Introduction to PSA

Probabilistic Safety Assessment (PSA) provides an integrated and structured safety analysis for a nuclear facility that combines consideration of engineering design and operational features in a consistent framework. This established and systematic technique identifies all significant fault sequences which can lead to a radiological release and assesses their contribution to risk, on a best-estimate basis.

The operation of facilities such as a nuclear power plant involves:

- significant nuclear or radiological hazards; and
- complexity, with a high degree of redundancy and diversity of control and protection systems.

Typically, a PSA comprises combinations of event trees (modelling accident sequences) and fault trees (modelling system/ equipment failures).

PSA is a complementary approach to deterministic analysis, and aims to:

- assess overall safety against explicit or implicit standards or criteria;
- determine the balance of the design, identify importance of systems and sensitivity to change; and
- identify potential areas of improvement and constraints of safe operations.

BOX 1 - LEVELS OF PSA

Level 1: Takes a wide range of initiating events, develops accident sequences using systems modelling, and derives fault sequences to determine the frequency of plant damage.

Level 2: Takes the output from level 1 and examines accident progression, to consider release magnitudes and frequencies from loss of the containment function. Used for determining accident management strategies and identifying potential design weaknesses in reactor containment buildings.

Level 3: Takes the output from level 2 in order to determine the individual risk and wider (societal) consequences of accidents by considering the risks to the public from off-site releases. Used for emergency planning.

This is summarised in Figure 1.

LEVELS OF PSA

The extent of a PSA is defined in levels, with level 2 extending the level 1 analysis and level 3 developing the level 2 analysis (see Box 1).

International regulation typically requires a level 2 PSA that is plant-specific and considers all relevant operational states, covering fuel in the core, spent fuel pond and on-site storage and all relevant internal and external initiating events.

PSA PROCESS

So, what is involved in undertaking a PSA?

1. Identification of PSA scenarios

The foundation of a PSA is the output of the fault and hazard identification process which is typically a list of all faults and hazards within the scope of the PSA together with initiating faults and their causes, preventive, protective and mitigative safety systems. Whilst the PSA will typically assess a wider range of faults than the deterministic design basis analysis, it is usual to apply screening criteria for events of a very low frequency (typically less than 10^{-8} per year) or events which

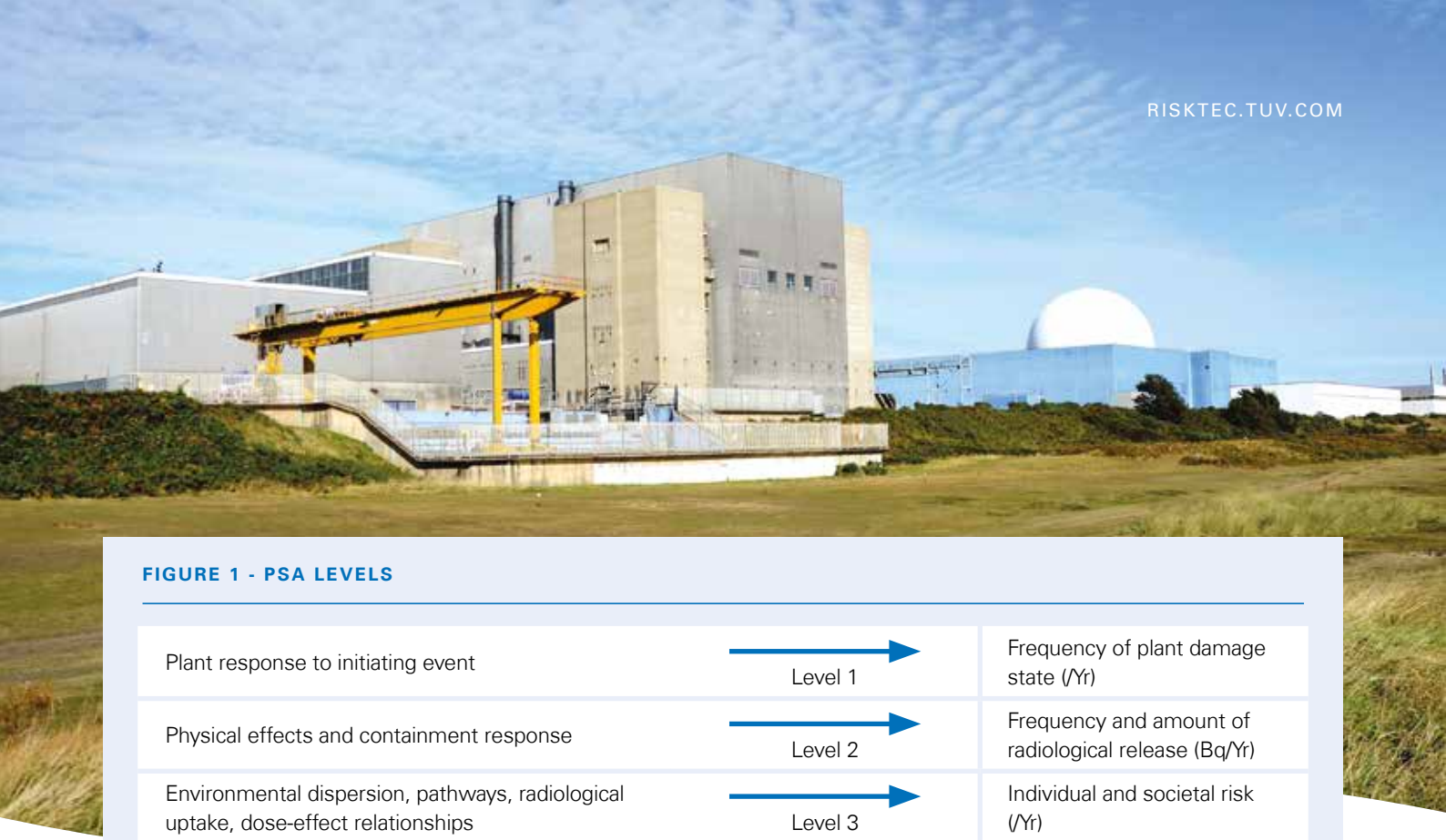

FIGURE 1 - PSA LEVELS

Plant response to initiating event	→ Level 1	Frequency of plant damage state (/Yr)
Physical effects and containment response	→ Level 2	Frequency and amount of radiological release (Bq/Yr)
Environmental dispersion, pathways, radiological uptake, dose-effect relationships	→ Level 3	Individual and societal risk (/Yr)

lead to insignificant radiological consequences.

2. Accident sequence analysis

This stage models the behaviour of the facility for the chosen faults and hazards, considering all possible combinations of success or failure of the protection systems to perform the safety functions. This, in combination with underpinning plant physics models, will identify the fault sequences which correspond to failure to maintain the facility within safe limits.

3. Systems failure analysis

This stage models the combinations of failures within the various safety systems which would lead to overall system failure. Fault trees will include events typically corresponding to component failure, common cause failure, component unavailability during maintenance or test and operator errors.

4. Data

A key challenge in the development of a PSA model surrounds acquisition of suitable data for the estimation of the frequencies and probabilities in the model. Where plant-specific data are available this is preferable, however generic data may also be required. These data require suitable manipulation to ensure that frequencies and probabilities are appropriately calculated. New designs may have a reliance on inherent or passive safety, for which specific failure data derivation techniques may be required.

An approach to modelling 'common mode' failures and specific values for operator errors also needs to be developed.

5. Internal and external hazards

A key expectation for a modern PSA is explicit modelling of internal and external hazards, such as fire, flood, extreme environmental and seismic events. This relatively new field uses the PSA model as a basis for a vulnerability assessment based on, for example, the zonal location of equipment or the potential for induced failures based on derived fragility parameters for equipment and structures.

CONCLUSION

PSA is an established discipline and forms a key input into the safety assessment of nuclear power plant, however it offers much more than a means to generate risk levels. It can be used as a way of identifying design weaknesses and assessing improvements as well as giving real insights into the effects of internal and external hazards.

As with all safety assessment techniques, PSA continues to adapt for changing requirements, for example in the assessment of advanced reactor designs or in support of security assessments.