Probabilistic safety analyses (PSA)

This Guide is in force as of 1 February 1997 until further notice. It replaces Guide YVL 2.8, issued 16 October 1987.

Second, revised edition
Helsinki 1997
Oy Edita Ab
ISBN 951-712-215-2
ISSN 0783-2346

Authorisation

By virtue of section 55, second paragraph, point 3 of the Nuclear Energy Act (990/87) and section 29 of the Council of State Decision (395/91) on General Regulations for the Safety of Nuclear Power Plants, the Finnish Centre for Radiation and Nuclear Safety (STUK) issues detailed regulations concerning the safety of nuclear power plants.

YVL Guides are rules an individual licensee or any other organisation concerned shall comply with, unless STUK has been presented with some other acceptable procedure or solution by which the safety level set forth in the YVL Guides is achieved. This Guide does not alter STUK's decisions which were made before the entry into force of this Guide, unless otherwise stated by STUK.

Translation by RV. Original text in Finnish.

FINNISH CENTRE FOR RADIATION AND NUCLEAR SAFETY
P.O.BOX 14, FIN-00881 HELSINKI, FINLAND
Tel. +358-9-759881
Fax +358-9-75988382

1 General

The risks of operation of nuclear power plants are quantitatively analysed by the probabilistic safety analysis (PSA).The safety functions for preventing or mitigating accidents are evaluated in the PSAs. Several safety systems, support systems and surrogate systems may be associated with these functions.

According to the Nuclear Energy Decree, section 36, the applicant for a licence has to submit the PSA to the Finnish Centre for Radiation and Nuclear Safety (STUK) while applying for an operating licence. According to the Council of State Decision (395/91), second paragraph, section 6, *nuclear power plant safety and the design of its safety systems shall be substantiated by accident analyses and probabilistic safety analyses. 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 used in the design, construction and operation of light water reactor plants in order for their part to ensure that the safety of the plant is good enough in all plant operational states.

The greatest benefit from probabilistic safety analyses is gained by using the Living PSA, i.e. continuously updated PSA. The participation of the personnel of the applicant for a licence in the drawing up and use of the PSA promotes a general understanding of plant operation and interactions between distinct systems.

When the safety of the plant is assessed probabilistic and deterministic safety analyses are used side by side so that these methods complement each other. Deterministic analyses are used to demonstrate that the systems and components fulfil the objectives set for them. 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 deterministic safety analyses however are not used to assess the total risk of the plant. The deterministic safety analyses are dealt with in Guide YVL 2.2.

STUK uses the results of PSA also to assess whether the analyses as per Guide YVL 2.2 sufficiently well cover the various types of transients and accidents at the plant.

2 Use of PSA in the licensing process and safety control of nuclear power plants

2.1 Design phase PSA

The applicant for a licence has to provide the Finnish Centre for Radiation and Nuclear Safety (STUK) with a preliminary probabilistic safety analysis for the application for a construction permit. In the following this analysis is called design phase PSA. STUK makes an assessment of the acceptability of the design phase PSA prior to giving a statement about the construction permit.

The results of the design phase PSA have to meet the numerical design objectives set forth in section 4 of this Guide. Should the required compliance be lacking, the plant construction needs to be redesigned to provide the necessary improvements.

If a PSA has already been accomplished for another plant similar to the one for which a construction permit has been applied, the analysis can be utilised for applicable parts.

2.2 Level 1 and 2 PSAs

The applicant for a licence has to submit level 1 and 2 PSAs to STUK at the latest in conjunction with the application for an operating licence. The STUK assesses the acceptability of the PSA before giving a statement of the operating licence.

The aim of level 1 and 2 PSAs is to ensure the conclusions made in the design phase PSA and to provide a basis for probabilistic safety management during plant operation. Should new risk factors appear during the detailed design, construction and operation, the applicant for a licence has to demonstrate that they do not substantially impair the safety from what it was assessed to be when the construction permit was applied for. If necessary, the safety of the plant has to be upgraded.

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

2.3 Updating of PSA

On the one hand the PSA supports the design and safety analysis of the nuclear power plant, and on the other hand the safety management and safety control through the service life of the plant.

The licensee has to maintain a data base of safety related components, initiating events and human errors. The licensee also has to update the PSA to correspond to the operating experience. STUK will review the results of the work in conjunction with the periodic inspection programme.

The licensee also has to update the PSA to correspond to any changes made during design, construction and operation.

2.4 Utilisation of the results of PSA during operation

The results of PSA must be used in support of decisions on operational safety issues as follows:

- directing and weighting of inservice inspections
- applications of Technical Specifications
- case by case assessment of risks resulting from component failures
- training of plant personnel
- working out of emergency operating procedures
- plant changes and backfits
- risk follow-up of Licensee Events
- preventive maintenance and surveillance programme planning.

Decision in principle on the construction of a nuclear power plant
— Design phase PSA initiated
Application for a construction permit
— Design phase PSA is submitted to STUK — Evaluation of the acceptability of Design phase PSA at STUK
Construction permit
— Supplementation of design phase PSA up to a complete level 1 and 2 PSA
Application for an operating licence
— Submission of level 1 PSA to STUK — Evaluation of the acceptability of level 1 PSA at STUK — Submission of level 2 PSA to STUK — Evaluation of the acceptability of level 2 PSA at STUK
Operating licence
— Updating of PSA — Utilisation of PSA in the safety management and safety control of a NPP — Evaluation at STUK

Diagram 1. *Timing of PSA study.*

If any plant modifications have an evident impact on plant safety, the licensee must submit to STUK a report on the intended modification and of its impact on safety. The report has to be submitted to STUK prior to the implementation of the modification independently of the safety class which the modified systems belong to.

3 Requirements for PSA

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

In the PSA for a new nuclear power plant, a data base collected from similar plants need to be used. As to the operating plants, the plant specific data need to be used in the PSA. If a data base of this kind is not available or the confidence of it is poor due to the lack of data, a generic data base or well argued expert judgements can be used.

If a safety related system is constructed using a technology such that there are no well established methods available for computing reliability estimate, both quantitative methods and methods based on expert judgement can be used in the assessment of total reliability of such systems. In using methods based on expert judgement, the estimation procedure shall be conservative enough and the uncertainties associated need to be studied and documented.

3.1 Scope of PSA

Design phase PSA

The purpose of the design phase PSA is to support the working out of a balanced design for a plant. It is also to reveal the interconnections and interactions between the safety, support and surrogate systems as well as common cause failures and any of their weak points.

At least the initiating events of most frequent accidents need to be considered in the design phase PSA. It also contains estimates on what is the probability of each initiating event resulting in core damage. The design phase PSA further provides probability estimates on radioactive substances to be released to the environment in each case.

The initiating events to be analysed in the design phase PSA are selected on the basis of analyses and operating experiences from similar plants. In general at least the following events are analysed:

— transients including loss of main heat sink or feedwater
— loss of off-site power
— leak of reactor coolant
— transients in conjunction with which the reactor scram fails
— significant fires, floods and harsh weather conditions
— initiating events of importance during shutdown.

The dependencies between initiating events and safety functions have to be taken into consideration in the analysis. Accordingly, the possible impact of initiating events on the performance of safety systems or support systems needs to be considered.

Level 1 PSA

The level 1 PSA is to identify the accident sequences leading to core damage and to determine their probabilities.

Initiating events such as internal initiators, loss of off-site power, fires, floods, harsh weather conditions, and other external and human caused initiators have to be taken into account.

Level 2 PSA

The level 2 PSA is to identify the amount and probability of radioactive substances to be released out from the containment. It is to analyse the bypass sequences of containment and to assess the physical progress and timing in various accident sequences which endanger the integrity of the containment.

In the level 2 PSA among other things the following issues have to be analysed:

— leak of 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 etc.
— impact of reaction forces and missiles during different phases of accident, especially in conjunction with the burst of reactor vessel or other damage of primary circuit
— amount and timing 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
— 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 while the core is partly damaged and some control material is lost from the core region e.g. in case boron concentration is lowering, the reactor vessel is being filled with water or when rapidly generated steam lifts a water block
— 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.

3.2 Content of PSA

The contents of the PSA have to be arranged so that the issues can be consistently traced from assumptions to final results.

The level 1 PSA includes the following issues:

— overall description of the plant
— determination and description of initiating events
— success criteria for the safety and support systems, and descriptions of physical, thermohydraulic or reactorphysical methods used for their determination
— description of the safety and support systems and an account of their interdependencies
— determination of distinct initiating event categories in which the countermeasures for preventing core damage are approximately similar
— event trees for each of the categories
— estimation of the frequency of initiating events
— determination of accident sequences by means of thermohydraulic analyses
— analysis of interdependencies and common cause failures between various systems and components resulting from actions of operating and maintenance personnel, and their modelling either by means of event trees or fault trees
— the prospects for recovery and repair of components are analysed at discretion
— fault tree analysis including descriptions of systems and functions
— analysis of reliability data based on either generic data or operating experiences of similar plants
— quantitative probabilistic analysis which takes into account the most important factors affecting the results
— sufficient information for the evaluation of the uncertainty and sensitivity of the results.

The level 2 PSA is to include the following issues:

— analysis of the core damage associated with various accident sequences and timing, classification of sequential events and diagram of containment event tree
— 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 in various accident sequences
— estimation of the amounts, height and timing of various radioactive substances released to the environment, and estimation of the respective probability of accident sequences with the associated uncertainties
— expert judgements with related grounds
— results and evaluation
— conclusions.

4 Probabilistic safety objectives

4.1 Utilisation of the numerical results of PSA in the licensing process

According to the Council of State Decision (359/91), section 13, *accidents leading to extensive releases of radioactive materials shall be very unlikely*. According to Guide YVL 1.0, *the more severe an accident's consequences to man, the environment and property could be, the smaller the likelihood of its occurrence shall be.* STUK requires that the results of PSA submitted in conjunction with an application for a construction permit and an operating licence meet the numerical design objectives set forth in sub-section 4.2.

Should risk factors not recognised earlier appear during construction or operation, the common principle to remedy the situation is to make the plant as safe as reasonably achievable (SAHARA, Safety As High As Reasonably Achievable). When considering the sufficiency of measures aimed at reducing the probability of a core damage and the release of radioactive materials, STUK requires that the revised risk estimates do not demonstrate substantial reduction in the safety level from that which has been estimated in conjunction with the construction permit and operating licence.

4.2 Numerical design objectives

In order to be able rely on the most important safety functions, the mean unreliability of the functions during power operation shall be smaller than the design objectives set forth in diagram 2.

The failure probabilities of safety functions are to be computed making use of operating experiences and a data base from plants similar to that of concern. If a data base of this kind is not available, a generic data base can be used. Dependencies between systems and components affecting reliability must be included in the analysis.

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

Safety function	Probability of failure/demand
Reactor scram	≤ 1E-5
Supply of feedwater to the steam generators (PWR) or to the reactor vessel (BWR)	≤ 1E-4
Operation of emergency core cooling in the case of a small reactor coolant leak	≤ 1E-4
Isolation of the containment (including pipelines that are part of the reactor coolant system or directly connected to the open space inside the containment and that penetrate the containment)	≤ 1E-3

Diagram 2. *Numerical design objectives for safety functions.*

in section 12 of the Council of State Decision (359/91) must be smaller than 5E-7/a. However the containment has to be designed in such a way that its integrity is maintained with a high likelihood in case of both low and high pressure core damage.

The risks associated with various accident sequences of the PSA are to be compared with each other to ensure that no dominant risk factors deviating from the common risk level remain at a plant.

5 Definitions

PSA (probabilistic safety analysis) is a general concept which means a probabilistic safety analysis of any scope.

PSA levels describe the depth of an extensive safety analysis. Level 1 is the first part of the safety analysis. It determines the probability of core damage. In level 2 safety analysis a core melt, the progression of the accident and the release of radioactive substances from the containment to the environment are analysed. The environmental risk caused by releases of radioactive substances is analysed in level 3 safety analyses. This guide concerns not level 3 safety analyses.

Design phase PSA means a preliminary probabilistic safety analysis. In a design phase PSA the most likely accident sequences are analysed from the initiating event up to the amount and probability of the release of radioactive substances to the environment.

Safety functions are 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 hazard caused by man.

Safety system performs a safety function.

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

Surrogate system in this context means such an operating system which is designed to help or if necessary to replace a safety system in an accident situation.

Operating system is designed for maintaining plant normal operation. It contains liquid or gas. Many operational systems are significant from the point of safety and they can replace a safety system in some accident situations.

YVL guides

General guides

YVL 1.0 Safety criteria for design of nuclear power plants, 12 Jan. 1996

YVL 1.1 The Finnish Centre for Radiation and Nuclear Safety as the regulatory authority in control of the use of nuclear energy, 27 Jan. 1992

YVL 1.2 Documents to be submitted to the Finnish Centre for Radiation and Nuclear Safety concerning the regulation of nuclear facilities, 11 Sept. 1995 (in Finnish)

YVL 1.3 Mechanical components and structures of nuclear power facilities. Inspection licenses, 22 Oct. 1996 (in Finnish)

YVL 1.4 Quality assurance of nuclear power plants, 20 Sep. 1991

YVL 1.5 Reporting nuclear power plant operation to the Finnish Centre for Radiation and Nuclear Safety, 1 Jan. 1995

YVL 1.6 Nuclear power plant operator licensing, 9 Oct. 1995

YVL 1.7 Functions important to nuclear power plant safety, and training and qualification of personnel, 28 Dec. 1992

YVL 1.8 Repairs, modifications and preventive maintenance at nuclear facilities, 2 Oct. 1986

YVL 1.9 Quality assurance during operation of nuclear power plants, 13 Nov. 1991

YVL 1.11 Nuclear power plant operating experience feedback, 22 Dec. 1994 (in Finnish)

YVL 1.13 Shutdowns at nuclear power plants, 9 Jan. 1995 (in Finnish)

YVL 1.15 Mechanical components and structures in nuclear installations, Construction inspection, 19 Dec. 1995 (in Finnish)

Systems

YVL 2.1 Safety classification of nuclear power plant systems, structures and components, 22 May 1992

YVL 2.2 Transient and accident analyses for justification of technical solutions at nuclear power plants, 18 Jan. 1996

YVL 2.3 Preinspection of nuclear power plant systems, 14 Aug. 1975

YVL 2.4 Primary and secondary circuit pressure control at a nuclear power plant, 18 Jan. 1996 (in Finnish)

YVL 2.5 Pre-operational and start-up testing of nuclear power plants, 8 Jan. 1991

YVL 2.6 Provision against earthquakes affecting nuclear facilities, 19 Dec. 1988

YVL 2.7 Ensuring a nuclear power plant's safety functions in provision for failures, 20 May 1996

YVL 2.8 Probabilistic safety analyses (PSA), 20 Dec. 1996

Pressure vessels

YVL 3.0 Regulatory control of pressure vessels in nuclear facilities. General guidelines, 11 Sep. 1996

YVL 3.1 Construction plan for nuclear facility pressure vessels, 27 May 1997 (in Finnish)

YVL 3.3 Pressure vessels of nuclear facilities. Piping, 4 December 1996 (in Finnish)

YVL 3.4 Nuclear power plant pressure vessels. Manufacturer's competence, 16 December 1996 (in Finnish)

YVL 3.7 Pressure vessels of nuclear facilities. Commissioning inspection, 12 Dec. 1991

YVL 3.8 Nuclear power plant pressure vessels. Inservice inspections, 13 Dec. 1993

YVL 3.9 Nuclear power plant pressure vessels. Construction and welding filler materials, 6 April 1995 (in Finnish)

Buildings and structures

YVL 4.1 Nuclear power plant concrete structures, 22 May 1992

YVL 4.2 Steel structures for nuclear facilities, 19 Jan. 1987

YVL 4.3 Fire protection at nuclear facilities, 2 Feb. 1987

Other structures and components

YVL 5.1 Nuclear power plant diesel generators and their auxiliary systems, 23 Jan. 1997 (in Finnish)

YVL 5.2 Nuclear power plant electrical systems and equipment, 23 Jan. 1997 (in Finnish)

YVL 5.3 Regulatory control of nuclear facility valves and their actuators, 7 Feb. 1991

YVL 5.4 Supervision of safety relief valves in nuclear facilities, 6 April 1995 (in Finnish)

YVL 5.5 Supervision of electric and instrumentation systems and components at nuclear facilities, 7 June 1985

YVL 5.6 Ventilation systems and equipment for nuclear power plants, 23 Nov. 1993 (in Finnish)

YVL 5.7 Pumps at nuclear facilities, 23 Nov. 1993 (in Finnish)

YVL 5.8 Hoisting appliances and fuel handling equipment at nuclear facilities, 5 Jan. 1987

Nuclear materials

YVL 6.1 Control of nuclear fuel and other nuclear materials required in the operation of nuclear power plants, 19 June 1991

YVL 6.2 Fuel design limits and general design criteria, 15 Feb. 1983

YVL 6.3 Supervision of fuel design and manufacture, 15 Sept. 1993

YVL 6.4 Transport packages for nuclear material and waste, 9 October 1995

YVL 6.5 Supervision of nuclear fuel transport, 12 October 1995 (in Finnish)

YVL 6.6 Surveillance of nuclear fuel performance, 5 Nov. 1990

YVL 6.7 Quality assurance of nuclear fuel, 23 Nov. 1993

YVL 6.8 Handling and storage of nuclear fuel, 13 Nov. 1991

YVL 6.9 The national system of accounting for and control of nuclear material, 23 Nov. 1993 (in Finnish)

YVL 6.10 Reports to be submitted on nuclear materials, 23 Nov. 1993 (in Finnish)

YVL 6.11 Physical protection of nuclear power plants, 13 July 1992 (in Finnish)

YVL 6.21 Physical protection of nuclear fuel transports, 15 Feb. 1988 (in Finnish)

Radiation protection

YVL 7.1 Limitation of public exposure in the environment of and limitation of radioactive releases from nuclear power plants, 14. Dec. 1992

YVL 7.2 Evaluation of population doses in the vicinity of a nuclear power plant, 23 Jan. 1997 (in Finnish)

YVL 7.3 Evaluation of models for calculating the dispersion of radioactive substances from nuclear power plants, 23 Jan. 1997 (in Finnish)

YVL 7.4 Nuclear power plant emergency response arrangements, 23 Jan. 1997 (in Finnish)

YVL 7.5 Meteorological measurements of nuclear power plants, 28 Dec. 1990

YVL 7.6 Monitoring of discharges of radioactive substances from nuclear power plants, 13 July, 1992

YVL 7.7 Radiation monitoring in the environment of nuclear power plants, 11 Dec. 1995

YVL 7.8 Environmental radiation safety reports of nuclear power plants, 11 Dec. 1995 (in Finnish)

YVL 7.9 Radiation protection of nuclear power plant workers, 14 Dec. 1992

YVL 7.10 Monitoring of occupational exposure at nuclear power plants, 29 Aug. 1994

YVL 7.11 Radiation monitoring systems and equipment for nuclear power plants, 20 Dec. 1996 (in Finnish)

YVL 7.18 Radiation protection in the design of nuclear power plants, 20 Dec 1996 (in Finnish)

Radioactive waste management

YVL 8.1 Disposal of reactor waste, 20 Sept. 1991

YVL 8.2 Exemption from regulatory control of nuclear wastes, 19 March 1992

YVL 8.3 Treatment and storage of radioactive waste at a nuclear power plant, 20 Aug. 1996

The YVL-guides without any language marking are available both in English and Finnish.