies.
- Wide-area breakdowns of such large-scale engineering networks are often caused by technical equipment failures and their coincidence in time which eventually result in a series of fast cascading component outages.
- Illustrative examples are a number of large electric power blackouts and near-misses as has been increasingly experienced in the last few years