RELCON SCANDPOWER

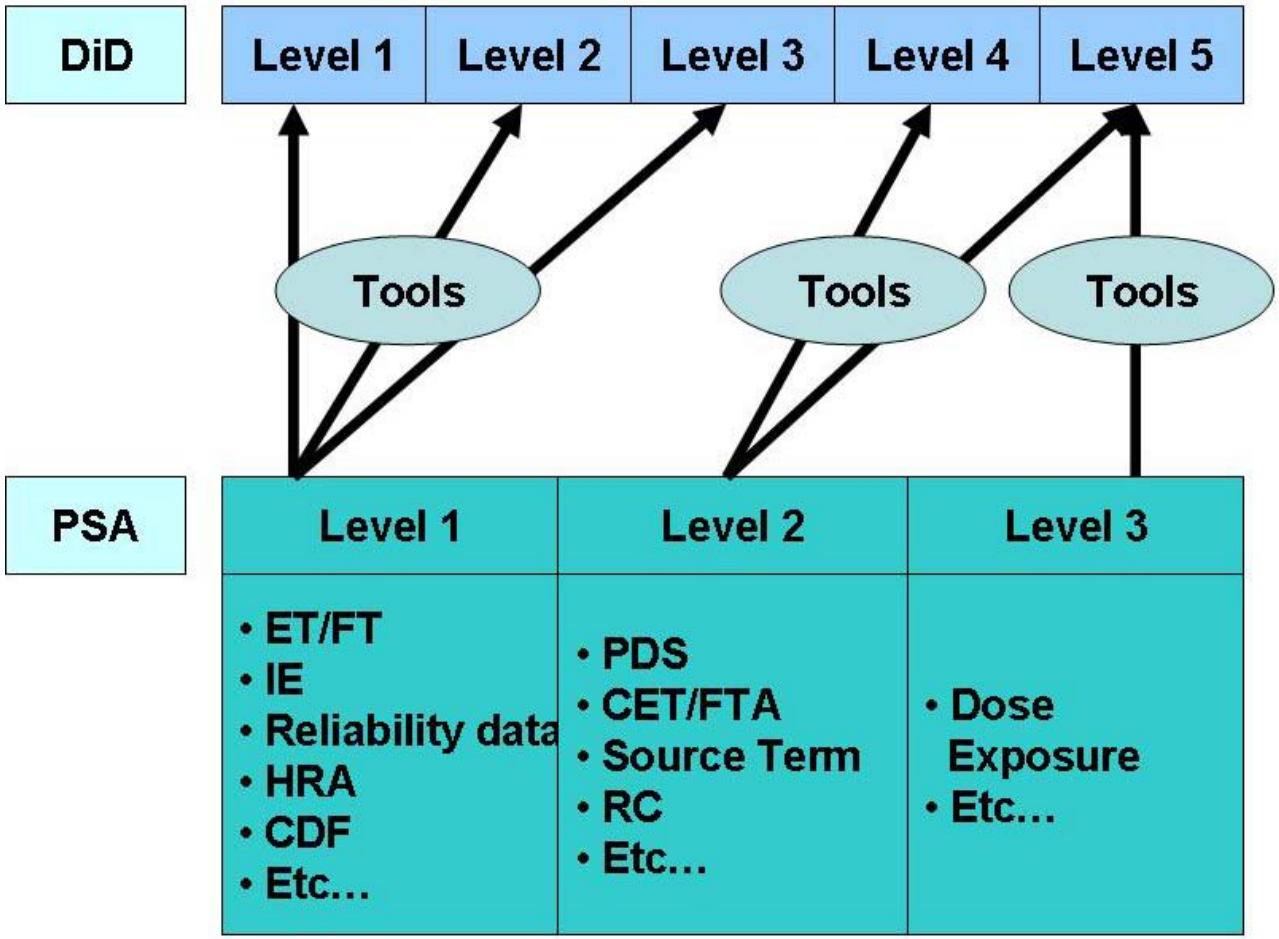
Risk Management

SKI research project on Defence in Depth PSA – Assessing Defence in Depth Levels with PSA Methods

Presented at PSAM-9,
Hongkong 19-23 May 2008
By Per Hellström, Relcon Scandpower AB

Co-authors:
Ralph Nyman – Swedish Radiation Safety Authority, Stockholm, Sweden
Tomas Öhlin, Staffan Björe - Westinghouse Electric, Västerås, Sweden
Michael Knochenhauer, - RelconScandpower AB, Stockholm, Sweden

Assessing DiD levels with PSA?



Project general purpose and scope

- **To find ways of evaluating (to the extent feasible) each of the five DID levels with PSA.**
  - Evaluation of existing DiD levels - structures, systems, components, manual actions and routines regarding risk importance for each of the five DiD levels
  - Evaluation of impact on DiD due to plant changes
  - Evaluation of events with regard to the DiD levels
- **First work in the project studied qualitative parameters of each level of defence in depth that should be considered in the method (s).**
- **Further phases will define quantitaitive parameters and develop methods and models and identify need for adjustment of current PSA models to evaluate each of the quantitative parameters defined.**

DEFENCE IN DEPTH AND PSA - DISCUSSION

- **A relevant end state for each DiD level is defined as a basis for the discussion on the feasibility of evaluating each DiD level by PSA.**

DID Level 1- Prevention of abnormal operations and failures

- Relevant end state defined as Reactor scram.
- Current Swedish PSA studies the frequency of initiating events is mostly based on operational experiences. Thus, no explicit evaluation of this DID level is performed in present Swedish PSA studies.
- Potential PSA developments can be improvements in operational experience evaluation, e.g.
  - Fault tree models of a large number of systems within the turbine plant, electrical power systems, control systems etc that are not extensively modelled in the current PSA.
  - Failure mode effects analyses of these systems to evaluate which failure modes that can cause reactor scram.
  - Extensive analysis of potential human errors during maintenance performed during power operation that could lead to reactor scram.

DID Level 2- Control of abnormal operation and detection of failures

- The DiD Level 2 relevant end state is defined as effects on safety barriers such that an operability evaluation is necessary before restart is possible, e.g. an event sequence that involves automatic depressurization of the RCPB.
- Current PSAs normally do not include any detailed evaluation of other consequences than core damage or unacceptable releases and thus, no evaluation of this DID level is normally performed. Potential development :
  - Define end states in the accident sequence analysis other than core damage and unacceptable releases.
  - The main work would be to include a larger number of initiating events (including estimating the frequencies of occurrence for these events) to reflect different events relevant for this purpose.
  - In most cases, the fault trees for the plant would be sufficient also for this purpose. In some cases, additional fault trees (or extension of current fault tress) can be necessary for the present purpose.

DID Level 3- Control of accidents within the design basis

- The DiD Level 3 relevant end state is core damage and other relevant fuel damage end states.
- A reasonable approach to evaluate this DID level via PSA would be via evaluation of the relevant end states.
- The core damage frequency and other end states is evaluated in the PSA Level 1, and thus, an evaluation of this DID level using PSA is already being performed.

DID Level 4 - Control of severe plant conditions, including prevention of accident progression and mitigation of the consequences of severe accidents

- The DiD Level 4 relevant end state is unacceptable release - can be expressed in release categories.
- From the point of view of evaluating DID level 4, the most valid measure would be the conditional probability of unacceptable releases, which is possible to be based on the existing PSA models.
- In most cases today, the focus is on the initiating event and the barrier against release given the initiator, similar to what is done for the core damage frequency. Thus, an evaluation of this DID level using PSA is already being performed.

DID Level 5 Mitigation of consequences of significant releases of radioactive substances

- There are no explicit end states for this level , the purpose is to mitigate consequences of releases of radioactive substances.
- This DID level encompass efficient use of emergency preparedness as a way to minimize radiation exposure.
- It is thus difficult to associate DID level 5 with a quantitative criterion describing the probabilities and consequences.
- The present PSA level 2 provides information about sizes and timing of release of radioactive substances and the associated frequencies that can be used for DID level 5.
- The possible way to evaluate this DID level via PSA would be to use a Level 3 PSA. In Sweden, no Level 3 PSA has been performed.

Conclusion

- **Three DID levels are currently not evaluated based on PSA.**
  - For DID level 1 it is proposed to develop a tool to identify risk implication (regarding influence on e. g. core damage frequency and unacceptable release frequency) for different groups of initiating events in the current PSA. The target values should reflect initiating events that have large implications on core damage frequency, unacceptable release frequency and for which the limiting functions that prevent progression of events that would need activation of safety systems are less robust. This tool can be used to identify trends that must be prevented, e. g. using more elaborate root cause analysis of events which have occurred. It is also proposed to investigate prevention features for different types of events in Swedish plants.
  - For DID level 2, the idea is to assess the probability for exceeding the acceptance criteria for fuel integrity.
  - For DID level 3-5, investigations will be made to define in what ways the result presentation in the current Level 1 and 2 PSA could be improved to provide further insights about these DID Levels.

www.scandpower.com

www.riskspectrum.com

Anytime – Anywhere – Under all conditions - Unconditionally