Säteilyturvakeskus
Finnish Centre for Radiation and Nuclear Safety

YVL-ohje
YVL Guide
18.11.1987

YVL 2.8

1 (19)

Translation

PROBABILISTIC SAFETY ANALYSES (PSA) IN THE LICENSING AND REGULATION OF NUCLEAR POWER PLANTS

CONTENTS

Helsinki 1987
Government Printing Centre

ISBN 951-47-1059-2
ISSN 0783-2346

PL-P.O.BOX 268
SF-00101 HELSINKI
FINLAND

Ydinturvallisuusosasto
Department of Nuclear Safety
Kalevankatu 4 1
Kumpulantie 7

Puh.-Tel.
(90) 70821

Telex
122691 STUK-SF

STUK 41.01 1985

8085035600 – 12/6354/PTP

DEFINITIONS

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

PRA (Probabilistic Risk Assessment) means an extensive probabilistic risk analysis, which includes an estimate of the effects of radioactive releases on the environment, property and man. The risk means the product of the likelihood of an accident and its consequences,

PSA levels mean here the parts of a full-scope probabilistic risk analysis. Level 1 means the first part of a risk analysis and it is used for analysing the probability of a core damage. Level 2 means the part analysing a core melt, progression of the accident and the release of radioactive materials from the core into the environment. Level 3 indicates the part which studies the environmental risk caused by radioactive releases.

Mini-PSA means here a probabilistic safety analysis which is conducted during the design phase of a nuclear power plant and is of a limited scope. A mini-PSA contains the simplified reliability analyses of the most important safety functions and only a few accident sequences derived from the most important initiating events.

Concise PSA Level 2 contains only the analysis of the most important accident sequences starting from a core melt and ending with the determination of the amounts of radioactive releases from the containment and the related conditional probability.

Updating PSA means that the PSA is made to correspond with the actual plant construction and/or data base.

Safety function means an integral function intended for preventing an accident or mitigating its consequences. Functions of this kind are, for instance, those which make the reactor subcritical, maintain a sufficient coolant volume in the reactor, reduce pressure in the reactor coolant system, remove residual heat from the reactor core and maintain the functions of the containment.

Initiating event is a single event as a consequence of which the plant or a part thereof falls outside the normal operating condition. The initiating event can be an internal or an external event e.g. a component failure, a natural phenomenon or an hazard caused by man.

Frontline system in this safety regulation means a system which has been designed for starting or directly maintaining a safety function.

Support system means a system which is generally intended for supporting the main functions of a safety system or a fluid system, for instance, through power supply, cooling, lubrication or control.

Operational system means systems containing liquids or gases and designed to maintain the normal operation of the plant. Most operational systems also have safety significance, and in some cases they can be used as an aid to a safety system in accident conditions.

Surrogate system means here an operational system which has been designed to help or substitute a front line system in accident conditions.

1 GENERAL

This guide shows how probabilistic safety analyses are used in the regulation of the design, construction and operation of light water reactor plants in order to

ensure that the safety functions of the plant are carried out reliably enough.

The probabilistic analyses and the deterministic safety analyses are used side by side so that they complement each other in the assessment of plant safety. The deterministic analyses are used to demonstrate that the systems and components fulfil the design objectives set for them. The assumptions on the loading of components, operating parameteres of systems, and faults impairing the performance of systems, which are made in the analyses, are defined in the design requirements. Because the deterministic analyses lack a quantitative assessment of the risks, they do not give an assessment of the total risk of the plant or the balance of the plant design.
The deterministic principles of safety analyses are dealt with in Guide YVL 1.0 and 2.2 /1, 2/.

STUK uses the probability of the accident sequences that are defined in connection with the PSA also to determine whether the analyses as per Guide YVL 2.2 are enough to cover the various types of transients and accidents at the plant.

By means of probabilistic analyses, a quantitative assessment of the risks involved in operation of the nuclear power plant is made. By these methods it is studied how accidents can be prevented or mitigated with combined functions involving several frontline, support and surrogate systems. This will be necessary since it is not always certain that systems which have been designed to ensure plant safety in connection with the initiating event of the most severe credible accident are also successful in dealing with less severe initiating events of different types.

Probabilistic research methods have shown that the greatest risk is not generally posed by the initiating

events that are regarded as the most dangerous /3, 4, 5, 6, 7/. Sequences of events starting from ordinary transients can be more important in regard to the risk. This is because the frequency of the more severe initiating events is often very low in comparison with the frequency of events of the transient type, and their countermeasures are more straightforward. Many minor transients may lead to a high number of accident pathways due to the possible erroneous operator actions in the management of these transients.

The probabilistic safety analysis is included in the licensing /8/ starting right from the preliminary design so that its level and depth will be planned to match each phase of design, construction and operation.

2 PURPOSE AND TIMING OF PSA

2.1 Mini-PSA

The power company has to provide STUK with a preliminary probabilistic safety analysis, for the application of a construction permit, which is hereinafter called the mini-PSA. The acceptability of the mini-PSA is one prerequisite for the granting of a statement in favour of the application for a construction permit. STUK assesses that it needs about half an year for the review of the mini-PSA. STUK works out an assessment of the plant based on the review of the mini-PSA before supplying the statement for a construction permit.

The mini-PSA comprises the analyses relating to the PSA level 1. The mini-PSA is based on the design concept from the preliminary design phase of the power plant and only on the most important initiating events.

The purpose of the mini-PSA is to support the preliminary design so that unbalanced design can be prevented. The

purpose of a mini-PSA is not to determine the final risk level of the plant, but to reveal the interconnections and interactions between the frontline, support and surrogate systems, as well as any weak points and common causes of failures. In fulfilling this purpose, the qualitative PSA methods have an essential role.

The assessments that are made in connection with the mini-PSA are even intended for ensuring that the probabilistic objectives of safety functions, which are given in this guide (section 4.2), can be met. The purpose is to find out which safety-related factors affect the crucial accident sequences and safety functions, and to ensure, by means of good design, that the probability of the failure of the most important safety functions can be maintained even during operation.

Because the mini-PSA is carried out during design, many system designs have not yet been completed. Therefore the analysis of the reliability of systems can concentrate on the most important components and functions with respect to each system and system interaction. In connection with the mini-PSA, sufficiently low design objectives shall be set also for the reliability of the non-designed systems. They determine for their part the minimum reliability of the safety functions and the level of probability of the most significant accident sequences.

2.2 PSA

The power company has to submit the PSA comprising level 1 and the concise level 2 to STUK in connection with the application for an operating license and the level 2 PSA before supplying the statement for an operating license. Their acceptability is one prerequisite for a favourable statement on the operating license. STUK assesses that not less than six months will be required to review the level 2 PSA.

Before supplying the statement for an operating license, STUK prepares an assessment of the safety of the plant based on the review of the PSA. This assessment evaluates, based on the PSA, the impact of the structural features, operation and maintenance and administration on the safety of the plant.

The contents of the PSA comprising level 1 and the concise level 2 are based on an updated design concept that has received a construction permit.

Immediately after the completion of the PSA comprising level 1 and the concise level 2, the PSA is supplemented with the full- scale level 2.

The contents and requirements which the level 1 and level 2 PSAs contain shall be more precisely dealt with in point 3 of this guide.

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 PSA

The purpose of the PSA is not only to be a disposable analysis tied to the design and construction phases, but it is also meant to provide a tool for controlling and regulating the safety of a nuclear power plant all through its service life. It is used both by the utility and the regulatory authority in resolving for the safety problems /9/ .

The power company has to update the PSA during the design and construction phases every time the design concept is substantially changed. In addition, it is required that the power company continuously supplements, follows and analyses the data base on operating experience and safety-

related systems, and updates the PSA to correspond with the operating experience.

The power company has to maintain a continously acceptable standard of safety during operation. When necessary, the power company must be able to demonstrate this by means of the PSA methods in a way presupposed by STUK.

2.4 Utilization of the results of PSA during operation

To avoid reactor accidents and to mitigate their consequences, the results of PSA shall be utilized in the training of the operating personnel, in the training on the use of simulator and in working out the emergency instructions.

2.5 Exception

If a probabilistic safety analysis for a series-produced reactor of this kind already exists, it can be utilized as far as it corresponds with the construction to be built and the requirements in this guide. If, for example, a series- produced plant has been subjected to a complete PSA level 1, a mini-PSA is no longer necessary, but the PSA level 2 shall have to be accomplished in accordance with this guide.

Decision in principle on the construction of a nuclear power plant

Mini-PSA started

Application for a construction permit

Mini-PSA is submitted to STUK
Evaluation of the acceptability of mini-PSA in STUK
Conclusions in STUK

Construction permit

PSA comprising level 1 and concise level 2 started

Application for an operating license

PSA comprising level 1 and concise level 2 is submitted to STUK

Supplementation of level 2 PSA started
Evaluation of the acceptability of PSA comprising level 1 and concise level 2 in STUK
Submission of the supplemented level 2 PSA to STUK
Evaluation of the acceptability of level 2 PSA in STUK
Conclusions in STUK

Operating license

Updating of PSA
PSA in training of operation personnel

Diagram 1 Timing of the PSA in the design, construction and commissioning phases

3 SCOPE, CONTENTS AND METHODS OF PSA

3.1 Scope of PSA

The level 1 PSA comprises the determination of the accident sequences resulting in a core damage and the calculation of their probabilities. The level 1 PSA comprises even the by-pass chains of the containment.

Level 2 contains the estimation of the physical progress and timing of the accident, the analysis of the interaction between the containment and the systems, and the estimation of the amounts and probabilities of radioactive releases.

Events that are initiated by faults and transients inside the plant are taken into account as initiating events as well as, the loss of off-site power, fires and floods.

In the mini-PSA which is performed in the design phase, only a few of the most important events will be analysed, depending on the plant type. Typical examples are:

- transients resulting in the loss of the main heat sink or feed water
- loss of off-site power
- a small reactor coolant leak
- ATWS

The analysis also encompasses the dependences between the initiating event and the safety functions. In determining initiating events, special attention is paid to the possible effect of the initiating event on the operability of frontline systems or their support systems. Examples of this include the leaking of reactor coolant through a system connected to the primary circuit and faults starting in the support systems which will finally damage the frontline systems, as well. The study of dependences of this kind is necessary to understand the actual nature

and situation of an accident. The choice of the correct countermeasures for preventing or mitigating the consequences of the initiating event supposes an identification of such dependences. It is important to notice this when placing initiating events into groups which are estimated to require similar countermeasures.

The procedures presented in references 10, 11 and 12 for analysing initiating events are useful.

3.2 Contents of PSA

The contents of the PSA are clearly arranged so that each issue can be consistently followed from the assumptions up to the final results.

The level 1 PSA includes the following issues:

- Overall description of the plant on the basis of the PSAR
- Determination of initiating events
- The physical, mainly thermohydraulic, methods which are used in determining the success criteria selected for frontline systems and support systems.
- Detailed description of the frontline and support systems and an account of their interdependences.
- Classification of initiating events. The criterion is that accidents in each class are dealt with by using similar countermeasures.
- Preparation of event trees for the classes of initiating events.

- Estimation of the frequency of initiating events.

- Determination of accident sequences by means of the thermohydraulic analyses relating to the branches of the event tree.

- The operational and physical interdependences and common-cause failures between systems, components and, when necessary, actions of the operating and maintenance personnel are studied and connected to the accident sequences as part of the event tree or the fault tree.

- The prospects of recovery and repair of the systems or components which have failed during an accident are analysed at discretion.

- Fault tree analysis with its descriptions of systems/functions.

- Analysis of the reliability data by means of a Bayesian or a classical method, the basis being either a generic data base or the operating experience of similar plants.

- Quantitative probabilistic analysis so that the most important factors come out.

- Uncertainty analysis, which comprises a quantitative analysis of the uncertainty due to the data base for the probability of a core damage and for the probabilities of the most important accident sequences, a qualitative analysis of the uncertainty of the calculational models, and an assessment of the completeness of the PSA.

- Sensitivity analysis of the most important systems.

- Presentation and evaluation of the results.

- Conclusions.

In connection with the PSA level 2, one shall furthermore consider the following points:

- Assessment of the interactions between the safety systems and the processes taking place in the containment in the course of the accident, e.g. the effect of a containment break on the cavitation of the emergency cooling pumps, distribution of water in the containment, effect of hydrogen fires, etc.

- Assessment and timing of the reactor core melts associated with various accident sequences.

- Analysis of the mode and timing of a reactor pressure vessel break.

- Estimation of the behaviour of a molten reactor core, analysis of the reactions between the core and the surroundings, and estimation of the amounts of radionuclides released from the damaged core into the containment in various accident sequences.

- Analysis of the possibilities of a containment break and their timing e.g. due to a rapid pressure rise, missiles, through-melt, slow pressure increase or a fault in the isolation of the containment.

- Estimation of the amounts of radionuclides released, the modes and places of release in various containment breaks and the estimation of the corresponding probabilities.

- Estimation of the uncertainties relating to the course of the accident including an assessment of the options that can be chosen by the personnel.

- The containment sequences and accident sequences leading to a core melt are joined together and the probability of the radioactive releases into environment and its uncertainty are assessed.

- Presentation and evaluation of results.

- Conclusions.

3.3 Methods

The estimation of uncertainties is one of the most important tasks of PSA. The unavoidable uncertainty associated with the PSA methods partly stems from inherent statistical uncertainty incorporated in the operating experience, partly from the uncertainty of the assumptions relating to the methods. The most important factors which cause uncertainty are related to human errors, the data of dependences and CCFs, modeling and the understanding of the phenomena which occur during severe accidents.

No absolute requirements for using specified methods are presented but the emphasis is placed on the clarification of the most substantial issues.

Most analysis methods relating to PSA on level 1 have become established and there are instructions for their correct application /10, 11 and 12/. The methods to be used must be shown to STUK before the analysis is begun.

The plans concerning the analysis methods and accident sequences with respect to level 2 must be shown to STUK before the analysis is begun.

4 PROBABILISTIC SAFETY OBJECTIVES

4.1 Comparable use of the results of the PSA

The general design objective for the nuclear power plants is that the likelihood of the damage of the reactor core and the release of radionuclides into the environment under accident conditions is very small.

No fixed acceptance standard is set forth for the probability of a core damage associated with the accident sequences. Instead the probabilites associated with the various accident sequences are compared with each other. On the basis of the comparison, it is considered whether there is a need to take any measures to diminish the probability of a core damage and the probability of releases into the environment.

Similarly, the amounts of radioactive releases and their probabilities in regard to the various accident sequences are compared with each other. One basis of acceptance is a low enough probability for those accident sequences the releases of which exceed the limits set for accidents in Guide YVL 7.1 /13/. A characteristic feature of these accident sequences is that the containment does not function as planned.

4.2 Numerical design objectives for the reliability of safety functions

The general requirement in regard to the safety systems is that an advanced, well-tested and reliable technology is used in the design and construction of the safety systems.

To ensure the high reliability of the most important safety functions, it is required that their unreliability be below the following design objectives, at least with a confidence of 90 %

Safety function	Probability of failure/ demand
Reactor scram	10^{-5}
Isolation of the containment (includes pipelines that are part of the reactor coolant system or directly connected to the open space inside the containment and penetrate the containment)	$5 \cdot 10^{-3}$
Supply of feed water when the off-site power is lost or the main feed water system has failed (all loops)	10^{-4}
Operation of emergency core cooling, including long-term recirculation, in the case of a small reactor coolant leak	10^{-4}
Rapid reactor pressure reduction together with long-term cooling of the condensation pool inside the containment (BWR)	10^{-4}

To calculate the probability of failure of these safety functions, a data base is used which has been collected and analyzed utilizing the operating experiences of similar plants. If a data base of this kind is not available, a generic data base will be utilized. To determine the confidence limits of the reliability data, either the Bayesian method or classical methods can be used /12/. Any dependences between systems and components affecting reliability will be included in the analysis.

5 BIBLIOGRAPHY

1. Guide YVL 1.0 Safety criteria for design of nuclear power plants. Finnish Centre for Radiation and Nuclear Safety

2. Guide YVL 2.2 Transient and accident analyses as a basis of the technical systems of nuclear power plants. Finnish Centre for Radiation and Nuclear Safety

3. Guide YVL 2.7 Failure criteria for the design of a light-water reactor. Finnish Centre for Radiation and Nuclear Safety

4. NUREG-1050, "Probabilistic Risk Assessment (PRA), Reference Document", Final Report, September 1984

5. NUREG-0933, "Prioritization of Safety Issues", December 1983

6. R. Bernero: "Source Terms, ACRS PRA Meeting, U.S. NRC, March 1984

7. NUREG-1070, NRC Policy on Future Reactor Designs: Decisions on Severe Accident Issues in Nuclear Power Plant Regulation, USNRC, July 1985

8. Guide YVL 1.1 The Institute of Radiation Protection as the supervising authority of nuclear power plants

9. IAEA-TECDOC-308, "Survey of Probabilistic Methods in Safety and Risk Assessment for Nuclear Power Plant Licensing", Vienna 1984.

10. NUREG/CR-2815, "Probabilistic Safety Analysis

Procedures Guide", January 1984

11. NUREG/CR-2728, "Interim Reliability Evaluation Program Procedures Guide", January 1983

12. NUREG/CR-2300, "PRA Procdures Guide"; Vol 1-2, Final Report, January 1983

13. YVL 7.1 Limitation of environmental radiation exposures from nuclear installations. Finnish Centre for Radiation and Nuclear Safety

In the event of any differences in interpretation of this guide, the Finnish version shall take precedence over this translation.