ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

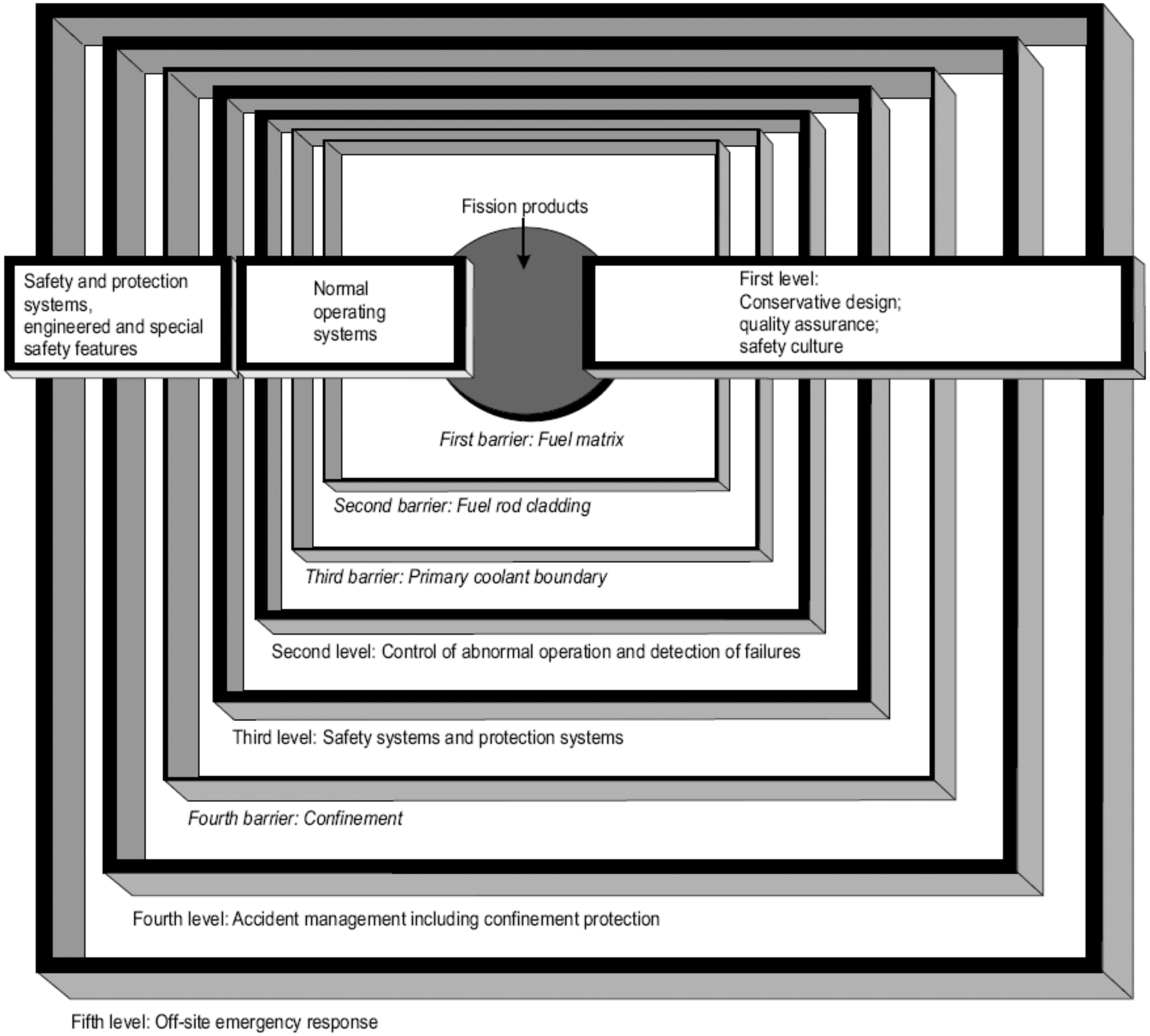
Laboratory for Safety Analysis
INSTITUTE FOR ENERGY TECHNOLOGY

# Handling risk in the electric power sector

Wolfgang Kröger, ETH Zürich, Switzerland

PSAM9, Hong Kong, 21 May 2008

# Strategy of defence-in-depth



# Supplementing probabilistic approaches

Although these concepts have been applied successfully, probabilistic methods (PRA) have been applied to provide an additional view, additional insights. In particular, PRA

- achieves a realistic description of risk and safety and proves safety margins;
- models performance of various safety measures and discloses weak points;
- reflects the consequences of dependencies and of men-machine-interdependencies;
- uncertainties become visible (they are not generated);
- identifies the relative importance (dominance) of specific accident sequences and allows the optimal use of available resources;
- allows the assessment of operational / maintenance related aspects and considers operational experience.

Quantitative attributes characterizing the risk are defined and calculated, the most commonly used are the core damage frequency (CDF) and the large early release frequency (LERF).

# Safety concept according to Swiss HSK-R-100

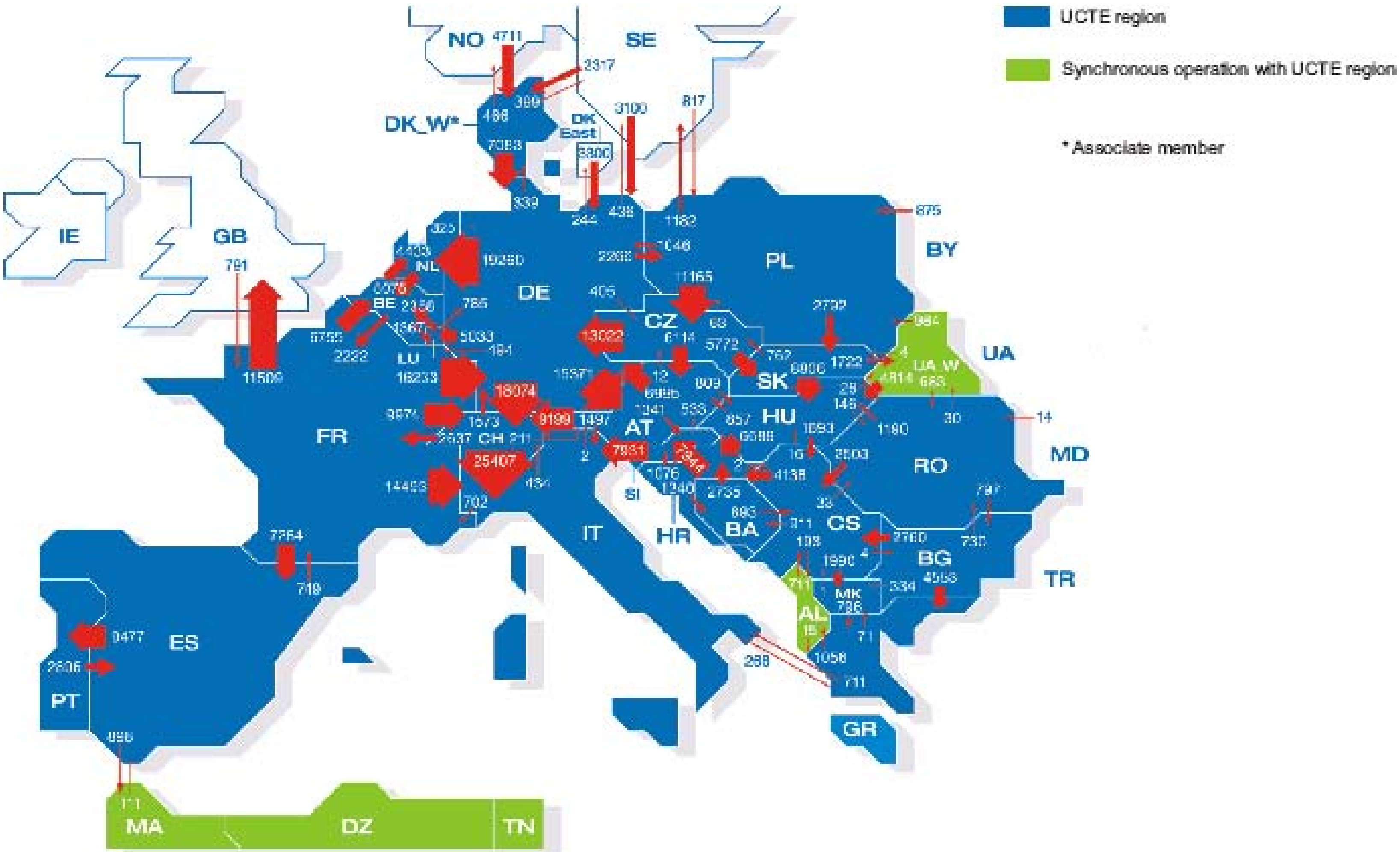
| Safety level | Cate-gory | Frequency H per year | Verification | Goal | Dose limit environment |
|---|---|---|---|---|---|
| Normal operation | | | | Prevention of incidents and accidents, minimisation of radiation to workers | |
| Incidents | | H>10E-01 | Covered by deterministic accident analysis | | Q-DRW [1)] |
| Design base accidents | 1 | 10E-02< H<10E-01 | Deterministic accident analysis, safety systems are available as required | Prevention of damage to:<br>- safety relevant components<br>- fuel clading | Q-DRW |
| | 2 | 10E-04< H<10E-02 | | Limitation of damage to:<br>- safety relevant components<br>- fuel clading | 1 mSv |
| | 3 | 10E-02< H<10E-04 | | Assuring the<br>- coolability of the reactor core<br>- integrity of the containment | 100 mSv |
| Beyond design base accidents | | H<10E-06 | PRA | Limitation of the consequences by including the radioactivity or the controlled release of radioactivity into the environment (internal accident management) | - |
| | | | Emergency preparedness | Mitigation of radiological consequences in the environment (external accident management | - |

[1)] specified guiding figures

# Operational record of NPPs

- About 13‘000 reactor-years accumulated
- Two severe accidents (TMI PWR 79, INES 5; Chernobyl RBMK, INES 7)
- Number of unplanned scrams narrowed down to one every two years (Western reactors)

# Trans-boundary physical energy flows (GWh) in Europe




Source: UCTE 2006

# The N-1 security criterion specifies that…

"….any probable single event leading to a loss of power system elements should not endanger the security of the interconnected operation, that is, trigger a cascade of trippings or the loss of a significant amount of consumption".

Source: UCTE Handbook

# Electric power supply systems: recent major blackouts

| Blackout | | Load loss [GW] | Duration [h] | People affected | Main causes |
|---|---|---|---|---|---|
| Aug. 14, 2003 | Great Lakes, NYC | ~ 60 | ~ 16 | 50 Mio | Inadequate right-of-way maintenance, EMS failure, poor coordination among neighbouring TSOs |
| Aug. 28, 2003 | London | 0,72 | 1 | 500´000 | Incorrect line protection device setting |
| Sept. 23, 2003 | Denmark / Sweden | 6,4 | ~ 7 | 4,2 Mio. | Two independent component failures (not covered by N-1 rule) |
| Sept. 28, 2003 | Italy | ~ 30 | up to 18 | 56 Mio. | High load flow CH-I, line flashovers, poor coordination among neighbouring TSOs |
| July 12, 2004 | Athens | ~ 9 | ~ 3 | 5 Mio. | Voltage collapse |
| May 25, 2005 | Moscow | 2,5 | ~ 4 | 4 Mio | Transformer fire, high demand leading to overload conditions |
| June 22, 2005 | Switzerland (railway supply) | 0.2 | ~ 3 | 200´000 passengers | Non-fulfilment of the N-1 rule, wrong documentation of line protection settings, inadequate alarm processing |
| Aug. 14, 2006 | Tokyo | ? | ~ 5 | 0.8 Mio households | Damage of a main line due to construction work |
| Nov. 4, 2006 | Western Europe (“controlled” line cut off) | ~ 14 | ~ 2 | 15 Mio. households | High load flow D-NL, violation of the N-1 rule, poor inter TSO- coordination |

# Conclusions

- The electric power supply system is a complex critical infrastructure comprising various interacting elements and multifaceted risk, operating in a fragmented environment.
- Historically deterministic demonstration of NPP safety and grid stability; transition to more comprehensive – probabilistic concepts as supplement.
- Call for numerical targets and risk-informed decision making as well as necessity of significant improvements.