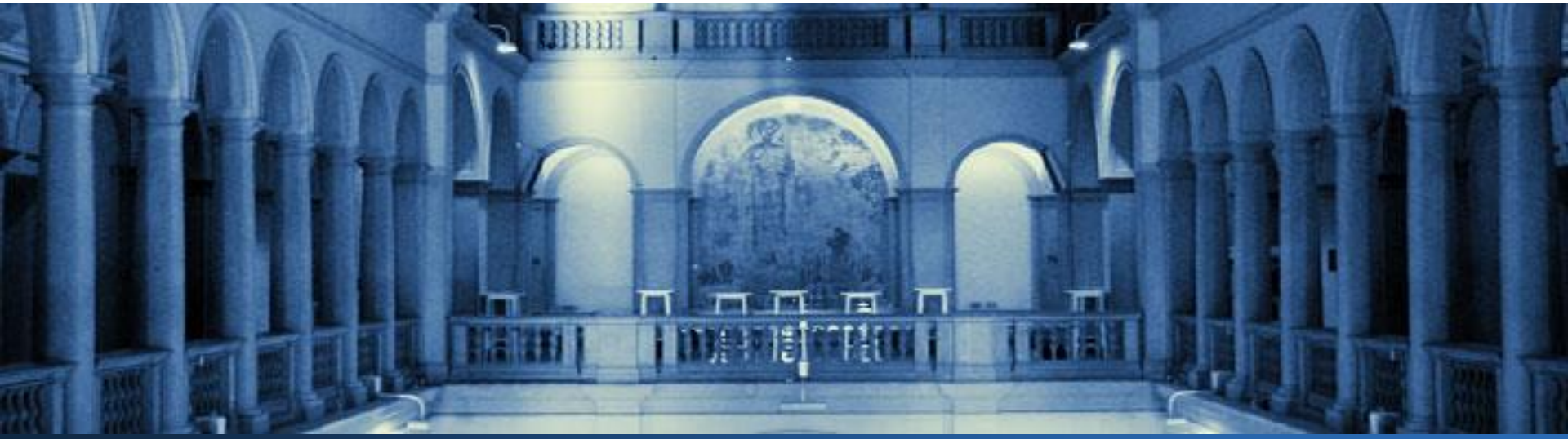
ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Laboratory for Safety Analysis
INSTITUTE FOR ENERGY TECHNOLOGY

LHC Operation and Safety

CERN, 23. März 2006

Prof. Dr. W. Kröger, ETH Zürich



Scope of the Presentation

- Basic safety goals in the nuclear field (safe shutdown and cooling of the core need to be assured)
- Concept of defence-in-depth
- Design basis accidents / beyond design basis accidents
- Reliability and availability
- Redundancy, diversity, maintenance, human factors
- PSA framework
- Targets, health and safety and investment related
- Safety Culture

Concept of Defence-in-Depth (1/3)

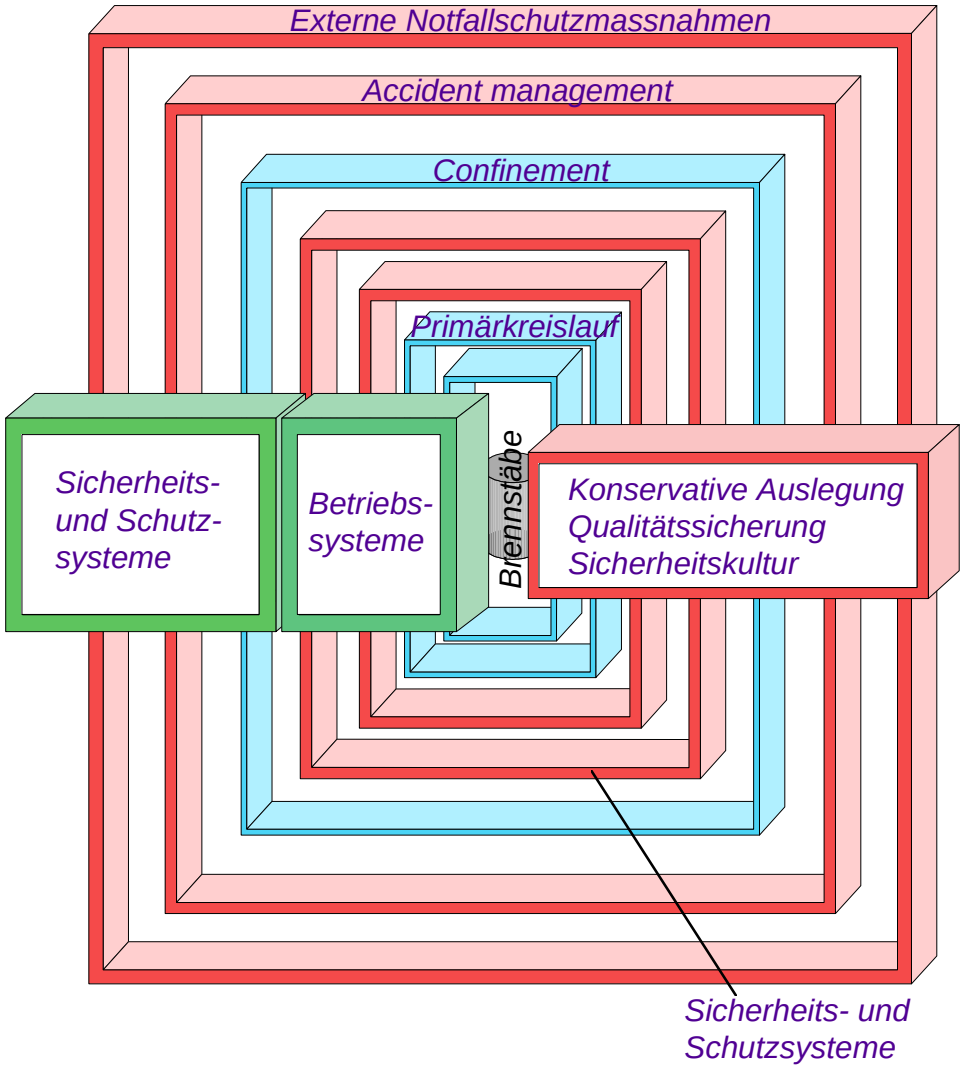
General strategy

- First to prevent accidents (RIAS, LOCA) and second, if prevention fails, limit the potential consequences of accidents (mitigation)

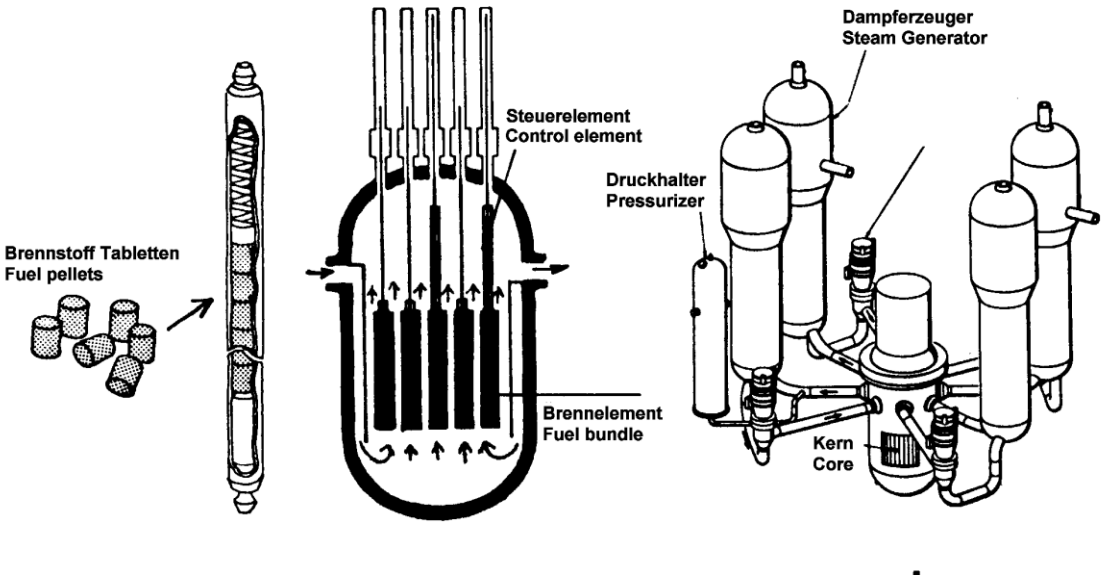
Structure

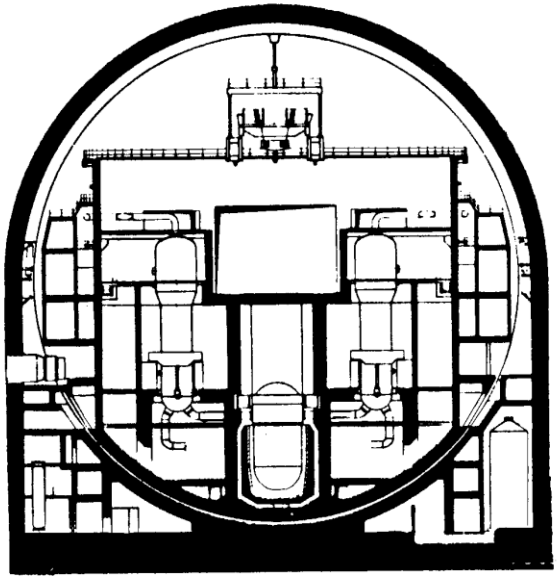
- Five levels of protection; of one level should fail, the subsequent levels come into play, and so on. Special attention is paid to hazards that could potentially impair several levels of defence coincidentally, e.g. earthquakes.

Concept of Defence-in-Depth (2/3)

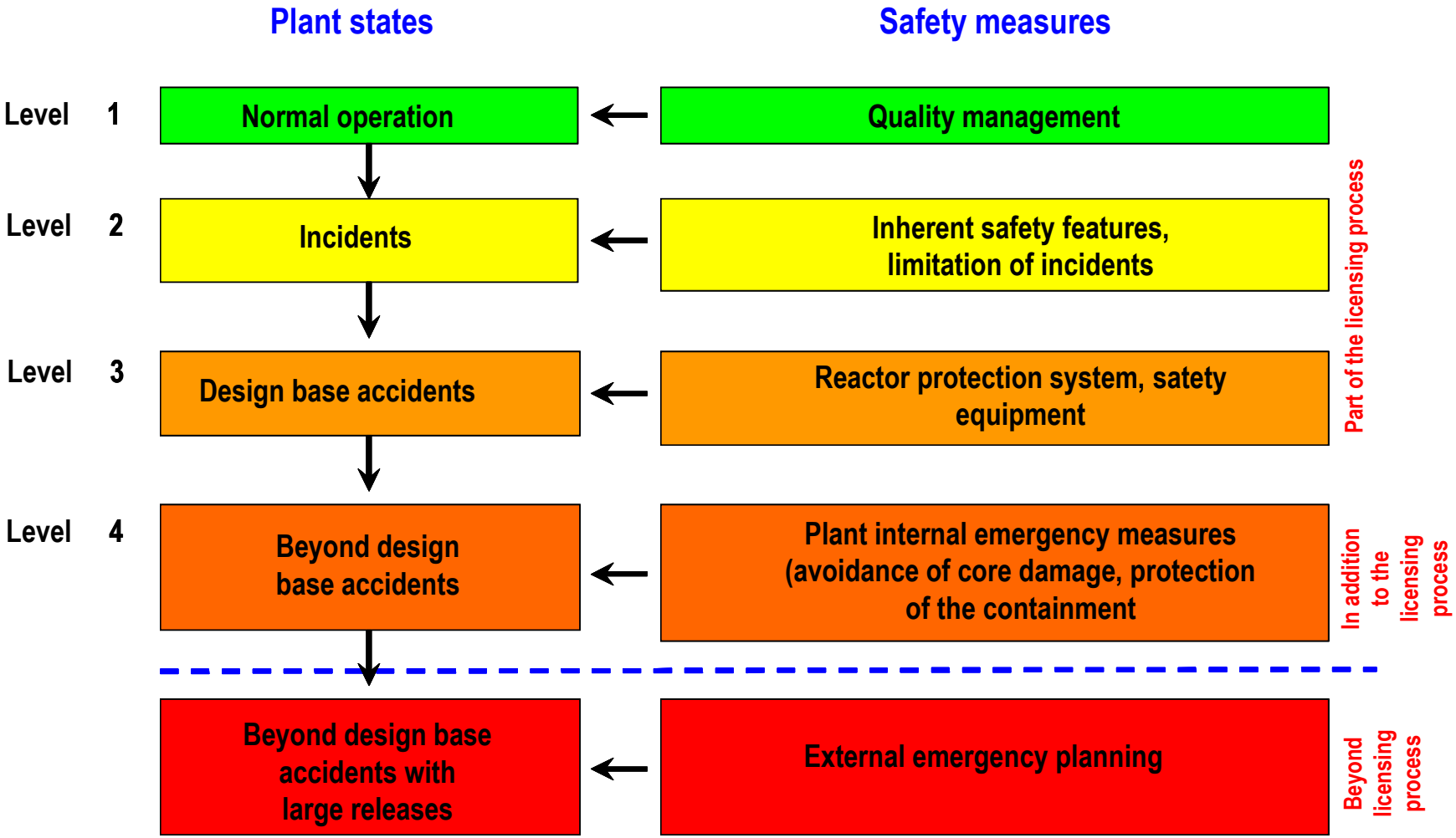


Concept of Defence-in-Depth (3/3): Physical Barriers





Overall Safety Concept Approach



Design Basis Accidents (1/2): Approach, Design Objective

- Selection of (representative, covering) accidents, which are expected during the lifetime of a nuclear power plant, or which can not be exclude following human discretion (i.e. accident frequency > 10^{-6} per year).
- Design of the plant in such a manner, that the occurrence of such an accident does not lead to unacceptable consequences in the environment.

Design Basis Accidents (2/2): Approach, Design Objective

- For the verification, both an accident initiating event and the unavailability of an independent safety system needed to handle accidents are assumed (redundancy criterion, there is no need to assume additional system failures).

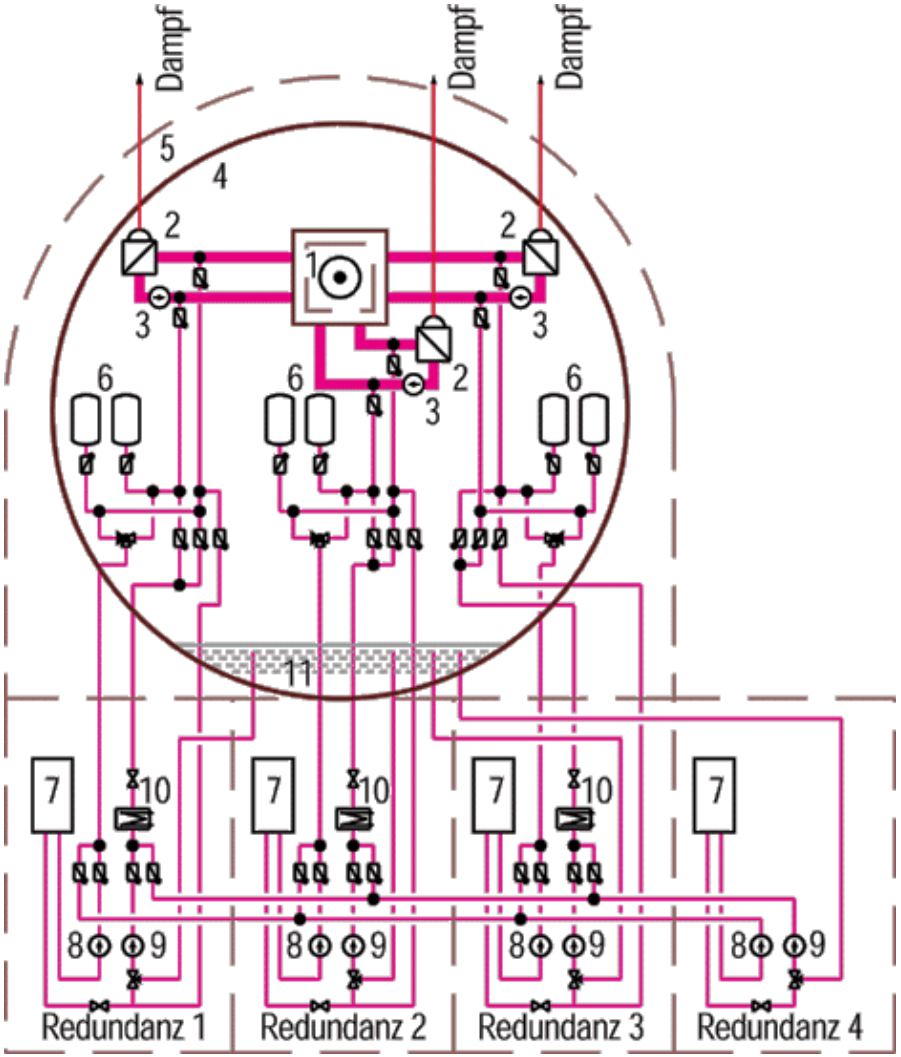
Beyond Design Basis Accidents

- Accidents are beyond design accidents, if they can be characterised by multiple failures of systems, which are needed for handling accidents, or if they are instantiated by very rare events. The occurrence of such accidents is understood based on the experience as very unlikely (frequency < 10^{-6} per year)
- In comparison to design base accidents, it can not be excluded the radioactive substances in a harmful amount are released to the environment; no dose limits for persons around the site are defined.

Safety Concept Based on Swiss HSK-R-100

Safety level	Category	Frequency H per year	Verification	Goal	Dose limit environment	Dose limit workers
Normal operation				Prevention of incidents and accidents, minimisation of radiation to workers	Q-DRW	20 mSv/year
Incidents		$H>10^{-1}$	Covered by deterministic accident analysis			
Design base accidents	1	$10^{-2}<H<10^{-1}$	Deterministic accident analysis, safety systems are available as required	Prevention of damage to: - safety relevant components - fuel clading	Q-DRW	50 mSv 250 mSv
	2	$10^{-4}<H<10^{-2}$		Limitation of damage to: - safety relevant components - fuel clading	1 mSv	50 mSv 250 mSv
	3	$10^{-6}<H<10^{-4}$		Assuring the - coolability of the reactor core - integrity of the containment	100 mSv	50 mSv 250 mSv
Beyond design base accidents		$H<10^{-6}$	PSA	Limitation of the consequences by including the radioactivity or the controlled release of radioactivity into the environment (internal accident management)	-	50 mSv 250 mSv
			Emergency preparedness	Mitigation of radiological consequences in the environment (external accident management)	-	50 mSv 250 mSv

Safety Systems (e.g. Cooling Systems of Gösgen NPP)



1. Reaktor
2. Dampferzeuger
3. Hauptkühlmittelpumpen
4. Sicherheitsbehälter
5. Reaktorgebäude
6. Druckspeicher
7. Flutbehälter
8. Sicherheitseinspeisepumpen (Hochdruck)
9. Nachkühlpumpen (Niederdruck)
10. Nachwärmekühler
11. Containmentsumpf

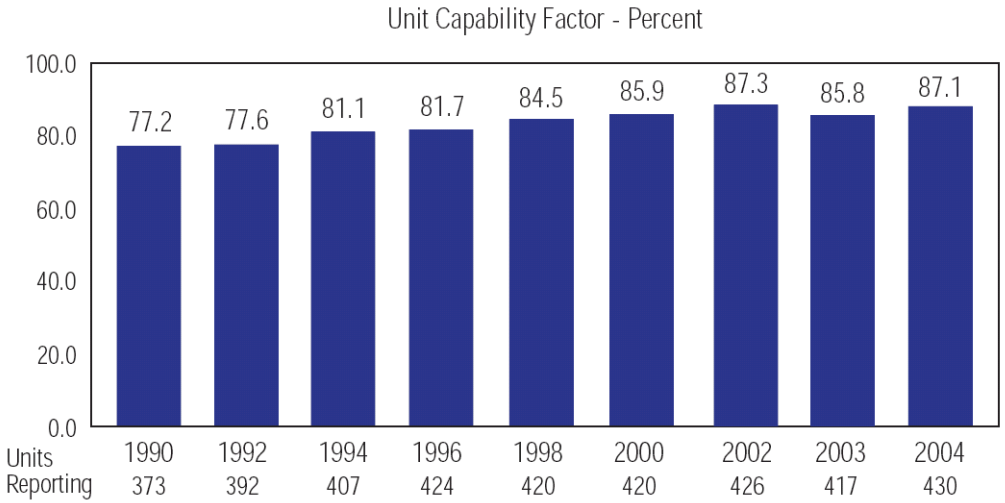
Reliability and Availability

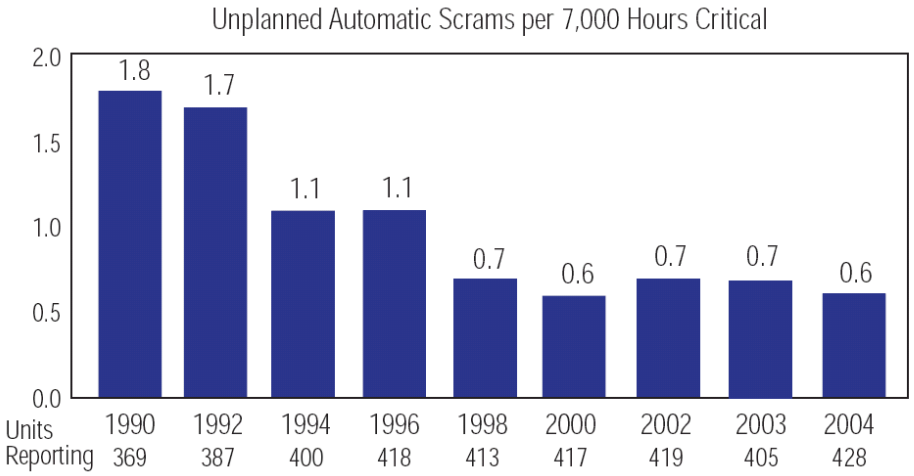
- Reliability → to keep the plant operating (for economic and safety reasons) → redundancy and diversity as key words → limitations of redundancy → common cause failures
- Availability → working on demand → maintenance as key word
- There is a conflict of interest between reliability and availability

Dependent Failures

- DF (dependent failure)
- MRF (multiple related failures)
  - CCF (common cause failure)
  - CMF (common mode failure)
  - CF (causal or cascade failures)
  - Common cause initiating events

KKW, Unit Capability / Scrams Worldwide





Human Reliability Analysis

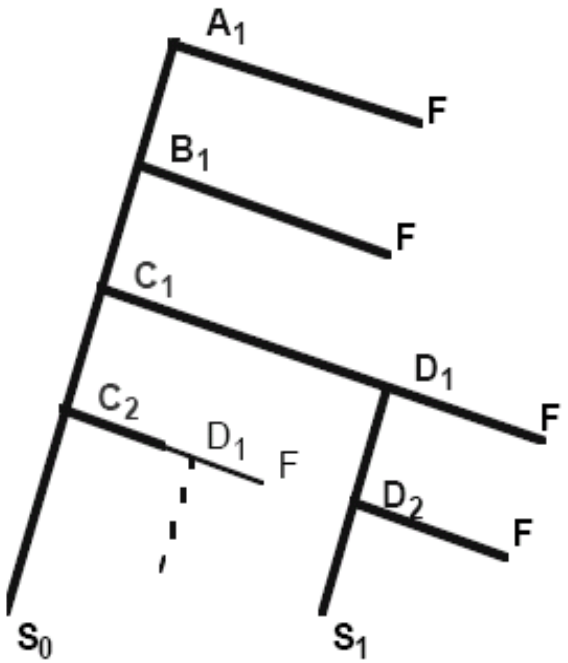
- AIPA (Accident Initiation and Progression Analysis)
- SLIM (Success Likelihood Index Methodology)
- THERP (Technique for Human Error Prediction)

PAUL SCHERRER INSTITUT
Nuclear Energy and Safety Research Department

THERP

- **Task Analysis**
- **Decomposition**

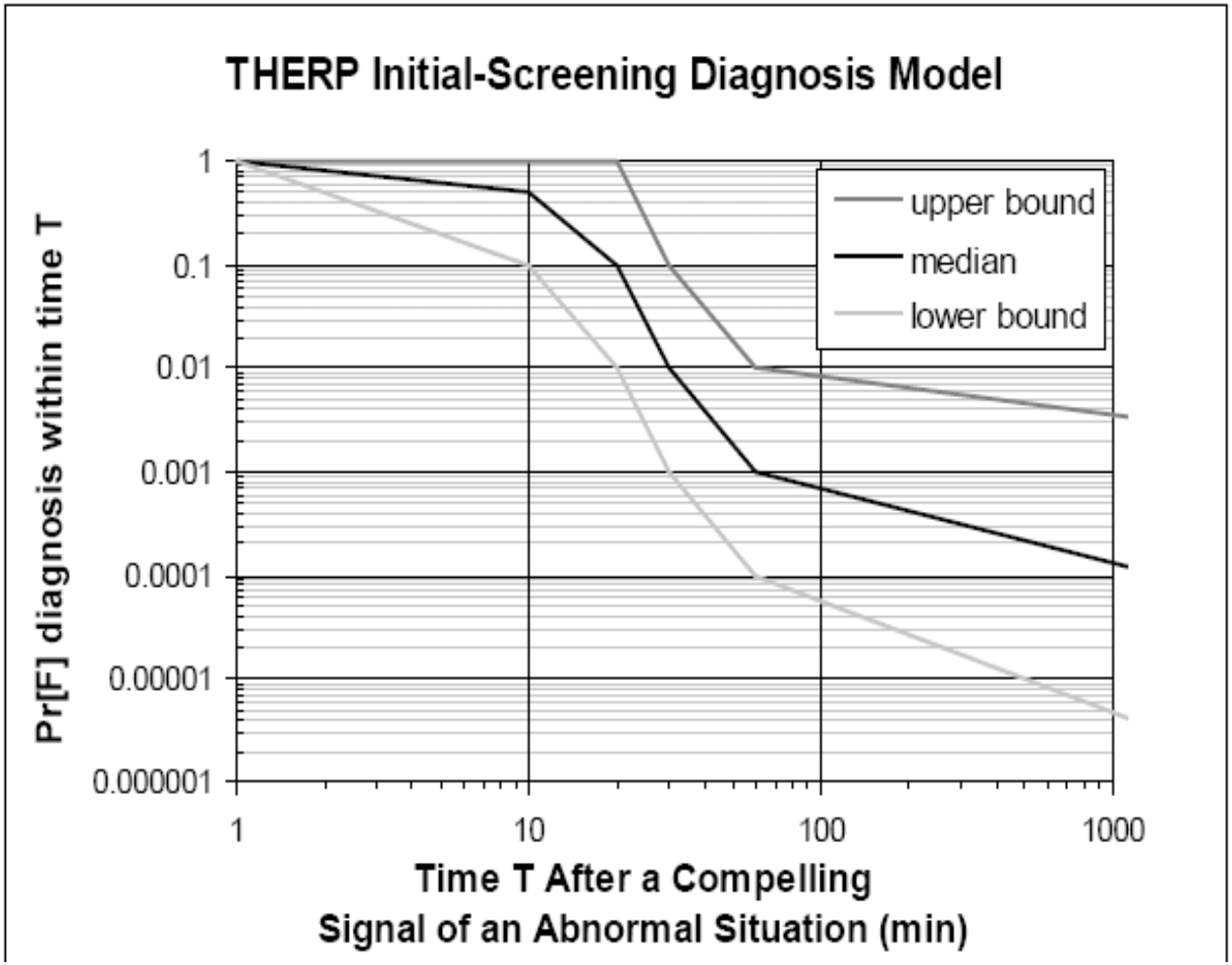
HRA Event Tree



Task ID	Description	Error ID	Human Error
A	Detect/identify Loss of Flow	A_1	Fail to detect/identify
B	Start correct procedure	B_1	Fail to start procedure
C	Start pump	**C_1**	**Omission (of procedure step)**
		C_2	**Select incorrect control**
D	Supervisor check	D_1	Error or omission
		D_2	Select incorrect control

PAUL SCHERRER INSTITUT
Nuclear Energy and Safety Research Department

Diagnosis Model THERP (2)



Probabilistic Safety Assessment Framework (PSA) (1/2)

- Deterministic design principles (“defence-in-depth”) have proven to be of value, PSA as a complementary tool.
- PSA is achieving realistic description of risk and safety, it is assessing safety margins.
- PSA models identify expected performance of various safety measures, they disclose weak points.
- PSA is reflecting the consequences of dependencies and of men-machine-interdependencies, **uncertainties become visible, they are not generated.**
- PSA identifies the relative importance (dominance) of specific accident sequences, it allows the optimal use of available resources.

Probabilistic Safety Assessment Framework (PSA) (2/2)

- PSA allows the assessment of operational / maintenance related aspects and considers operational experience.
- 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 frequency of occurrence and resulting plant states are modelled.
- Physical phenomena of the postulated scenarios are modelled, and respective consequences are assessed – inside and outside the plant.

Targets

Health and safety related

- IAEA targets
  - 10^{-4} / 10^{-5}/a CDF (core damage frequency) old / new installations
  - 10^{-5} / 10^{-6}/a LERF (large early release frequency) old / new installations

Investment related

- 10^{-4}/a: commonly used loss-of-investment goal (sum of frequencies of all events leading to damage states which might cause loss of investment; core damage not inevitable).

Safety Culture

- In INSAG-4, safety culture is defined as: “that assembly of characteristics and attitudes in organisations and individuals which establishes that, as an overriding priority, nuclear plant safety issues receive the attention warranted by their significance.”

Safety Culture ILK-19 (1/3)

- German utilities are in the process of implementing safety culture self-assessment systems taking into account organisational and personnel aspects
- Safety culture is part of an organizational culture, which may be understood as patterns of shared values and beliefs that in time produce behavioural norms adopted in preventing or solving problems.

Safety Culture ILK-19 (2/3)

- According to INSAG- 4, the two components of safety culture are as follows
  - The necessary framework within an organization. Establishing this framework is management's responsibility.
  - The attitude of staff at all levels in responding to and benefiting from the framework.
- Three categories of safety culture:
  - compliance-oriented
  - performance-oriented
  - process-oriented

Safety Culture ILK-19 (3/3)

- A direct quantitative assessment of safety culture is not feasible; therefore a combination of suitable safety culture indicators is used. These indicators should be periodically monitored, e.g. within the framework of a safety management system. Weakening of safety culture is indicated by
  - failure of corporate memory
  - Low status of quality assurance
  - Lack of corporate oversight
  - Isolationism
  - Lack of organizational learning
  - Lack of interdepartmental communication and cooperation

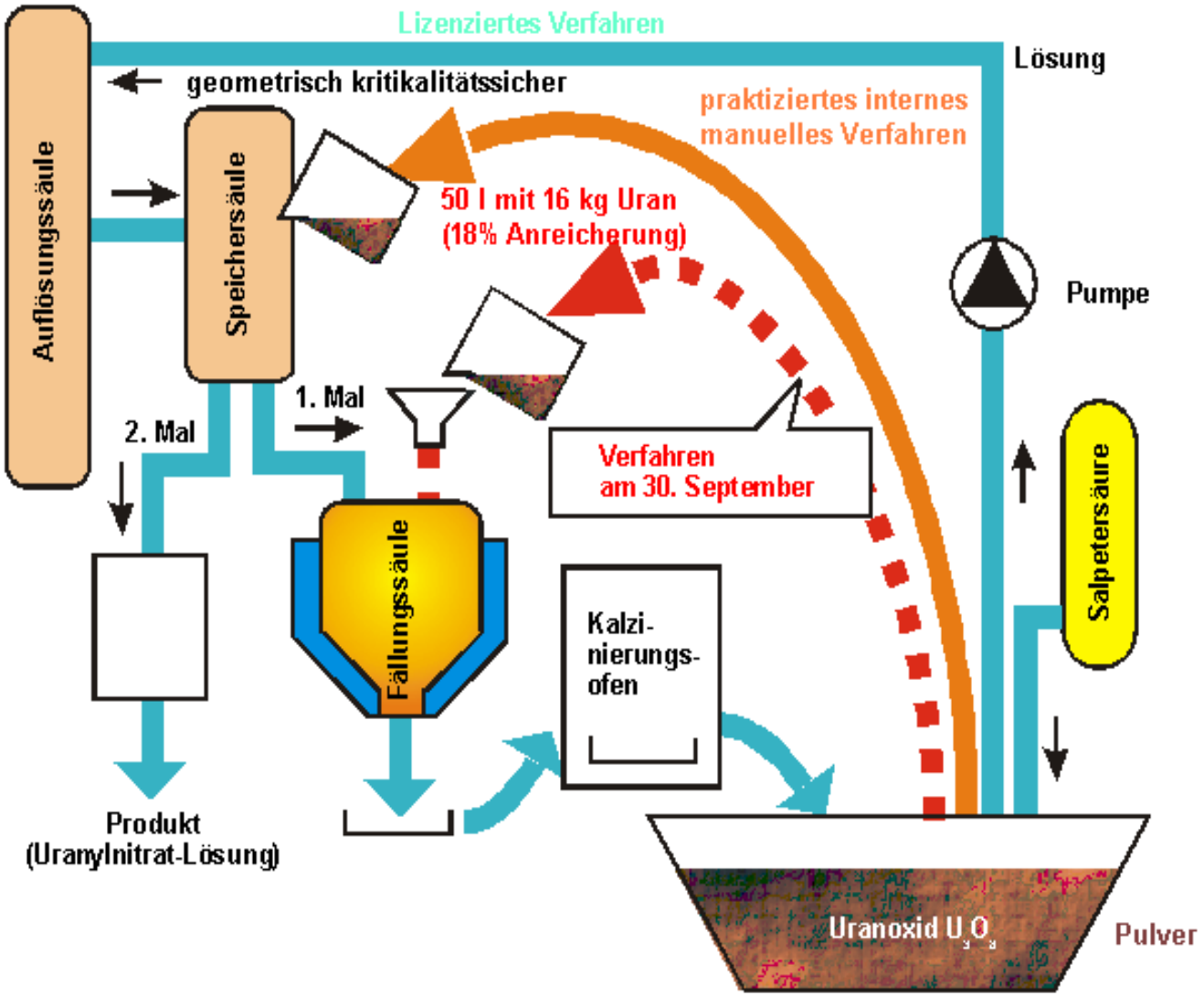
Tokaimura Criticality Accident, 30 September 1999 (1/2)

- On 30 September 1999 three workers received high doses of radiation in a Japanese plant preparing fuel for an experimental reactor. Two of the doses proved fatal.
- The accident was caused by bringing together too much uranium enriched to a relatively high level, causing a "criticality" (a limited uncontrolled nuclear chain reaction), which continued intermittently for 20 hours.

Tokaimura Criticality Accident, 30 September 1999 (2/2)

- A total of 119 people received a radiation dose over 1 mSv from the accident, but only the three operators' doses were above permissible limits, and two of these have since died.
- The cause of the accident appears to be "human error and serious breaches of safety principles", according to IAEA.

Source: Uranium Information Centre Ltd, Melbourne, Australia


Lizenziertes Verfahren
Lösung
geometrisch kritikalitätssicher
praktiziertes internes manuelles Verfahren
Auflösungssäule
Speichersäule
50 l mit 16 kg Uran (18% Anreicherung)
Pumpe
1. Mal
2. Mal
Verfahren am 30. September
Salpetersäure
Fällungssäule
Kalzi-nierungs-ofen
Produkt (Uranylnitrat-Lösung)
Uranoxid U_3O_8
Pulver

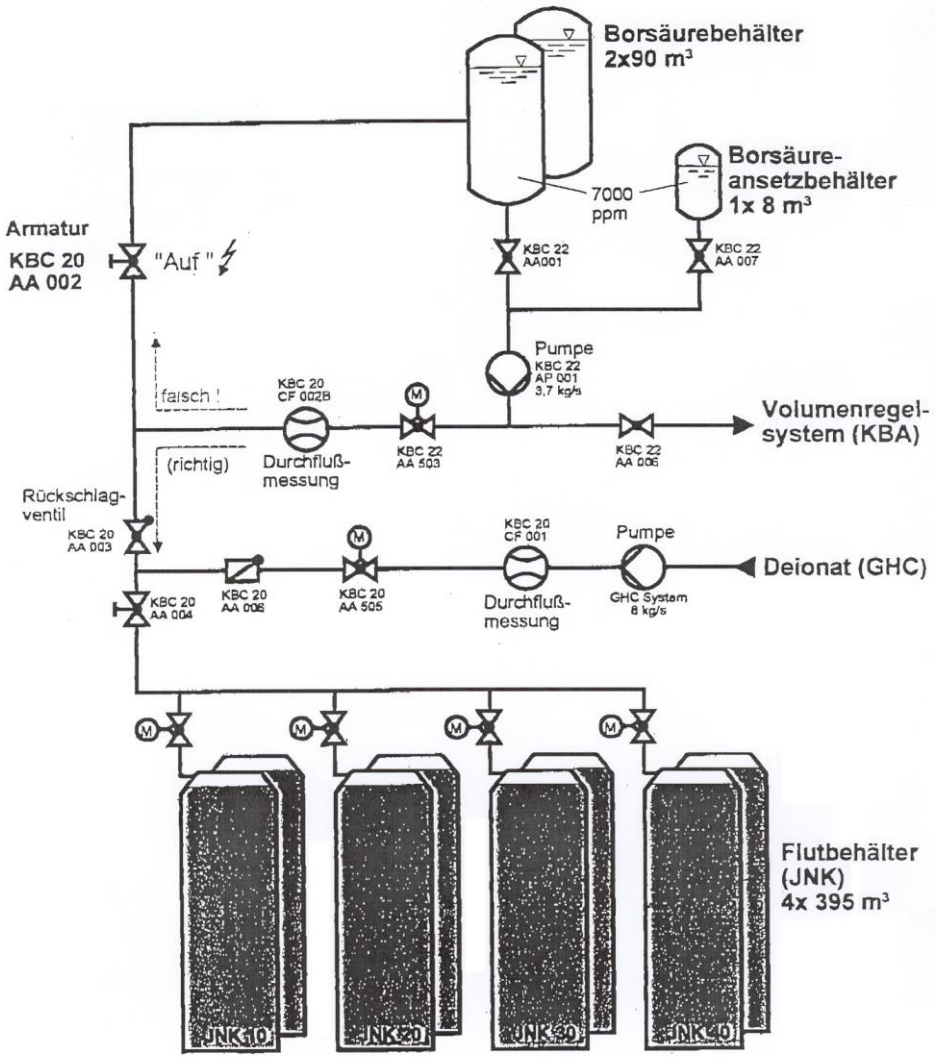
NPP Philippsburg Boron Dillution Incident (1/2)

- Errors made in the filling of the water storage tanks led to the restart of the plant while three of four storage tank pairs had lower concentration levels of boron than the 2200 ppm prescribed by the operating manual
- The concentration levels went unnoticed until about two weeks after the restart. A further one-and-a-half weeks passed while the situation was remedied during commercial operation.
- About seven weeks after restart, the licensee shut down the plant in order to investigate the events in more detail and to undertake safety-related improvements.

NPP Philippsburg Boron Dillution Incident (2/2)

- no lessons were derived from the precursor event in 2000,
- no feedback was given on valves that were in an unexpected position,
- non-observance of the fill-level in the boric acid container,
- tardy filling of the storage tanks,
- tardy measurement of the boric acid concentration,
- delayed start of investigations into the causes of boron dilution and thus delayed recognition of the common-mode potential.

Source: ILK Statement ILK-09 E



FALSCH: KBC - Valve "AUF" :
Borsäure wird im Kreislauf gefahren
⇨ keine Zumischung von Borsäure zum Deionat

RICHTIG: KBC - Armatur "ZU"