Collection de notes internes
de la Direction
des Etudes et Recherches

Production d'énergie (hydraulique, thermique et nucléaire)

APPLICATIONS DES ETUDES PROBABILISTES DE SURETE : BONNES PRATIQUES ET DOCUMENTATION

PSA APPLICATIONS : GOOD PRACTICES AND DOCUMENTATION

98NB00017

EDF
Electricité
de France

RECHERCHES
SERVICE RÉACTEURS NUCLÉAIRES ET ECHANGEURS
DÉPARTEMENT ETUDES DE SÛRETÉ ET DE FIABILITÉ

EDF
Electricité de France

Octobre 1997

DEWAILLY J.
MAGNE L.

APPLICATIONS DES ETUDES PROBABILISTES DE SURETE : BONNES PRATIQUES ET DOCUMENTATION

PSA APPLICATIONS : GOOD PRACTICES AND DOCUMENTATION

Pages : 16

98NB00017

Diffusion : J.-M. Lecœuvre
EDF-DER
Service IPN. Département PROVAL
1, avenue du Général-de-Gaulle
92141 Clamart Cedex

ISSN 1161-0611

SYNTHÈSE :

Nous présentons ce qu'une documentation synthétique des principaux choix stratégiques et hypothèses techniques relatives à une EPS pourrait contenir : comment sélectionner les événements initiateurs internes et externes, comment détailler la configuration de la tranche et l'organisation générale de la tranche et du personnel d'exploitation, comment mettre en évidence les hypothèses relatives aux modèles physiques, etc.

Les propositions faites dans ce document reposent sur l'expérience de la DER en matière d'EPS (construction de modèles EPS, utilisations de ces modèles pour l'exploitation ou la maintenance, outils EPS).

Ce document expose également les différents types de règles ou recommandations relatives à la modélisation EPS pour des applications diverses concernant l'exploitation des tranches nucléaires de production d'électricité. Il est souvent apparu que les EPS existantes soient mal adaptées pour certaines applications. Des adaptations ont été effectuées en vue de les utiliser comme support de décision. Cette expérience acquise nous fait ressentir une forte nécessité de définir plus formellement des bonnes pratiques pour la modélisation et les applications des EPS.

Finalement, la note souligne les principales difficultés rencontrées (utilisation appropriée des incertitudes, communication des résultats de l'EPS à des utilisateurs non-spécialistes) et esquisse des perspectives pour l'avenir.

EXECUTIVE SUMMARY :

In this paper, ~~we show~~ it is shown what the condensed documentation of the main strategic choices and technical assumptions related to a PSA could contain : how to select the internal and external initiating events, how the detail the plant configuration and the general organization of the plant and operating staff, how to highlight the assumptions related to physical models, etc.

The proposals in this documentation are based on the R&D D's experience with PSA (construction of PSA models, use of PSA models for operation or maintenance, PSA tools).

This document also presents different types of rules or recommendations related to PSA modelling for various applications involved in nuclear power plant operating. ~~Existing PSAs are often found to be ill adapted for some applications. Adjustments have been made in order to use them as decision support. From the experience acquired up to now, there is felt to be a strong need to more formally define good practice for PSA modelling and applications.~~

Finally, the paper stresses the main difficulties encountered (appropriate use of uncertainties, communication of PSA results to non-specialist users) and it also outlines some prospects for the future.

I. Introduction. Context

At EDF, since 1990, PSAs have come to be utilized for applications such as reliability centred maintenance (RCM), technical specifications, and analysis of the potential consequences of incidents [1], [2], [3]. Since 1994 the RCM project has aimed at optimizing maintenance choices relating to safety, availability, and costs. In this project, PSAs are used to evaluate the effects of equipment failures on nuclear-power-plant safety equipment. The contribution to risk is measured for each component. This means components can be ranked, and a list of components drawn up, for which preventive maintenance tasks will then be defined. We carried out studies concerning a series of systems that are important in terms of safety, and in 1996 the method was transferred to another EDF Engineering and Construction division which carried out studies for further systems.

The EDF "precursor programme" began in 1993. Its purpose is to complement operating feedback on the most significant incidents by studying them from the point of view of their potential consequences. The method consists in using models made for PSAs to develop the main aggravating scenarios which might have developed out of an incident. Specific lessons can thus be learnt, and the importance of incidents can be evaluated in order to better rank their processing priorities.

Incident analysis and RCM are now emerging from their experimental phase. The know-how has been transferred to other divisions, and PSAs will thus progressively become part of the EDF decision-making process.

II. The need for synthetic PSA documentation

The proliferation of PSA applications may result in PSA being deployed with users who were not involved in the PSA modelling activity. The problem is particularly true at EDF where operational activities (design, operation, maintenance) are distributed over distant geographical locations. The need for PSA documentation is therefore considered to be increasingly important. At EDF, hard-copy and on-line documentation has been developed. The work was mainly carried out on EPS 1300 PSA accident sequences and system studies. Recommendations were proposed on providing clear documentation for PSA users who did not participate in the construction of the models [4].

Synthetic documentation of the main strategic choices and technical assumptions greatly facilitates the appropriation of PSA models and their use for applications. Here, as an example, we present two parts of this guide: the part concerning selection of internal and external initiating events, and the part dealing with detection of the hypotheses concerning physical models.

II.1 Initiating events

II.1.1 How to select internal and external initiating events

An **initiating event** is an event that makes operation deviate from a standard operating state by modifying one or more safety functions (reactivity, cooling, confinement). However:

- if there is no transient, but the Operating Technical Specifications (OTS) are applied, it is not a PSA initiating event. However, this OTS event is taken into account in the modelling of PSA missions (unavailability of equipment or sets of equipment making all or part of a system inoperative).

- A slight transient that can be corrected by automatic control systems is not considered to be a PSA initiating event.

II.1.2 Tracing sources and references for establishing the initial (comprehensive) list

The initial list of initiating events depends in particular on the sources of discharge adopted (core, spent fuel pit, handling, etc.) and the coverage of the initiating events (internal initiating events excluding aggression, etc.). This list must be based on:

- design situations;

- analysis of incidents and accidents already observed on French and foreign reactor units;

- bibliographic search of existing studies;

- results of predictive analysis of systems or accident sequences which reveal certain initiating events.

Documentation: a two-column table:

- 1st column: a list of potential initiating events

- 2nd column: the associated reference(s).

II.1.3 Documenting assumptions leading to elimination of initiating events

The following are not included in the initial list:

- initiating events outside the scope of coverage of the PSA, but in the specifications of the PSA

- events which do not engender operating transients

- operating transients which can be corrected by automatic control systems

Potential initiating events may be eliminated:

1. because their frequency is lower than a threshold value;
2. by theoretical analysis. If there is any doubt, the potential initiating event is considered to be a PSA initiating event;
3. by close analysis of operating feedback;
4. if an initiating event is negligible relative to others. In this case, it must be ensured that the consequences the eliminated initiating event would have had on the systems are among those of a predominant initiating event.

Documentation: a three-column table:

1st column: initiating events eliminated

2nd column: reasons for elimination (does not engender a transient, estimated frequency below the threshold, etc.)

3rd column: where it is found (another study, nowhere).

II.1.4 Documenting assumptions leading to grouping of initiating events

Numerous events and occurrences can disrupt a plant and the response of the plant to many of the events can be virtually identical. Referring to [7], in such cases, it is acceptable to group initiating events resulting in the same accident progression (i.e., requiring the same systems and operator actions for mitigation). To avoid a distorted assessment of risk and to obtain valid insights, grouping of initiators with significantly different success criteria should be avoided. In addition, all grouped initiators should have the same impact on the operability and performance of each mitigating system and the operator. Consideration can also be given to those accident progression attributes that could influence the subsequent Level 2 analysis.

Documentation: a 3-column table

1st column: final initiating events

2nd column: potential initiating events

3rd column: reasons for grouping (success criteria for each system required for mitigation, expected effects on mitigating system, etc.)

II.2 How to highlight the assumptions related to physical models

II.2.1 At plant level and for each initiating event

The objective is to document the accident scenarios engendered by an initiating event. The documentation recommendations concern a generic programme. Provision should be made for additional documentation in accordance with the modelling method (e.g. when a PSA is made up of several models, cross-reference rules must be given).

An **accident scenario** is an initiating event followed by failure of one or more mitigating systems and operator actions for mitigation.

Mitigating systems and operator actions for mitigation are the necessary countermeasures (**PSA missions**) following an initiating event. These missions can be divided into four classes. Front-line mitigating systems serve to reinstate the functions necessary for avoiding undesirable events (core damage, etc.). To do this they rely on operator action (performance of actions by the control crew), Instrumentation & Control, and support system (see II.2.2) at system level.

An **accident context** is a plant state linked to an initiating event and possibly followed by PSA mission failures. This notion of accident context is useful for defining the framework for implementation of PSA missions.

Documentation at two levels:

1. General level: sequencing of contexts
2. PSA mission level: characteristics of each PSA mission

II.2.1.1 Sequencing of contexts

The various accident contexts in which PSA missions are involved will be represented in tabular form. The information given may be of any kind, but must simply be explicit. The columns in the table are:

- 1st column: Name - Context (description of the context)

- 2nd column: Objective of control (in functional terms)

- 3rd column: Associated resources

- 4th column: Corresponding PSA missions

- 5th column: Associated references (procedures, etc.)

II.2.1.2 Documentation of missions

For each PSA mission it is necessary to give the information required for understanding safety missions and the occurrence of the accident sequence. This information may be presented in the form of data sheets. There are three types of data sheet, i.e. as many as there are classes of mission distinguished: front-line, human factors, and I&C. Appendices 1 to 3 give the zones (bold type) and the fields for each of these data sheets.

The zone of fields concerning **Identification of the mission** includes information such as "which mission, in what contexts?".

The zone **Description of the mission** includes the main information on the mission "aim of mission, how, how long?"

The zone **Mission effects** describes how the sequence followed. If success led to an acceptable consequence, the reasons will be given. It will be marked "OK". If failure led to an undesirable consequence, the reasons will also be given (e.g. loss of Reactor Coolant System inventory). This will be marked "D" (core Damage). In other cases, a free-format description of the countermeasures, normal-emergency operation, sequencing of missions, etc. should be given.

The zone **Missions useful for this mission** gives downline links with the other PSA missions of the project.

The fields **mission, accident families, reactor states,** and **initiating events** are coded.

Accident contexts are described in any format, possibly with the addition of details on the initiating event (e.g.: small LOCA, then failure of medium-pressure safety injection).

II.2.2 At system level

II.2.2.1 Description of the system

The description of the system must be subject to exhaustive documentation in a system study report which must include:

- a description of its **topology**, its **functions**, and its **configurations** before and during operating phases

- a list of components modelled and their interfaces (power supply, I&C),

- a preliminary functional analysis of the system (different operating modes of the system and associated configurations).

All this does not have to be re-written in the document synthesizing the whole. The EXPRESS software developed by EDF helps in the construction of fault trees on the basis of a topological description of the system and a description of the missions (configuration and undesirable events). It automatically documents each system study and ensures there is coherence between the different system studies.

On the other hand, specific assumptions and the choices linked to the description of the system (e.g. the assumption which led to a given component not being modelled) must be traced. In so far as possible, the assumptions must be distributed among three classes: design assumptions (linked to the unit), operation assumptions, or modelling assumptions.

II.2.2.2 Table recapitulating system missions

In principle all the descriptive data sheets derived from the synthesis carried out at unit level cover all the **front-line** missions. Some of the missions can be grouped. Any grouping of close missions must be documented. The synthesis produces a list of missions associated with **accident contexts** and unit states.

A *system mission represents what the required system must do within an accident context.* It is described by a set of parameters: parameters linked to the system and parameters linked to the unit.

For each mission of the system, a table aimed at summarizing and presenting side-by-side the point of view of the system (what the system performing the mission must do) and the point of view of the unit (what context it relates to) must be filled in. It must contain the parameters listed below:

1. **The coding of the mission**
2. **Unit parameters**

   - **Accident families, reactor states**

   - **Accident contexts** described in free format, possibly with the addition of details on the initiating event (e.g.: small LOCA, then failure of medium-pressure safety injection).

3. **System parameters**

- The **success criterion** describes the function or functions to be carried out by the system during the mission (in number of lines, pumps, flow rate, etc.). Failure of the mission of a system corresponds to non-compliance with this criterion.

- The **configuration of the system** indicates its material availability at the time of the accident, e.g. steam generator No. 1 isolated.

- The **initial state of components** describes the overall state of the system at the start of the mission (on standby, operating, which lines operating, etc.), based on the state of the main components (valves closed/open, pumps operating, etc.).

- The **state during the mission of the components** describes the overall state of the system during the mission (operating, which lines operating, etc.), based on the state of the main components (valves closed/open, pumps operating, etc.).

- The **availability of support systems** specifies the state of the support systems at the time of the accident (number of trains available).

- The **mode of solicitation** describes whether manual or automatic operation is involved, and on which signal it acts.

- The **duration of the mission** is the time at the end of which the mission is considered to be *accomplished.*

- **Other**: information that does not fall into any of the above categories can be entered here (maintenance "bubble" [all equipment items taken out of service while maintenance is performed on a given item], human error, failure to recover, etc.)

System and unit parameters have common links, e.g.:

- The unit state gives information on the initial state of components and the mode of solicitation.

- The initiating event can be used to deduce information on the configuration of the system (initial availability of the system, etc.) and the functional criterion of success.

II.2.2.3 Simplified Failure Mode and Effect Analysis (FMEA)

System-specific assumptions must be highlighted. This step in the analysis of dysfunction at the macro-component level (groups of components) precedes that of constructing fault trees. Assumptions are made and questions are asked: can reverse flow be set up? what are the consequences of the loss of zero flow? effect of ruptures? effect of short-circuits?

In practice, for a thermohydraulic system for example, it was necessary to systematically ask about the effect on the system of each of the following micro-failures: rupture, loss of flow without rupture, loss of exchanger, loss of regulation, internal leak (or refusal to close).

This analysis is formalized by a simplified FMEA for each macro-component (no more than about 10 pages), and will involve the following columns:

- 1st column: macro-component (description)

- 2nd column: macro-failure (rupture, loss of flow without rupture, loss of exchanger, loss of regulation, internal leak or refusal to close)

- 3rd column: effect on the system and its missions (of each macro-failure)

- 4th column: comments and references.

In this simplified FMEA, non-obvious unexpected effects on the system must be traced.

Example:	rupture => leak	(expected)
	loss of flow on the zero flow line =>loss of pump	(unexpected)

The assumptions linked to the simplified FMEA must be traced. In so far as possible assumptions must be distributed among three classes: design assumptions (linked to the unit), operation assumptions, or modelling assumptions.

II.2.2.4 Definition of common-cause failures

Consideration of common modes must be traced.

In EDF's EPS 1300 PSA, common-cause failures were considered for the following equipment:

- Sensors (on solicitation)

- Check valves (on solicitation and during operation, for ruptures)

- 6.6 kV and 380 V motor switches (on solicitation)

- Circuit breakers (on solicitation)
- Diesel generator (on solicitation and during operation)
- Motor (on solicitation and during operation)
- Pumps (on solicitation and during operation)
- Relief valve (on solicitation)
- Turbines (on solicitation and during operation)
- Valves (on solicitation)

III. A strong need to define good practices more formally

In 1996, EDF undertook to formalize its policy for use of PSAs. This policy is broken down into two different fields, depending on whether it applies to units in operation or to future units.

For units already operating or under construction, the objectives of PSA are (1) to contribute to the overall appreciation of the level of safety, (2) to highlight and rank the main components of the risk, (3) to help in the choice of the changes to be made to units. These objectives are pursued through different applications (Periodic Safety Reviews, probabilistic analysis of NPP incidents, assistance in optimization of maintenance programmes, support/substantiation for changes to the Operating Technical Specifications, etc.).

For future units, the objectives of PSA are similar to those for operating units, but the applications (assistance for design, substantiation of design) fall under entirely different conditions (at the design stage, before anything is built).

EDF has therefore expressed the desire to "codify" practices for use and construction of PSAs.

In the United States, the PSA Applications Guide [5] is intended to provide utilities with guidance on the preparation, utilization, interpretation, and maintenance of plant-specific PSAs for regulatory and non-regulatory applications. This guide does not focus on any one PSA application or application type. In this regard, the guide is intended to provide the overall framework within which utility and industry PSA applications can be developed and evaluated.

The idea of standardization is therefore as prevalent in the USA as in France. EDF has undertaken to compare its documentation and construction methods with international practice, and is currently working with EPRI to develop a guide to good modelling and documentation practice [6].

IV. Some prospects for the future

EDF has set itself the objective of developing PSAs that are representative of each nuclear power plant series in operation, that will produce standard results (coremelt risk, ranking of risk components, etc.), that meet the main requirements of applications, and that use common tools. These PSAs are called "reference PSAs". After the recently completed PSA for the 900 MW series, those for the 1300 MW and N4 series will be drawn up as part of projects bringing together several EDF divisions.

The new EPS 1300 PSA will be used for the safety review of the 1300 series. This PSA will incorporate the generalized APE state-based approach. The N4 PSA will be derived from the EPS 1300 PSA to a very large extent. The main special feature of the N4 PSA will be consideration of the computerized control room and, if possible, better representation of control in emergency sequences. EDF has also set itself the objective of drawing up user's manuals for the reference models.

As part of co-operation with EPRI for preparation of a guide on good practice in modelling and documentation, a future step is further work on two topics identified as being of particular interest: (1) appropriate use of uncertainties, (2) communication of PSA results to non-specialist users.

For the first topic, it will be mostly a matter of situating sources of uncertainty and assessing the interest of evaluating uncertainty (evaluation method, use of evaluations in applications). For the second, modes of communication and instruments for distribution will be recommended for different PSA users.

References

1. Dewailly J., Deriot S. Dubreuil- Chambardel A., François P., Magne L. *Living PSA Issues in France on Pressurized Water Reactors* IAEA Technical Committee Meeting on Procedures for Use of PSA Optimizing NPP Operational Limits and Conditions 20-23 September 1993, Barcelona, Spain.

2. Magne L., Pesme H. *Living PSA tools. Instructions for Using a Computerized PSA* PSA'95, November 26-30, 1995, Seoul, Korea

3. Magne L., Pesme H. *Improvements and Traceability of a PSA to Help Applications and Decision Making.* Probabilistic Safety Assessment and Management'96 ESREL'96 - PSAM-III June 24-28 1996, Crete, Greece

4. Dewailly J., Magne L. (EDF-EPRI) *PSA Applications: Practical Recommendations for Modelling and Documentation,* EPRI System Analysis Forum (ESAF), May 2 1995, Charlotte, North Carolina, U.S.A.

5. True D., Fleming K., Parry G., Putney B., Sursock J-P, *PSA Applications Guide* EPRI TR-105396, Final Report, August 1995.

6. Magne L., Dewailly J., *Guidelines for PSA Good Practices and Documentation (Outline)* EPRI System Analysis Forum (ESAF), November 12 1996, Chicago, U.S.A.

7. NUREG-1602. *The Use of PRA in Risk-Informed Applications.* Draft Report for Comment. Date Published : June 1997.

Appendix 1

A front-line mission data sheet should include the following zones (bold type) and fields:

Identification of the mission

Class of mission (front-line)

Mission coding, accident families, reactor states, initiating events

Accident contexts

Description of the mission

Safety function (control reactivity, control Reactor Coolant System inventory, transmit residual power)

Success criterion (describes the function to be performed in terms of number of lines, pumps, flow rate, etc. The failure criterion may be given in exceptional cases, with clear indication that it is the failure criterion, if it is easier to formulate).

Mission duration (time at the end of which the mission is considered to be accomplished (e.g.: 12 h on auxiliary feedwater in the case of feedwater tube rupture, to achieve the temperature and pressure conditions required for connection of the residual heat removal system). Other time factors may also be mentioned:

- if the PSA mission is not immediately available: what minimum time after the initiating event or accident context until the start of this mission?

- if the PSA mission is not indispensable immediately: what maximum time after the initiating event or accident context until the start of this mission?)

Mission effects (in case of success, in case of failure)

Missions useful for this mission (excluding support missions)

Human factors, instrumentation and control

Additional information (References, other assumptions)

Appendix 2

A human factors mission sheet should include the following zones (bold type) and fields:

Identification of the mission

Class of mission (human factors)

Mission coding, accident families, reactor states, initiating events

Accident contexts

Incident/accident procedures (criteria for entry into procedures, procedures)

This zone gives information on the framework of post-accident management into which a human-factors mission fits. In particular, it is important to trace the criteria for initiating and carrying out procedures. Action criteria can also be mentioned (test, surveillance, etc.).

Description of the mission

Success criterion

Type of mission (to be complemented by "Recovery of system failure" (e.g. opening of SCRAM system circuit breakers), "Desirable" or "Unwarranted" (e.g.: spurious shutdown of safety injection in the case of small LOCA).

Initiator of actions carried out (local agents, control room), times for intervention, recovery possible (Yes, No, Comment), recovery times

Mission effects (in case of success, in case of failure)

Missions useful for this mission (front-line, other classes of missions)

Additional information (References, other assumptions)

Appendix 3

An instrumentation and control mission sheet should include the following zones (bold type) and fields:

Identification of the mission

Class of mission (I&C)

Mission coding, accident families, reactor states, initiating events

Accident contexts

Description of the mission (success criterion)

Mission effects (in case of success, in case of failure)

Additional information (References, other assumptions)

EDF
Electricité
de France

DIRECTION DES ÉTUDES ET RECHERCHES

1, AVENUE DU GENERAL-DE-GAULLE - BP 408 - 92141 CLAMART CEDEX FRANCE - TÉL. 33 1 47 65 58 11 - FAX 33 1 47 65 49 27 - e.mail elisa.nuc @ der.edfgdf.fr