Probabilistic Safety Assessment (PSA): Case Study Leibstadt NPP

Dr. Olivier Nusbaumer
Probabilistic Safety Analysis
Kernkraftwerk Leibstadt AG

- **Background**
- **Methodological Aspects**
- **Swiss Atomic Law**
- **Scope of an Industrial PSA Study**
- **Applications and Results**
- **Conclusions**

Grundlagen der PSA
Vergleichstabelle natürliche / vom Menschen erzeugte Risiken

Risiko	Frequency (Person/Jahr)	Sterberisiko (Person/Jahr)
Grippe	2.00E-04	1 in 5000
Leukämie	8.00E-05	1 in 12,500
Autounfall (UK)	6.02E-05	1 in 16,600
Autounfall (USA)	5.00E-05	1 in 20,000
Schlangenbiss (UK)	2.00E-07	1 in 5 Millionen
Überflutung (USA)	2.20E-06	1 in 455,000
Dammbruch (Niederlande)	1.00E-07	1 in 10 Millionen
Tornado (Mittlerer Westen USA)	2.20E-06	1 in 455,000
Erdbeben (Kalifornien)	1.70E-06	1 in 588,000
Blitzschlag (UK)	1.00E-07	1 in 10 Millionen
Flugzeugabsturz (USA)	1.00E-07	1 in 10 Millionen
Flugzeugabsturz (UK)	2.00E-08	1 in 50 Millionen
Explosionen, Tankfahrzeuge (United States)	5.00E-08	1 in 20 Millionen
Meteorit	1.00E-11	1 in 100 Milliarden
Freisetzung aus einem KKW		
Umreis 1 km (UK)	1.00E-07	1 in 10 Millionen
Am Standort (USA)	1.00E-07	1 in 10 Millionen

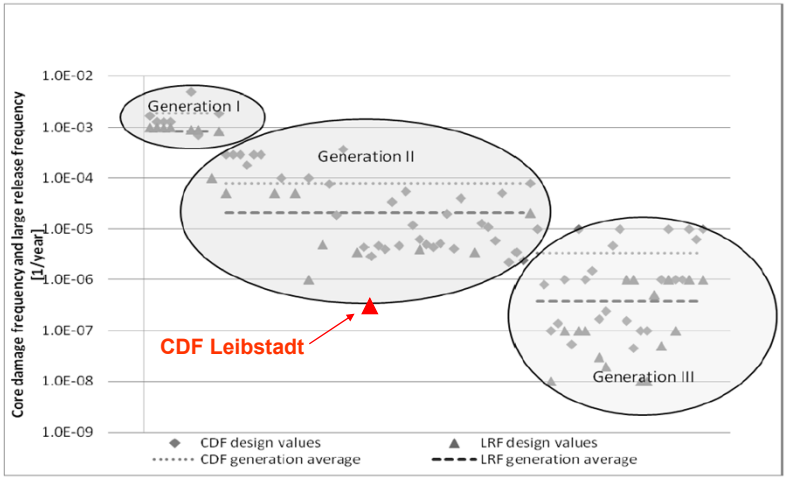
Source: Adapted from Dinman, B.D., "The Reality and Acceptance of Risk," Journal of the American Medical Association, Vol. 244 (11): 1126–1128, 1980
Link : http://www.psandman.com/articles/cma-appb.htm#B-4

Grundlagen der PSA
Verlorene Lebensjahre in Bezug auf Ursachen

Ursache	Verlorene Lebensjahre
Rauchen (männlich)	6.16
Herzkrankheiten	5.75
30% Übergewicht	3.56
Krebs	2.68
Schlaganfall	1.42
Gefährlicher Job (Unfall)	0.82
Verkehrsunfall	0.57
Alkohol (USA)	0.36
Arbeit im radioaktiven Umfeld	0.11
Sturz	0.11
Fussgängerunfall	0.10
Sicherer Job (Unfall)	0.08
Brände	0.07
Natürliche Strahlenbelastung	0.02
Kaffe	0.02
Coffee	0.02
Reaktor Unfälle (UCS)	0.01
Reaktor Unfälle (NRC)	0.00
Airbags im Auto	-0.14

Source: Adapted from Cohen, B. and Lee, I. "A Catalog of Risks." Health Physics, 36, June, 1979, 707–722
Link : http://www.psandman.com/articles/cma-appb.htm#B-4

Vergleich der Sicherheit KKL mit Neuanlagen
Entwicklung der CDF von Kraftwerkstypen Gen. I - III



Background: PSA

- **Complement the deterministic Design Basis Requirements**
- **Make use of probabilistic calculation tools (Fault Tree / Event Tree) and statistics (plant specific reliability data)**
- **Give answers as to:**
  - What can happen ?
  - How likely is it ?
  - What are the consequences ?
  - How large are the uncertainties ? (“make uncertainty visible”)
  - What are the dominant contributors ?

Improvement measures

Level 0 PSA
Level 1 PSA
Level 2 and 3 PSA
Uncertainty analysis
Risk Informed Applications

Background: Modeling

- **Postulation of an Initiating Event (IE) and its frequency *f***
- **Modeling of the safety barriers (equipment and measures)**
- **Quantification of phenomenological events and damage level**

Level 0 PSA

Level 1 PSA

Level 2 and 3 PSA

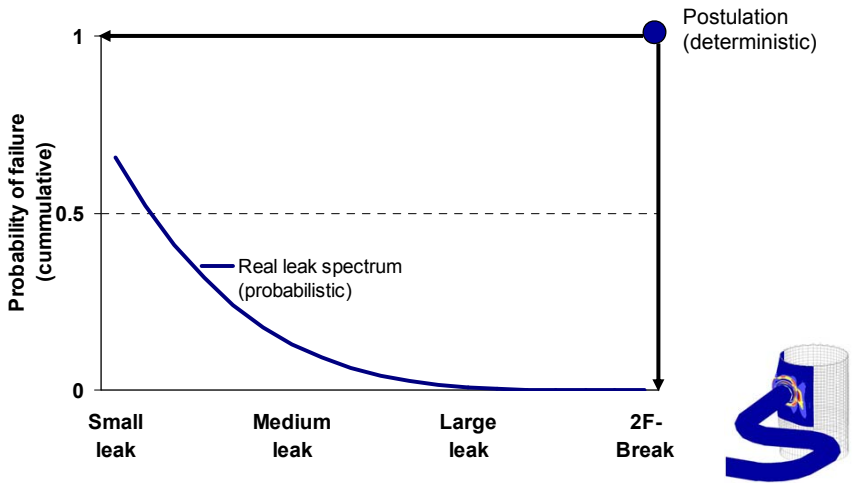
Background: Levels of PSA

Response to initiating events, Assessment of safety barriers	**Level 1** →	Frequency of core damage (CDF)
Physical effects, consequences	**Level 2** →	Radiological consequences (source term)
Athmospheric dispersion, potential and expected doses, dose-effect/risk relation	**Level 3** →	Frequency and quantities of environmental and health effects

Background: Approaches

- **Deterministic (postulative)**
  - Events completely determined through causality chains
  - Effect analysis of postulated causes
- **Statistic (retrospective)**
  - Experience laws derived from a large number of similar observations
  - Incorporation of the observations at system and event level
- **Probabilistic (prognostic)**
  - Events determined by probability or frequency
  - Use of observations at component level (axiom of Kolmogorov)

Background: Approaches



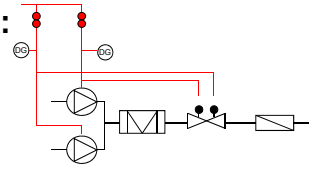
Methodological Aspects: Level 1

- **Fault Trees are logical models of fault combinations that could cause a mitigating system to fail to perform its function when required**
  - Basis: all causes leading to system failure
  - System modeling → System reliability
- **Event Trees depict the potential event sequences from initiating event to consequences**
  - Basis: plant response
  - Modeling of accident progression → Frequency of accident sequences

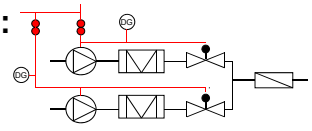
Methodological Aspects: Fault Trees

- **Which of those designs is more reliable ? (failure to inject water)**

A:



B:



Reliability Data

Offsite power unavailability: 15 min / yr = 0.25 / 8760 = 2.85E-5

Pump failure (mech.): 2 / 100 demands = 2E-2

Diesel Generator failure: 1 / 100 demands =1E-2

Valve failure (mech.): 2.5 / 1000 demands = 2.50E-3

Double-valve failure (mech.): 1 / 100 = 1E-2

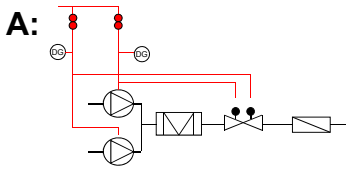
Check valve failure: 5 / 10'000 = 5E-4

Transformer failure: 1E-8

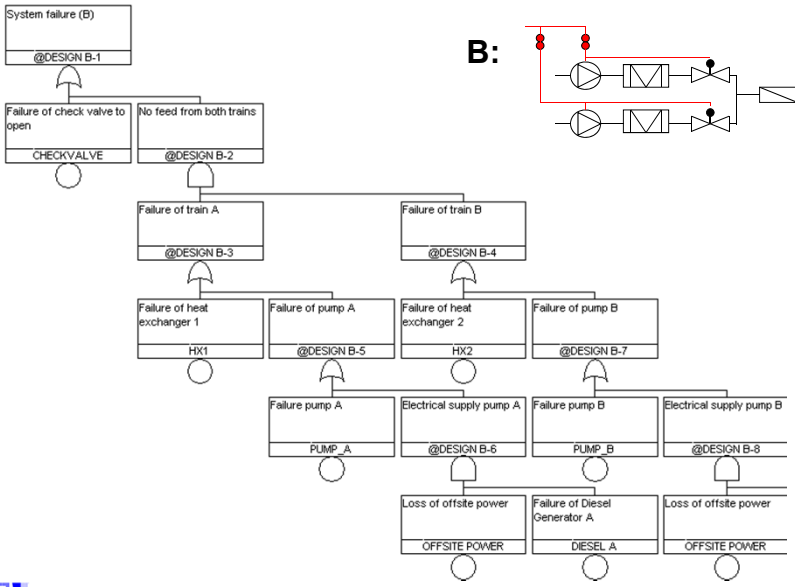
Heat exchanger failure: 1E-8

Methodological Aspects: Fault Trees

A:



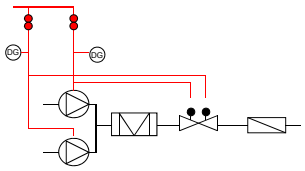
Methodological Aspects: Fault Trees



B:

Methodological Aspects: Fault Trees

Design A

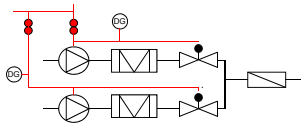


P(top) = 1.09E-2

Top Event probability Q = 1.089E-02

No.	Prob.	%	Event 1	Event 2	Event 3
1	1.000E-02	91.82	2MOV		
2	5.000E-04	4.59	CHECKVALVE		
3	4.000E-04	3.67	PUMP_A	PUMP_B	
4	1.000E-08	0.00	HX		
5	5.700E-09	0.00	DIESEL A	OFFSITE POWER	PUMP_B
6	5.700E-09	0.00	DIESEL_B	OFFSITE POWER	PUMP_A
7	2.850E-09	0.00	DIESEL A	DIESEL_B	OFFSITE POWER

Design B



P(top) = 9.00E-4

Top Event probability Q = 8.998E-04

No.	Prob.	%	Event 1	Event 2	Event 3
1	5.000E-04	55.57	CHECKVALVE		
2	4.000E-04	44.45	PUMP_A	PUMP_B	
3	5.700E-09	0.00	DIESEL_B	OFFSITE POWER	PUMP_A
4	5.700E-09	0.00	DIESEL A	OFFSITE POWER	PUMP_B
5	2.850E-09	0.00	DIESEL A	DIESEL_B	OFFSITE POWER
6	2.000E-10	0.00	HX2	PUMP_A	
7	2.000E-10	0.00	HX1	PUMP_B	
8	2.850E-15	0.00	DIESEL_B	HX1	OFFSITE POWER
9	2.850E-15	0.00	DIESEL A	HX2	OFFSITE POWER
10	1.000E-16	0.00	HX1	HX2	

Methodological Aspects: Risk Importance Measures

- **Risk Increase Factor (RIF / RAW)**

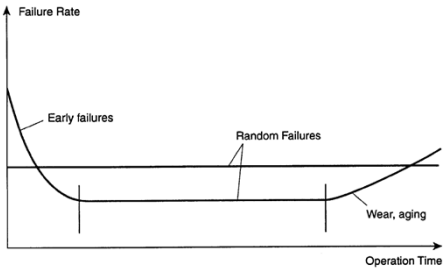
$$RIF(x) = \frac{P(top)\big|_{p(x)=1}}{P(top)}$$

- **Fussell-Vesely (FV)**
  - Fractional contribution of sequences in which component *x* is involved
  - Measure of the involvement level of a given component
- **Differential Importance Measure (DIM)**

$$DIM(x) = \frac{\partial P(top)}{\partial p(x)}$$

Zuverlässigkeit von Basis Ereignissen

- **Component reliability**
  - Startversagen: Q=q
  - Dauerversagen:



$$d(N_0 - N(t)) = -\lambda \cdot N(t) \cdot dt$$

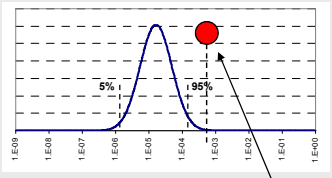
$$Q(t) = 1 - e^{-\lambda \cdot t} \xrightarrow{Tailor} \cong \lambda \cdot t$$

$$\overline{Q} = 1/T \cdot \int_0^T (1 - e^{-\lambda \cdot t}) \cdot dt = 1 + 1/\lambda \cdot T \cdot (e^{-\lambda \cdot T} - 1) \xrightarrow{Tailor} \sum_{i=2}^{\infty} \frac{(\lambda \cdot T)^{i-1}}{i!} \cong 1/2 \cdot \lambda \cdot T$$

$$Failure\ rate := \frac{1}{\underbrace{1 - Q(t)}_{Survived}} \cdot \lim_{\Delta t \to 0} \frac{Q(t + \Delta t) - Q(t)}{\Delta t} = \lambda$$

Methodological Aspects: Reliability Data

Generic or international data (observations)



Plant specific observations:

6 failures out of 10'000 demands = 6.0E-4

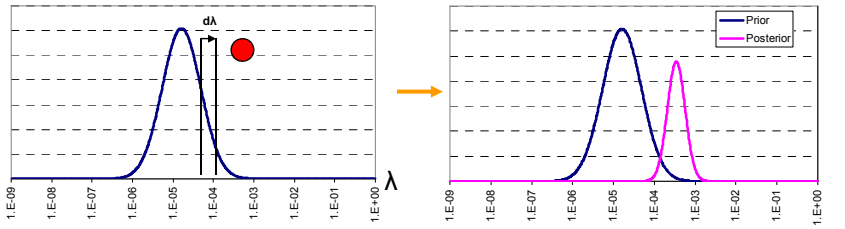
Bayesian Update → PSA model

Data specialization

Methodological Aspects: Reliability Data

- **Bayesian Law** $p(H|E)\cdot p(E) = p(E|H)\cdot p(H)$
- **…can be derived for continuous functions**

H: Hypothesis (here: λ)
E: Evidence (observations)



$$\underbrace{f(\lambda|E)}_{p(\lambda|E)}\cdot d\lambda \cdot \underbrace{\int_0^\infty f(\lambda)\cdot\lambda(E|\lambda)\cdot d\lambda}_{p(E)_{\forall\lambda}} = \underbrace{\lambda(E|\lambda)}_{p(E|\lambda)}\cdot \underbrace{f(\lambda)}_{p(\lambda)}\cdot d\lambda$$

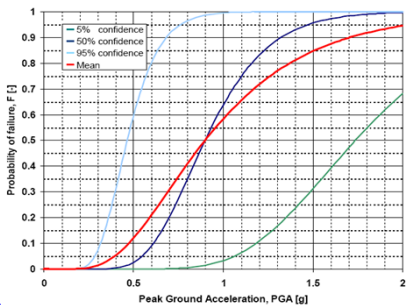
with $\lambda(E|\lambda) = \begin{cases} \frac{n!}{r!(n-r)!}\cdot\lambda^r\cdot(1-\lambda)^{n-r} & \text{for failures} \\ e^{-\lambda\cdot T}\cdot\frac{(\lambda\cdot T)^r}{r!} & \text{for failure rates} \end{cases}$

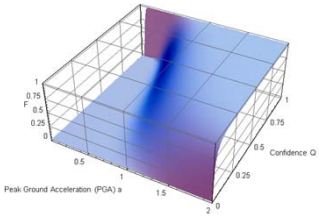
Methodological Aspects: Seismic Hazards

- **Earthquake likelihood is given by an hazard curve**
- **"Fragility" is a function of the sustained earthquake magnitude**

$$F(a,Q) = \phi\left[\frac{\ln(a/a_m) + \beta_u\cdot\phi^{-1}(Q)}{\beta_r}\right]$$

where:
ø(): Gaussian cumulative function
Q: confidence level (0..1)
a_m: median ground-acceleration capacity
β_u: uncertainty in capacity
β_r: randomness in earthquake and effects
a: sustained ground motion level.

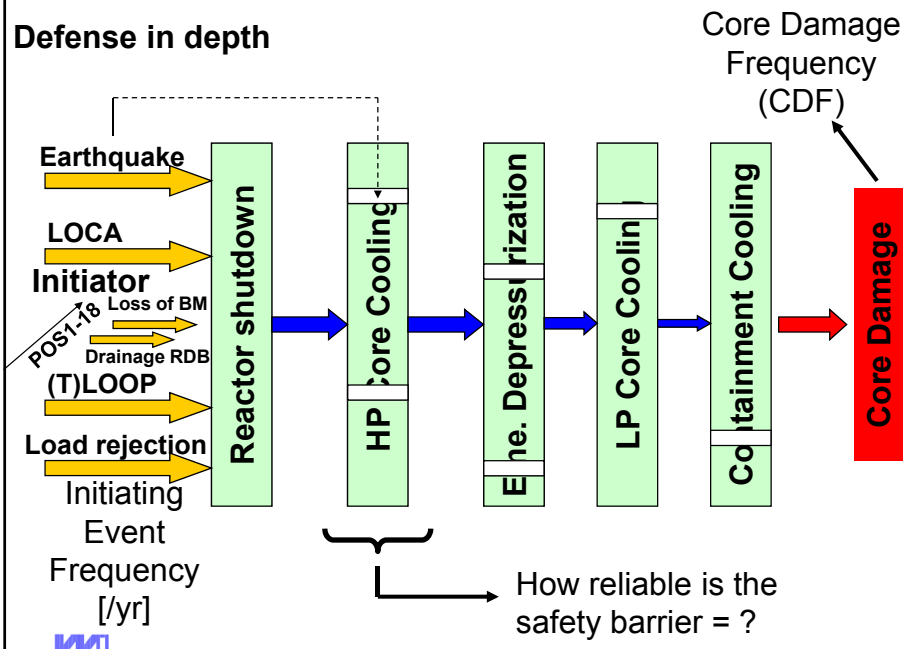




Methodological Aspects: Other types of data

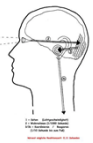
- **Other types of data assessment include**
  - Human Reliability Analysis (HRA)
    - In Switzerland: THERP / SLIM
  - Common Cause Failures (CCF)
    - Also subject to Bayesian updates !
  - Equipment unavailabilities
  - Impacts (example: fire, airplane crash, wind, …)
  - Initiating Event (IE) frequencies

Defense in depth



Methodological Aspects: Event Trees

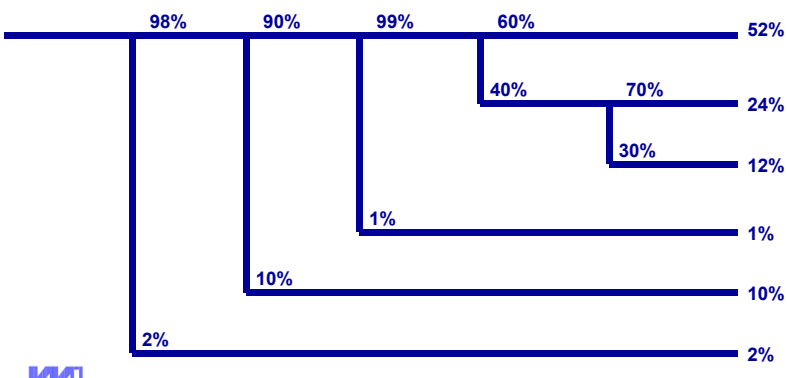




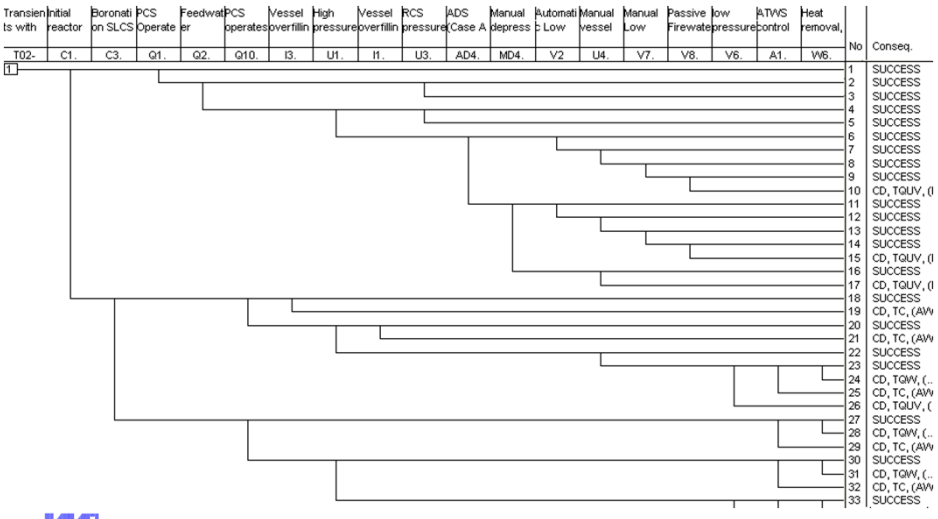
Break

Road wet

Girl draws aside (recovery action)

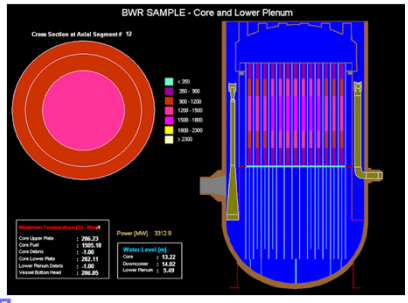


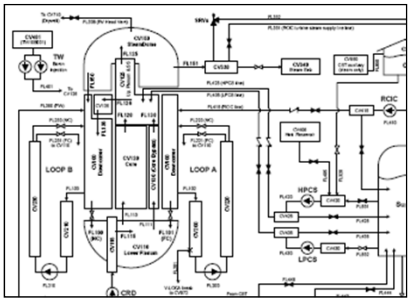
Methodological Aspects: Event Trees



Methodological Aspects: Level 2

- **Containment Response**
- **Accident progression and phenomenology**
- **Calculation of radiological consequences (source term)**
- **Uncertainty assessment**





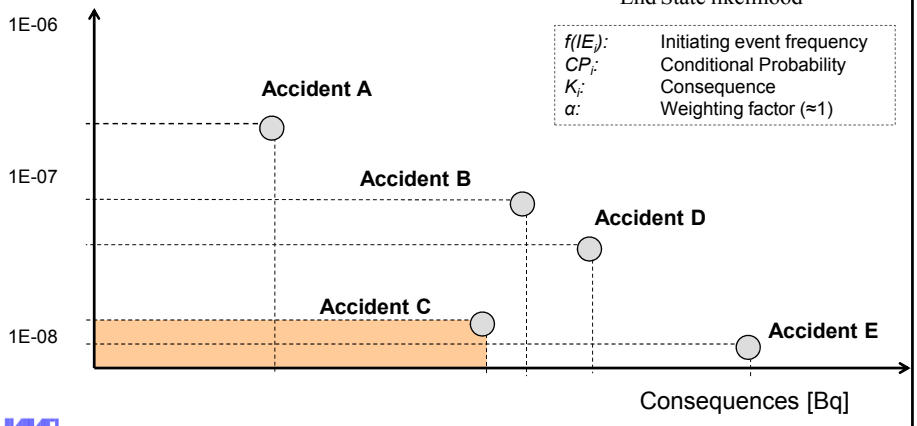
Methodological Aspects: Integral Risk

Core Damage Frequency [yr^{-1}]

(non-cumulative)

$$R = \sum_i \underbrace{f(IE_i) \cdot CP_i}_{\text{End State likelihood}} \cdot K_i^{\alpha}$$

$f(IE_i)$:	Initiating event frequency
CP_i:	Conditional Probability
K_i:	Consequence
α:	Weighting factor (≈1)



Swiss Atomic Law

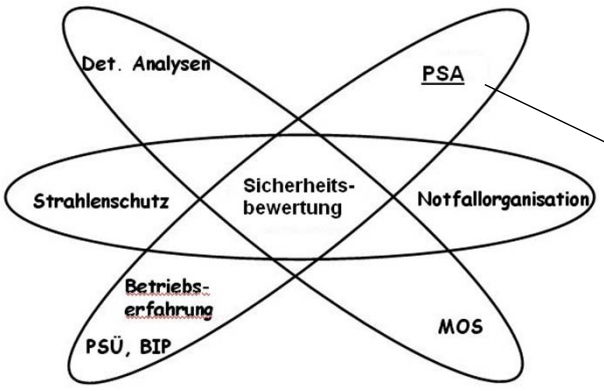
- **Swiss Atomic Law (KEG)**
  - Law for peaceful use of atomic energy
  - No claim about PSA in the text
- **Swiss Atomic Ordinance (KEV)**
  - Came into effect in February 2005
  - Defines basic requirements on PSA
  - Detailed in guidelines ENSI-A05 und A06

Safety goals
(as IAEA and NRC)

1E-4 for Core Damage Frequency (CDF)
1E-5 for Large Early Release Frequency (LERF)

Regulatives Umfeld
PSA in der Integrierten Aufsicht

- **PSA ist (nur) ein Element der Integrierten Sicherheitsbewertung**



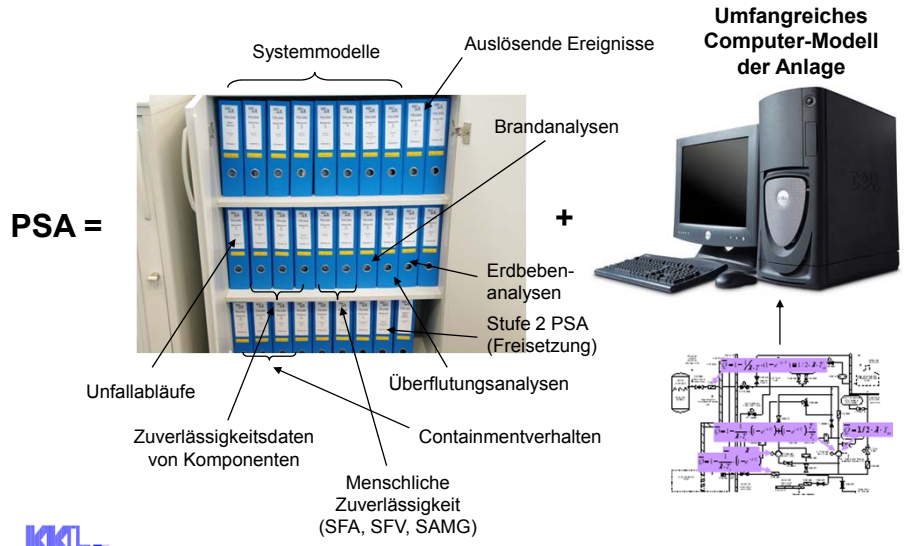
KEG

KEV

ENSI-A05

ENSI-A06

Überblick über die KKLPSA
Umfang einer PSA



Scope of an Industrial PSA Study

- **Analysis Scope (ENSI-A05, www.ensi.ch)**
  - Fullpower
    - Internal, external and area events
    - Level 1: Calculation of Core Damage Frequency (CDF)
    - Level 2: Calculation of radiological consequences
  - Low power and Shutdown (*KKL: 12 Plant Operating States*)
    - Internal, external and area events
    - Level 1: Calculation of Fuel Damage Frequency (FDF)
    - Level 2: Calculation of radiological consequences *(New !)*

Scope of an Industrial PSA Study: Types of Events

- **Internal Events**
  - Transients (24)
  - Loss of Coolant Accidents (LOCA) (37)
- **External Events**
  - Earthquakes, extreme winds, tornadoes, external flooding and aircraft crashes (20)
- **Area Events (internal hazards)**
  - Fires (85)
  - Flood (35)
  - Turbine missile (1)

202

Scope of an Industrial PSA Study

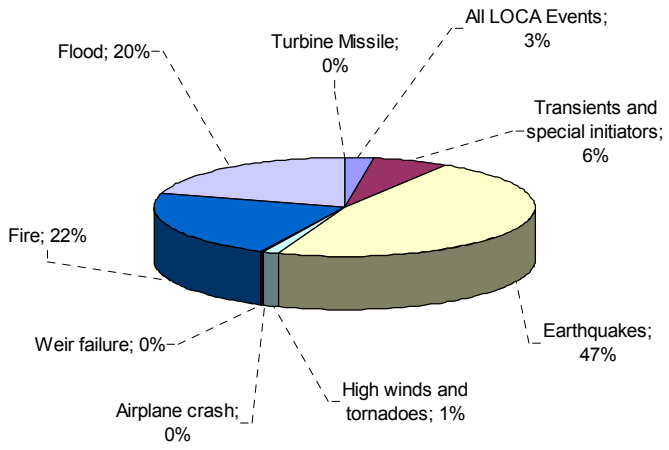
- **Component failure modes: ~ 10'000**
- **Human actions: ~ 400**
- **Fault trees: ~ 2000**
  - Up to 80 depth levels
- **Event Trees: ~ 300**
- **Common Cause Failure Groups: ~350**
- **Man-power**
  - Development & maintenance: 3 Man-Yr / Yr
  - Applications: 1 Man-Yr / Yr

  } >1M CHF / yr
- **Documentation: ~ 10'000 pages**

Applications and Results

- **Application scope (ENSI-A06, www.ensi.ch)**
  - Evaluation of the Safety Level (CDF < 1E-5)
  - Evaluation of the Balance of the Risk Contributors
  - Evaluation of the Technical Specifications
  - Evaluation of Changes to Structures and Systems
  - Risk Significance of Components (FV ≥ 1E-3 or RIF ≥ 2)
  - Evaluation of Operational Experience

Applications and Results: Risk Contributors



Root Cause Analysis Fukushima - First steps

M-9 class earthquakes in the past 100 years

The Fukushima Daiichi Accident

VGB PowerTech

- **Question: Is this accident a matter of residual risk of nuclear energy?**

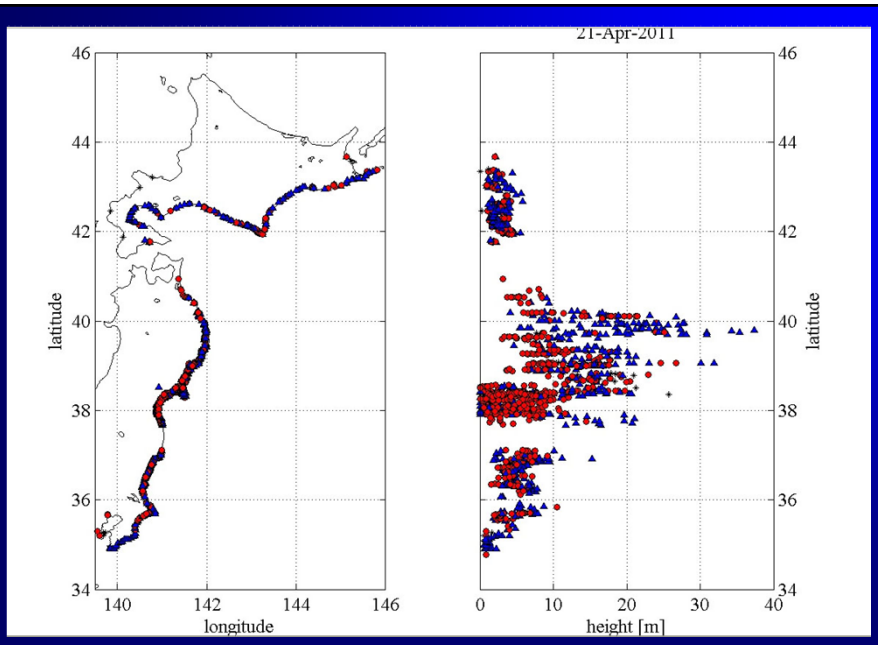
History data of earthquake-induced tsunamis with maximum amplitudes above 10 m hitting the coasts of Japan and the Kuril Islands (Russia) over the past 513 years

Date and Country		Affected Region	Earthquake [1]	Tsunami [2]	Victims
11.03.2011	Japan	Japan	M = 9.0	23 m	> 10 000
04.10.1994	Russia	Kuril Islands	M = 8.3	11 m	Not specified
12.07.1993	Japan	Sea of Japan	M = 7.7	31.7 m	330
26.05.1983	Japan	Noshiro	M = 7.7	14.5 m	103
07.12.1944	Japan	Kii Peninsula	M = 8.1	10 m	40
02.03.1933	Japan	Sanriku	M = 8.4	30 m	3 000
01.09.1923	Japan	Tokaido	M = 7.9	12 m	2 144
07.09.1918	Russia	Kuril Islands	M = 8.2	12 m	50
15.06.1896	Japan	Sanriku	M = 7.6	38 m	26 360
24.12.1854	Japan	Nankaido	M = 8.4	28 m	3 000
29.06.1780	Russia	Kuril Islands	M = 7.5	12 m	12
24.04.1771	Japan	Ryukyu Islands	M = 7.4	85 m	13 500
28.10.1707	Japan	Japan	M = 8.4	11 m	30 000
31.12.1703	Japan	Tokaido-Kashima	M = 8.2	10,5 m	5 200
02.12.1611	Japan	Sanriku	M = 8.0	25 m	5 000
20.09.1498	Japan	Nankaido	M = 8.6	17 m	200

- **Simple Estimation:**
  Within the past 513 years 16 tsunamis with maximum amplitudes above 10 m and induced by earthquakes of magnitudes between 7.4 and 9.2 have been recorded for Japan and the adjacent Kuril Islands (Russia).
- **Experienced Frequency:**
  $f = 16/513\ a \approx 0.0312\ a^{-1}$
  Thus, within a thirty years period one severe tsunami with a maximum amplitude of more than 10 m has to be expected in Japan!

- **No, it is rather a matter of obviously having ignored a high specific risk!**

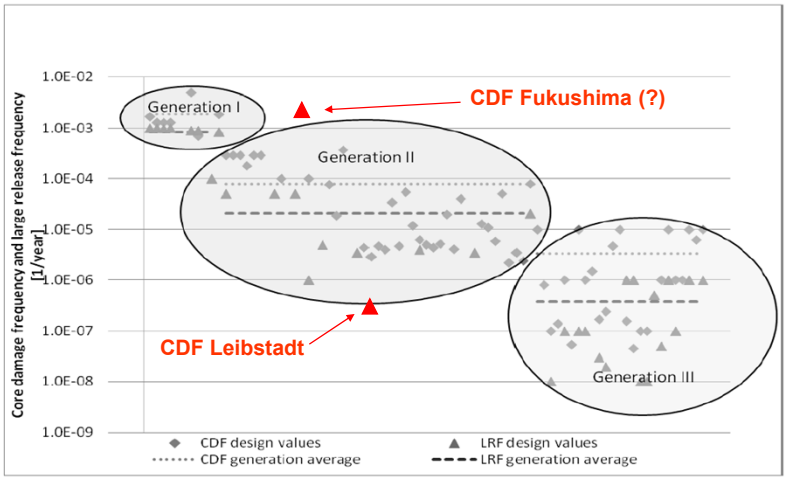
Sources: Dr. Johannis Nöggerath, Swiss Nuclear Society, March 28, 2011, www.tsunami-alarm-system.com [1]) magnitude [2]) maximum amplitude



Wave height distribution as for 21.04.11. Red circle: inundation depth. Blue triangle: run-up height

Vergleich der Sicherheit KKL mit Neuanlagen

Entwicklung der CDF von Kraftwerkstypen Gen. I - III



Conclusions

- **PSA aim to realistically describe risk and safety levels; assess safety barriers**
- **Give insights about the performance of safety measures; indentify weak points**
- **Assess the relative important of accident sequences, optimize the use of available resources**
- **Enable safety assessment of operating aspects and operating experience**