Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Safety Performance Indicators | Learning from Others

Wolfgang Kröger, ETH Zurich

SASCON‘12, November 14, 2012, Olten

Performance Indicators | Definition and Categorization

A jargon for a type of performance measurement used by an organization to evaluate its success or the success of a particular activity, e.g. delivering aircraft services, providing means/tool for improvements. The selection of PIs is specific and closely associated with the use of various assessment techniques.

Safety-related PIs can be categorized as

- quantitative, presented as a number,
- practical, interfacing with existing company processes,
- directional, specifying whether an organization is getting better or not,
- actionable, sufficiently in an organization’s control to affect change,

and can be

- reactive showing, e.g., a number of accident over a predefined period,
- proactive showing, e.g., a number of near-misses, further developed into causal chains (accident scenarios),
- predictive showing potential future accident scenarios build on analysis of incident data and application of analytical techniques.

Performance Indicators | Requirements

PIs must be simple, measurable, reliable and commonly accepted; for safety management purposes there is a need of a mix of outcome indicators (like fatal accidents) and process indicators (like record keeping).

Performance-based regulation concentrates on those PIs to assess safety, in contrast to compliance-based and risk-informed regulation.

An important concern is the availability of quantitative and qualitative data fulfilling requirements such as

- sufficient population/completeness/stability,
- suitability/transferability/compatibility,
- adequate evaluation techniques/objectivity of analyst.

Low-frequency high-consequence events are of special concern!

Performance Indicators | Objectives and Methods

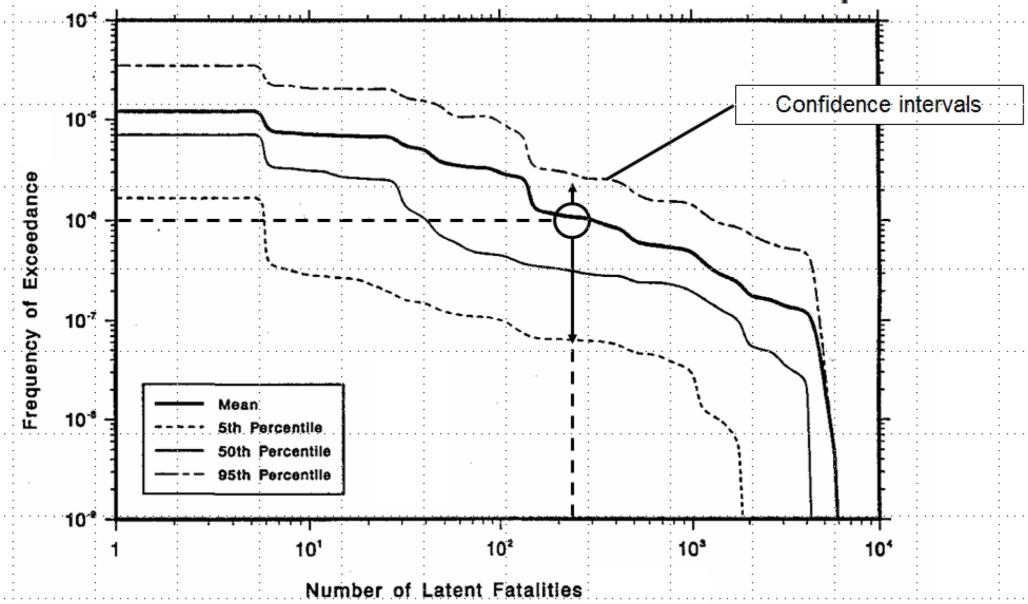
1. Provide information about systems' outcomes (security of service, disruptions/incidents - accidents, safety margins, etc.) and underlying processes over a certain past period ➡ statistical data analysis
2. Demonstrate compliance with static goals/requirements ➡ like (1)
3. Avoid repetition of undesired events (accidents), identify safety-affecting trends ➡ specific (1), root cause and causal chain analysis
4. Identify safety deficits, demonstrate effectiveness and efficiency of risk-reducing measures ➡ (3), logic tree analysis, cost-benefit /ALARP
5. Support active management processes, allow for medium and longer term projection, include dynamic safety goals ➡ (4), advanced modeling techniques

Key Terms | Safety and Risk

Safety in absolute sense means absence of any danger/harm (unattainable); in relative sense (a) an absence of a specific danger, (b) involving a comparatively low and thus acceptable risk or (c) complying with normative requirements.

Risk in general depicts the possibility that damage/harm results from a state or process; it is a function of frequency F of an undesirable event and its consequence C. Expected value:

$$Risk = f(F,C) = F \cdot C \quad \text{respectively} \quad \sum_i F_i \cdot C_i \quad \text{(for more than one event)}$$



F/C diagram often used for results representation

➡ "Measures of safety and safety performance should focus on the aviation system's ability to manage safety risks to acceptable levels." (SMICG, 4/10)

Key Terms | Residual or Remaining Risk (Restrisiko)

Risk which remains after implementation of all planned safety measures, arising from

- consciously accepted risks,
- incorrectly-assessed risks, and
- unrecognized risks.

Basic Methods | Root Cause Analysis (RCA)

RCA is typically used as a reactive method of identifying event causes, revealing problems, and solving them, done after an event has occurred aiming to prevent recurrence. Insights in CA make it useful as a method used to forecast or predict probable events even before they occur. RCA can be applied In a completely separate process to Incident Management.

RCA is not a single, sharply defined methodology; there are many different tools, processes, and philosophies for performing RCA. Several very-broadly defined approaches or “schools” can be identified by their basic approach or field of origin: based on safety, production, process, failures, and systems.

Basic Methods | Failure Mode and Effects Analysis (FMEA)

Goals and purposes

- Qualitative analysis of units in respect to various failure modes and to impacts on adjoined units and the whole system (inductive questioning)
- Meeting of company goals (high quality products, etc.), customers' increasing demands (high quality service, etc.)
- Fulfillment of regulations and standards (e.g. in chemical industry)

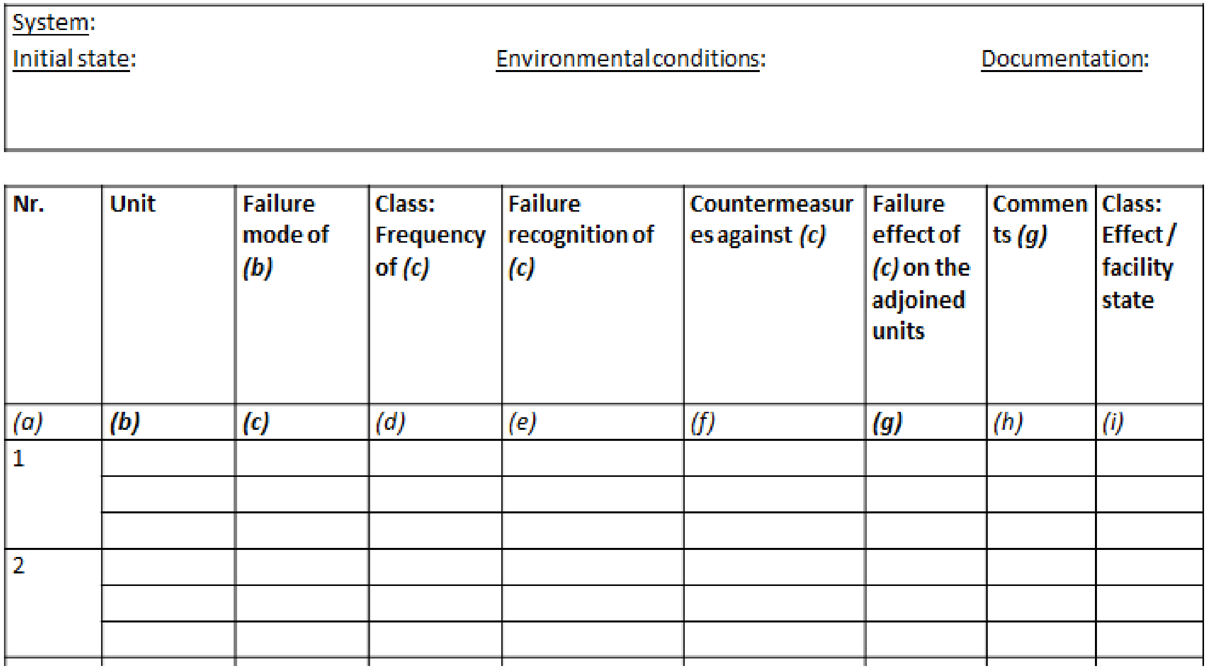
Working steps

1. Listing of failure modes of all units

.

.

5. Completing the FMEA form



System:

Initial state: Environmental conditions: Documentation:

Nr.	Unit	Failure mode of *(b)*	Class: Frequency of *(c)*	Failure recognition of *(c)*	Countermeasures against *(c)*	Failure effect of *(c)* on the adjoined units	Comments *(g)*	Class: Effect / facility state
(a)	*(b)*	*(c)*	*(d)*	*(e)*	*(f)*	*(g)*	*(h)*	*(i)*
1								
2								

Basic Methods | Hazard and Operability Study (HAZOP)

Goals and purposes

- Qualitative analysis of processes based on given guide words, which highlight causes and consequence of deviations from desired physical parameters, i.e.
  - identification of hazards within the system and caused by the system
  - identification of causes of operational disturbances...
- Fulfilment of regulatory requirements and recommendations, e.g., in chemical industry

Working steps

1. Preparation: Definition of the focus of the analysis, guide words, process variables, etc.
2. Selection of the team members
3. Collection of up-to-date plant data and information
4. Completing the HAZOP-form (mass flow as example variable)

Guide word	Deviation	Possible cause	Consequences	Action required
no	mass flow			
less	‘’			
more	‘’			

Methods for Causal Chain Development | Event Tree Analysis

Goals and Purposes

Inductive procedure that begins with an initiating (accidental) event and “propagates” this event through the system under study by considering all possible ways in which it can effect its behavior; the nodes of an event tree represent, e.g., the functioning or malfunctioning of a (sub)system.

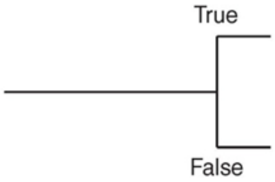
Design and procedural weaknesses can be identified, and probabilities of the various causal chains can be determined.

Working steps

1. Identify (define) relevant initiating event that may give rise to undesired consequences
2. Identify relevant subsequent events such as safety functions, protection layers, human actions, etc.
3. Assign the frequency of the initiating event and the (conditional) branch probabilities in the event tree; calculate the frequency for the identified consequences (outcomes)

Generic Event Tree

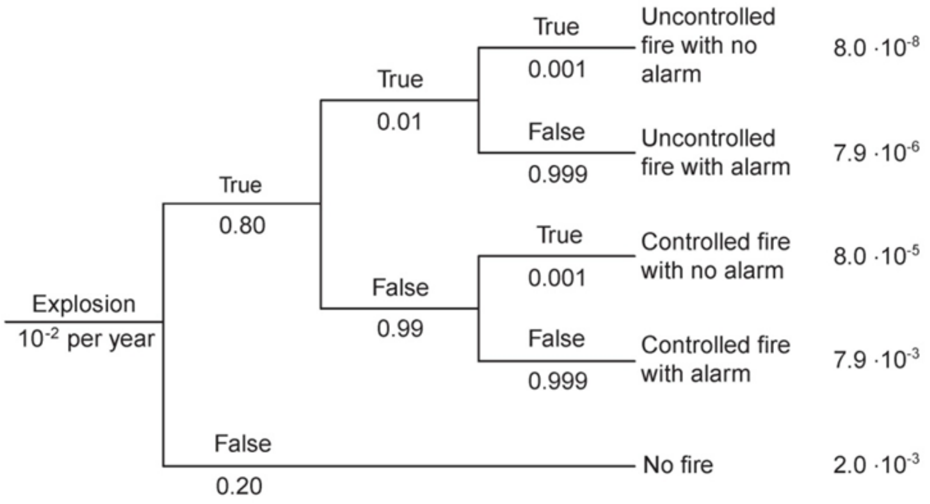
	B_1	B_2	B_3	B_4	B_5	
Accidental event	Additional event I occurs	Event I	Event II	Event III	Additional event II occurs	Outcome / consequence



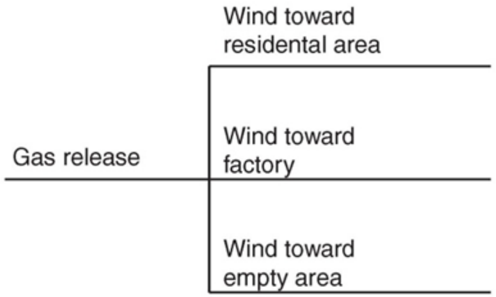
By this way the most severe consequences will come first

Example

Initiating event	Start of fire	Sprinkler system does not function	Fire alarm is not activated	Outcomes	Frequency (per year)

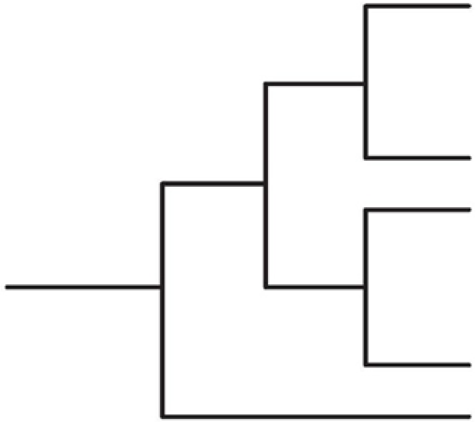


In most applications only two alternatives ("true" and "false") are considered. It is, however, possible to have three or more alternatives:



Present the results

Consequences Analysis

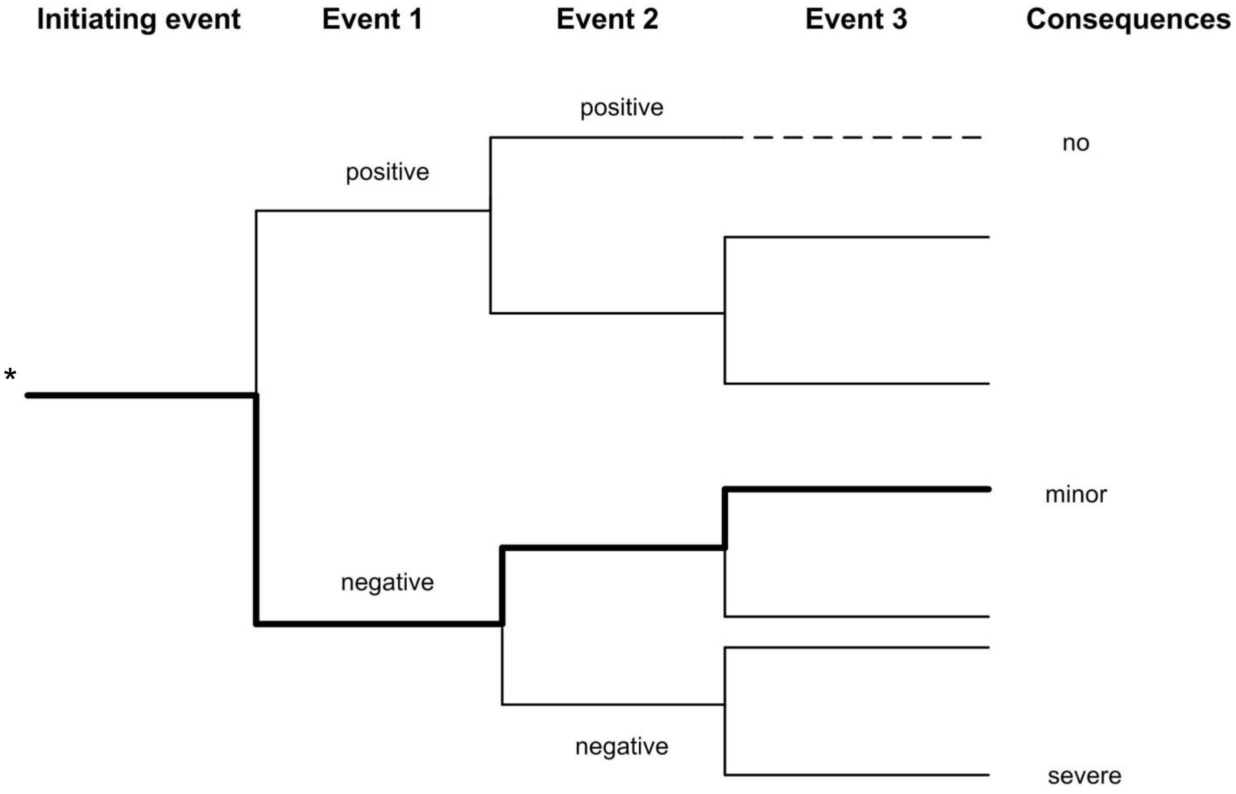


Outcome descr.	Frequency	Loss of lives					Material damage				Environmental damage			
		0	1-2	3-5	6 - 20	> 20	N	L	M	H	N	L	M	H

Methods for Causal Chain Development | Precursor Studies

Approach, Goals and Purposes

Accidental events and incidents, stopped by successful actions, functioning of safety systems, etc. to turn into an accident, are further developed into causal chains, e.g. by use of Event Tree Methodology, to gain insights and/or to check validity of assessments.



*experienced elements: bold

Learning from the Others | Electricity Supply Sector

Performance Measure: Quality/Security of Supply*

- ***SAIDI:*** System Average Interruption Duration Index

$$SAIDI = \frac{\sum_{i\in R} U_i N_i}{\sum_{i\in R} N_i}$$

U_i: Jährliche Unverfügbarkeit am Lastpunkt *i* [h/Jahr]
N_i: Anzahl unterbrochene Lastpunkte
R: Menge der Lastpunkte im betrachteten System

- ***SAIFI:*** System Average Interruption Frequency Index

$$SAIFI = \frac{\sum_{i\in R} \lambda_i N_i}{\sum_{i\in R} N_i}$$

λ_i: Jährliche Fehlerrate am Lastpunkt *i*

- ***CAIDI:*** Customer Average Interruption Duration Index

$$CAIDI = \frac{\sum_{i\in R} U_i N_i}{\sum_{i\in R} \lambda_i N_i} = \frac{SAIDI}{SAIFI}$$

- Reporting system: Longer-term development plans, grid loadings, unusual events, etc.

➡Quantitative measures without target values, based on statistical data; vague qualitative requirements

*Swiss Electricity Administrative Ordinance (Strom VV)

Learning from the Others | Electricity Supply Sector (cont.)

Performance Measure: Security of Supply Focused on Transmission Grid

In addition to regulatory requirements ‘Key Performance Indicators’ have been established by the Swiss transmission grid operator based on **monthly evaluation of actual data** including grid internal factors (grid stability, approaching/exceedance of safety margins, availability of grid capacity, quality of infrastructure incl. IT, etc.) and external factors (production, trading, political/regulatory framework, etc.).

➡ Performance-based management but Swissgrid strives for risk- based management approach and probabilistic-predictive tool.

Learning from the Others | Use of Nuclear Energy

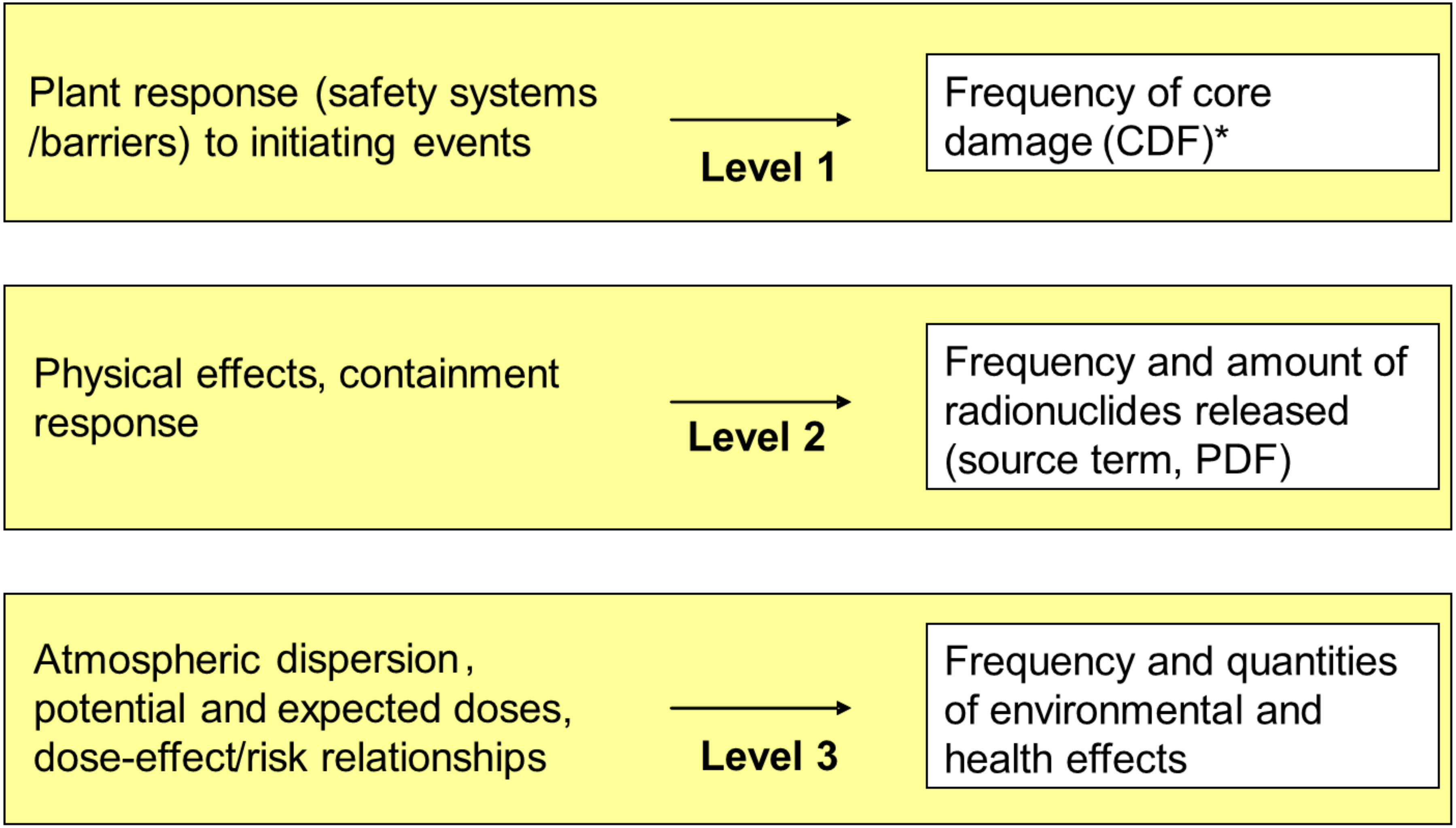
National legal requirements (e.g. Swiss nuclear law (KEG, 2003/07), nuclear ordinance (KEV, 2004/07)) aiming to protect man and environment against hazards; international framework (IAEA conventions) and cooperations (regulators, operators)

- Reporting of abnormal events of risk safety relevance (mandatory) and data collection (evaluation including number of unplanned (spurious) reactor shut downs per year; international Incident Reporting System (IAEA/OECD-NEA)

- Predicted core damage frequency (CDF) is of central importance for licensing and oversight. Art. 24 of KEV claims that the applicant (licensee) has to demonstrate a CDF of less than 10^{-5} per reactor-year (internal and external events, all plant conditions, plant specific data, periodical updates), etc.

Operators check performance against „electricity produced per year“ with/without consideration of planned shutdowns, development of CDF while taking plant modifications into account („living PSA“ or „Risk Monitor“), etc.

Structure of Probabilistic Safety Analysis (PSA) for Nuclear Power Plants



Plant response (safety systems /barriers) to initiating events

Level 1

Frequency of core damage (CDF)*

Physical effects, containment response

Level 2

Frequency and amount of radionuclides released (source term, PDF)

Atmospheric dispersion, potential and expected doses, dose-effect/risk relationships

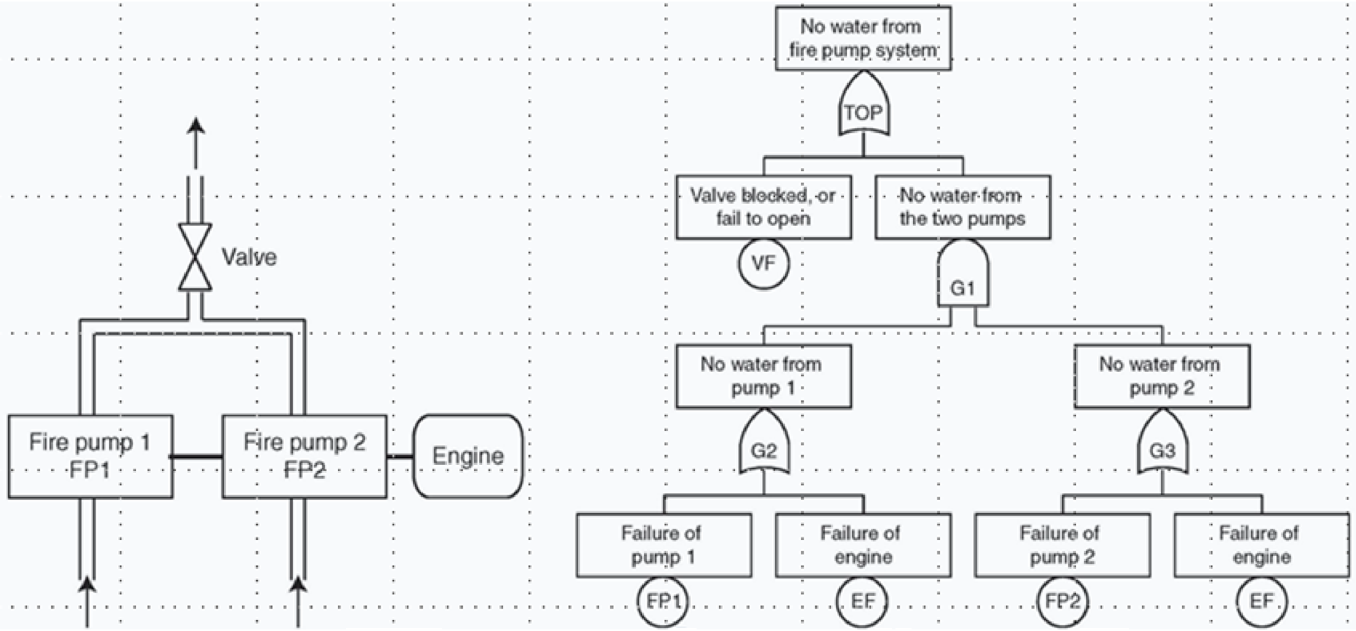
Level 3

Frequency and quantities of environmental and health effects

Backbone PSA-Method | Fault Tree Analysis

Starting point is a predefined failed system state („top event“). The subsequent task is to find event combinations leading to the „top event“. The branches are tracked top-down (> intermediate events -> basic events connected through logic gates), the reasoning is deductive.

Example: Redundant Fire Pump System



Development of PSA Methodology | A Long Way

- US Reactor Safety Study, 1968-75 as pioneering step, followed by German Risk Study A, -1979, and others.
- Significant improvements (human reliability, dependant failures, uncertainties, database, etc.) – revised studies (e.g. NUREG-1150, German Risk Study B, both 1990).
- Development of first set of guidelines in the 80's, e.g. IAEA, US NRC, GER BMI; revision of guidelines in the late 90's, and recent updates, e.g. CH ENSI, 2009.
- Nowadays, PSA is a well established method to assess safety and demonstrate compliance with target values in most countries – tendency „to make them living".

- Breakthrough caused by severe accidents (TMI, 1975; Chernobyl, 1986) and „fear" of operator of high investment risks and inefficient safety measures/backfits claimed by the authority.

Safety Performance Indicators | Take Home Messages

- Well designed SPIs are suitable to check both the quality of outcomes (services) and processes (incl. safety culture); they must be jointly developed and agreed upon by key actors.
- The data base must be appropriate and sound; information is highly valuable, even if qualitative.
- Techniques for data evaluation and investigation on accidents/incidents are mostly available, need to be harmonized and applied carefully.
- A total system approach to take all components into account and to provide a „full picture" is recommended.
- Development of SPIs needs finally to be accompanied by established acceptable levels of safety and by enforced safety culture.
- The whole process calls for a stepwise approach (with feedback loops) and cautousness.