STUK

GUIDE **YVL 2.8** / 28 MAY 2003

PROBABILISTIC SAFETY ANALYSIS IN SAFETY MANAGEMENT OF NUCLEAR POWER PLANTS

This Guide remains in force as of 1 December 2003 until further notice.
It replaces Guide YVL 2.8, 20 December 1996.

Third, revised and corrected edition
Helsinki 2003
Dark Oy

ISBN 951-712-786-3 (print)
ISBN 951-712-787-1 (pdf)
ISBN 951-712-788-X (html)
ISSN 0783-2346

STUK • **SÄTEILYTURVAKESKUS**
STRÅLSÄKERHETSCENTRALEN
RADIATION AND NUCLEAR SAFETY AUTHORITY

Osoite/Address • Laippatie 4, 00880 Helsinki
Postiosoite / Postal address • PL / P.O.Box 14, FIN-00881 Helsinki, FINLAND
Puh./Tel. (09) 759 881, +358 9 759 881 • Fax (09) 759 88 500, +358 9 759 88 500 • www.stuk.fi

Authorisation

By virtue of the below acts and regulations, the Radiation and Nuclear Safety Authority (STUK) issues detailed regulations that apply to the safe use of nuclear energy and to physical protection, emergency preparedness and safeguards:

- Section 55, paragraph 2, point 3 of the Nuclear Energy Act (990/1987)
- Section 29 of the Government Resolution (395/1991) on the Safety of Nuclear Power Plants
- Section 13 of the Government Resolution (396/1991) on the Physical Protection of Nuclear Power Plants
- Section 11 of the Government Resolution (397/1991) on the Emergency Preparedness of Nuclear Power Plants
- Section 8 of the Government Resolution (398/1991) on the Safety of a Disposal Facility for Reactor Waste
- Section 30 of the Government Resolution (478/1999) on the Safety of Disposal of Spent Nuclear Fuel.

Rules for application

The publication of a YVL guide does not, as such, alter any previous decisions made by STUK. After having heard those concerned, STUK makes a separate decision on how a new or revised YVL guide applies to operating nuclear power plants, or to those under construction, and to licensees' operational activities. The guides apply as such to new nuclear facilities.

When considering how new safety requirements presented in YVL guides apply to operating nuclear power plants, or to those under construction, STUK takes into account section 27 of the Government Resolution (395/1991), which prescribes that *for further safety enhancement, measures shall be taken which can be regarded as justified considering operating experience and the results of safety research as well as the advancement of science and technology.*

If deviations are made from the requirements of a YVL guide, STUK shall be presented with some other acceptable procedure or solution by which the safety level set forth in the guide is achieved.

Translation. Original text in Finnish.

1 General

The risks of operation of nuclear power plants are quantitatively analysed by probabilistic safety analysis (PSA). Safety functions for preventing or mitigating accidents and the associated systems necessary to carry out the safety functions are evaluated by these analyses. PSA supports both the design of a nuclear power plant (NPP) and the safety management and control of a NPP all through its service life.

Level 1 is the first part of PSA. It determines the accident sequences leading to core damage and estimates their probability.

Level 2 is the second part of PSA. It analyses the amount, probability and timing of a release of radioactive substances from the containment to the environment.

Level 3 is the third part of PSA. It analyses the risk to people and the environment caused by releases of radioactive substances. This guide deals with levels 1 and 2 of PSA.

Guides YVL 7.2 and YVL 7.3 concern the assessment of radiation effects.

According to the Nuclear Energy Decree, the applicant for a licence has to submit a PSA to the Finnish Radiation and Nuclear Safety Autority (STUK) while applying for an operating licence. According to the Government Resolution (395/1991), section 6, *nuclear power plant safety and the design of its safety systems shall be substantiated by accident analyses and probabilistic safety analyses. The analyses shall be maintained and revised if necessary, taking into account operating experience, the results of experimental research and the advancement in calculating methods.*

This Guide shows how probabilistic safety analyses are to be performed and used in the design, construction and operation of light water reactor plants.

In order to gain the greatest benefit from a PSA for plant safety, the applicant for a licence has to participate in the performance of the design phase PSA and in its completion during the construction phase and to manage to use and maintain the PSA during the operation of a NPP.

When the safety of a plant is assessed, probabilistic and deterministic safety analyses are used side by side so that these methods complement each other.

Accident analyses are used to demonstrate that the design basis for the systems, structures and components is adequate.

The assumptions made on the loading of components, operating parameters of systems, and faults impairing the performance of systems which form the basis for the analyses, are defined in the design requirements for systems and components.

The general safety principles are set forth in Guide YVL 1.0. The accident analyses are dealt with in Guide YVL 2.2. The application of probabilistic analysis methods is dealt with in Guides YVL 1.8, YVL 1.11, YVL 2.0, YVL 2.1, YVL 2.6, YVL 2.7, YVL 3.0, YVL 3.5, YVL 3.8, YVL 4.3, YVL 5.2 and YVL 5.5.

2 PSA during the design and construction of a NPP

2.1 Probabilistic design objectives

According to the Government Resolution (395/1991), section 13, *accidents leading to large releases of radioactive materials shall be very unlikely.*

The following numerical design objectives cover the whole nuclear power plant:

- The mean value of the probability of core damage is less than 1E–5/a.
- The mean value of the probability of a release exceeding the target value defined in section 12 of the Government Resolution (359/1991) must be smaller than 5E–7/a.

Should substantial risk factors not recognised earlier appear during operation, the licensee shall upgrade the safety of the plant.

In conjunction with the design of safety upgrades the licensee shall demonstrate that the safety of the plant assessed after the upgrades is substantially at the same level or better than the objectives presupposed for the design phase.

2.2 Design phase

The applicant for a licence shall provide the Finnish Radiation and Nuclear Safety Autority (STUK) with level 1 and 2 design phase PSAs corresponding to the design and site of the plant for the application for a construction licence. These analyses shall meet the contentual requirements set forth in section 4 of this Guide.

The risks associated with various initiators and accident sequences, taking into account their uncertainties, shall be compared with the numerical safety objectives and with each other in order to ensure that no single or few prevailing risk factors will stay at the plant.

The design phase PSA shall be used for its part to demonstrate that the plant design basis is adequate and design requirements are sufficient.

Particularly, such phenomena whose frequency of occurrence and consequences include large uncertainties shall be carefully examined. These are for example exceptional weather conditions, other possible harsh environmental conditions and seismic events.

The design phase PSA shall be used to demonstrate that the plant meets the numerical design objectives set forth in section 2.1 of this Guide.

The safety classification document shall be submitted to STUK in conjunction with the application for a construction licence. Guide YVL 2.1 deals with safety classification.

Safety classification shall be assessed by PSA. The assessment shall be used to demonstrate that the requirements for quality management system concerning the safety classification of each component are adequate compared with the risk importance of the component. The probabilistic review of the safety classification shall be submitted to STUK in conjunction with the safety classification document.

STUK makes a review of the design phase PSA prior to giving a statement about the construction licence.

2.3 Construction phase

The applicant for a licence shall submit level 1 and 2 construction phase PSAs to STUK in conjunction with the application for an operating licence at the latest. The level 1 and 2 PSAs shall meet the contentual requirements set forth in section 4.

The purpose of the level 1 and 2 construction phase PSAs is to ensure the conclusions made in the design phase PSA on the plant safety and to set a basis for risk informed safety management during the operation phase of the plant. The level 1 and 2 PSAs shall be based on the plant specifications submitted in conjunction with the application for an operating license.

The application for an operating license shall demonstrate that the plant meets the numerical design objectives set forth in section 2.1 of this Guide. Should substantial risk factors not recognised earlier appear before the commissioning of the plant, the applicant for a licence shall upgrade the safety of the plant.

In conjunction with the design of safety upgrades the applicant for a licence shall demonstrate that the safety of the plant assessed after the upgrades is substantially at the same level or better than the objectives presupposed for the design phase. STUK evaluates whether the risk factor is so important that the safety upgrades shall be implemented before the commissioning of the plant.

The technical specifications shall be reviewed by PSA in such a way that the coverage and balance of technical specifications are ensured. The review must cover all operating states of the plant. Especially such failure states, in which the change of operating state of the plant may result in a greater risk than the repair of the plant during operation, shall be reviewed with PSA. The results of the review shall be submitted to STUK in conjunction with the application for an acceptance of technical specifications.

The results of PSA shall be applied in the review of safety classification as in the design phase if extensive changes are performed in the plant design in the construction phase.

The results of PSA shall be applied in the working up of programs of safety significant systems testing and preventive maintenance during operation, and in the working up of disturbance and emergency operating procedures as set forth in section 3.

STUK reviews the construction phase PSA before giving a statement about the operating licence.

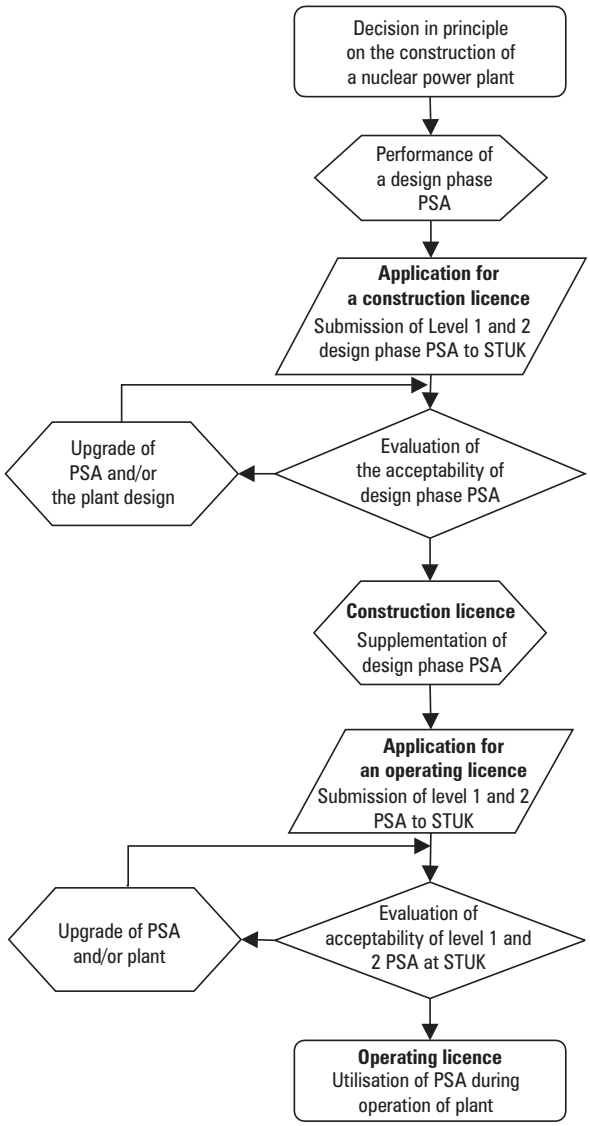

Diagram 1. PSA in a licensing of a nuclear power plant.

Diagram 1 shows an outline of the timing of the PSA during the design, construction, and commissioning of a nuclear power plant.

3 PSA during the operation of nuclear power plants

3.1 Updating of PSA

The licensee has to regularly update the PSA to correspond to the operating experience.

In addition the PSA model shall be updated always when a substantial change is made in the plant design or in the procedures or when a new substantial risk factor is found. The licensee shall provide the PSA model in computerised form to the use of the regulator in a way agreed separately.

The licensee shall maintain a database of the reliability of safety related components, initiating events and human errors.

STUK reviews the updates of PSA and evaluates their acceptability.

3.2 Risk informed safety management

Plant changes

PSA results shall be applied to the enhancement of safety and to the manifestation of needs for plant changes and to the evaluation of their priority. PSA methods shall be applied to evaluating the optional solutions of the design of system changes.

Guide YVL 2.0 concerns the design of systems. Accordingly the licensee shall submit to STUK a probabilistic assessment of the impact of the change on the plant safety in conjunction with the preliminary inspection document. Corresponding assessment shall be submitted to STUK for information also of those changes for which the preliminary inspection document is not be submitted, if the change is deemed to be of safety significance. Guide YVL 1.8 concerns plant changes.

A proposal for a safety class shall be submitted to STUK in conjunction with the preliminary inspection document of a system change in accordance with Guide YVL 2.0. In conjunction with extensive changes concerning whole systems the safety class shall be re-evaluated with PSA as in the design phase.

Technical specifications

The results of PSA shall be applied to the assessment of needs for technical specifications changes in conjunction with extensive plant changes in a corresponding way as in the construction phase. In the same way the needs for the changes of technical specifications shall be evaluated, if earlier unidentified risk factors are found. A preliminary proposal for the change of technical specifications shall be performed in accordance with Guide YVL 1.8 in context of the preliminary inspection document.

A risk estimate for the safety significance of

planned exemptions from the technical specifications shall be set forth in conjunction with the applications for an exemption. The requirements for case-specific risk estimates are presented in section 4.4.

Condition of systems, structures and components

Analysing the surveillance testing periods and procedures of safety significant systems and components their availability can be upgraded. PSA can be used to identify those systems and components by developing the surveillance tests of which the risk can most be reduced. PSA can also be used to upgrade the identification of potential failures and common cause failures.

The testing program of safety significant systems and components which is set forth in the context of technical specifications shall be argued by the aid of risk assessment and the results of analysis shall be submitted to STUK for information. The testing program shall be regularly evaluated on risk basis during the operation of the plant.

The on-line maintenance of safety significant systems and components is allowed during operation in accordance with the restrictions set by technical specifications. If the preventive maintenance is wanted to be performed during operation an estimate of the risk significance of preventive maintenance shall be presented. Guide YVL 1.8 concerns the preventive maintenance programs.

The results of PSA shall be used in the drawing up and development of the inspection programs of piping as per Guide YVL 3.8. Combining the information from PSA and the damage mechanisms of pipes and the secondary impacts of damages, the inspections are focused in such a way that those are weighted temporarily and quantitatively on those pipes whose risk significance is greatest. While drawing up the risk informed inspection program, the systems of classes 1,2,3,4 and EYT (not safety related) must be regarded as a whole. Similarly how far the radiation doses can be reduced by focusing inspections and optimising inspection periods shall be regarded.

Reporting of operating events

The risk significance of events shall be taken into consideration while deeming the performance of a special report as per Guide YVL 1.5.

Disturbance and emergency operation procedures

In order to ensure the coverage of disturbance and emergency operating procedures PSA shall be used to determine those situations for which the procedures shall be drawn up.

Personnel training

The results of PSA shall be taken into account in the planning of personnel training. The most important accident sequences and significant operator actions in terms of risk shall be trained at least in the period of three years which shall be ensured in conjunction with the planning of training of control room crew. In the planning of training of maintenance crew, attention needs to be paid to risk significant measures which are identified in context of PSA. STUK evaluates the training programs of the personnel inter alia in context of the inspection program of operation control.

4 Content and documentation of PSA

4.1 General

In addition to power operation, low power and shut down states and the transfers between them shall be considered in the PSA.

In the design phase PSA, operating experiences collected from similar plants or corresponding applications shall be used. As to the PSA of an operating plant, the plant specific data and if necessary, combined with data received from other similar plants or corresponding applications shall be used, and in the absence of such a data, general data shall be used. The feasibility and uncertainty of the data shall be justified.

Provided that no adequate design, site and reliability data are available for the design phase

PSA or if some safety related systems are constructed using a technology such that there are no well established methods available for computing the system reliability estimate, expert judgment, experiences and information from corresponding applications and corresponding sites can be used. In that case the estimation procedure must be justified.

The methods used in PSA have to be demonstrated.

4.2 Level 1 PSA

The level 1 PSA shall identify the accident sequences leading to core damage and to determine their probabilities. PSA shall be documented in such a way that at least the following matters can be logically traced from assumptions to the final results:

- overall description of the plant
- determination, description, categorisation and frequency estimation of initiating events
- success criteria for the safety and support systems, and descriptions of physical assessment methods used for their determination
- event trees for each of the initiating event categories
- description of accident sequences and procedures used for their determination
- human reliability analysis
- analysis of dependencies and common cause failures
- fault tree analysis including descriptions of systems and functions
- reliability data including expert judgement with necessary arguments
- importance measures for basic events and systems
- uncertainty analysis
- results and their evaluation with conclusions.

Events such as internal failures, disturbances and faults, loss of off-site power, fires, floods, harsh weather conditions, seismic events and other external and human caused initiators shall be dealt with as initiating events.

This guide does not deal with the intentional damaging of a plant.

4.3 Level 2 PSA

The level 2 PSA shall determine the amount, probability and timing of radioactive substances to be released out from the containment. The assessment shall cover the leaks, damage, controlled releases of radioactive substances and bypass sequences of the containment. The level 2 PSA shall assess the physical progress and timing of a reactor accident in various accident sequences which endanger the integrity or functional tightness of the containment or in which a release from the primary circuit takes place through systems outside the containment (containment bypass).

The level 2 PSA shall introduce the following issues:

- interface between level 1 and 2: description of plant damage states used at level 2, division of level 1 minimal cut sets to level 2 plant damage states, and dependences of level 2 systems and functions from level 1 systems model
- containment event trees
- analysis of the interactions between safety systems and the processes taking place in the containment in the course of an accident
- reliability analysis of the systems used for severe accident management taking into account the conditions prevailing in the containment during an accident and the possibility of erroneous measures
- estimation of the amounts of radioactive substances released from the damaged reactor core into the containment and estimation of the transportation and retention of radionuclides
- estimation of the amounts, quality, height and timing of various radioactive substances released to the environment, and estimation of the respective probability with associated uncertainties
- assessment of the appropriateness and efficiency of the strategy of accident management and the balance between systems (by the aid of e.g. a containment matrix)
- expert judgements with related grounds
- results and their evaluation with respective conclusions.

In the level 2 PSA, the following issues, among other things, shall be analysed:

- leak or bypass of the containment e.g. due to a fault in the isolation of the containment, steam generator tube ruptures, systems interfacing LOCAs, or due to seal failures of wall penetrations or access locks
- impact of reaction forces and missiles during different phases of accidents, especially in conjunction with the burst of reactor vessel or other damage to primary circuit
- amount and timing of occurrence of hydrogen generated in various accident sequences, the spreading of hydrogen in the containment, and the likelihood and impact of hydrogen combustion or burning
- steam spiking and steam explosion due to interactions between molten corium and coolant
- melt-through mechanisms of the reactor vessel, their timing and the impact of bursting materials on the integrity of the containment
- other factors endangering the integrity of primary circuit
- rapid growth of pressure in the containment due to e.g. damaged primary circuit, hydrogen combustion or interactions between molten corium and coolant
- recriticality of the reactor core
- slow growth of pressure in the containment due to decay heat or generation of non-condensable gases
- melt-through of the containment due to interactions between molten corium and structures.

4.4 Case specific analyses

The requirements for content and documentation of such modest, case specific analyses which the licensee performs for decision making are presented in this chapter (among others, applications for exemption from technical specifications, urgent reparation and modification works and analyses of operational events). However, the aforementioned general PSA requirements shall be applied for extensive plant changes.

As far as a case specific risk assessment computation is concerned, such a PSA model shall be used which describes the plant well enough in relation to the event under consideration.

The PSA computer model used in computation shall be available at STUK for possible review computation.

The licensee shall provide STUK with all substantial information necessary for tracing the assessment. The document submitted shall include at least:

- assumptions on analysis
- description of model changes and distinct calculations
- impact on the main results of PSA
- assessment of factors affecting the results most (e.g. completed with importance measures)
- qualitative assessment of analysis uncertainties
- identification data for PSA computer code used in the analysis.

If the time available for the analysis is short, the extent of the assessment can be reduced in accordance with the available resources. However the weight of the case specific analysis depends among others on how well the aforementioned requirements are fulfilled.

5 Quality management

The licensee has the responsibility of the performance, maintenance and application of PSA.

The licensee shall have a guide on the working up and application of PSA, which includes the responsibilities and acceptance procedures associated with PSA, references to procedures guides and procedures for PSA applications.

In addition, corresponding guides shall exist for the maintenance of PSA computer program, handling of errors and flaws, dealing with changes, time schedules for update, internal review and acceptance, documentation and submission to STUK. The licensee shall submit the aforementioned guides to STUK for information.

The licensee shall keep account of the changes made in the PSA model and data, reasons for the changes and impacts on PSA results and to submit the information to STUK in conjunction with an appendix of the updated PSA.

6 Definitions

PSA

means a probabilistic safety analysis.

PSA levels

describe the sequential parts of an extensive safety analysis. Level 1 is the first part of the safety analysis. It determines the accident sequences leading to a core damage and their probabilities. In level 2 safety analysis a core melt, the release mechanisms of radioactive substances from the containment to the environment and the amount, probability and timing of radioactive substances are analysed. The risk to people and the environment caused by releases of radioactive substances is analysed in level 3 safety analyses.

Safety functions

are functions intended to prevent the appearance or progression of disturbance and accident situations or to mitigate the consequences of accidents.

Initiating event

is a single event which requires the starting of the plant safety functions. The initiating event can be an internal or external event e.g. a component failure, a natural phenomenon or a human caused hazard.

Safety system

is a system which performs a safety function.

Support system

is a system which makes possible the main function of a safety or operating system e.g. by supplying electric power, cooling, lubrication or control.

Common cause failure

means that several systems, components or structures fail due to a same single event or cause either simultaneously or within a short time period.

Minimal cut set

means a shortest combination of events consisted of initiating event, failures or errors which is capable to lead to a core melt.