57

INTERNATIONAL SEMINAR ON PSAs AND HUMAN RELIABILITY

Paris, November 21st-23rd 1994

Topic 1 : PSA Methodology

L. MAGNE

CONTENTS

INTRODUCTION 3

PART ONE - PSA METHODOLOGY : BOOLEAN OR MARKOVIAN ? 4

1. DESCRIPTION OF THE DIFFERENT METHODOLOGICAL APPROACHES 4
   1.1 General procedure for construction of a PSA 4
   1.2 Methods 4
   1.3 Characteristic points of each method 5

2. ILLUSTRATION BY EXAMPLE 6
   2.1 Introducing the example 6
   2.2 Quantification 7
   2.3 Comments 10

3. GENERAL ELEMENTS OF COMPARISON OF THE METHODOLOGICAL APPROACHES 12
   3.1 Integration of dependencies 12
   3.2 Different analysis philosophies 12
   3.3 Which method, for which purpose ? 13

PART TWO - PROBABILISTIC SAFETY ASSESSMENTS : WHY, HOW, WHO ? 14

1. STARTING FROM THE NEEDS 14
   1.1 The objectives of use - WHY ? 14
   1.2 The approach for use - HOW ? 15
   1.3 The users - WHO ? 16

2. EXAMPLES 17
   2.1 Probabilistic incident analysis 17
   2.2 Use of PSAs for maintenance 19

3. DEFINING TECHNICAL REQUIREMENTS 21
   3.1 Requirements relative to objectives of observation 21
   3.2 Requirements related to prospecting objectives 22
   3.3 Requirements related to safety demonstrations 23
   3.4 Requirements related to the approach of understanding phenomena 24

4. POSITIONING OF SOME PSAS 26

PART THREE - QUESTIONS TO BE DEBATED 27

APPENDIX 1 RELIABILITY DATA USED IN THE EXAMPLE OF PART ONE 29

APPENDIX 2 POSITIONING OF SOME PSAS 30

NOTATIONS AND REFERENCE 32

INTRODUCTION

Methods and tools used for nuclear Probabilistic Safety Assessment (PSA) are subject to debate : which methods are best : dynamic or static ones ? Boolean or Markovian ones ? Are large event trees or large fault trees better ? In fact each of these possible choices has its advantages and drawbacks. The debates have no absolute answer. In fact, it is according to the needs which PSAs must meet that the question of methods and tools, among others, should be asked. The choice should then be undertaken in terms of pertinence to those needs.

Reality is totally different : the question of the needs which PSAs must meet has (until recently) been asked only after the execution of PSAs. This is how methodological problems were set "in an abstract way", without any concrete foundation on which to judge the pertinence of the choices. Similarly, the contents of PSAs and the level of realism of the models are defined beforehand without taking the future uses into account.

***

The purpose of this text is first to ask a certain number of questions on the methods related to PSAs. Notably we will explore the positioning of the French methodological approach - as applied in the EPS 1300[1] and EPS 900[2] PSAs - compared to other approaches (Part One). This reflection leads to more general reflection : what contents, for what PSA ? This is why, in Part Two, we will try to offer a framework for definition of the criteria a PSA should satisfy to meet the clearly identified needs. Finally, Part Three will quickly summarize the questions approached in the first two parts, as an introduction to the debate.

PART ONE

-

PSA METHODOLOGY : BOOLEAN OR MARKOVIAN ?

The methods used in the first French PSAs include some characteristics that make them original compared to other PSAs in Europe or in the United States. These characteristics are essentially derived from the partial but frequent use of the Markovian method, or from the dynamic methods derived from it.

We are going to describe some methodological approaches used in the international community, before trying to start a comparative test.

1. DESCRIPTION OF THE DIFFERENT METHODOLOGICAL APPROACHES

1.1 General procedure for construction of a PSA

A PSA is a set of accident scenarios (or accident sequences), generally represented by means of event trees. The events integrated in these scenarios are called "top-events". Most of the time they are complex events representing, for instance, the failure of the missions of elementary systems, or of operators' actions. The first stage in building a PSA is thus the *identification of scenarios*.

The next stage is *modelling*. A set of models for two levels of analysis is built : the event trees are prepared at the most global level possible, taking account of the main operation interactions between the elementary systems, and also of plant control by the operators. The top-events are elaborated from a more accurate analysis, at the level of the elementary systems themselves, or at the level of analysis of operator actions.

Finally, *quantification* consists in assessing the probability of scenarios by regrouping the studies of top-events with the event trees, in order to obtain a complete model.

Of course this is a schematic presentation : the three steps always overlap each other and work frequently moves from one to the other.

1.2 Methods

This work arrangement (identification of the scenarios, modelling, quantification) is very general. It is during the methodological implementation of the modelling or of the quantification that some distinctions appear. The following are three different methods used in Europe or in the United States :

JJ

1 - "Fault-tree linking"

This approach retains a single method of modelling (the Boolean method). The results of the top-events (fault trees) and the event trees are linked by pooling the fault trees. Fault-tree linking enables automatic processing of the functional dependencies, and requires manual processing of the sequence dependencies. Today it is the most comonly used approach internationally. Some examples of support software : CAFTA (SAIC)[3], RISK-SPECTRUM (RELCON)[4], or NUPRA (NUS).

2 - "Event-tree linking"

This approach also retains a single method of modelling : the Boolean method. The results of the top-events (fault trees) and the event trees are brought together by numerical linking : the numerical results of the top-events are transferred into the event trees. It is then necessary to analyze the functional dependencies manually. The simplicity of the calculations performed in the accident sequences (multiplications) enables a very accurate level of detail. This method, implemented with the RISKMAN software (PLG)[5], is used by some American utilities.

3 - Dynamic numerical linking ("dynamic method")

Depending on needs, this approach enables the use of various methods of modelling : fault trees, states graphs, products of convolution for accident sequences[6]. As for the above approach, the results of the top-events and the models of scenarios are brought together by numerical linking. The functional dependencies have to be analyzed manually, but this method enables automatic processing of the time dependencies. It has only been used for the French PSAs (EPS 900 and EPS 1300 PSAs), and is implemented with the LESSEPS software (EDF)[7].

1.3 Characteristic points of each method

The fault-tree linking approach is entirely concentrated on fault trees. A sequence does not represent a scenario per se, but rather a combination of system failures leading to the undesirable event. Thus, all the efforts for model building are based on Boolean reasoning : search for the causes of failure, reflections on the "minimality" of event combinations.

On the contrary, the dynamic approach is centred on event trees : the main efforts are devoted to building these trees : reflections on the scenarios, reflections on the functional or sequence dependencies between systems, definition of the system missions (each system can have many missions) or of those of the operators. Studies of systems are "easier", in so far as the contents of these studies have been defined by the event trees beforehand.

The event-tree linking method is centred on reflections upstream of the methods : a precise analysis of functional dependencies between all the plant systems must be performed first, and then an analysis of the operation under accident conditions. Then the results of these analyses are transcribed into event trees and rules to define system missions.

All these approaches are very different, and it is not easy to compare them, as will be seen. It can be said that the event-tree linking method is the most complete one, since it very clearly separates the analysis from the processing of the problems. On the contrary, the other methods (fault-tree linking or dynamic method) mix analyses and processes.

2. ILLUSTRATION BY EXAMPLE

2.1 Introducing the example

The purpose of the example we are going to study is not to illustrate the totality of the possible fields of comparison between all the methodological approaches, but only to discuss the qualitative and quantitative interests of the dynamic methods.

It is a simplified scenario initiated by the loss of external power supplies. We assume that the nuclear plant studied here has electric power supplies backed-up by two diesel generating sets and a turbine-driven auxiliary feedwater pump (TDP).

The scenario is simplified from a technical point of view (other scenarios could be built with the same initiating events), from a human point of view (the human actions are all disregarded), and from the probabilistic point of view (no uncertainty calculation will be performed). For easier reading, no calculation will be detailed in this document.

Assumptions

- We consider 2 kinds of losses of external power supplies : short losses have a rather high frequency and are recoverable in an average time of 1 hour ; long losses have a frequency approximately 70 times lower, and are recoverable in an average time of 48 hours. This data is practically realistic, and is derived from French operating feedback.

- After the loss of the external power supplies, the two diesels and the turbine-driven auxiliary feedwater pump start up automatically.

- Start-up signals are perfectly reliable.

- When the 3 auxiliary systems (both diesels and the turbine-driven pump) are all lost, a period of one hour is available to recover the external supply of one of the 3 systems. After this time, if nothing is recovered, unacceptable consequences are reached.

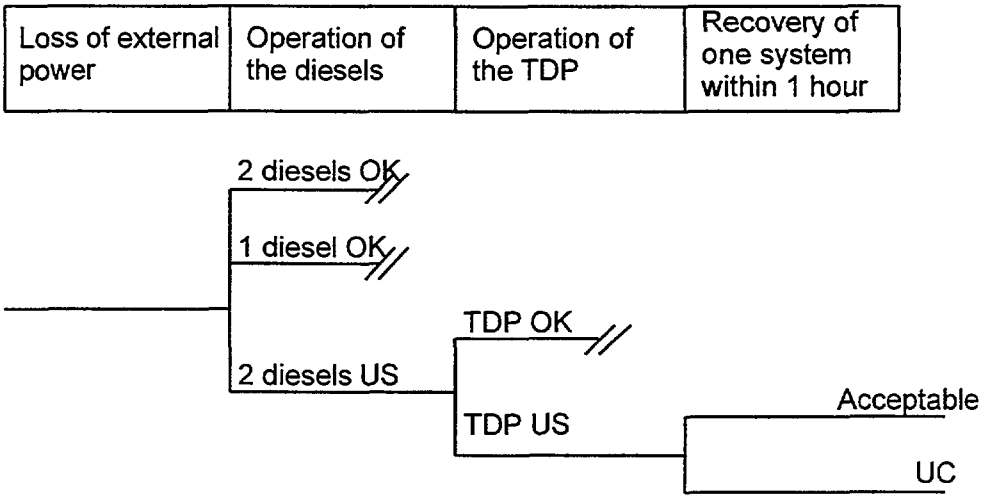
- To simplify the exercise, we consider the diesels and the pump as simple components, and not as complex systems.

- The data related to the equipment is provided in Appendix 1.

Qualitative model

The qualitative model obtained is the following :

Partial event tree for loss of external power



2.2 Quantification

Quantification with a dynamic method

One possible method for obtaining a "rigorous" quantification of this scenario (we will discuss this idea of rigour further on) is as follows :

- Calculate the reliability law for all the emergency supplies (represented by both diesels). This is a reliability calculation with repairable components : we choose the Markov graph method.

- Calculate the reliability law for the turbine-driven pump, here limited to the law of the component. In reality, the turbine-driven pump consists of a set of components in series : we would have chosen to represent it by a fault tree.

- For each initiating event, calculate the product of convolution between the reliability law for all the auxiliary supplies, the reliability law for the turbine-driven pump, and the law for recovery of the external power supplies, taking account of equipment repairs and the time before unacceptable consequences are reached.

This calculation integrates all the input parameters : the frequencies of short and long losses of external supplies, their mean times to repair, and also the failure and repair laws for all the engineered safeguard systems.

Result : $R_{Dynamic} = 1.8\ E\text{-}6$

Quantification with a Boolean method

In this example, there is no need to distinguish the fault-tree linking approach from the event-tree linking approach. Using a purely Boolean method generally leads to the following consequences in terms of modelling :

- It is necessary to choose a single mission time for the engineered safeguard systems, otherwise things could become inextricably complex. Generally, this mission time will be fixed arbitrarily as 24 hours.

- It is very difficult to take account of repairs of the systems and of the initiating event.

  This scenario is quantified by multiplying the total probability of loss of the external supplies by the product of probabilities of failure of the engineered safeguard systems within 24 hours (here, there is no important functional dependency), and taking no repair into account.

  Result : $R_{Boolean\text{-}1} = 6.5\ E\text{-}5$

We will discuss the "pessimistic" character of this result in the following paragraph. We can improve it by multiplying it by a recovery factor. This factor can be calculated in different ways.

For example, we can calculate the probability of recovering at least one system within a period of one hour (i. e. before unacceptable consequences), considering everything to have been lost at $t = 0$. This gives the following result :

$R_{Boolean\text{-}2} = 2.4\ E\text{-}5$

This recovery factor can also be perfectly adjusted by means of precise complementary analyses external to the model. These complementary analyses consist in making the calculation in the same way as for "dynamic quantification". The difference between the two approaches lies in the representation : the Boolean

representation is used and is adjusted with a precise corrective factor. The corrective factor is written as follows :

$$CF = R_{Dynamic}/R_{Boolean\text{-}1}$$

The result is then :

$$R_{Boolean\text{-}3} = R_{Boolean\text{-}1} \times CF = R_{Dynamic}.$$

This recovery factor thus allows us to preserve complete Boolean modelling, while guaranteeing a rigorous assessment[8].

Importance of the external power supplies

Suppose that we want to compare the relative contributions of the long losses to the short losses of the external electric power supplies.

The dynamic model enables us to reply to the question with simple sensitivity studies on the initiating events. The Boolean model can also give a reply, but unfortunately a wrong one (we choose the model with the best possible recovery factors, but it changes nothing for the contributions) :

Contributions of the short and long losses of external supplies :

	Contributions measured with the dynamic model		Contribution measured with the Boolean model	
	Frequency	%	Frequency	%
Short losses of external supplies	1.5E-8	0.8%	1.8E-6	98.6%
Long losses of external supplies	1.8E-6	99.2%	2.5E-8	1.4%
Total	1.9E-6	100%	1.9E-6	100%

The contributions of short or long losses of the network are dramatically inverted. The Boolean model highly underestimates the long losses, and highly overestimates the short losses. We see that the pessimism of the initial Boolean results was not constant at all.

In fact, the interaction between the long periods of loss of the external supplies with the mediocre values of failure rates of the engineered safeguard systems is not at all appreciated by the Boolean model : therefore there is a risk of drawing erroneous conclusions from these contributions. In reality, more precise contributions could be obtained with the Boolean model, at the cost of a certain complication of the model, which would tend to be a more dynamic one : distinction of the mission times of the equipment and recovery factors.

On the contrary, if the contributions calculated by the dynamic model are effectively exact, one might ask about uncertainty on operating feedback. Is the probability of a climatic incident on the system not too strong ? Is this probability pertinent for realistically appreciating the failures of the system at the terminals of a nuclear plant ? Are the rates of equipment failure during operation not overestimated relative to the probabilities of failure on start-up ? Finally, do all these uncertainties linked to operating feedback not make accuracy of the model illusory ?

2.3 Comments

Particularity of the example

The example chosen in § 2. 2 has been voluntarily chosen to show the quantitative (and qualitative) interest of the dynamic methods. However, such examples do not represent the majority in PSAs. Most thermohydraulic accidents can be processed in a sufficiently precise way (in terms of order of magnitude) without having recourse to any dynamic methods.

Therefore general comparisons between the different methods should not be based on this single example. We will give more general elements of comparison in § 3. We will limit ourselves here to some comments on the above example.

Global assessment of the safety level

The first element of information we can obtain from a reliability model refers to the main results : is the risk admissible or not ?

The dynamic model enables us to reply to this question correctly, since the quantification appears rigorous enough. Nevertheless, the scientific rigour of the calculation must be moderated. Indeed, the input data of the model derived from operating feedback is tainted with major uncertainties. The model integrates many parameters, and consequently has as many uncertainties to manage.

Boolean processing can give an answer to the question too. The order of magnitude of the results seems valid, given the uncertainties on the data ; if we want to make sure of it, some complementary dynamic calculations, which enable us to adjust the results (using recovery factors), will suffice.

Incident analyses

Let us suppose that during the operation of the nuclear plant, external sources are unavailable for a period of 12 hours. What potential risk has the plant run during that time ? The results provided by the dynamic model will be qualitatively safer : the interest of the "rigour" of the model is to avoid risking wrong interpretations resulting from erroneous orders of magnitude.

However, if the problem manifestly includes strong temporal interactions, the use of Boolean methods does not prevent using complementary dynamic methods to validate the analyses : thus to analyze such an incident, the Boolean model will enable us to anticipate the general potential consequences on the plant. Complementary analyses will be necessary to study the particular consequences regarding the emergency supplies.

3. GENERAL ELEMENTS OF COMPARISON OF THE METHODOLOGICAL APPROACHES

3.1 Integration of dependencies

Several types of dependencies can be involved in a dependability study :

- *functional dependencies between systems* (for example, common elements between systems),
- *time dependencies between systems* (for example, the starting of a system, as back-up to another one),
- *functional dependencies between components* (for example, failures with a common cause, or probabilities of failure of a component depending on the status of another component),
- *time dependencies between components* (for example, components considered as repairable (or not) according to the failures that have occurred previously).

Each method is more or less well adapted to the integration of each of these dependencies. Dynamic models enable sequence dependencies to be integrated naturally, while Boolean models are better suited to functional dependencies. But things are more subtle in reality : the use of Boolean methods could be improved so as to represent sequence interactions quite suitably[9].

In any case, whatever the method, it is very important to identify the significant dependencies of all types, since they are predominant with respect to safety. Thus, beyond a more or less automatic systematization of the methods used, might the important point be rather to know and to master the limits of these methods ?

3.2 Different analysis philosophies

Comparisons between these methods are delicate, maybe impossible to carry out definitively. Nevertheless, we can deduce different "analysis philosophies".

A PSA studied with Boolean methods enables us to reply to the following question : in the event of an accident, *which are the systems whose availability is sufficient to control the accident ?* Whereas with dynamic methods, we would be better placed to reply to the question : *in the event of an accident, what is the behaviour of the system that leads to unacceptable consequences ?* The Boolean methods are *structural*, the dynamic method is *behavioural*.

In many cases, a PSA involves some scenarios for which these two types of approach are equivalent. In other cases (according to whether there are sufficiently important functional or sequence dependencies) the two types of approach are not equivalent. But they are complementary : they provide different points of view, and can validate each other.

3.3 Which method, for which purpose ?

Furthermore, according to the type of problems, we will be able to emphasize either one or the other type of approach. In the case of incident analysis, it is essentially behaviour, of the system, and particularly of operators, that will be emphasized. This analysis may be usefully completed by a study of the main functional interactions involved.

In the case of a study aimed at justifying or proposing classifications of the equipment, for maintenance or for operating technical specifications, one concentrates on the importance of the availability of this equipment with respect to safety. This method in turn may be complemented by a temporal analysis : is this equipment important on a short or long-term basis ?

Beyond the methods, which are difficult to compare in absolute terms, we have come across more general questions of the philosophy of analysis. In reality, depending on the objectives of use, the question that arises is far more that of the pertinent and mastered contents of the studies than that of the final choice of a method. Methods are only a means of meeting the objectives. Thus, in an article about comparisons of the fault-tree linking and event-tree linking methods[10], D. RASMUSSON does not conclude, but gives a certain number of methodological recommendations for the realization of PSAs whose objective is to process level-2 consequences (release into the environment).

This question of the technical requirements PSAs must fulfil to meet exact needs is the one we are going to develop in the second part of this document.

PART TWO

-

PROBABILISTIC SAFETY ASSESSMENTS : WHY, HOW, WHO ?

The use of PSAs for assistance in taking decisions (operation, design, maintenance) is developing rapidly in all countries. Generally this gives rise to some difficulties regarding existing PSAs, since they were not sufficiently adapted. Therefore PSAs have been gradually improved to reply to these new needs. A general idea that seems to be appearing internationally is to define the technical requirements PSAs must fulfil in order to meet these needs, as a recent meeting organized by the IAEA[11] showed.

First, we are going to propose an attempt to classify the needs (§ 1). Despite its shortcomings, this classification can be used to better assess what is at stake in PSA applications, as will be seen with some short examples (§ 2). Finally, this classification will enable us to propose an outline definition of the technical requirements PSAs must or should meet (§ 3).

1. STARTING FROM THE NEEDS

In the following developments, we would like to adopt the following approach : first, define the needs we wish to satisfy, then according to these needs, specify the "product" that we want to make, then make it, etc. But this approach is difficult to follow, since twenty years of experience on PSAs cannot be dispensed with over night. We know the "product" (the PSA), and it is not a matter of defining other products here. It may be a matter of proposing improvements to PSAs, or to the products derived from them. The question of needs is therefore going to be asked "in reverse" : given what a PSA is in global terms (a global model of a nuclear plant, representing a set of probabilized scenarios leading to unacceptable consequences), what types of needs can we satisfy with such a product ?

The needs PSAs must fulfil can be defined in accordance with the following three questions : what type of use is a PSA planned for (objectives) ? how do we use a PSA (approach) ? who uses a PSA (users) ?

1.1 The objectives of use - WHY ?

What types of uses is a PSA planned for ? We propose two categories of objectives for use : *observation objectives and prospecting objectives.*

A PSA can be considered as a tool to help in the analysis of operating feedback. It gives global information on risks ; it enables us to rank the relative importance of the system's components, for example in order to intervene on the safety ranking of the components (graded QA) ; it can be used to compare one plant with another in terms of safety : all these types of needs will be classified as *observation* objectives.

A PSA can also be considered as a tool that enables assessment of the consequences of a modification of a plant. We can try to assess the potential consequences (in terms of increase of the risks) of a particular incident situation ; we can envisage using a PSA to propose maximum durations of on-load operation in the event of equipment unavailability ; a PSA can be used to define a safe fallback configuration in a particular situation : these kinds of needs are classified as prospecting objectives.

What is the pertinence of this first classification ? It is only an attempt ; one that will probably give rise to objections. Notably, this first classification is certainly of no use in distinguishing the objectives of assistance for operation from those linked to design. However, it will enable us to better analyze the needs linked to PSA applications, as will be seen in § 2. Moreover, it will enable us to define distinct technical requirements. The technical requirements associated with observation objectives will be linked to characteristics relative to safety assessment (definition of the unacceptable situations regarding safety, coverage of the situations taken into account, accuracy of the data, etc.). The technical requirements associated with prospecting objectives will concern the use of the models : a PSA considered as a prospecting tool must be a re-usable, robust, and effectively productive model etc. All these technical requirements are defined in § 3.

1.2 The approach for use - HOW ?

How is a PSA used ? We will distinguish two approaches for use : the *safety-demonstration approach* and the *approach for understanding phenomena.*

The *safety-demonstration approach* consists in replying to the requirements specified by a higher authority or by the Safety Authority. Because of the technical, social and financial stakes associated with the nuclear field, these demands are frequent. Therefore, it is necessary to justify a level of safety, or a decision, based on the results of a PSA, or on some uses of a PSA. This approach is firstly quantitative, which does not prevent quantitative results being supported by qualitative arguments.

The *approach for understanding phenomena* consists in using the PSA as a knowledge base in order to develop questions related to safety. The complexity of a nuclear plant, the large number of more or less arbitrary assumptions that have to be undertaken to build a PSA, and the fact that the results are difficult to check statistically (rare events), show that this type of model is fragile and very limited. The question of developing these models is therefore posed, undoubtedly more so than in other technological areas. This approach of understanding phenomena is first qualitative, qualitative reasoning being weighted by quantitative elements. For

example, if a PSA is used to help to determine the maximum duration of operation in the event of unavailability of a piece of equipment, beyond the quantitative results, we will endeavour to emphazise the predominant scenarios ; we will endeavour to study the interactions between this equipment and other systems ; we will possibly complete the PSA with new analyses ; we will develop analysis of the human factor, etc.

Is the distinction between these two models pertinent ? Its first aim is to lead to a reflection on the notion of "model". It constitutes a model of risk assessment of a nuclear plant and is representative of the state of reliabilistic knowledge, techniques, and practice at a given moment.

This model can then be used, without querying it again (*demonstration* approach), or it can be continually pushed to its limits in order to master them — or at least to take them into consideration in order to get the best out of the model — (approach of *understanding*).

This reflection is of an epistemological nature : PSAs belong to two kinds of sciences. On the one hand they use some knowledge of physical, statistical and mathematical fields : thus, from this point of view, they belong to the "natural" sciences. The work approach for the natural sciences is often based on proof or demonstration. On the other hand PSAs use elements of theory of systems, they try to integrate human elements, they assess the safety of complex socio-technical organizations : thus from this point of view they belong to the social (or human) sciences. The work approach for social sciences is more of a conjectural approach : making conjectures in order to understand. It is with this in mind that we have distinguished the demonstration approach from the approach of understanding.

Even if these two approaches are different, they should not be opposed. In the field of probabilistic modelling, qualitative and quantitative properties are not opposed, but are complementary ; giving a demonstration to justify a choice does not prohibit seeking to develop knowledge to make the next demonstration more precise. Not can it be said that one approach is "better" than the other : there is a time for thinking, and a time for action. We can only regret that, in France and elsewhere, the quantitative demonstration approach is all too often preferred to the qualitative approach of understanding, particularly since where safety is concerned, it is imperative and beneficial to frequently query present certainty.

1.3 The users - WHO ?

Let us now deal with the question of the users. Two classes of users can be characterized : *specialists*, and *end-users*.

PSA *specialists* are those that produce or analyze the results of the studies. Dealing with PSAs is their major function. They are the first users, since all the applications of the PSAs are produced by them. *End-users* can be very varied : systems engineer-designer, reactor operator, plant maintenance engineer, manager, etc. They should

be using the results of the studies to take decisions, or to develop their knowledge of risks. Do these end-users, whose function is not to be PSA specialists, know enough about the contents of the PSAs to use the results appropriately ?

A first idea could be to distribute the PSAs to the end-users, so they could use them themselves occasionally. Is there today such a thing as an occasional user of PSAs ? Even if the desire to make PSAs accessible to non-specialist users has been emerging for a few years, it does not seem to have been accomplished anywhere, neither in Europe nor in the United States[12].

More generally, the problem is that of communication between the specialists and the end-users. Work should be undertaken by the specialists to translate the results into qualitative terms, to explain them, to present them in a legible way, and to transmit them to the end-users. This shows the necessity to implement an approach of understanding (whatever the chosen objective is) in order to favour communication and discussion between specialists and end-users.

The transmission of knowledge induces at least a requirement for legibility of the PSA results. Although it is a fundamental question, we will not develop this point here.

2. EXAMPLES

In this paragraph, we shall try to situate some examples of PSA applications through the classification of the needs presented above. We choose two examples : probabilistic analysis of incidents, and the applications of PSAs for maintenance. On the one hand, these examples will give us an opportunity to question the pertinence of the classification, and on the other hand, they will enable us to deal with the question of the complementarity of methods (this question was dealt with in § 3 of Part One).

2.1 Probabilistic incident analysis

Objectives

What are the objectives of probabilistic incident analysis ? This question is thoroughly analyzed in the article related to this topic in the International Seminar (topic No. 4)[13]. In this article, four objectives are presented : assessment of safety-level indicators, operating feedback on incidents, the distribution of a probabilistic safety culture, and the improvement of PSAs.

All these objectives are based on the use of PSAs to assess the potential consequences of incidents. Therefore they are all *prospecting* objectives. This prospecting can have a quantitative aim (case of safety indicators) or a qualitative

aim (operating feedback, safety culture). The technical requirements regarding PSAs are thus rather important : the PSA must be flexible and robust enough, so that an incident situation can be identified with the parameters studied in the PSA. Besides, it can be seen that, under their current form, PSAs are neither flexible nor robust enough to meet these objectives : these insufficiencies are palliated by building models specific to the incident analysis, or by making "manual" analyses, diverging strongly from the initial models.

Approach

What is the approach used in incident analysis ? The approach used in order to assess safety indicators is close to a *demonstration* approach. The approach recommended in the American ASP (Accident Sequence Precursor) method is a static approach, that moreover must not evolve at all times, so that indicators can be followed up over a period of time.

On the contrary, the approach used in connection with the other objectives is essentially an approach of *understanding*. For example, operating feedback on incidents aims at exploring, in a qualitative way, the causes of the severity of the incidents and the way they could have degenerated.

Similarly, the dissemination of safety culture is an objective aimed at inciting operators to have an interrogative attitude with respect to safety. Therefore the PSA is used here as a basis for questioning in order to better understand what the sensitive points of the installation during one incident situation or another are, what the consequences would have been if the incident had occurred when the unit was in another status, if it had occurred on another series, etc.

A relevant classification ?

Regarding the objectives of incident analysis, the analysis structure proposed by the classification does not provide us with a lot of information. Indeed, in France this application was the subject of a precise definition of the objectives that are chosen and those that are not. Incident analysis being classified among the prospecting objectives, this only emphazises some types of technical requirements PSAs should meet (and that they generally do not, at least in France). These requirements are developed in § 3. 2.

Regarding the approach, the implementation of both approaches (demonstration and understanding) is described. This can be useful to better centre the efforts and the planning of incident analysis : indicators may be assessed within the operational and controlled framework of the safety demonstration, which will induce regular publications, while time could be taken to develop operating feedback in detail.

Which methods ?

A precise review of the choice of the methods for carrying out incident analyses is not our subject here. Nevertheless, the examples given in the article quoted above[14] give some information on the choice of methods. The incident described as case 2 shows important sequence dependencies : the use of dynamic methods seems appropriate. On the contrary, the incident described as case 3 shows important functional dependencies : the use of Boolean methods (event-tree-linking, for example) would probably enable them to be clearly taken into consideration.

Finally, the diversity of the situations encountered within incident analysis is a sound justification for using diversified methods that validate each other, in order to avoid errors of interpretation.

2.2 Use of PSAs for maintenance

Objectives

The objectives of using PSAs for maintenance are presented in the article on the applications of PSAs within the International Seminar (topic No. 2)[15]. Here we retain only the links between maintenance and safety. The major objective consists in performing a hierarchical classification of the various components of a nuclear unit, in order to separate those for which preventive maintenance must be ensured from those which will be given only corrective maintenance.

This objective is mainly an objective of *observation* : it is matter of using PSAs to determine the classification of the components : one technical requirement is thus that of being able to perform such a ranking (feasibility of importance calculations).

The question might be asked as to what a *prospecting* objective could be. Once the components have been ranked, maintenance experts must build another maintenance programme. This new programme will modify the operating conditions of the unit. Further thinking can then be given to the influence of this group of modifications on unit safety. This checking of the safety level obtained can be implemented with the aid of PSAs : this objective would then be a prospecting objective.

Approach

The approach for use of PSAs for maintenance is mostly a *demonstration* approach. The PSA has first enabled a demonstration regarding the global level of safety to be carried out : one then wants to get information out of it, and to demonstrate that, to some extent, maintenance costs can be reduced while still guaranteeing an acceptable safety level.

What could an *understanding* approach be ? In most cases, maintenance specialists are neither operation nor safety specialists. Conversely : safety specialists are not maintenance specialists. The use of PSAs for maintenance could be an opportunity on the one hand to disseminate a safety culture in maintenance departments, and on the other hand, to enable more realistic modelling of equipment in PSAs. The approach for implementation of these two new objectives would be an approach of understanding.

A relevant classification ?

In this example, the analysis structure proposed by the classification of the preceding chapter has enabled us to situate the precise needs of the use of PSAs for maintenance. Furthermore, it has enabled us to bring to light other kinds of needs. Finally, an advantage of this classification is that it may be a tool (although succinct and insufficient) that enables us to develop the analysis of needs and the associated objectives.

Which methods ?

As for the example of incident analyses, detailed development of the choice of methods for the maintenance-related uses of PSAs is not our subject here. The necessity to undertake frequent importance calculations seems to impose the choice of structural (Boolean) methods. However, we have seen in the example presented in the first part (§2) that calculations of contributions can be erroneous in the case of dynamic scenarios. The complementarity of the methodological approaches can be perceived again in this case.

3. DEFINING TECHNICAL REQUIREMENTS

Depending on the relative importance of each of these requirements, a PSA will have to answer a certain number of technical requirements that differ from one PSA to another. It is clear that a PSA whose objective is only to provide some numerical assessments in the framework of a punctual safety demonstration will not have the same characteristics as a PSA used to improve maintenance, or to develop safety culture by daily analysis of incidents during operation.

We are going to try to more precisely define, in global fashion, all the possible characteristics associated with the technical requirements associated with each need. It is an attempt at definition, which should be further developed.

3.1 Requirements relative to objectives of observation

Criteria relative to undesirable events

Definition of undesirable events is essential, since it enables us to give a meaning to the word "safety". Three levels of criteria relative to undesirable events are usually defined.

Level 1 concerns core meltdown, or more exactly the beginning of damage to the core. Depending on the scenario, it may lead to uncovering of the core, or to excess cladding temperature (above the threshold).

Level 2 concerns release into the environment, or more exactly the assessment of the "source term" of radioactive release. This criterion level may be too restrictive : level-2 PSAs generally focus on Large and Early Release, which occurs after a core meltdown. This criterion would be more general if one focused on all types of release, even those (the least rare) that occur without any melting.

Level 3 concerns the consequences of release, in terms of damage (death) to the population.

Technical cover

Depending on the type of assessment to be performed, it is necessary to precisely define the coverage of the PSA : internal accidents, external or internal events, shutdown conditions taken into account or not. The coverage can also be defined by the generic or specific character of the assessment. Generic assessment is a satisfactory average for a group of plants over an average time period, while specific assessment is valid for a particular plant, over a particular interval of time.

Accuracy of the results

The results of a PSA should always appear in the form of central values (averages, medians, estimates) associated with an assessment of uncertainties (error factors, confidence intervals). Depending on the type of assessment sought, more or less accuracy can be required, in relation to the central values and also in relation to the assessment of uncertainties. In some cases, very pessimistic values can be accepted. In other cases, the best possible realism will be sought for.

Accuracy of the input data

The accuracy required for results will be governed by the accuracy chosen for input data : a particular effort must be made with respect to operating feedback. On the contrary, the accuracy of the input data is a restriction that inevitably limits the accuracy of the results.

Choice of the results - importance factors - legibility

The assessment only makes sense if it produces results. There are therefore requirements regarding the type of results produced and their presentation. The results can be presented by minimum cutsets or by accident sequences, according to whether one would rather have an equipment or a system view : one can consider only the cutsets, or the predominant sequences, or the overall results, depending on the information sought after. Lists of equipment or systems classified in order of importance are often required. The general requirement of legibility of PSAs should be studied thoroughly : it probably depends on the "reader" (the end-user).

3.2 Requirements related to prospecting objectives

An adequate assessment

Any "prospective" application requires a safety assessment in keeping with the objectives of the application. For example, if an objective is to help define a safe fallback configuration in a particular situation, it will be necessary to cover the shutdown conditions. If the purpose is to classify the operating incidents with respect to safety, it will be necessary to study their effects not only regarding damage to the core, but also regarding external release : the PSA should be a level-2 one. Thus, all the characteristics presented within the framework of objectives of observation will have to be defined according to the requirements related to the type of application.

Possibility of re-use

As a rule, the use of a PSA for a prospecting objective requires that the model is not static, but usable as a tool. More precise characteristics going under the name of "re-use capacity" can be defined.

Robustness characterizes models whose result accuracy is not modified by a change of assumptions or data, within a defined range.

Flexibility or the feasibility of *sensitivity studies* characterizes models whose inputs are easily accessible and modifiable in order to assess the effects of the modifications.

The *level of detail* of the models is a characteristic first induced by the requirements related to the type of assessment one wishes to make, but also, especially, by the requirement of robustness.

Performances

PSA applications require frequent use of computerized PSA models. Response-times and capacities must therefore be sufficient to avoid penalizing the performance of the applications. This is particularly true for "real time" applications, but they are still very little developed today. Let us simply say that tool performances must not prevent reaching the other technical characteristics required by the applications.

3.3 Requirements related to safety demonstrations

Validity of the results - Quality Assurance

There are no real technical characteristics specific to the objectives of demonstration. The demonstration has to be in accordance with the demand, which can emanate from the higher authority of the plant operator, or from the Safety Authority. These replies require a sufficient level of quality (notably of traceability) confirmed by adequate Quality Assurance. What is at stake here is the validity of the results produced by the demonstration.

The objective of the request for a demonstration can be of the "observation" or "prospecting" type : the characteristics presented in the above paragraphs must be checked as part of a safety demonstration.

3.4 Requirements related to the approach of understanding phenomena

Realism of models

Beyond the validity of the results, the realism of models, i. e. the realism of the functional and dynamic reasoning that provides results, is essential in a development approach. The approach of understanding phenomena is essentially interrogative and qualitative. Therefore the model is especially useful as a description of the phenomena. For instance, it may be proved, during a demonstration approach, that the scenarios derived from the addition of source losses have a negligible probability. A rough model is sufficient for that. Beyond results, the approach of understanding will search to study the interactions between electrical sources and to bring to light the fragility of the installation due to addition of this kind. For this purpose, realistic models are required.

Mastering the validity of the models

The question here is one of effectively mastering validity rather than ensuring absolute validity alone. The objective is to know the limits of the validity of the models, to try to develop them, and not necessarily to obtain a final validity, that would only be a pipe-dream. Without going into detail (this is not the purpose of this text), we will mention here some limits of PSAs, which are all fields of development in which knowledge of the phenomena should be developed :

- *operating feedback* provides data whose accuracy is very variable. Furthermore, it only gives access to events of relatively high frequency. It is the basis of probabilistic studies, but an incomplete and vague basis ;

- the *human factor* is taken into account through models of probabilistic assessments that are very succinct, even if, as in France, it relies on many test campaigns on simulators ;

- *social and organizational aspects* are ignored by PSAs - would we know how to model them ? - yet it is known that they play a predominant role in the functioning (and the dysfunctioning) of complex socio-technical systems ;

- current techniques allow satisfactory modelling of neither *instrumentation and control* nor *software* ;

- PSAs are global and abstract models that can make people forget the *physics of phenomena* ;

- even if PSAs are global models, *cumulative effects* and functional and temporal interactions are insufficiently modelled ;

- *uncertainty* is often measured with arbitrary models. Furthermore, these models are "central" models (probability densities decrease with distance from the average) : is this really representative of reality ?

- PSAs are based on *static classifications* : classified accident initiating events, constant samples of operating feedback, etc. These equipment lists are never queried, although they determine a large part of the contents of PSAs . . .

Transparency

This characteristic derives from those outlined above. A PSA (even a supposedly simplified PSA) is a complex model. Mastery of the validity of models, work on their limits, assumes that the totality of the assumptions, of modelling choices, is traced out and accessible to users. Therefore the PSA must be a "transparent box", as opposed to a "black box" that would only give access to the inputs and outputs. Here again, we find the problem of communication between the various users (specialists and end-users) mentioned in § 1. 3.

4. POSITIONING OF SOME PSAS

From the above developments, we can try to situate existing PSAs according to their capacities to reply to possible requirements. All the demands we have presented are as many criteria that can enable us to position PSAs. Does a given PSA enable us to perform a given application ? Is a given PSA suitable for developing knowledge relative to one type of accident or another.

As an illustration, we have carried out this positioning exercise for some typical PSAs. This exercise must be considered as merely an illustration of no demonstrative character : this is why it is presented in appendix 2.

PART THREE - QUESTIONS TO BE DEBATED

The above text, which could be described in Latin as "Abusus non tollit usum" (abuse does not exclude use) raises a certain number of questions regarding PSAs. We are going to raise them as more or less provocative and schematic affirmations which summarize the positions presented in this document, as an introduction to the debate.

1. ***The choices of methods are not the essential question raised by PSAs. The essential question is rather that of the mastered contents of models according to needs.***

We have seen in the first part that comparisons cannot reach definitive results. Moreover, every reliability engineer knows that any problem can be solved with any method by adding a dose of appropriate expertise. Then the important thing is to trace this expertise exactly to justify the results and to be able to use them again.

2. ***Concerning methodology, we should search for complementarity between methods, rather than stick to a definitive and unique choice.***

Methods are only a means : we should use the best means for the problems raised. This also sets the question of the tools supporting each methodological approach : today these tools are too "compartmented" : we have to succeed in making them communicate.

3. ***There is too often a tendency to use PSAs to make safety demonstrations, to use the results without querying them, forgetting the limits of the models.***

Therefore it is necessary to work on the approach of understanding, by improving, for instance, the legibility, traceability, and transparency of the models. We should also work on the junction between the demonstration approach which aims to produce operational results, and the approach of understanding which aims to make us question the limits and uncertainties of models.

4. ***The objective of distribution of PSAs to non-specialists has not been reached today, and is still a distant ambition.***

Considering the complexity of the models, and their fragility, the use of PSAs today seems to be reserved for specialists. It is their responsibility to disseminate information collected from the PSAs in a transparent enough way to help in taking decisions. This is the question of communication between specialists and end-users of PSAs. How should we go about making the end-users receive the knowledge dealt with in the PSAs ? What kind of requirements should PSAs (and the specialists) fulfil to meet this requirement ?

APPENDIX 1

RELIABILITY DATA USED IN THE EXAMPLE OF PART ONE

- *External supplies : functional incident on the network*

Frequency :	f_r	= 2.5E-2/year
Mean time to repair	τ_r	= 1h

- *External supplies : major malfunction on the substation or on the network*

Frequency :	f_p	= 3.5E-4/year
Mean time to repair	τ_p	= 48h

- *Diesel generator*

Probability of failure on start-up	γ_d	= 3.4E-3/demand
Rate of failure during operation	λ_d	= 7.7E-3/hour
Mean time to repair	τ_d	= 30h

- *Turbine-driven Pump (turbine and pump)*

Probability of failure on start-up	γ_t	= 2.7E-3/demand
Rate of failure during operation	λ_t	= 3.6E-3/hour
Mean time to repair	τ_t	= 15h

APPENDIX 2

POSITIONING OF SOME PSAS

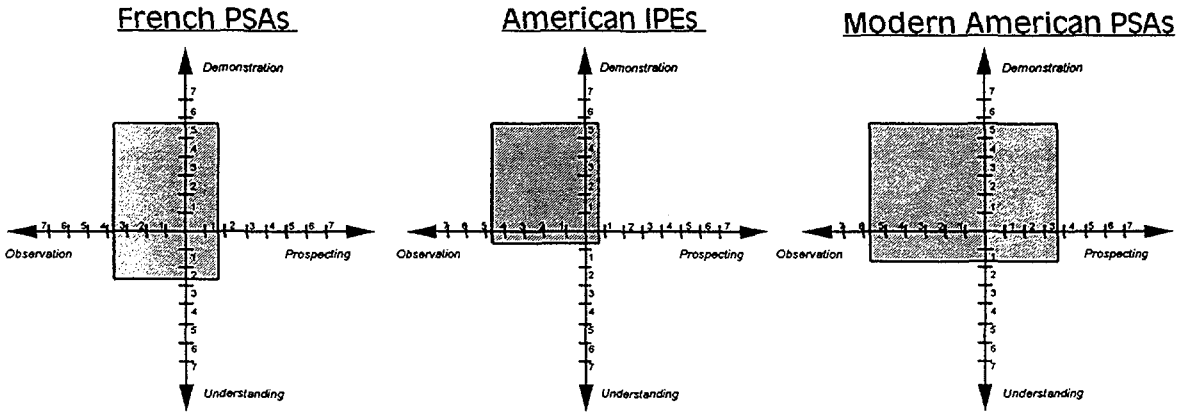
As an illustration for the second part of this document, we have carried out a positioning exercise for some typical PSAs of the international community, depending on the degree of the match with the categories of needs we have defined. We have chosen only a few PSAs : the first French PSAs from the late 80s, the American IPEs (Individual Plant Examination) of the 80s, and the recent American PSAs developed for plant operators.

The proposed positioning is illustrated with a four-axis measurement, representing the four categories of characteristics we have presented (see next figure). The horizontal axis represents the characteristics related to the objectives of the PSAs (objectives of observation, objectives of prospecting). The vertical axis represents the characteristics related to the approach for using the PSAs (safety demonstration, understanding of phenomena).

To carry out this exercise, the axes are given a totally arbitrary notation from 0 to 7. The hatched zone synthesizes the "marks" assigned to the four categories of characteristics.

We should specify that the "marks" are assigned as a guide, and that they are solely the opinion of the author of this document.

Positioning of some PSAs



Some comments on the graphs

- The characteristics related to the demonstration of safety are relative : they depend on the requirements of the requesting bodies. An assumption : published PSAs correspond rather well to these requirements.

- Regarding the objectives of observation, French PSAs are among the first to process shutdown conditions and the only ones to process long-term defences against LOCAs. But for the moment, they are only level-1 PSAs : they do not process external events, nor do they provide any list of contributions of systems and components. The American IPEs have a larger coverage and produce more numerous results. Modern PSAs are still progressing, since a lot of them also process shutdown conditions.

- Regarding the "prospective" objectives, we have made the assumption that American IPEs were not suitable for that, and therefore do not check the characteristics of re-use capacity and robustness. Applications of the prospective type (based on various sensitivity studies) were mentioned in the specifications of French PSAs. However experience shows that these applications require numerous and difficult adjustments (in progress). Recent American PSAs, intended for plant operators, are subject to many developments for the applications. The "marks" given show the American advance in the field of PSA applications. They also highlight the improvements which remain to be performed in this field.

- Finally, we have considered that French PSAs were more oriented than others towards the approach of understanding (efforts relative to sequence interactions ; effort of traceability, notably for the studies of elementary systems, with the development of expert systems for assistance in model building ; effort on operating feedback and probabilistic assessment of human reliability). We have made the assumption that this was not the objective of American IPEs. However, by making efforts on applications, recent American PSAs have necessarily progressed in this field. In any case, the margin of progress remains enormous for everybody.

NOTATIONS AND REFERENCE

[1] Ref. : "Probabilistic Safety Assessment of Reactor Unit 3 in the PALUEL Nuclear Power Centre (1300 MWe)" EDF-Electricité de France (1990)

[2] Ref. : "Probabilistic Safety Assessment of 900 MWe Standard Nuclear Power Unit " CEA - Commissariat à l'Energie Atomique (1990)

[3] Ref. : "CAFTA User's Manual" SAIC (1992)

[4] Ref. : "RISK SPECTRUM V2 User's Manual" RELCON (1993)

[5] Ref. : "RISKMAN PRA Software V 5 User's manual" PLG (1993)

[6] Choice of the different methods for the 1300 PSA :
Models representing the top events.
For the engineered safeguard system (eg : Safety Injection), whose mission times are generally short, and where we can consider that there are few reconfigurations and repairs, the fault-tree method has been chosen.
For the support systems (ex : power system supply), that are in permanent operation, we have choosen to take into account reconfigurations and possible repairs : the state graph method has been chosen.
Models representing the scenarios
Most of the scenarios have no great temporal interactions (eg : breaches in the secondary system, where all the engineered safeguard systems start at the same time). Therefore the event trees just perform simple multiplications between the probabilities of the top-events.
Some more complex studies make important temporal interactions intervene (repair of the initiating events, delayed starting time, time before core meltdown). Then the event trees perform products of convolution between the various laws of probability of the top-events.
Finally, for long-term studies of LOCAs, where systems' repair can intervene during various phases of operation, the state graph method has been chosen.

[7] Ref. : "LESSEPS V2 User's Manual" EDF (1994)

[8] For example, Ref : DOUGHERTY E M, "Time Consideration in Recovery Analysis", Reliability Engineering and System Safety, 35, (1992)

[9] Ref : MAGNE L., BALMAIN M. "Comparisons of Various Methods Used in PSAs : First Lessons" PSA'93 (1993)

[10] Ref : RASMUSSON D M, "A comparison of the Small and Large Event Tree Approaches Used in PRAs", Reliability Engineering and System Safety, 37, (1992)

[11] For this topic refer to
- DEWAILLY J. : "Applications des évaluations probabilistes de sûreté pour l'exploitation des centrales nucléaires" (Report of a Technical Commitee Meeting IAEA 20-23/9/1993), EDF-DER, HT51/94/001A, (1993)
- DEWAILLY J, DERIOT S, FRANCOIS P, DUBREUIL-CHAMBARDEL A, MAGNE L, "Living PSA Issues in France on PWR", EDF-DER, 93NB00183 (1993)

[12] However, some products derived from PSAs, such as risk-monitors, are intended for non specialists. But on the one hand, these users do not deal with a PSA directly, and on the other hand, the operational risk-monitors are rare, with the notable exception of the ESSM product of Nuclear Electric Co

[13] Topic 4 : FRANCOIS P, "Incident Analysis" §2

[14] Topic 4 : FRANCOIS P, "Incident Analysis" § 3.2

[15] Topic 3 : DUBREUIL-CHAMBARDEL A "PSA Applications" § 2.5.