

Deterministic vs. Probabilistic Approach

Introduction to Basic Methods and Structure of Probabilistic Risk Assessments (PRA)

Prof. Wolfgang Kröger

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



Legal Basis for Application of PRA to Swiss NPP

- Federal Act on Nuclear Energy (KEG 2003/09) regards PRA as a well established tool to identify safety improvements and assess associated measures.
- Federal Ordinance on Nuclear Energy (KEV 2004/11) claims to integrate PRA level 1, 2 into the licensing and oversight procedure and demonstrate
 - that CDF due to internal and external is 10^{-5} /a at maximum for new plants and existing plants, if reasonably achievable.
 - Furthermore, plants have to be protected against natural hazards such as earthquakes with occurrence rates of $\geq 10^{-4}$ /a.
- Usually, sabotage, acts of terrorism and war are not included in PRAs.

Further requirements are specified in ENSI-guidelines; PRAs are available for all plants, have to be updated periodically.

Scope of Probabilistic Risk Assessment (PRA)

- Both accident initiating events and the unavailability of safety equipment or measures needed to handle accidents are assumed.
- The technical system and specific chains of events (scenarios) including their frequencies of occurrence and resulting plant states are modeled.
- Physical phenomena of the postulated scenarios are modeled, and respective consequences are assessed – inside and outside the plant.
- The risk of the analyzed technical system is the sum of the products of realistically identified consequences x and their frequencies $h(x)$
$$R = x_1 \cdot h(x_1) + x_2 \cdot h(x_2) + \dots$$
for a representative number of exclusive initiating events and event chains.

Deterministic vs. Probabilistic Approach (1/2)

Deterministic (postulating)

- Events completely determined by cause-effect-chains (causality).
- Analyse of the effects of assumed enveloping causes, single failure criterion postulated

Statistically (retrospective)

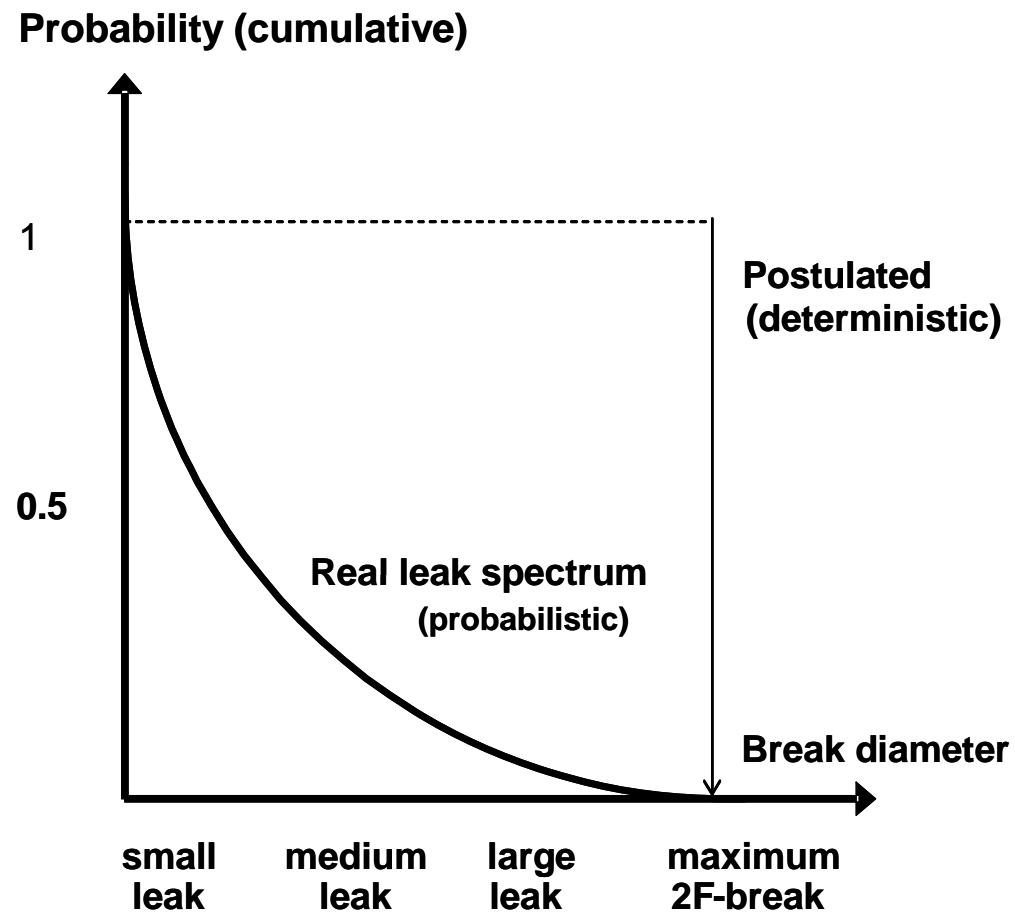
- Rules can be derived from a large number of similar events (based on experience).
- Directly applicable observations can be transferred to the system or to the event level.

Probabilistic (prognostic)

- Events can be identified by the probability of occurrence, whole spectrum of events taken into account
- Use of observations on the level of components.

Deterministic vs. Probabilistic Approach (2/2)

Example „leakage of the primary coolant boundary”



Approaches		
statistic	deterministic	probabilistic
a great number of similar events hold experiential values	events are completely predetermined through effect chains (causality)	Events can be identified through their probabilities of occurrence
Methodology (within risk analyses)		
Analyse of a great number of directly usable observations on the level of systems / events	Analyse of the effects of assumed causes on the level of relevant systems / events	Complete analyse of system caused event chains and realistic estimation of frequencies and consequences as well as of uncertainties
(descriptive)	(definitive)	(prognostic)
Risk definition		
risk = expected value ≥ 0		risk = dependent probability
Prerequisites		
relative frequency		Kolmogoroff axiom system

Definition of Some Terms

Absolute Frequency

- How often a given measured value occurs within a sample (≥ 0)

Relative Frequency

- Ratio between the number of certain events to the number of all events (≤ 1)

Probability

- Measure for the uncertainty of future events (between 0 and 1)

Frequency

- Time related frequency (e.g., number per year, ≥ 0)

Failure Probability

- Probability that a system (component) will fail to perform a required function under stated conditions for a stated period of time (between 0 and 1)

Failure / repair rate

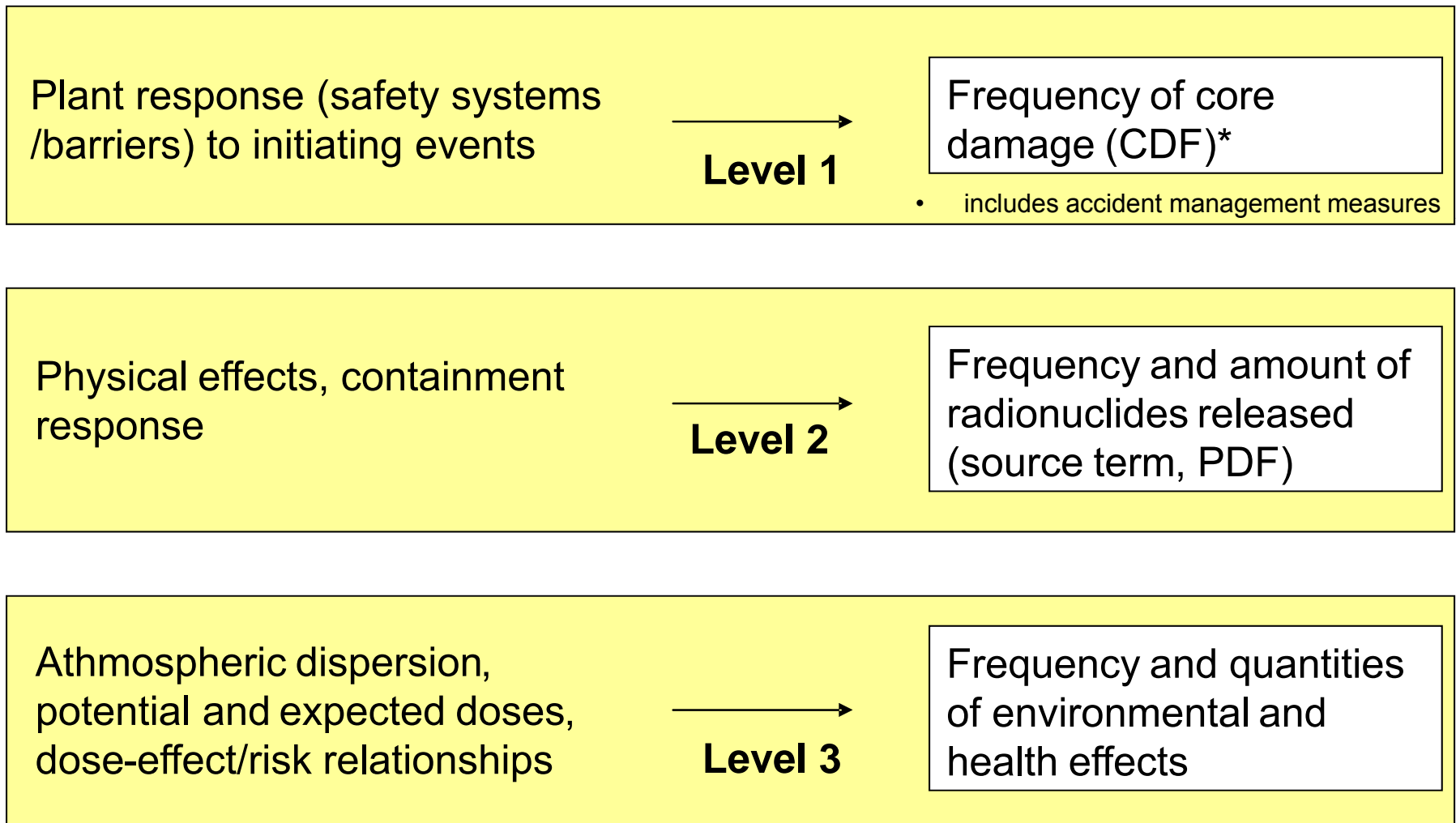
- Frequency with which a system (component) fails/ is repaired (e.g. number of failures/repairs per time)

statistically	probabilistically
Risk = expected value ≥ 0	Risk = related probability
Example: throwing a coin (“heads” = „0“ and “tails” = „1“)	
$E(X) = \sum_{i=1}^2 x_i \cdot \hat{\Pr}(X=x_i)$ <p>E(X): Expected value X: Probability variable “heads”/“tails” $\hat{\Pr}(\bullet)$: Relative frequency</p> <p><u>Observation:</u></p> $x_i = \begin{cases} 1 & \hat{\Pr}(X=x_i) = \frac{550}{1000} = 0,55 \\ 0 & \hat{\Pr}(X=x_i) = \frac{450}{1000} = 0,45 \end{cases}$ <p>$\Rightarrow E(X) = 0,55$ The „expectation“ for „1“ is closer to 100%</p>	<p>Risk = $\Pr(X) = \Pr(X E) \cdot \Pr(E)$ Pr(E): Probability that a coin will be thrown Pr(X): Probability that “1” occurs Pr(X E): Probability of “1” under the condition that a coin has been thrown Pr(X) = Pr(X E) · Pr(E) = 0,5 · 1 = 0,5 The probability of heaving “1” is 0.5</p> <hr/> <p>Axiom system of Kolmogoroff:</p> <ol style="list-style-type: none"> $0 \leq \Pr(x) \leq 1$ Pr(sure event) = 1 $\Pr\left(\bigcup_{i=1}^n x_i\right) = \Pr\left(\sum_{i=1}^n x_i\right)$

Probabilistic Risk Assessments (PRA) Compared to Deterministic Approaches

- PRA as a complementary instrument.
- PRA aims at realistic description of risk and safety.
- PRA models provide information on expected performance of different safety measures; they disclose weak points.
- PRA reflects consequences of dependencies and man-machine interdependencies
- PRA shows uncertainties.
- PRA shows the relative importance of each accident sequence, it allows focusing on dominant accident sequences.
- PRA allows optimal allocation of available resources.

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



Initiating Events

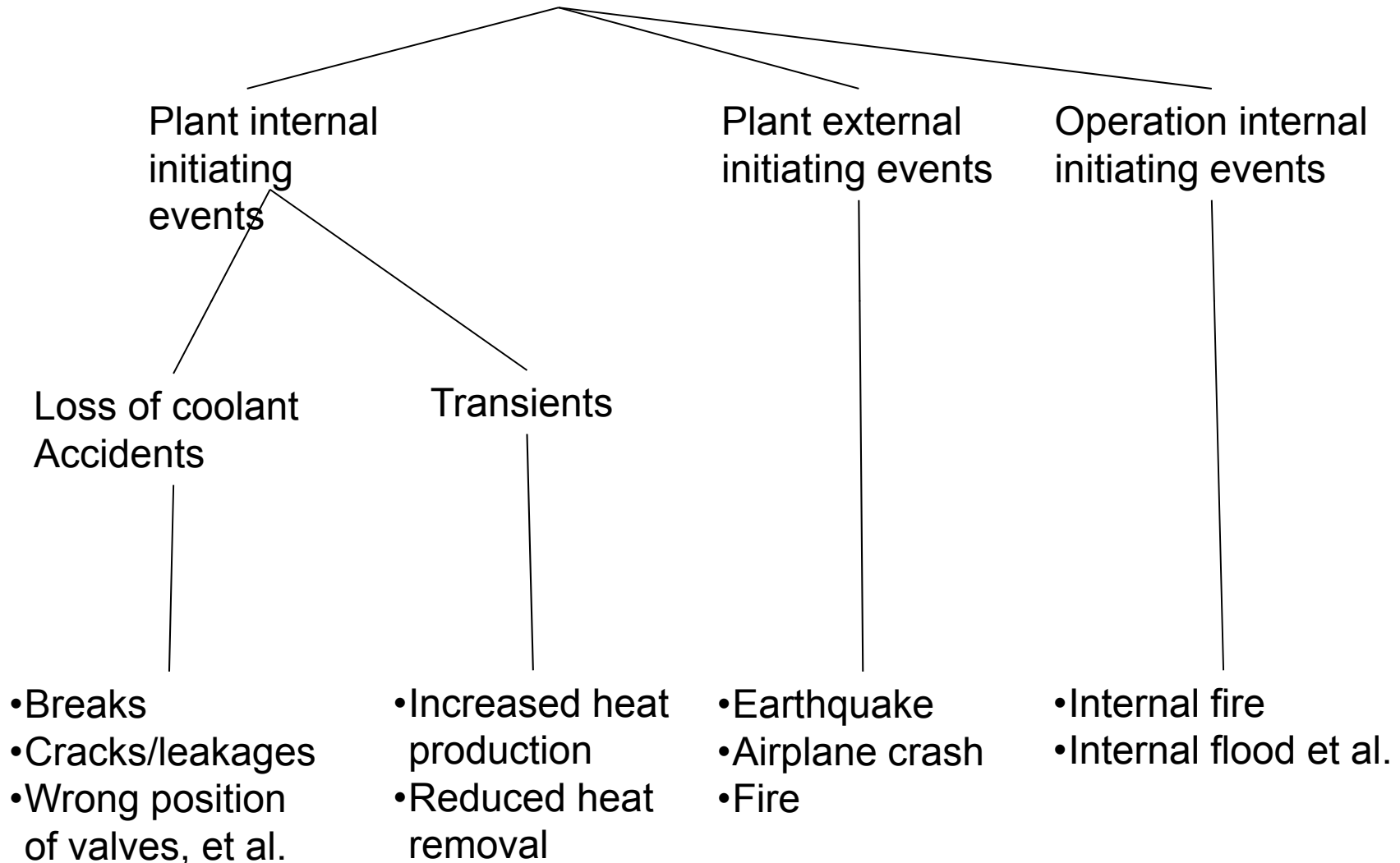
Definition:

An initiating event is an incident which necessitates automatic or operator actions in order to bring the plant into safe steady state conditions; without such actions the core may be damaged.

The tasks within a PRA level 1 are:

1. Identification of the initiating events,
2. their classification into categories,
3. estimation of their frequencies.

Classification of initiating events



Note: Common cause (wide area) initiating events are of special interest

Method of Fault Tree Analysis (FTA)

- Fault Tree Analysis (FTA) is a top-down approach for failure analysis, starting with a potential undesirable event (failed state) called TOP Event, and then determining deductively all the ways it can happen.
- The analysis proceeds by determining how the TOP Event can be caused by individual or combined lower level failures or events. The causes of the TOP Event are “connected” through logic gates.
- FTA is the most commonly used technique for causal analysis

Working steps of a FTA

- Definition of the “top event”
- Identification of all basic event combinations which result in the “top event”

If quantitative

- Assignment of failure probabilities to basic events
- Boolean modelling and calculations of probabilities
- Analysis of dominating failure combination and impacts (importance analysis), proposals for system improvement/optimisation

1. Definition of the “top event“:

- **In general:** system failure.
- **In particular:** loss of specific functions and services meaning the failure of the overall system

2. Identification of basic event combinations:

The formal combination of events constitutes the logical structure of the system considered or the derived Boolean model (fault tree). The model consists of:

- Input events: Lower event (“input” to the gate).
- Gates (logic operation): Show the relationship of lower events needed to result in a higher event (logic AND, OR).
- Output events: Higher event (“output” of the gate).



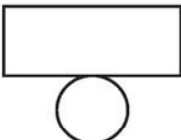
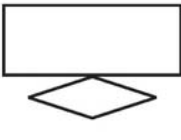



The behaviour of the gates is determined by the **Rules of Boolean Algebra**.

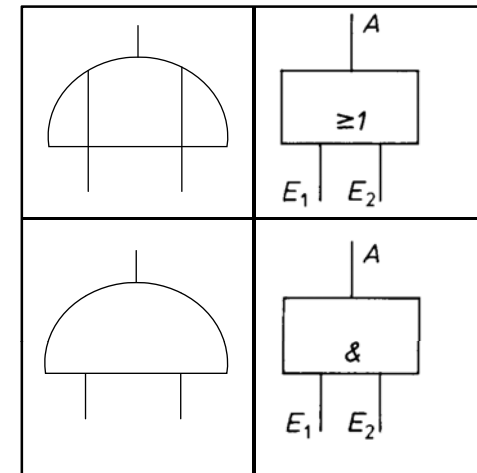
Required information for a FTA

- **Component level:**
 - Different relevant failure modes of individual units (to fix most relevant one).
 - Relevant external “influences”, e.g. maintenance, environmental impacts.
 - For quantitative analyses: Failure probabilities.
- **System level:**
 - Precise definition of the operation mode in question.
 - The system boundaries (which parts of the system are included in the analysis, what type of external stresses should be included in the analysis).
 - The level of resolution (how detailed should the analysis be?).

Fault Tree Symbols

Alternative Symbols

Logic gates	 OR-gate	The OR-gate indicates that the output event occurs if any of the input events occur
	 AND-gate	The AND-gate indicates that the output event occurs only if all the input events occur at the same time
Input events (states)		The basic event represents a basic equipment failure that requires no further development of failure causes
		The undeveloped event represents an event that is not examined further because information is unavailable or because its consequences are insignificant
Description of state		The comment rectangle is for supplementary information
Transfer symbols	Transfer out  Transfer in 	The transfer-out symbol indicates that the fault tree is developed further at the occurrence of the corresponding transfer-in symbol



3. Assignment of failure probabilities:

Problems

- Lack of specific data (e.g. reliability figures of highly reliable tailor-made components in nuclear power plants, components designed to work under changing operating conditions in the chemical industry, etc.).
- Development of the database usually causes an extensive amount of work.

4. Boolean modelling and calculation of probabilities:

Summary of the assumptions/preconditions

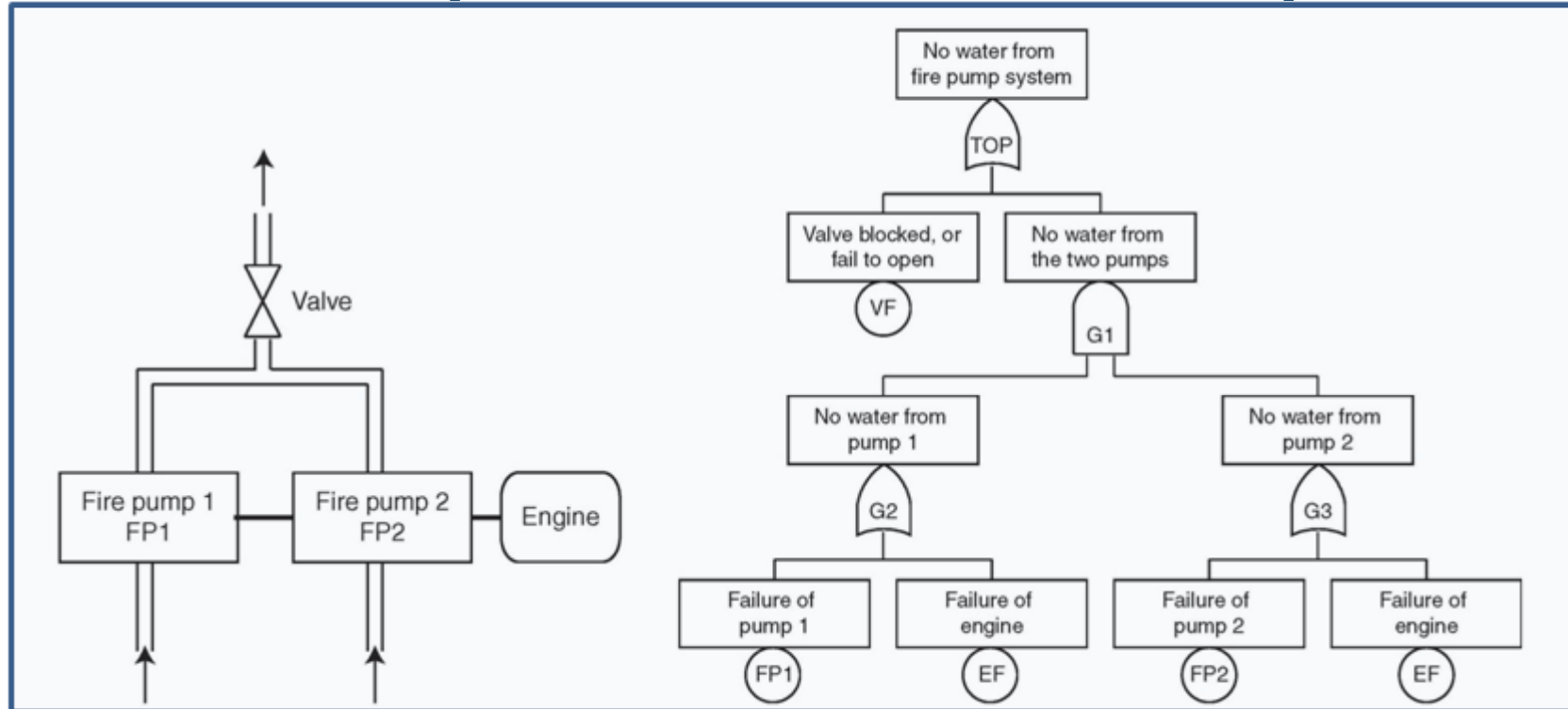
- A technical system consists of units (components).
- The units are both technically and logically connected.
- The state of each unit follows a binary logic (TRUE/FALSE, on/off, intact/defect).
- Available logic operators are:
 - conjunction: AND (\cap).
 - disjunction: OR (\cup).

Labelling of the probabilities:

p_i : probability of survival of the i -th unit.

q_i : probability of failure of the i -th unit.

Example: Redundant Fire Pump

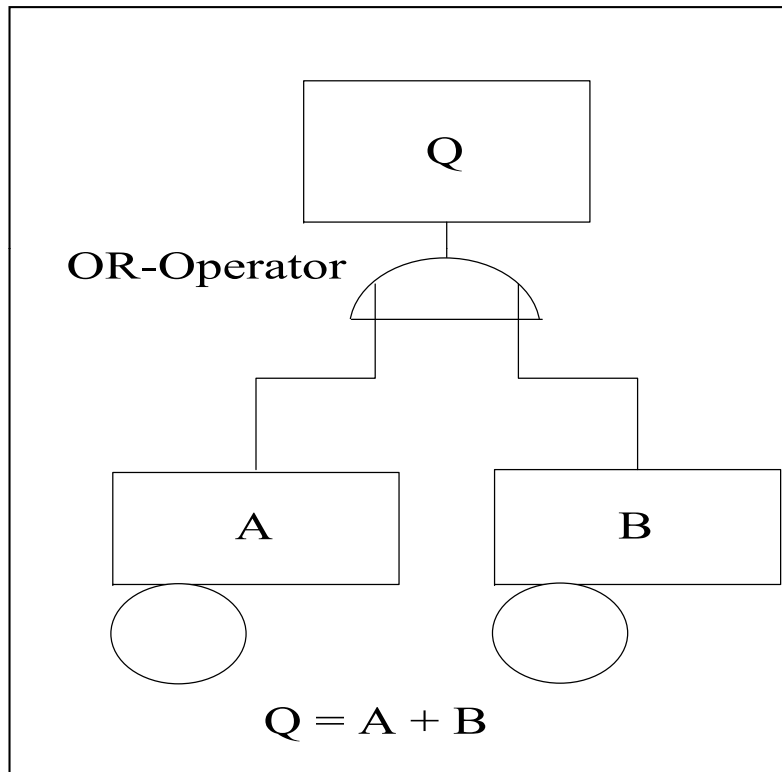


TOP Event: No water from fire water system.

CAUSES for TOP Event:

- VF = Valve Failure
- G1 = No output from any of the fire pumps
- G2 = No water from FP1
- G3 = No water from FP2
- FP1 = Failure of FP1
- FP2 = Failure of FP2
- EF = Failure of Engine

Fault Tree Analysis I



Probability:

$$P(Q) = P(A) + P(B) - P(A \cap B)$$

$$P(A) + P(B) - P(A) \cdot P(B | A)$$

some conclusions:

- 1) A and B mutually exclusive:

$$P(A \cap B) = 0$$

$$P(Q) = P(A) + P(B)$$

- 2) A and B independent: $P(B | A) = P(B)$

$$P(Q) = P(A) + P(B) - P(A) \cdot P(B)$$

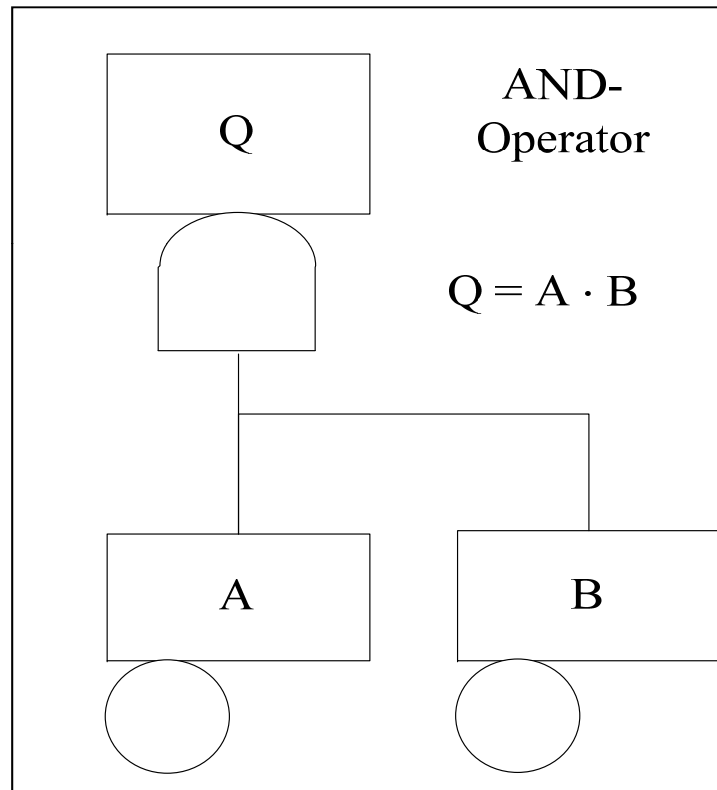
- 3) A and B completely dependent: $P(B | A) = 1$

$$P(Q) = P(A) + P(B) - P(A) = P(B)$$

$$P(Q) \approx P(A) + P(B)$$

always a conservative approach

Fault Tree Analysis II



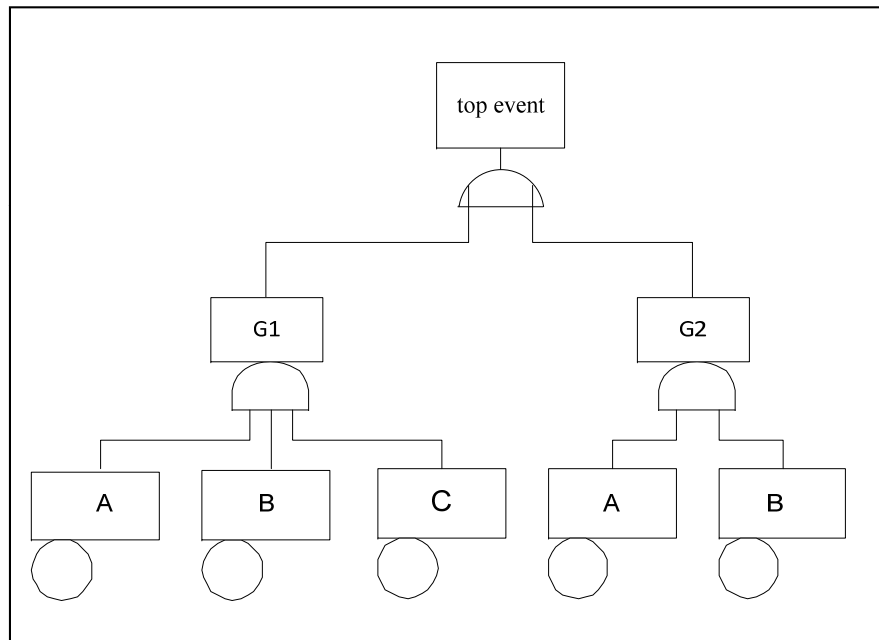
Probability:

$$P(Q) = P(A \cap B) \\ = P(A) \cdot P(B | A) = P(B) \cdot P(A | B)$$

some conclusions:

1. A and B independent: $P(B | A) = P(B)$ and $P(A | B) = P(A)$:
 $P(Q) = P(A) \cdot P(B)$
2. A and B dependent:
 $P(Q) > P(A) \cdot P(B)$
3. total dependence: $P(B | A) = 1$
 $P(Q) = P(A)$
approximations can be dangerous!

Fault Tree Analysis II



The systems fails (top event occurs), if

cut sets

1. $A \cap B$

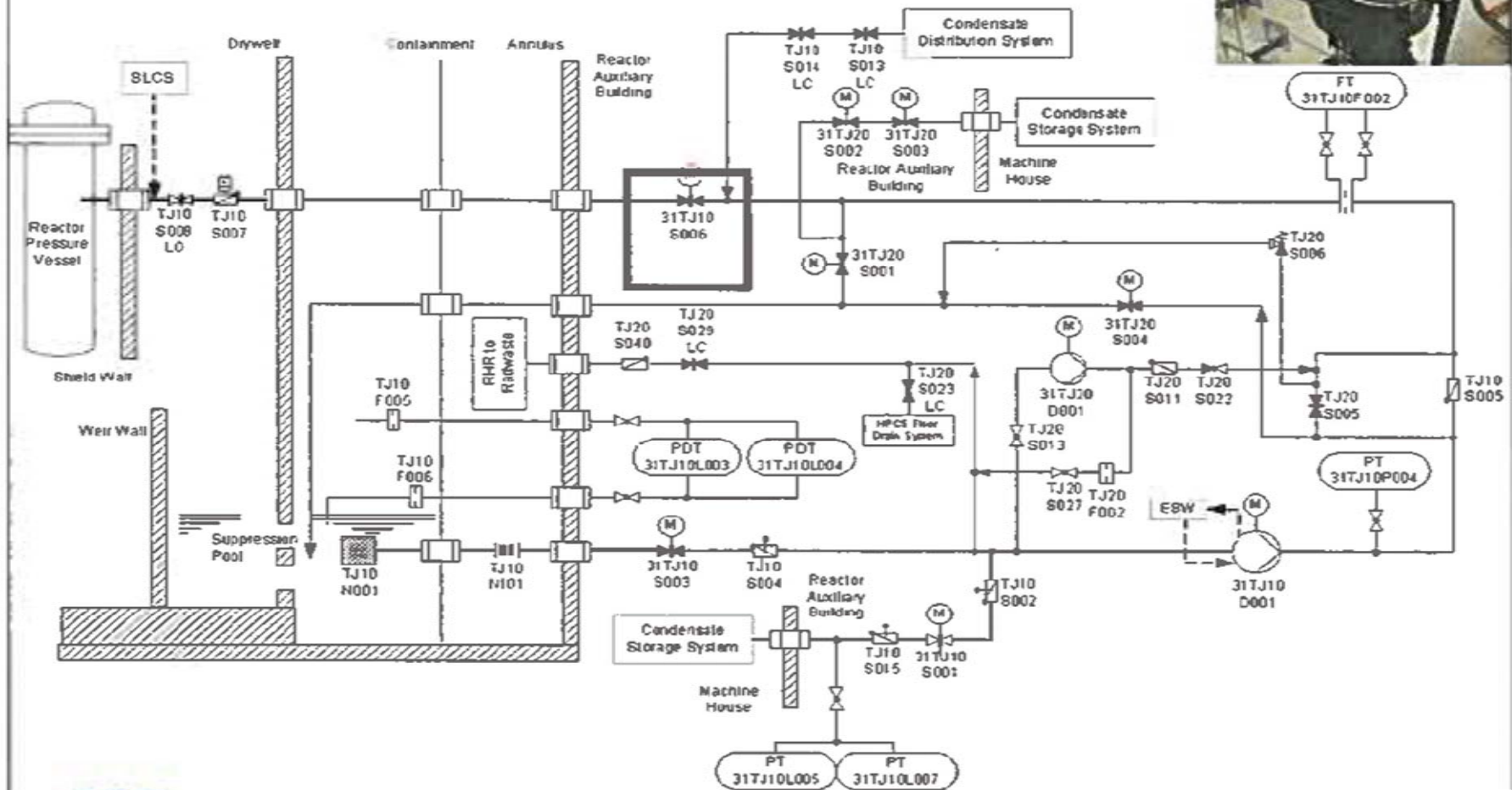
2. $A \cap B \cap C$

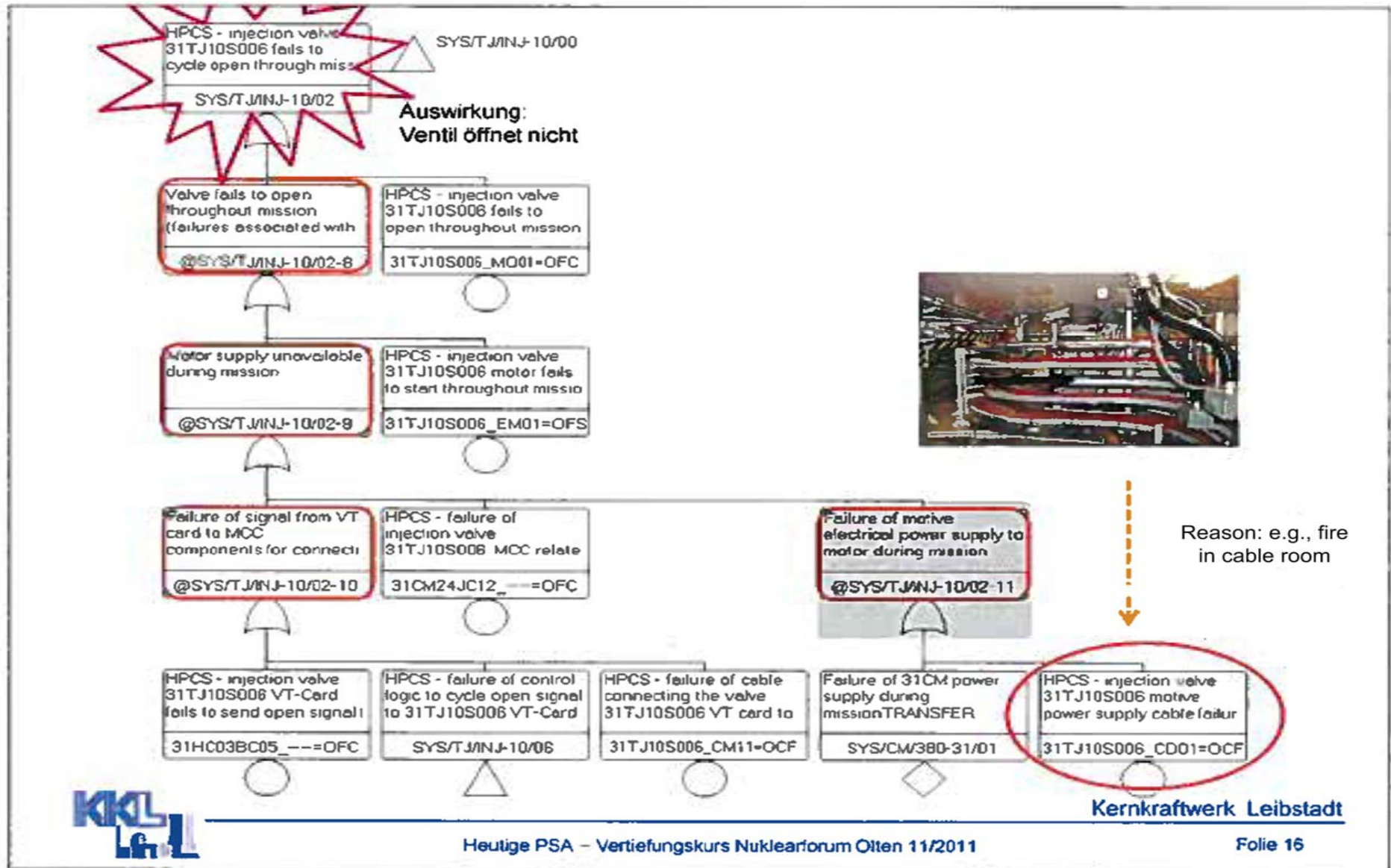
or minimal cut sets:

1. $A \cap B$

fail.

Fault Tree (KKL-HP Injection System) for failure of monitor-driven valve to open





Event Tree Analysis (ETA)

- An event tree analysis (ETA) is an inductive procedure that begins with an initiating (triggering, accidental) event and “propagate” this event through the system under study by considering all possible ways in which it can effect the behaviour of the system. The nodes of an event tree represent the possible functioning or malfunctioning of a (sub)system.
- By studying all relevant accidental events, the ETA can be used to identify all potential accident scenarios and sequences in a complicated system.
- Design and procedural weaknesses can be identified, and probabilities of the various outcomes from an accidental event can be determined.

Working steps of a ETA

1. Identify (and define) a relevant accidental (initial) event that may give rise to unwanted consequences.
2. Identify the events that are relevant to the initiating event and can affect the propagation of the latter through the system. These events can be barriers, safety functions, protection layers, etc. and may be technical and/or administrative (organizational).
3. Construct the event tree, describe the (potential) resulting accident sequences.
4. Determine the frequency of the accidental event and the (conditional) probabilities of the branches in the event tree.
5. Calculate the probabilities/frequencies for the identified consequences (outcomes).
6. Compile and present the results from the analysis.

1. Identify (and define) a relevant accidental (initial) event

When defining an accident event, we should answer the following questions:

- What type of event is it (e.g., leak, fire)?
- Where does the event take place (e.g., in the control room)?
- When does the event occur (e.g., during normal operation, during maintenance)?

In practical applications there are sometimes discussions about what should be considered an accidental event (e.g., a gas leak, the resulting fire or an explosion). Whenever feasible, we should always start with the first significant deviation that may lead to unwanted consequences.

An accidental event may be caused by:

- System or equipment failure.
- Human error.
- Process upset.

The accidental event is normally “anticipated”. The system designers have put in barriers that are designed to respond to the event by terminating the accident sequence or by mitigating the consequences of the accident.

2. Identify the events

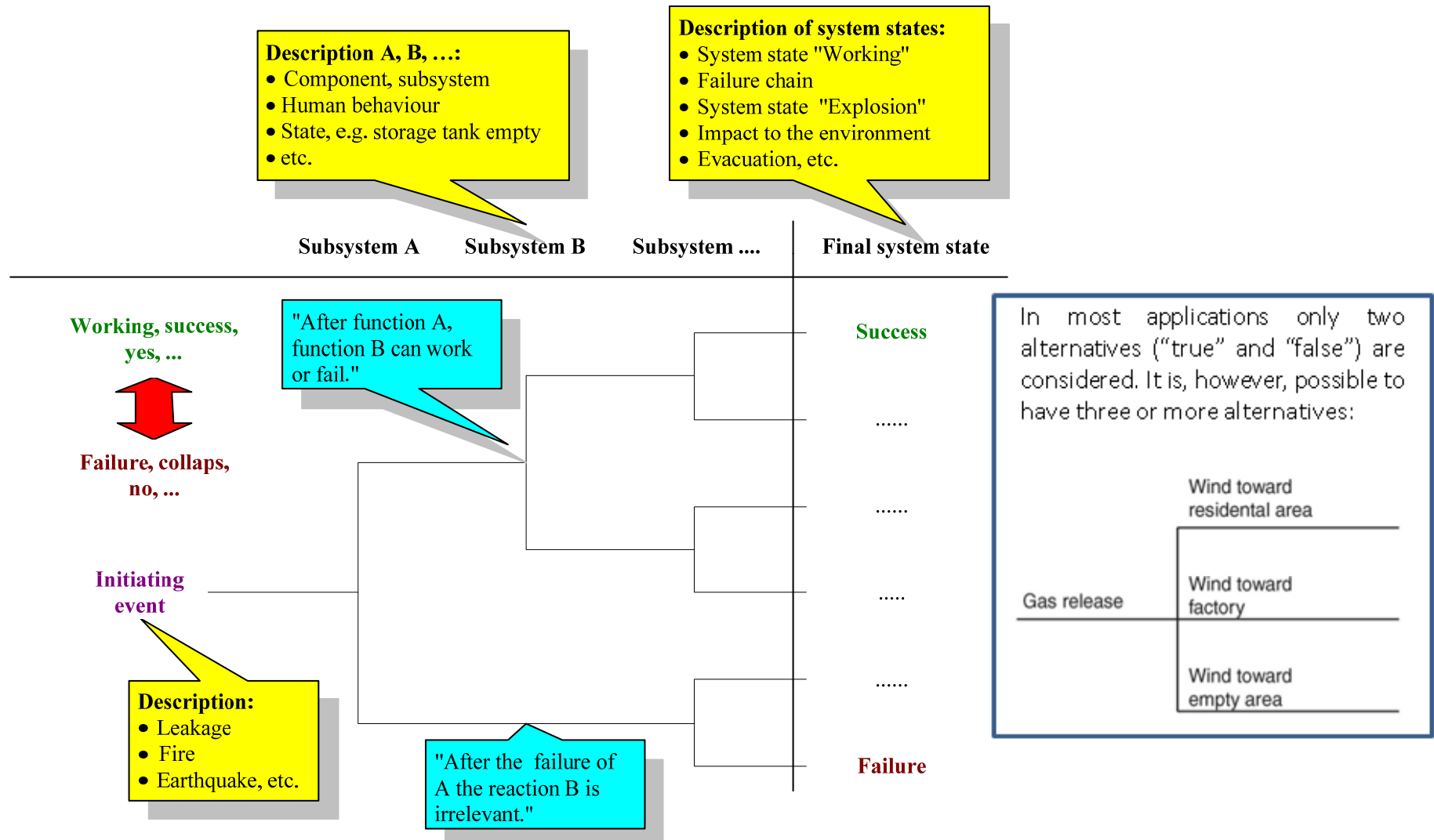
The events that are relevant to a specific triggering (initiating) event should be listed in the sequence they will be activated. Examples include:

- Automatic detection systems (e.g., fire detection).
- Automatic safety systems (e.g., fire extinguishing).
- Alarms warning personnel/operators.
- Procedures and operator actions.
- Mitigating barriers.

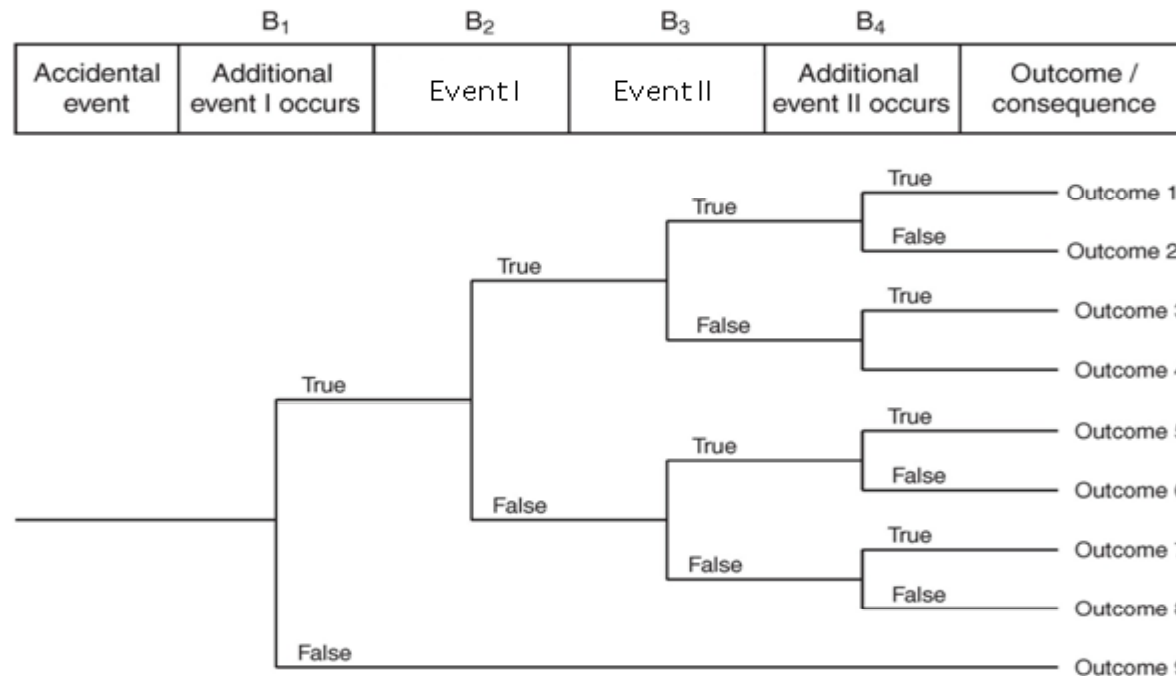
Each event should be described by a (negative) statement, e.g., “ X does not function” (This means that X is not able to perform its required function(s) when the specified accidental event occurs in the specified context).

Additional events and factors should also be described by (worst case) statements, e.g., gas is ignited, wind blows toward dwelling area.

3. Construct an event tree/resulting sequences



Generic Example



$$\Pr(\text{Outcome 1} | \text{Initiating Event}) = \Pr(B_1 \cap B_2 \cap B_3 \cap B_4)$$

$$= \Pr(B_1) \cdot \Pr(B_2 | B_1) \cdot \Pr(B_3 | B_1 \cap B_2) \cdot \Pr(B_4 | B_1 \cap B_2 \cap B_3)$$

Note that all the probabilities are conditional given the result of the process until “Barrier *i*” is reached.

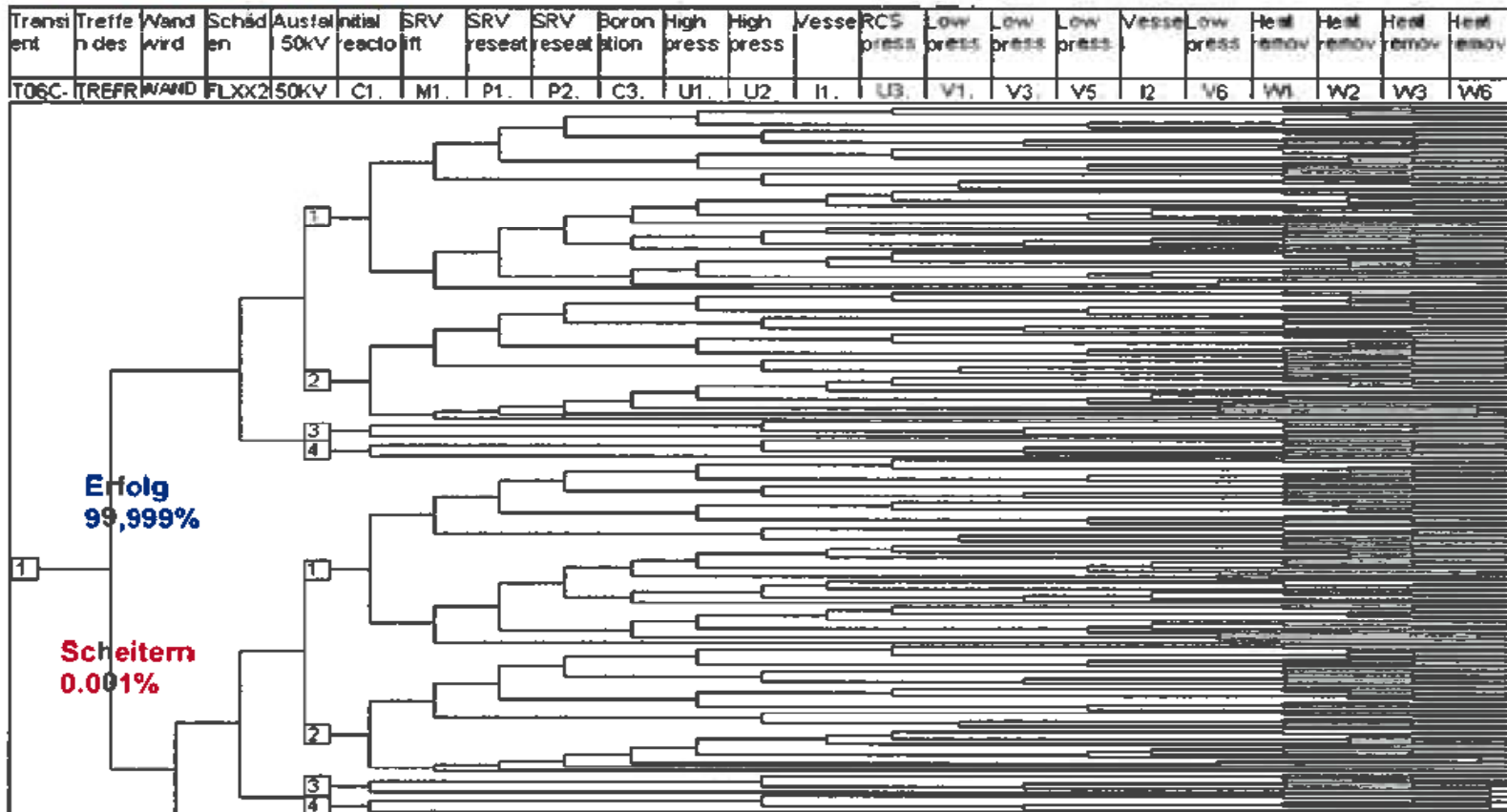
The frequency of the Outcome 1 is : $\Pr(\text{Initiating Event}) \cdot \Pr(B_1 \cap B_2 \cap B_3 \cap B_4)$.

where $\Pr(\text{Initiating Event})$ is the frequency of the initiating event

The frequencies of the other outcomes are determined in a similar way.

ETA (KKL) of aircraft crash

Wahrscheinlichkeitssequenz für Erfolg oder Versagen von notwendigen Sicherheitsfunktionen um zu einem sicheren Zustand oder zum Kernschmelzen zu gelangen



Kernkraftwerk Leibstadt

Heutige PSA – Vertiefungskurs Nuklearforum Olten 11/2011

Folie 14

7. Present the results

Consequences Analysis

Out- come descr.	Freq- uency	Loss of lives					Material damage				Environmental damage							
		0	1-2	3-5	6 - 20	> 20	N	L	M	H	N	L	M	H				

Characterization of a full PRA (KKL as an example)

Example: KKL

- About 200 initiating events (power operation + shut down states): 24 Transients, 37 LOCA, 20 external, 85 fires & 35 flooding, all internal
- Millions of accident sequences added to a total core damage frequency (CDF) $4 \cdot 10^{-6}$ /a; combined use of fault tree (2000), and event tree (300) techniques
- 8'000 sequences ($\geq 10^{-10}$ /a) binned into 20 plant damage states (PDS)
- 15 to 20 release categories and 10 to 15 damage indicators per release category formed

Overview of PRA methodology

