BASIC SAFETY RULE

DEVELOPMENT AND UTILISATION OF PROBABILISTIC SAFETY ASSESSMENTS

I PURPOSE OF THE RULE

The safety of French nuclear reactors is based essentially on a deterministic approach. Probabilistic safety assessments (PSA) use a particular method of investigation which supplements the conventional deterministic analyses.

PSAs consist of a set of technical analyses for assessing the hazards related to nuclear installations in terms of frequencies and consequences of undesired events.

As such, they are of assistance in the definition and the prioritisation of the actions to be taken in order to attain or maintain a satisfactory safety level.

The purpose of this rule is to define acceptable methods for the development of PSAs and proven applications of PSAs for operating or future pressurised water reactors (PWR) of the French nuclear power programme, incorporating available French and international experience in this area.

The standing group of experts for nuclear reactors has been consulted for the drafting of this rule.

II STATEMENT OF THE RULE

II.1 PSA DOCTRINE

II.1.1 LINKAGE BETWEEN THE DETERMINISTIC AND PROBABILISTIC APPROACHES

II.1.1.1 DESIGN JUSTIFICATION

The safety of the pressurised water reactors (PWR) of the French nuclear power programme relies essentially on a deterministic design based on the concept of defence in depth.

The design provisions adopted by the operator are justified by, among other elements, the study of a limited number of design-basis operating conditions(*) resulting from simple initiating events, and the application of deterministic rules and criteria which include margins and conservative assumptions.

The results of such studies must satisfy criteria intended to limit the consequences of the specified events. More severe consequences can be accepted for less frequent events or conditions.

(*) Terms followed by an asterisk are defined in the glossary at the end of this rule.

This justification also concerns the analysis of the operating conditions involving multiple failures likely to lead to consequences exceeding those of the design-basis operating conditions, for which arrangements must be made to reduce their probability or to limit their consequences to those of the design-basis operating conditions.

II.1.1.2 CONTRIBUTIONS OF PSAS

PSAs provide a risk assessment method based on systematic investigation of accident scenarios. They provide an overall view of safety, including both equipment and operator behaviour.

In practice, PSA considers a list of initiating events which is as realistic and complete as possible. It highlights operating situations covering complex events and combinations of events, including situations involving the loss of redundant systems and, depending on the scope (refer to paragraph II.2), those involving the occurrence of an internal(*) or external(*) hazards.

For each initiating event, PSA establishes the accident sequences resulting from the success or failure of the operation systems and actions brought into play to perform the safety functions(*) and assesses the frequency of an undesired event which depends on the type of PSA (refer to paragraph II.2.1). By summing all the calculated frequency values, it estimates the total frequency of the undesired event, the contribution of each initiating event to the calculated frequency, and the importance for safety of the equipment and the operating actions.

PSA helps to assess whether the arrangements made by the plant operator are satisfactory. It can be used to prioritise the safety problems relating to the design or operation of reactors, and is a tool for dialogue between the plant operators and the authorities.

For operating reactors, PSA contributes to assessment of their overall safety level and highlights points for which design or operating changes can be examined or even judged necessary.

For future reactors, PSA is developed while the design is being defined, so as to highlight situations involving multiple failures for which arrangements must be made to reduce their frequency or limit their consequences.

II.1.2 REFERENCE PSA

II.1.2.1 OPERATING REACTORS

For each type of reactor, the plant operator drafts a reference PSA.

Its scope is defined in paragraph II.2 and the acceptable methods for completing it are described in paragraph II.3.

In the safety analysis report compiled for each periodic safety review, the plant operator includes a summary of the reference PSA consistent with the reference and operating condition of the reactors. This summary includes the main study assumptions and the predominant contributions to the calculated core damage frequency.

The reference PSA is produced and updated so that it can be used for the main applications, including those described in paragraph II.4.

II.1.2.2 FUTURE REACTORS

The reference PSA is produced in consecutive steps during reactor design.

In the same way as for operating reactors, the scope of the reference PSA is defined in paragraph II.2 and the acceptable methods for completing it are described in paragraph II.3. A summary of the reference PSA, including the main study assumptions and the predominant contributions to the calculated core damage frequency, is given in the preliminary safety analysis report.

II.1.3 PRINCIPLES OF USE OF PSAS

The term “PSA application” qualifies any approach to reactor safety that makes use of probabilistic methods to aid decision-making, particularly in terms of changes in design, operation and preparation for accident management.

The method of use and the characteristics of the PSAs associated with each application—including their scope (paragraph II.2)—depend on the application considered. The relevance of the PSA results must be assessed case by case, according to the application implemented.

For certain applications, the method of use can include a reference to probabilistic objectives (absolute or relative values, total or partial), taking the uncertainties into account. These objectives must be considered as guideline values and not as strict limits.

Applications which can give rise to design or operating changes, introduced either by the plant operator or on request from the authorities, or which provide justification for maintaining the present state of an installation, are cited in paragraph II.4.

II.2 PSA SCOPE

II.2.1 INTRODUCTION

An installation is characterised by a construction condition and by the organisation of its operation. A PSA can be representative of a reactor or of a reactor type. The reference PSA is defined for a reactor type and deals with the consequences on a single reactor.

The scope of a PSA, for a given installation, is defined by the nature of the consequences examined and by the events studied.

Three types of PSA can be produced, depending on the consequences studied:

- a level 1 PSA identifies the sequences leading to core damage(*) and determines their frequencies,
- a level 2 PSA assesses the nature, magnitude and frequencies of releases outside the containment,
- a level 3 PSA assesses the calculated frequencies of consequences expressed in dosimetric or contamination terms (or in terms of frequencies of cancers or other effects on health).

The events studied can include initiating events(*) originating inside the installation (equipment or human failures, internal fire or flooding, etc.) or originating outside (earthquake, external fire or flooding, tornado, etc.), associated with the different reactor states.

Other scenarios can also be considered probabilistically, for example those based on loss of the spent fuel pool cooling system. Release scenarios without core damage can also be examined probabilistically. These types of scenario are not explicitly part of a PSA as defined in this BSR.

II.2.2 RELEVANT SCOPE

For any application, the plant operator defines the scope and justifies its relevance.

The reference PSA covers events of internal origin (excluding fire, flooding, etc.) affecting the reactor as realistically and completely as possible, considered in all the reactor states in which they are likely to occur, and examines the corresponding accident sequences(*) up to core damage.

Its scope can be extended to the treatment of certain internal and external hazards and to the assessment of release frequencies with core damage, depending on the magnitude of the results obtained, the relevance of the analyses and the interest of the applications derived from them.

II.2.3 SPECIFIC STUDIES

The plant operator may decide to develop specific studies to meet needs not covered by the reference PSA, such as:

- adapting or supplementing the reference PSA for applications, for example for probabilistic analysis of certain events,
- validating or justifying certain simplifying assumptions of the reference PSA, for example by a study of the sequences over a longer period than that used in the reference PSA,
- between two consecutive versions of the reference PSA, dealing with new safety concerns (highlighting of safety problems by operating experience or by improved knowledge) or assessing the impact of a design or operating change defined outside the periodic safety reviews,
- extending the scope of the reference PSA, for example:
  - by grouping the accident sequences leading to core damage according to characteristics relating to the magnitude of the releases,
  - for an initiating event affecting several reactors on a site, by dealing with the consequences on all the reactors considered.

As far as possible, specific studies are conducted using the methods described in paragraph II.3.

The possible incorporation of the specific studies into the reference PSA and the associated procedures (simplification of the studies, for example) are decided on a case-by-case basis, when the reference PSA is updated.

The term "*the PSAs*" refers to the package constituted by the reference PSA and the special studies.

II.3 ACCEPTABLE METHODS FOR CONDUCTING LEVEL 1 PSA

This section describes acceptable methods for conducting the reference PSA and the special studies used in a dossier submitted to back up an authorisation application.

The methods cited are limited at present to the study of initiating events of internal origin, excluding fire and flooding.

They apply to PSAs conducted for operating reactors and for future reactors, except on particular points which are mentioned explicitly.

II.3.1 IDENTIFICATION OF INITIATING EVENTS

II.3.1.1 DEFINITION

An initiating event is an event which disturbs the normal operation of the installation and leads to drift of the values of certain parameters of the installation (pressure, temperature, reactivity, etc.), from which an accident sequence can develop.

This section discusses initiating events of internal origin (excluding internal fire or flooding), loss of external electrical power supplies and loss of water intake.

II.3.1.2 SELECTED INITIATING EVENTS

The list of initiating events studied is as complete as possible. The best approach, in order to tend towards completeness, is to use all the available information sources:

- the safety analysis report, on the basis of the operating conditions,
- French and foreign reactor operating experience,
- international practices,
- improved knowledge and special studies,
- previous PSAs.

To make the list as complete as possible, the use of deductive methods is recommended in order to determine the elementary failures or combinations of elementary failures which would contribute to the loss of each safety function concerned.

Initiating events are identified for all the reactor states to be examined in the PSA.

II.3.1.3 GROUPING OF INITIATING EVENTS

To simplify the study and the interpretation of the results, the initiating events can be grouped according to their consequences on the operation of the safety functions.

The groups and the choice of assumptions are documented and justified.

II.3.1.4 INITIATING EVENTS NEGLECTED IN THE STUDY

The neglected initiating events are justified, considering both their frequency and their consequences.

II.3.2 CONSTRUCTION OF ACCIDENT SEQUENCES

The plant operator models the behaviour of the installation following an initiating event through accident sequences, considering the occurrence of additional failures.

An appropriate method for constructing accident sequences is the event tree(*) method.

It can be used to view the running of possible scenarios, determine the events to be studied (system missions or operator missions designed to limit the consequences in the course of the accident sequence) and take into account the temporal and functional dependencies between events.

The analysis of the accident sequences is conducted either to a failure state, characterised by the exceeding of one or more surrogate criteria equivalent to inevitable core damage, or to a success state in which core damage can be excluded.

The points below should be considered for the construction of accident sequences and the quantification of their frequencies.

II.3.2.1 ACCIDENT SEQUENCE FAILURE OR SUCCESS STATES

The objective of a level 1 PSA is to determine the frequencies of the different accident sequences leading to core damage. Nevertheless, in practice core damage is replaced by surrogate criteria introduced to simplify the study.

Examples of criteria can include prolonged uncovering of fuel assemblies with no possibility of sustained restoration of the water inventory, stresses on the reactor vessel exceeding design basis conditions, injection into the core of a critical volume of insufficiently-borated water, a maximum cladding temperature.

The surrogate criteria adopted to characterise the failure state are documented and justified.

The success state is characterised by sustained control of the reactor safety functions. It can result from the elimination of the initial failure.

II.3.2.2 ACCIDENT SEQUENCE STUDY TIME

Each accident sequence is studied for the time necessary to attain the success state.

For the sake of simplification, a common time can be defined for the majority of the accident sequences (24 hours is generally adopted, if the study does not consider any initiating event of external origin).

In certain cases it is nevertheless necessary to take into account events that would occur inevitably later or failure modes specific to equipment that is not used in the short term.

Shorter times can also be considered, in the case of early attainment of the success state.

The accident sequence study times and the simplifying assumptions adopted are documented and justified. Particular methods such as state graphs(*) can be used for this purpose.

II.3.2.3 DETERMINATION OF SYSTEMS MISSIONS AND OPERATORS MISSIONS

The study of accident sequences can identify the system missions and the operators missions whose failure has an influence on the course of the accident scenario. These missions vary according to the initiating event considered and the state of the installation:

- The mission of each system is thus clearly defined according to the accident scenario; it is characterised by a success criterion(*) representing compliance with functional requirements. Such requirements are usually expressed in terms of configuration, number of trains necessary for performing the function, required values of physical parameters, time during which the function must be performed. For the systems involved in the study, the corresponding functional requirements and the mission success criteria are documented and justified.

- In most cases, the success of an operator mission corresponds to the execution of an appropriate action within a given time. The failure of an operator mission can also be due to an inappropriate action. Studies of the thermohydraulic course of an accident sequence can determine the maximum time available to the operators to perform the action considered in order to satisfy the success criterion, or define the consequences of an inappropriate action and possibly the time available for its recovery. The operators missions adopted and the associated success criteria are documented and justified.

The assumptions used in the PSA for generating and quantifying accident sequences must be as realistic as the state of knowledge allows. Insofar as possible, the introduction of excessively conservative assumptions should be avoided, as they can distort the prioritisation of the sequences or the assessment of possible improvements.

In the case where knowledge is insufficient for informed rulings on the success criteria involved in sequences of significant frequency, sensitivity studies are carried out.

II.3.2.4 PHYSICAL CALCULATIONS ASSOCIATED WITH ACCIDENT SEQUENCES

The determination of the success criteria of systems missions and operator missions is generally based on the results of physical calculations.

The realism requirement applies both to the physical studies used for support and to the consistency between the sequence of events concerned by the probabilistic quantification and the sequence of events concerned by the support study (usually thermohydraulic). It is thus necessary to conduct a certain number of physical studies specific to the PSA, the deterministic studies included in the safety report being conducted with generally conservative conventional assumptions.

Use of the most probable values of physical parameters (initial conditions and boundary conditions) is generally accepted. Sensitivity studies should be carried out to make sure that there are no “cliff effects” when these parameters vary around the chosen values. If a cliff effect is observed, more detailed modelling is necessary.

Moreover, in certain cases conservative assumptions cannot be avoided, for example to allow for lack of knowledge in a given area. If available knowledge for an accident sequence is insufficient to demonstrate that core damage can be avoided, the value of carrying out further developments must be assessed, given its probability, and the sequence must be considered to lead to core damage, if necessary.

II.3.2.5 PROCESSING OF DEPENDENCIES

There may be dependencies between an initiating event and the events (systems missions, operator missions) considered in the event trees, or between the events themselves. These dependencies are of two types:

- functional dependencies; the events representing system missions are generally modelled by fault trees; components, parts of systems or support systems(*) may be common to several systems; the probabilities of these events are therefore not "independent",

- temporal dependencies; the startup time of a system and its operating time may depend on the time between failures or the downtime of another system.

PSA deals with both these types of dependency; the simplifications applied are documented and justified.

II.3.2.6 PROCESSING OF RESTORATIONS

In order to establish realistic scenarios, including in the case of sequences for which core damage occurs in the medium or long term, the various restoration(*) options should be taken into account, whether they involve repair of components of a system, failure of which contributes to the initiating event or aggravates its consequences, or a manual intervention to implement the appropriate strategy.

The time between system failure and core damage can be used in the PSA to process the repair of one of the systems whose failure is involved in the accident sequence studied.

II.3.2.7 EVENT TREE SIMPLIFICATION

Neglected scenarios are subject to justification considering both their frequencies and their consequences.

II.3.3 ANALYSIS OF SYSTEM MISSIONS

The study of accident sequences identifies the list of system missions that should be analysed.

For each mission of a system modelled in the PSA, involved either in an accident sequence (refer to para. II.3.2.3) or as an initiating event, different combinations of failures which cause the failure of the mission considered are identified and the corresponding probabilities are determined.

Each system is modelled from a certain number of input data parameters: the missions in which it participates, the identification and the role of its various components, its configurations in

normal, incident or accident situations, the testing and maintenance of the equipment, its functional limits, its interfaces with the other systems, its physical environment.

The level of detail of the modelling depends on the planned applications.

The probability of failure of a mission is assessed during the quantification of the sequences. The failure of a mission is characterised by the fact that the success criterion is not satisfied.

II.3.3.1 FAILURE ANALYSIS

For each system considered, the plant operator identifies the failures of the equipment and components, active or passive, affecting the operational character of the system. This process requires thorough knowledge of the system and its operation. It can be accomplished by a failure mode and effects analysis(*) (FMEA).

The following points are examined in particular:

- pre-existing faults (following a human error, for example incorrect system reconfiguration after periodic testing, or a hardware failure),
- component common cause failures(*),
- equipment common to several systems,
- time-related failures, such as depletion of a water inventory over time,
- equipment implementation conditions (automatic controls or manual actions),
- system configurations likely to lead to equipment failures in the system or in connected systems,
- impact of operation on the availability of equipment (test and maintenance procedures, technical specification stipulations, normal or emergency operating procedures),
- restoration options.

Operating experience (events occurred in the system or in systems of other plants) is examined as part of this analysis.

II.3.3.2 *MODELLING METHOD*

The modelling methods identify the event combinations leading to failure of the considered mission and quantify the corresponding probabilities.

The fault tree(*) method is the classic method. It is used for cases where equipment is operating with active redundancy (simultaneous operation) and for components considered to be non-repairable. In the more complex cases (equipment operating with passive redundancy (normal-backup), processing of consecutive configurations or operating modes, restoration of failed equipment, time-related dependencies), it may be judged necessary to use other types of modelling, such as state graphs.

The method employed is documented and justified, in particular where methods such as fault trees are used for dealing with complex cases. Specific studies can be conducted to validate or justify the simplifying assumptions used in the reference PSA.

II.3.4 QUANTITATIVE INPUT DATA

The data necessary for PSAs can be divided into several categories:

- operating data, such as the mean times of the standard states(*) of the reactor, the equipment downtimes in these different states (for corrective maintenance, for preventive maintenance or for periodic equipment testing),
- frequencies of initiating events and the associated restoration times,
- equipment reliability data,
- failure probabilities of equipment operating outside its qualification conditions,
- data related to common cause failures,
- data specific to human factors.

The uncertainties associated with the most important data are identified and quantified.

II.3.4.1 GENERAL INFORMATION ABOUT DATA COLLECTION METHODS

II.3.4.1.1 OPERATING REACTORS

For operating reactors, preference is given to the use of operating experience from French installations.

To generate representative reliability data for PSAs, the plant operator sets up an organisation for on-site collection of raw data and identification of all the elements describing the observed anomalies and failures. The total operating times of the equipment and the number of times it is used are recorded. Examination of the raw data is supplemented by an analysis to identify the observed or potential common cause failures.

Data collection concerns all the equipment that has a significant impact on core damage frequency.

In the absence of sufficient French operating experience, other methods are employed.

International data banks can be consulted. For example, they can be used to estimate the frequencies of infrequent initiating events using worldwide operating experience. Critical analysis of the data contained in this type of data bank is nevertheless necessary.

In the case of absence of representative data for an equipment item, the χ^2 distribution at a 50% confidence level or expert opinions(*) can be used to estimate the reliability data. The estimates and the associated uncertainties are documented.

II.3.4.1.2 FUTURE REACTORS

For PSAs conducted for the design of future reactors, in the absence of proven data, a reliability database is compiled using data obtained from operating experience for similar equipment (case of a reactor of evolutionary design) or from international data (case of a new type of reactor).

II.3.4.2 *OPERATION PROFILE*

II.3.4.2.1 OPERATING REACTORS

For operating reactors, the operation profile used in the PSA incorporates the mean times spent in the different standard states and the frequencies of certain operation transients.

The profile is determined from the operating experience of reactors observed over the most recent years, taking operating changes into account. Once changes in operating procedures have been decided, it is accepted that they be considered in the reference PSA.

The plant operator keeps very infrequent reactor states in the PSA if the hazard associated with such states can be significant.

II.3.4.2.2 FUTURE REACTORS

For PSAs conducted in the design of future reactors, the operation profile used in the study is a predicted profile. Its basis includes operating experience of recent reactors, predicted times between refuelling operations and reactor outage scheduling.

II.3.4.3 QUANTIFICATION OF INITIATING EVENT FREQUENCIES

Initiating events are divided into three categories:

- frequent initiating events, observed regularly in French reactors,
- rare initiating events, observed at least once in French or foreign reactors,
- hypothetical initiating events, which have never occurred anywhere in the world.

The method for calculating the frequency of an initiating event depends essentially on which of the above categories the event belongs to.

For frequent initiating events, French operating experience should be used. Depending on the initiating event concerned, data relating to a reactor type or data relating to all French reactors are used. The data are more robust the longer the observation period. Nevertheless, if justified, certain observation periods can be excluded, to take into account changes introduced in reactor operating or changes in the state of the equipment.

For rare initiating events, the values used are determined on the basis of worldwide operating experience, taking into account specific features of design, manufacturing and installation and the operating and in-service monitoring rules of French reactors.

For hypothetical initiating events, the values are estimated by expert opinions, based as a general rule on design studies, taking into account the worldwide absence of observations and the values used in foreign PSAs.

In addition, for certain types of initiating events resulting from system failures, the frequency of the initiating event is calculated as the combination of the corresponding elementary failures, using the method described in paragraph II.3.3.

Finally, for a given initiating event, different hourly frequencies can be used for different reactor states; here again, the corresponding values are documented and justified.

II.3.4.4 *EQUIPMENT RELIABILITY DATA (INDEPENDENT FAILURES)*

For each equipment item in a system modelled in the PSA there are associated failure modes likely to lead to the failure of the system missions.

Depending on the equipment considered and the predicted failure modes, the following reliability parameters should be determined: demand failure rate, operating or standby failure rate, unavailability rate, time to repair, together with the associated uncertainties.

Membership of an equipment family is defined for any given equipment item in order to enable statistical evaluation of the reliability parameters, based on considerations of the technological and functional characteristics of the equipment, and also on the observation period. Justification is provided for the relevance of the samples used (relevance being judged according to sample representativeness).

The raw data collected on site are used to distinguish critical failures of an equipment item (failures leading to failure of the function assigned to it in the mission of a system) from non-critical failures (partial failures, damage not preventing the accomplishment of the function). It should be noted that the critical character of failures is sometimes difficult to assess, and certain failures considered as non-critical can be included, for the estimation of the failure rate, with weighting by a factor representing an estimate of the probability of their criticality. The choice of the failures included and the weighting factors used is documented and justified.

When a major design or operating change has been applied to an equipment item that has been affected by a declared failure, and this change is judged effective on the basis of operating experience or, failing this, by predictive analyses, the failures and the cumulative operating times to be taken into account should be reassessed. The plant operator provides justification for the new estimate of the reliability parameter.

II.3.4.5 RELIABILITY OF EQUIPMENT OPERATING BEYOND ITS QUALIFICATION CONDITIONS

In certain accident sequences, equipment is subject to demands beyond its qualification conditions. The data obtained from operating experience are then no longer applicable and, in the absence of data, justifications or the possible existence of margins in their qualification, the equipment is considered as failed.

However, if the impact of this failure on core damage frequency is significant, tests or studies should be carried out, and expert opinions should then be obtained to determine a realistic failure probability and the associated uncertainty.

II.3.5 COMMON CAUSE FAILURES (IDENTIFICATION AND QUANTIFICATION)

The failures designated by the term “common cause failures” are failures that can affect several components simultaneously or during the course of the mission and which have the same cause, for example an error in design, manufacture, installation or assembly, a maintenance error, or an effect of the environment.

The consequences of failures of support systems (supplies of electricity, compressed air, heat sinks, etc.) and the internal or external events leading to the failure of several equipment items are not included in this definition and are dealt with elsewhere.

Failures related to incorrect equipment configuration are not considered to be common cause failures.

Determination of the common cause failure rates has two major steps: identification of components for which common cause failures can be considered, and the acquisition of data.

First, the groups of equipment likely to be the location of common cause failures should be selected. This selection is based on analysis of operating experience and on theoretical analysis of the consequences of cumulative failures.

In practice, the selection of these equipment groups brings together, as a minimum, identical equipment items of a given system performing the same function under comparable conditions.

So, depending on the type of dependency identified, common cause failures that can affect the equipment on demand or when operating, according to the equipment considered, are included in the study. It is also necessary to examine, for “normal-backup” operation of equipment, whether certain dependencies are likely to cause simultaneous failure of the operating component and refusal of the standby component to start up.

To obtain common cause failure rate values, analysis of available operating experience data is necessary. Given the rareness of common cause failures that have actually occurred, the observations can be extended to events revealing potential failures of this type. Use can also be made of international data collections. To estimate the associated values, appropriate adjustments should be made.

II.3.6 ASSESSMENT OF HUMAN RELIABILITY

The method selected for assessment of human reliability must be consistent with the state of the art and comply with the rules below, related to the following aspects:

- analysis of human reliability in normal operation,
- analysis of human reliability in accident operation,
- acquisition of quantitative data,
- human reliability in PSAs conducted in the design of future reactors.

II.3.6.1 ANALYSIS OF HUMAN RELIABILITY IN NORMAL OPERATION

Human actions involved in normal operation are divided into two categories:

- one category includes actions contributing to equipment unavailability, for example incorrect setting of a sensor or incorrect positioning of a valve; such actions are modelled in the systems analysis,

- a second category includes human actions that can lead to an initiating event. They should be identified as completely as possible, using operating experience together with analysis of normal operating procedures, tests and maintenance. These actions are considered in the estimation of the frequency of the initiating event concerned.

Particular attention is paid to the processing of recovery from errors and dependencies between errors for the actions of these two categories, depending on the information available to the operators.

II.3.6.2 ANALYSIS OF HUMAN RELIABILITY IN ACCIDENT OPERATION

Study of the accident sequences helps to identify the operator missions whose potential failures should be analysed qualitatively and quantitatively (refer to paragraph II.3.2.3).

The number of operations that must be completed by the operators following an accident is often very high. Nevertheless, only a few of these operations have an effect on the course of the accident scenario; they are modelled in the operator missions. The failure of an operator mission may be a consequence of incorrect execution of an appropriate action or of execution of an inappropriate action.

Analysis of an operator mission and quantification of its failure take the following main parameters into account:

- the time available to accomplish the mission,

- the time necessary to accomplish the mission,

- the difficulty and complexity of the mission,

- the stipulated operating procedures,

- the man-machine interface,

- the operating documents associated with the design basis state and the general operating rules,

- the training of the personnel involved,

- the organisation of operations,

- the environmental factors (smoke, heat, radioactive conditions, etc.).

Furthermore, particular attention should be paid to the specific context of the accident sequence during which the operator mission is executed, in order to reinforce the realism of the study. Finally, the dependencies between the various operator missions identified for the accident sequence and the options for recovery from their failure are examined.

In certain cases, quantification can lead to results that are highly sensitive to small changes in certain parameters (“cliff effect”). Detailed quantifications of the situations to be differentiated should then be obtained.

The options adopted in the analysis of operator missions and the quantification of their failure are documented and explained.

II.3.6.3 ACQUISITION OF QUANTITATIVE DATA

For the acquisition of quantitative data and the estimation of the associated uncertainties, the following information sources should be used, in order of preference: plant operating experience, observations obtained on simulators, international data and expert opinions.

The method of analysis and quantification of the failure of operator missions in accident situations requires full-scale simulator testing.

The information sources used should be documented and their pertinence justified, in particular for the use made of tests performed on simulators.

II.3.6.4 HUMAN RELIABILITY IN PSAS CONDUCTED IN THE DESIGN OF FUTURE REACTORS

For PSAs conducted in the design of future reactors, some important data such as operational procedures, operation organisation, simulator studies or the man-machine interface are not available. It is nevertheless desirable that the human reliability assessment reflect at least the major options adopted by the designer of these reactors in areas related to operation and human factors.

II.3.7 ACCIDENT SEQUENCE QUANTIFICATION METHOD

The quantification takes into account the complexity of the models, and the determination to carry out as realistic and complete an assessment as possible, but also the need to obtain a model that can be used easily. The choice of the method results from a compromise between the quality of the study and its flexibility of use.

The general principle of all the existing methods is to link the various established models (system mission analysis models, scenario representation models) to obtain an overall quantification from quantitative input data. Within this scheme there is no single solution for the quantification, but rather different options which can be chosen according to the application considered.

The “Boolean merge” method consists in representing the systems by fault trees and combining them, for each sequence identified in the event tree, into a logic model to assess the associated core damage frequency. This approach facilitates the processing of functional dependencies, such as the integration of support systems. Nevertheless, dynamic aspects such as normal-backup operation or the consideration of restorations can only be processed by approximations.

The numerical sequencing method consists in calculating the failure probabilities of the system missions and operator missions separately, then incorporating the numerical results into the sequence frequency calculations. This approach requires an a priori analysis of the functional dependencies. It takes dynamic aspects into account (for example using state graphs). It is

generally limited to specific cases, such as for validating the approximations made in a simpler model.

The methods employed and the simplifications introduced are documented and explained. In particular, the processing of dynamic aspects must be justified.

II.3.8 EXTENSION OF LEVEL 1 PSA: GROUPING OF ACCIDENT SEQUENCES ACCORDING TO THE MAGNITUDE OF THE ASSOCIATED RELEASES

A specific study enabling the extension of level 1 PSA consists in grouping level 1 accident sequences according to the magnitude of the releases that might result from such sequences.

Although these groups are not release categories, they nevertheless supply information on the releases that might result from the different accident sequences. For example, they can contribute to prioritisation of the accident sequences leading to core damage, particularly as part of the reactor periodic safety review.

These groups may be preceded by additional development of the level 1 PSA event trees so that they take into account the state of the systems and equipment participating in maintaining reactor containment or in control of releases.

The accident sequences are grouped according to characteristics that have an effect on the magnitude of the associated releases, for example:

- the state of the containment function, in particular the possibility of containment bypasses,
- the possibilities of controlling the accident or limiting its consequences, by means of systems or actions intended for that purpose,
- the level of loading of the reactor coolant system during core damage,
- the state of systems for transferring part of the after-power outside the containment.

II.3.9 USE OF THE RESULTS

II.3.9.1 EXPECTED RESULTS

The reference PSA gives the frequencies of sequences leading to core damage and the values of a certain number of quantities useful for the application of the results.

For each reactor state, the contributions of the initiating events and the accident families, the core damage hourly frequency and the list of predominant sequences are determined.

To supplement the presentation of the predominant sequence frequencies, other results can be generated using PSAs. For example, the determination of certain importance factors(*) can be used to prioritise the contributions of equipment or operation actions, or to assess the severity of certain failures.

The results of the reference PSA are not limited to just the raw results supplied by the software used for quantification. The set of results, and particularly those related to the predominant sequences, is

accompanied by a review of the main assumptions and a highlighting of their effect on the results. The interpretation is based on the results of sensitivity studies, among other factors.

II.3.9.2 UNCERTAINTIES

The main uncertainties are identified and the impact of these uncertainties on the results is assessed quantitatively or qualitatively. Several means can be employed to do this: uncertainty calculations, studies of sensitivity to data or assumptions having a major impact on the results or, as a minimum, qualitative identification of the major sources of uncertainties.

Identification and assessment of these uncertainties are used to target the points on which the precision of the studies should be improved.

This assessment concerns not only the overall result of the study, but also the predominant sequences and, more generally, each result used within the context of an application.

The uncertainties of the results related to the quantitative input data are distinguished from those related to simplifications and assumptions.

For the uncertainties related to the most important quantitative input data, Monte Carlo simulation(*) can be used to obtain the uncertainty of an overall result.

The uncertainties generated by the simplifications and inherent in the assumptions made for modelling and quantification include the initiating event grouping choices, the choices of scenarios for the supporting thermohydraulic and neutronics calculations, the uncertainties of the results of these calculations, the uncertainties related to knowledge of the phenomena, the uncertainties related to the modelling of human actions, to the simplified modelling and the estimation of software reliability, to the estimation of the reliability of equipment operating beyond its qualification conditions, and to the choice of probabilistic methods. The variation of the results according to the principal simplifications and assumptions is assessed by means of sensitivity studies.

II.3.9.3 PSA LIMITS

Despite systematic determination of accident scenarios, PSAs have identified limits in terms of completeness. The level of completeness is assessed according to the complexity of the models, the difficulties associated with quantification and with respect to the use of the results.

Incompleteness concerns, for example:

- the scope (lack of processing of internal fire or flooding events or external events),
- the choice of human interventions processed in the PSAs,
- the definition of the component families affected by the common cause failures (common cause failures affecting components belonging to different systems not being processed in all cases).

The impact of study incompleteness cannot usually be assessed quantitatively. Nevertheless, its assessment contributes to defining the limits of the scope of PSAs.

II.3.9.4 PRECAUTIONS WHEN USING PSA RESULTS

The uncertainties and the limits associated with PSAs mean that certain precautions must be taken when interpreting the results and using PSAs in the decision-making process.

Primary importance must be given to assessing whether the use of PSAs is pertinent when making a decision.

It should be noted that the state of the art in PSA development is evolving constantly. This evolution is aimed mainly at reducing all types of uncertainties and limits. Changes in the state of the art will be taken into account when PSAs are updated.

II.3.10 DOCUMENTATION AND QUALITY

The plant operator documents all the technical content of the study to ensure its traceability and facilitate analysis. In particular, the results of the reference PSA and the uncertainty assessments and the sensitivity studies are laid out in a clear and legible manner to enable detailed external review of the PSA.

The following should be clearly described or referenced:

- the state of completion of the installation, the organisation of its operation and the other technical elements impacting the study,
- the information sources and the analyses necessary for the establishment of the assumptions and the data,
- the methods used, and in particular the process used for questioning experts and using their answers.

The plant operator applies its quality system for conducting a reference PSA (in particular with regard to input data review, definition of output data, generation of results, design review).

This quality system must satisfy the requirements of the order of 10 August 1984 on the quality of design, construction and operation of basic nuclear installations.

II.4 APPLICATIONS OF PSAs

II.4.1 PERIODIC SAFETY REVIEW

II.4.1.1 USEFULNESS OF THE APPLICATION WITH REGARD TO SAFETY

II.4.1.1.1 GENERAL PROCEDURE

The periodic safety review procedure, applicable to existing reactors, is a periodic process implemented for a given reactor type, which incorporates recent operating experience and updated knowledge.

In the first step, the periodic safety review procedure aims to demonstrate the conformity of the "reference plant situation" with the "safety reference system". The "safety reference system" consists of all the safety rules, criteria and specifications applicable to a reactor type resulting from the safety analysis report. The "reference plant situation" consists of the state of the installation and its operating conditions. Any observed deviations are corrected or justified.

In the second step, the safety reference system is assessed. The assessment is based on an analysis of national or international operating experience or on special studies, and on examination of the provisions adopted on the most recent reactors. Corrections may be incorporated into the safety reference system; the reference plant situation is updated if necessary.

II.4.1.1.2 CONTRIBUTION OF PSAS

In application of the general procedure, PSAs are used during the periodic safety review to assess the core damage frequency and its change compared with the assessment made on completion of the previous review, including an analysis of the changes in system characteristics (equipment reliability, for example) and in operating practices.

In addition, identification of the main contributions to the core damage frequency highlights any weak points for which design and operation changes can be studied, or even judged necessary. They can be ordered so as to target the priority work.

II.4.1.2 METHOD

During the first step of the periodic safety review, the reference PSA is updated, incorporating the most recent operating experience (identification and frequency of initiating events, equipment reliability data, operating profile), the standard construction condition (design and operation) and new knowledge about the behaviour of the installation obtained from the most recent studies.

An acceptable method for highlighting and prioritising the principal contributions to the core damage frequency consists in grouping elementary sequences with similar functional characteristics into "functional sequences", then assessing the hazard associated with the latter. The priority of the grouping method is to constitute "functional sequences" whose frequency and consequences could be reduced by implementing a given provision in order to optimise the identification of opportunities for improvement.

The scope of the reference PSA and the grouping into functional sequences are likely to change at each periodic safety review.

Following the periodic safety review, a new version of the reference PSA is produced, taking into account the changes decided on completion of the review process.

II.4.1.3 PSA CONTRIBUTION TO THE DECISION-MAKING PROCESS

For the PSA scope considered, assessment of the overall core damage frequency is an element which can be used to estimate the change in safety level compared with the assessment made after the previous review.

This assessment is supplemented by an analysis of the principal contributions to the core damage frequency (for example an analysis of the predominant functional sequences); selection thresholds in terms of calculated core damage frequency can be chosen for this purpose. In particular, the analysis must take into account the frequency of the sequences, the possible consequences on containment integrity and the uncertainties.

After review of any conservative assumptions of the PSA, this analysis results either in a status quo or in an indication of the usefulness of implementing design or operation changes. In the case where changes are made, PSAs can be used to assess the advantages and drawbacks of the various solutions considered. The satisfactory character of such changes must be demonstrated by an analysis of their impact on the contributions to the core damage frequency and on the overall core damage frequency.

II.4.2 PROBABILISTIC EVENT ANALYSIS

II.4.2.1 USEFULNESS OF THE APPLICATION WITH REGARD TO SAFETY

The application forms part of the overall operating experience analysis process, one of the main objectives of which is to limit the frequency of significant safety-related events. Conventional methods for analysis of event causes are used mainly to define corrective measures in order to meet this objective.

Moreover, one of the principles of operating experience analysis is that events must undergo appropriate processing with respect to their severity in terms of actual or potential consequences. As most of the analysed events have low or zero actual consequences, it is important to have tools for analysing the potential consequences of such events in order to identify the events which, under less favourable circumstances or following accumulation of other failures, could lead to core damage or major releases, and to define priorities for the implementation of corrective measures decided within the framework of operating experience analysis.

The usefulness of the probabilistic approach has two main aspects:

- analysis of the potential consequences is based on the most systematic and realistic possible investigation of degradation scenarios, which leads to greater completeness of the situations studied,

- probabilistic assessment also supplies quantitative information on the probability of such scenarios.

The main objectives of probabilistic analysis of events are the prioritisation of events according to the conditional probability of core damage and the assessment of the pertinence of the corrective actions.

These main objectives are supplemented by two other objectives: enrichment of the safety culture of the plant operator (dissemination of the lessons of PSAs based on analysis of events that have occurred on the sites) and PSA improvement (comparison of models with the course of actual events).

II.4.2.2 METHOD

The application consists of the qualitative and quantitative assessment of the potential consequences of certain events that have actually occurred, selected according to a documented and justified method. For such events the analysis identifies the different potential degradation scenarios and quantifies their conditional probabilities.

In the general case, the analysis is performed on the basis of the reference PSAs. However, specific studies can be used or developed to take into account the specific features of the event (for example, extended equipment unavailabilities necessitating the development of a model suitable for dealing with repairs).

Not all events are easily analysable with the reference PSAs or with specific studies, for example:

- events involving out of normal operating conditions or the exceeding of certain physical parameters defined in the technical specifications, for which the use of PSAs would be inappropriate,
- certain equipment degradation without critical failure, for which the quantification would be too uncertain.

For the analysed events, a detailed description and a full examination of the actual consequences of the event identify the degradations, the failures and the inappropriate actions which have actually occurred. The potential consequences of the event are then analysed using the accident sequences modelled in the PSAs.

The probabilistic assessment leads to a calculation of the conditional probability of core damage under the conditions of the event. This probability is a “measurement” of the difference separating the actual event from core damage.

The analysis is developed in two possible directions (which may be combined), according to the type of event to be analysed:

- for “initiating” events, the analysis consists of an assessment of the probability of failure of the lines of defence limiting the consequences of the event,
- for “degradation of a line of defence” events, the analysis consists of an assessment of the probability of all the scenarios making use of this line of defence.

The quantitative results obtained from these analyses must be interpreted with caution, because of the associated uncertainties. These uncertainties are of two sorts:

- uncertainties related to the PSA data and assumptions (refer to paragraph II.3.9.2),

- uncertainties specific to event analysis, for example the pertinence of the PSA assumptions in a particular incident situation.

In consequence, any analysis is accompanied by the identification of the principal modelling assumptions and includes a section providing information on the “robustness” of the analysis. This section may include a sensitivity study on the assumptions that have a significant impact on the result.

Although in the general case the consequence considered is core damage, specific consequences (for example, recriticality) can be assessed, which may necessitate the use or the development of specific studies.

II.4.2.3 PSA CONTRIBUTION TO THE DECISION-MAKING PROCESS

When the conditional probability of core damage associated with an event is greater than a defined reference value, the event is called a “precursor event” and is subject to a thorough analysis.

For the most important precursor events, the plant operator defines specific processing and lead times for the implementation of corrective measures. If possible the expected improvement is assessed.

The results obtained are not used on their own: they are only one of the elements contributing to the taking of the decision to implement a corrective measure.

II.4.3 DESIGN OF FUTURE REACTORS

II.4.3.1 USEFULNESS OF THE APPLICATION WITH REGARD TO SAFETY

As for the operating reactors, demonstration of the safety of the design of future reactors is based on deterministic studies. For the new generations of reactors, PSA is used as a supplemental tool in safety assessment during the design phase.

The contributions of these assessments include the following:

- help with the design of safety systems, particularly in terms of redundancy and diversification,
- verification of a balanced design of reactor safety related to the absence of scenarios having a predominant contribution to the frequency of core damage,
- estimation of the deviations with respect to the safety requirements applied to operating reactors,
- comparison of the level of safety of the future reactor with that of operating reactors or of other reactors under development,
- help with the definition of operating conditions related to multiple failures,

- preliminary assessment of the safety improvement resulting from the planned measures in the case of a severe accident,

- participation in the demonstration that the sequences leading to large early releases are practically eliminated.

II.4.3.2 METHOD

During the design of future reactors, PSAs are developed in consecutive steps throughout the reactor development cycle: they are enriched as the design studies advance.

In the design phase, a minimal reference PSA covers all the accident situations of internal origin which, in view of the PSAs conducted on operating reactors, are considered to be important for safety.

Extension of its scope can supply an assessment of the frequency of sequences leading to core damage, throwing light on the potential consequences of the different core damage situations on the containment function.

The acceptable methods for conducting these PSAs are those described in paragraph II.3. The principal specific features are as follows:

- the functional analyses of the accident scenarios are limited by the level of detail of the information available on the behaviour of the installation and on the changes in the physical parameters,

- the reactor operating profile is estimated from predictive studies of reactor outages, scheduled and unscheduled,

- in the absence of precise knowledge of the equipment that will be installed, the reliability database is compiled using data obtained from operating experience for similar components or from international data,

- similarly, generic common cause reliability data are used in the PSA, unless specific data are available,

- in the absence of precise knowledge of accident operation (procedures, man-machine interface, shift organisation), the probabilistic analysis of human reliability is simplified; in particular, it may be based on international predictive models,

- in the absence of a detailed maintenance programme, the equipment unavailabilities due to preventive maintenance operations can be processed in the reference PSA in a generic manner. Specific sensitivity studies are then carried out to assess the impact of maintenance work on the results.

These specific features introduce large uncertainties into the PSA results. The methods applicable for assessment of the uncertainties are described in paragraph II.3.9.2.

II.4.3.3 PSA CONTRIBUTION TO THE DECISION-MAKING PROCESS

Assessment of the overall core damage frequency is an element in appraising the level of safety of the design, and in particular the improvement compared with operating reactors. Reference values

are used to analyse the PSA results; they must be considered as orders of magnitude, and must not be the only elements of appraisal of the results.

The qualitative and quantitative analyses of the main contributions can be used to:

- identify arrangements supplementing the deterministically-defined design basis to reduce the frequency of certain functional sequences and to limit their consequences with regard to loss of the containment function,
- help with the definition of particular requirements for attaining a satisfactory level of reliability for the most important equipment,
- contribute to the design of operational procedures and to the training of operators, taking into account operation actions which, if they fail; may lead to a significant increase in the frequency of core damage.

II.4.4 IMPORTANCE OF SYSTEMS AND EQUIPMENT WITH REGARD TO SAFETY

II.4.4.1 USEFULNESS OF THE APPLICATION WITH REGARD TO SAFETY

PSA is an element, among others, used to identify:

- the systems playing a major role with regard to safety; for such systems, improved operation can in principle contribute the most significant safety improvements and maintain their reliability at a satisfactory level,
- the critical failure modes of the equipment; these are the failure modes whose occurrence might have consequences on the safety of the installation and whose frequency should be limited.

In particular, this approach can be used in the definition of technical specifications, periodic tests or equipment maintenance programmes.

II.4.4.2 METHOD

II.4.4.2.1 IDENTIFICATION OF SYSTEMS PLAYING A MAJOR ROLE WITH REGARD TO SAFETY

Systems playing a major role with regard to safety are identified, using PSAs, by assessing their contribution to the frequency of core damage (relative importance of accident sequences in which the system is involved).

II.4.4.2.2 IDENTIFICATION OF CRITICAL FAILURE MODES WITH REGARD TO SAFETY

To identify and prioritise the failure modes of equipment considered in the scenarios leading to core damage, two importance factors are generally used: the “risk reduction worth” (RRW) and the “risk achievement worth” (RAW).

The risk reduction worth is the relative decrease in the frequency of core damage if the probability of the failure mode is considered to be 0.

The risk achievement worth is the relative increase in the frequency of core damage if the failure of the equipment is considered to be certain.

These two importance factors are complementary. The RRW is a direct function of the reliability of the equipment; it can be used to assess the contribution of the failure mode to the frequency of core damage. The RAW is a measure of the importance of the function performed by the equipment. It identifies the equipment playing a major role with regard to safety, even if the failure rate of such equipment is very low.

II.4.4.3 PSA CONTRIBUTION TO THE DECISION-MAKING PROCESS

PSAs are a decision-making aid for assessing the importance for safety of systems and equipment.

Depending on the type of use, thresholds can be defined to identify:

- systems playing an important role with regard to safety according to their contribution to the frequency of core damage,
- the critical failure modes of equipment.

II.4.5 OPERATION TECHNICAL SPECIFICATIONS

II.4.5.1 USEFULNESS OF THE APPLICATION WITH REGARD TO SAFETY

II.4.5.1.1 GENERAL PROCEDURE

The general objective of the technical specifications is to define the minimum rules that must be obeyed during normal operation of the reactor in order to maintain the reactor within the scope of the studies of the safety analysis report.

They thus have the role of:

- defining the normal operating limits of the installation in order to remain within the reactor design and design-basis assumptions,
- requiring the availability, depending on the state of the reactor considered, of systems or equipment necessary for the accomplishment of the safety functions essential for the monitoring, protection and maintenance of barriers and for the operability of the incident or accident operation procedures,
- stipulating the rule to be applied in the case of unavailability of a required system or equipment item, or if a normal operating limit is exceeded, which, depending on the case, may consist in imposing a maximum time to repair in the reactor state in which the unavailability occurred or limiting the authorised time for maintaining the reactor in its state before changing to a “fallback” state, which is a reactor state in which either the equipment is no longer required or the unavailability of the equipment is judged to have less impact on reactor safety.

II.4.5.1.2 CONTRIBUTION OF PSAS

For the definition of the required systems and equipment as stipulated by the technical specifications, the probabilistic approach can be used to verify the provisions adopted for operation.

PSAs can throw light on the best operating procedure to implement in the case of unavailability of equipment required in the technical specifications and prioritise the requirements according to the importance of the potential unavailabilities for safety.

PSAs can assess the increase in the frequency of core damage for all the states of the reactor, given the unavailability or unavailabilities considered, and during the transients when switching from one state to another.

PSAs can also be used by the plant operator when requesting authorisation for carrying out specific work and/or for operating in a reactor state that does not conform to the technical specifications, in order to demonstrate that the consequent increase in core damage frequency is limited, taking into consideration any palliative measures that the operator plans to implement.

II.4.5.2 METHOD

The method consists in assessing the increase in the frequency of core damage assuming that the equipment studied is unavailable.

It is necessary to verify that, in the reference PSA, the functional analysis and the modelling adopted in the different reactor states are sufficiently consistent for the needs of the application. In practice, certain simplifications introduced into the reference model may not be relevant for the application considered. It may be necessary to develop specific studies.

II.4.5.3 PSA CONTRIBUTION TO THE DECISION-MAKING PROCESS

The usefulness of requiring the availability of an equipment item in the technical specifications for a given reactor state can be assessed on the basis of the increase in the frequency of core damage when the equipment is considered to be unavailable throughout the duration of the state. Other elements must nevertheless be considered in the decision-making, such as the need to be able to carry out equipment maintenance in certain reactor states.

Probabilistic assessments must be considered as guidelines. The determination of maximum times to repair and fallback times and states must also take into account certain maintenance and operation requirements such as the time needed to undertake and complete repair work under good conditions. Moreover, in the technical specifications, very long equipment unavailability times should be avoided if the equipment can be repaired in much shorter times.

With regard to requests for waivers from the technical specifications, the plant operator must provide evidence that, given the conditions related to the work, and in particular the implementation of any palliative measures, the resulting increase in the frequency of core damage is small; a reference value is used as assessment criterion.

GLOSSARY

Accident sequence

Common cause failures

Core damage

Design-basis operating conditions

Event tree

Expert opinion

External hazard

Failure mode

Fault tree

FMEA

Importance factor

Initiating event

Internal hazard

Monte-Carlo simulation

Restoration

Safety function

Standard state

State graph

Success criterion

Support system

Accident sequence

An accident sequence is a sequence of events starting with an initiating event followed by events corresponding to the failure or the success of system or operation missions.

An accident sequence can lead either to a success situation (sustainable control of the safety functions) or to a failure situation (occurrence of an undesired consequence).

Common cause failures

Common cause failures are failures that can affect several components simultaneously or during the course of the mission, and which have the same cause, for example an error in design, manufacture, installation or assembly, a maintenance error, or an effect of the environment.

The consequences of failures of support systems (supplies of electricity, compressed air, heat sinks, etc.), failures related to incorrect equipment configuration and the internal or external events leading to the failure of several equipment items are not included in this definition.

Core damage

Core damage is the failure situation used in level 1 PSA. Nevertheless, in practice, core damage is replaced by surrogate criteria introduced to simplify the assessment. Examples include prolonged uncovering of fuel assemblies with no possibility of sustained restoration of the water inventory, stresses on the reactor vessel exceeding design basis conditions, injection into the core of a critical volume of insufficiently-borated water, a maximum cladding temperature.

Design-basis operating conditions

Design-basis operating conditions are the initiating events of the incident or accident sequences used to determine the design basis of the buildings and the systems and equipment necessary to accomplish the safety functions.

These design-basis operating conditions are envelopes, in terms of consequences or incurred loads, for a certain number of initiating events. The list of the design-basis operating conditions is included by the plant operator in the safety analysis report and thus submitted to the authorities for approval.

Event tree

The event tree method is an inductive method consisting in considering systematically, for an initiating event, the success or failure of the operation systems and actions implemented to halt the progress of the incident or the accident.

An event tree is a logic diagram used to define the accident sequences. Each branch of the event tree consists of combinations of success or failure of the operation systems and actions, and corresponds to an accident sequence.

Expert opinion

Opinion of a person, chosen because of his or her competencies, experience, sound judgement and independence, on a technical problem.

In the case under consideration, the call for an expert opinion often concerns the assignment of a probability or a probability distribution to an event for which there are no direct statistics.

External hazard

Event originating outside the installation, either natural or related to industrial or human activity, likely to have effects on the safety of nuclear power plants, such as earthquakes, extreme weather conditions, explosions, aircraft crashes.

Failure mode

A failure mode is defined as the effect by which a failure is observed in an element of the system.

Fault tree

The fault tree method is a deductive method, the objective of which is to determine all the possible event combinations leading to the occurrence of a unique undesired event. These different combinations are represented using a tree structure (logic gates: AND, OR, etc.). This deductive approach is pursued until basic events are obtained, which must be mutually independent and whose probability of occurrence can be estimated (e.g. equipment failures, human errors).

FMEA (failure mode and effects analysis)

FMEA is a qualitative system analysis method used for systematic study of the causes and modes of failures that can affect the components of the system.

In particular, FMEA can identify all the failure modes of the components of a system and assess the effects of each such failure mode on the various functions of the system and the surrounding systems.

The results of the analysis are presented in tabular form.

Importance factor

An indicator which measures the impact of variation of the probability of an elementary event (examples: failure mode of a component, operation action) on the frequency of the undesired event.

Two importance factors are generally used: the “risk reduction worth” (RRW) and the “risk achievement worth” (RAW).

The risk reduction worth is the relative decrease in the frequency of core damage if the probability of the failure mode is considered to be 0.

The risk achievement worth is the relative increase in the frequency of core damage if the failure of the equipment is considered to be certain.

These two importance factors are complementary. The RRW is a direct function of the reliability of the equipment; it can be used to assess the contribution of the failure mode to the frequency of core damage. The RAW is a measure of the importance of the function performed by the equipment. It identifies the equipment playing a major role with regard to safety, even if the failure rate of such equipment is very low.

Initiating event

An initiating event is an event that perturbs the normal operation of the installation, leading to drift of certain parameters of the installation (pressure, temperature, reactivity, etc.) from which an accident sequence may develop.

Internal hazard

Event originating inside the installation, likely to have effects on the safety of nuclear power plants, such as internal fire or flooding.

Monte-Carlo simulation

A numerical method, based on the simulation of histories of the system: random input parameters are fed into the system model, then a solution of the model is obtained for each input, and finally statistical processing is applied to all the results obtained. The Monte-Carlo method is used in two cases: to measure the uncertainty of the results related to reliability model input data and to solve certain reliability models that are too complex for analytical solution (for example: any probability distributions or complex success criteria).

Restoration

The restoration of an initiating event, a system or a function corresponds to:

- the repair of a component whose failure contributes to the initiating event, the system failure or the loss of the function considered,
- the implementation of a palliative strategy (for example establishment of a system which replaces the lost function).

Safety function

The term safety function includes the equipment and systems implemented to avoid degradation of the barriers or to limit the consequences of such degradation. The reactivity, cooling, and containment safety functions and the support functions are distinguished.

Standard state

A standard state of a reactor is defined by a combination of conditions on the power level of the reactor, the reactivity and the means of controlling it, the pressure and the average temperature of the reactor coolant system.

State graph

The state graph method is an inductive method with the objective of building a logic diagram showing the operating and failure states of a system, together with the transitions between these states, due to failures or repair of the system.

When the transition rates are constant, the process is Markovian (Markov graph).

Success criterion

Each system or operator mission taken into account in the assessment is characterised by a success criterion.

In the case of a system mission, the success criterion represents compliance with functional requirements, usually expressed in terms of configuration, number of trains necessary to perform the function, required values of physical parameters, or time during which the function must be performed.

In most cases of an operator mission, success corresponds to the completion of an appropriate action within a given time. Failure of an operator mission may correspond to the completion of an inappropriate action.

The success criteria are generally deduced from the results of thermohydraulic and neutronic calculations.

Support system

In functional terms, a system not directly performing a safety or backup function but without which the function cannot be accomplished.

This category commonly includes: electrical power supplies, the intermediate cooling system, compressed air, ventilation.

II.4.6