83

INTERNATIONAL SEMINAR ON PSAs AND HUMAN RELIABILITY

Paris, November 21st-23rd 1994

Topic 2 : PSA Applications

A. DUBREUIL CHAMBARDEL

CONTENTS

1. INTRODUCTION

At the outset, PSAs were made in order to assess or to demonstrate the level of safety of nuclear power plants. For the most part they were studies carried out "after the event" (the unit had been designed and in some cases was already in operation when the PSA was performed). The role of PSA has gradually changed: from purely regulatory use in demonstrating safety, it has found more technically and economically oriented uses as support for the design and operation of nuclear power plants.

The IAEA now defines three types of PSA applications [1]:

- validation of design and of operations procedures,
- optimization of plant operation, and
- regulatory applications.

The applications of PSA are manifold: only a few are dealt with here (precursor analysis is dealt with in session 3 , topic 4). For each of them, we will do the utmost to demonstrate the main difficulties encountered, EDF's viewpoint on the matter, and the points remaining to be solved.

2. APPLICATIONS

NB: In what follows, unless explicitly stated otherwise, we have made every effort to represent the different applications as they are practised by all concerned in the international community, and to describe the inherent difficulties the international community has encountered with these applications with all objectivity. It goes without saying that the comments below are simply those of the ESF department, and are submitted here for discussion by the experts.

FOREWORD

The first difficulty and limit encountered in PSA applications is obviously that of their validity. PSA validity problems have a large number of varied causes.

Regardless of the efforts made to improve their exhaustivity, there are scenarios that have not been taken into account and events that have not been imagined, as Professor Östberg has explained [2].

Moreover, PSAs are highly complex models. Mistakes are consequently practically inevitable. There is no means of completely validating them, whether it be through feedback or any other means, contrary to a thermohydraulic model, for example, which can be validated with a mock-up on a test loop. Precursor analysis, which can be a means of comparing incidents that have actually occurred with the start of PSA accident scenarios, is thus the best means of partially validating PSA.

PSAs often run up against the boundaries of current knowledge of the operation of the plant. It is not generally possible to go beyond the limits of the codes of thermohydraulics or neutronics[1]. Similarly, it can be considered that common mode failures are evidence of the improper knowledge of interactions between plant items (if it was possible, we would modelize these interactions explicitly).

Reliability data concerning equipment, and especially operators, is often tainted with error. It is often generic and imperfectly adapted to the power plant being studied, or, if it is specific, has a relatively wide confidence interval.

Whatever the application to which PSA is put, it is therefore necessary to properly estimate the degree of confidence one can have in the result before it is used.

2.1 DEMONSTRATION OF SAFETY

2.1.1 Description

This is the "oldest" application. It consists in assessing the level of safety of the unit (risk of core melt, of emission of radioactive matter or radiological consequences) and ensuring that:

- the risk is low, and above all well "distributed" across all the accident scenarios and systems,
- there are no predominant cut sets,
- and, consequently, there is no serious defect in the design or operation (procedures).

Sometimes PSA is also used to demonstrate that quantitative safety objectives have been attained. Finally, PSA can also be used to assess the impact on safety of a modification to the design or to an operating rule, and thus to justify the implementation (or non-implementation) of the modification.

2.1.2. Specific Difficulties

This application of PSA is one of the least controversial. It is performed *post hoc*, or in deferred time, by PSA specialists, and the results can be thoroughly analyzed before they are used.

However, when a quantitative safety objective is to be demonstrated, there is inevitably a bias in the study which can then be carried out not to objectively assess a design or a procedure, but to demonstrate that a certain result has indeed been achieved.

---

1 *Unless expert judgement is used to probabilize the consequences of a given situation that thermohydraulics or neutronics codes cannot assess! But what control does one have over the results?*

Assessment can then become subjective and, worse yet, analysis can home in on the (desired) final result, whereas it is essentially qualitative results interpreted in the light of numerical results that are of real interest (what are the "common modes" that give the lie to deterministic design principles ? What are the main contributors to risks ? Is a given risk spread broadly throughout the different states of the unit ? Are there any dangerous operating configurations that should be avoided ?, etc.).

2.2 PSA : A DESIGN-SUPPORT TOOL

This application is dealt with in more detail in the paper presented on Topic 3.

2.2.1 Description

The objective is the same as for the safety assessment of an operational reactor, i.e. to check the uniformity of design, in terms of safety, to determine weak points in design, to compare two architectures, etc.

2.2.2 Specific Difficulties

The problem of the validity of PSA is particularly acute for reactors at the design stage which are being "optimized". On these reactors, the "defects" identified from feedback on operational reactors or by PSAs have been corrected. The preponderant accident scenarios in the first PSAs therefore become improbable or even impossible; the risks are therefore displaced, and what was a negligible risk for the older reactors may become the preponderant risk. It is therefore constantly necessary to improve the exhaustivity of PSAs, and this becomes excessively complex when one is dealing with risks of core melt of about 10^{-7}/year. From EDF point of view, this kind of value seems quite impossible to prove, unless "very same scenarios" as those of operating plants are used and new potential scenarios are supposed to be negligible..

In addition, to be able to have an effective impact on design, these studies are often carried out before design is complete. This means the operating practices (procedures, organization, training,...) or details of instrumentation and control of the unit are not necessarily available; but it is precisely these elements that are often major contributors to risks. The assessments that can be made and the conclusions that can be drawn from them may sometimes be biased.

Common-mode failures pose a particularly intricate problem for reactors of new design : the systems of such future reactors have higher degrees of redundancy than current reactors, and have been subject to more or less major diversification. It is therefore extremely difficult to extrapolate common-mode failure rates for the future reactors on the basis of feedback from existing reactors. For example, given the uncertainties on common-mode failure rates, the comparison between a two-times-100% scheme and a four-times-50% scheme has no real significance.

For PSAs for "passive" reactors, a large number of additional difficulties appear : evaluation of the earthquake resistance of large tanks high above the ground, probability of triggering of thermohydraulic problems like natural convection in highly impaired situations, reliability and "testability" of passive components, irreversibility of some phenomena, appreciably modified operator role, etc. For EDF, it is seen to be a particularly delicate undertaking to demonstrate the risks of core melt or of extremely low emissions, as some have done.

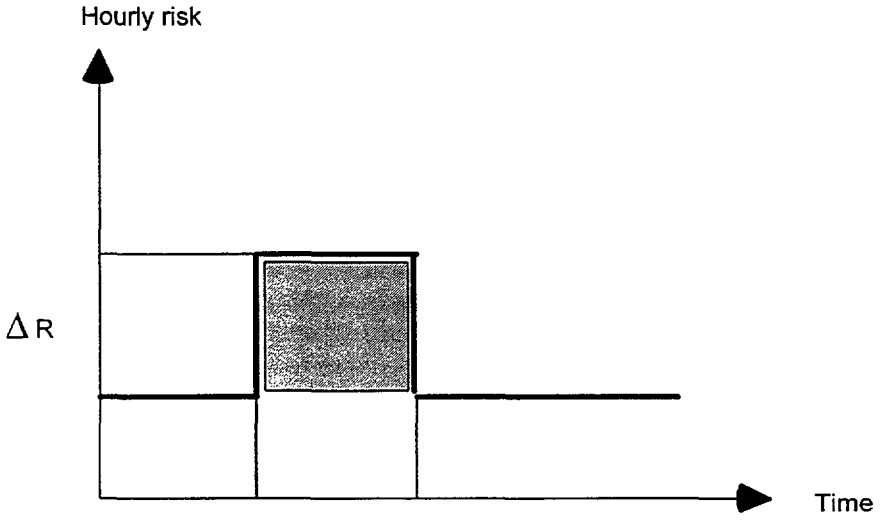
Moreover, the OECD recommends pursuing research and development on thermohydraulics and neutronics codes in order to validate the design of future reactors, and to make use of large-scale test loops to check the design of the passive systems of this type of reactor [3].

2.3 OPERATING TECHNICAL SPECIFICATIONS

2.3.1 Description

In the event of scheduled or unscheduled unavailability of a safety-related equipment item, operating technical specifications (OTS) are there to ensure that continued reactor operation does not engender an excessive increase in risks.

PSA can be used to assess any increase in risk :



The additional risk is the product of the increase in the hourly risk, ΔR and the duration of unavailability while the unit remains operational.

Criteria vary from one country to another. However, they can be summed up as follows : if the increased risk brought about by keeping the unit operational with the item of equipment unavailable exceeds a certain absolute value or a certain percentage of the basic risk determined by the PSA, the unit must go into a fallback state in which the consequences of unavailability of the equipment will be lesser. This is to be done more or less quickly, depending on the risk.

2.3.2 Specific Difficulties

There are two types of problem for this application.

The first concerns the method used to calculate the increased risk. It is tempting to use importance factors (particularly Risk Achievement Worth which is generally calculated by numerous softwares : CAFTA, RISKMAN, RISK SPECTRUM, ...) to estimate this risk. But importance factors are often calculated from a set of preponderant cut sets obtained during a Boolean reduction of event trees. In order to avoid combinatorial explosion, probabilistic truncation thresholds are used : these can be in fault trees, in event tree sequences, or in the full model. If the thresholds vary from one model to another (fault trees or branches of event trees), it is absolutely impossible to guarantee that the preponderant cut sets in which a given equipment item is concerned are indeed those which are actually quantified. Consequently, the relevance of importance factors and the resulting calculation of operating technical specifications cannot be guaranteed.

For these factors to be correct, a single truncation threshold must be used, and it must be used at least at the level of the accident sequences or of the full model. In this way it can be guaranteed that all the cut sets whose probability is greater than the threshold are retained. The disadvantage of this approach is that a threshold entirely suitable at full PSA level is by far inadequate at system level. A trade-off must be made between the two types of thresholds, which implies a small number of cutsets that can be retained and a relatively long full PSA processing time.

Another way of handling the problem is to carry out sensitivity studies on a case-by-case basis. This can be envisaged in the case of a processing code using numerical-linking, which can be much faster in terms of computer time than a Boolean code (this aspect is detailed in session 1 of Topic 1). However, the models must be sufficiently robust to take the probability of failure of an equipment item to 1, and the tools must be sufficiently advanced to easily carry out these sensitivity studies.

The second problem concerns the validity of this type of operating technical specifications which are based only a calculation of risk for an operational reactor. It must be remembered that taking a unit to a fallback state can increase the risk :

- protective automatic systems often cease to operate as soon as the reactor is shut down,
- in addition, during reactor shutdown and start-up transients, there is a definite but not-easy-to-quantify risk (start up of equipment, human intervention, fragilization of the containment and other equipment due to thermal or mechanical fatigue linked to variations in physical parameters, etc.).

It is therefore necessary to carry out a calculation for each reactor state, taking the best possible account of the risks induced by transients, and to do so, the PSA must cover shutdown states in order to define a correct fallback state (if there is one), and to compare the risk linked to sustained operation with that linked to the change to the fallback state.

2.4 RELIABILITY CENTRED MAINTENANCE

2.4.1 Description

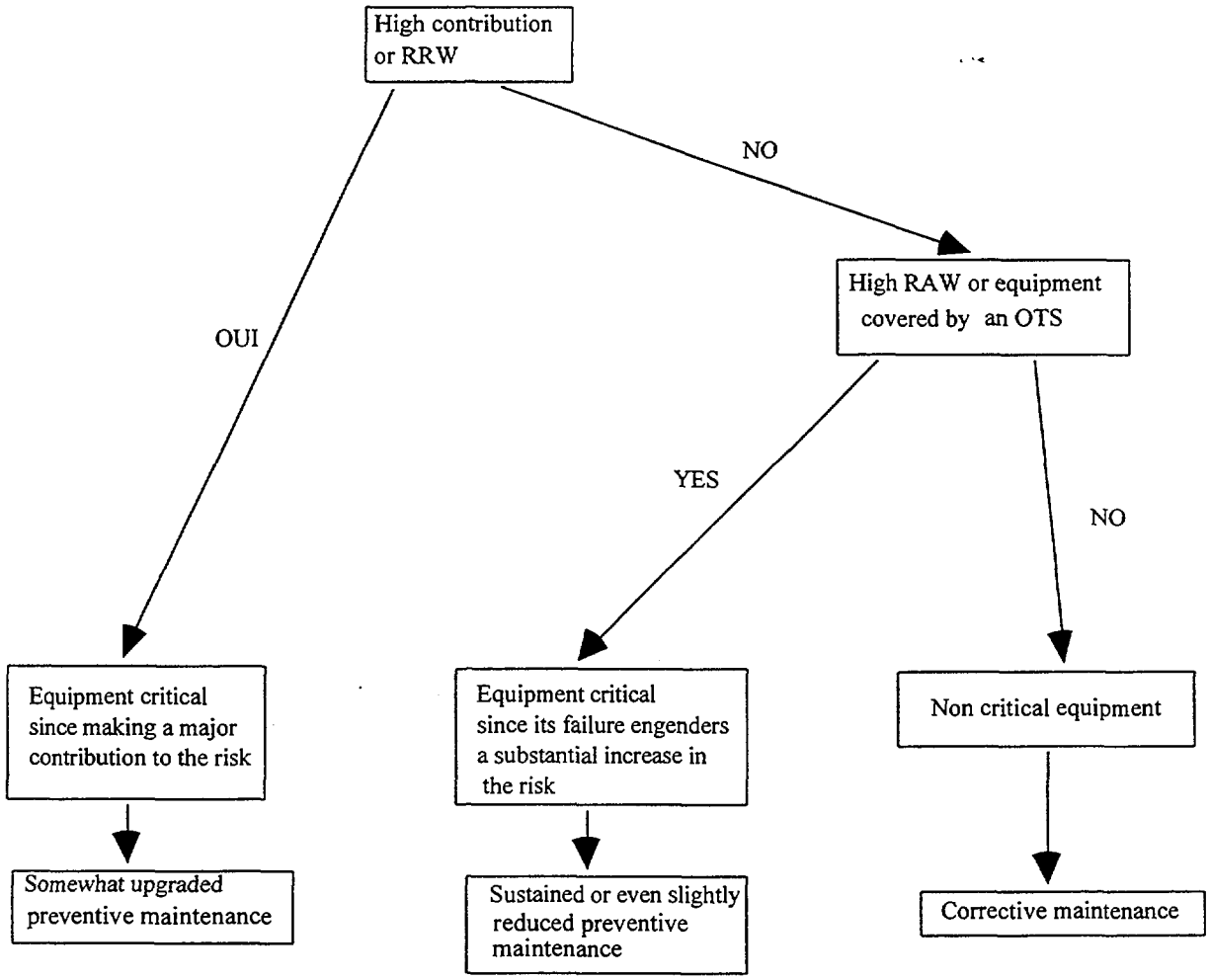
The objectives of Reliability Centred Maintenance (RCM) or Reliability Based Maintenance (RBM) are generally as follows :

- to reduce maintenance costs (preventive and corrective) while guaranteeing or even improving levels of safety and availability of units;
- to have an approach for drawing up traceable and updateable basic preventive maintenance programmes (living programmes).

In what follows we will discuss only RCM approaches, without mentioning the cost-benefit ratio of this kind of study (cf. debate between conventional RCM and "streamlined" RBM approaches). Similarly, RCM approaches may or may not use PSA results. We present here an EDF proposal under tuning for an approach based on the use of PSA.

EDF Approach

Only the links between RCM and safety aspects are presented.



With the help of importance factors (Risk Achievement Worth and Risk Reduction Worth), equipment is classified into three categories :

- equipment requiring somewhat upgraded preventive maintenance, for an increase in its reliability results in a substantial gain in safety;
- equipment requiring sustained or slightly reduced preventive maintenance, for a decrease in its reliability results in a substantial loss in safety; this maintenance need not be upgraded, for an increase in the reliability of the equipment does not give rise to a major gain in safety;
- equipment requiring only corrective maintenance, for its unavailability does not result in a major increase in risk.

Even level-2 PSAs cannot cover all aspects of safety (like dosimetry problems); the approach must be complemented with operating technical specifications.

In addition, for equipment requiring a preventive maintenance programme, importance factors, together with other indications like failure modes or impairment modes actually encountered with the equipment, the efficiency and cost of current maintenance or of a proposed new maintenance programme, can be used to define it.

2.4.2 Specific Difficulties

Such an approach[2] makes intensive use of importance factors : these calculations are performed for all equipment. This poses problems with Boolean tools for equipment whose contribution is low[3] (this equipment is not involved in the preponderant cut sets and the calculation of the importance factor is difficult, if not impossible), and the calculations are more complex with numerical linking codes.

This use of PSA requires high-quality data, and therefore makes extensive use of feedback on experience. But feedback introduces a problem of bias : equipment which is not particularly critical because it is reliable with the current maintenance programme may cease to be so reliable if its maintenance is reduced, and may then become critical. Importance factors must consequently be used with caution : no decision can be made to upgrade or reduce maintenance, and even less so to eliminate it, on the simple basis of an importance factor. These factors must be used in conjunction with other information obtained from feedback or from expert judgement on equipment (see diagram above). Experts can indeed judge the predictable evolution of the reliability of equipment in accordance with the envisaged maintenance programme, whereas safety experts can, with the help of PSA, judge whether this evolution is acceptable or not.

RCM studies (and particularly the selection of failure modes for critical equipment) therefore call for different skills to be brought together.

Finally, it is difficult to measure the impact of maintenance on the failure rate of equipment and on the rate of unavailability for maintenance purposes (scheduled or unscheduled). It is thus necessary to take account of the risk of improper equipment configurations as a result of errors in maintenance operations (the significance of these last two points was brought to light by the EPS 1300 PSA).

---

2 *In other RCM approaches, PSA is used only to detect important safety functions and the systems involved. This obviously raises fewer problems with respect to the utilization of PSA, but does not provide a comprehensive answer to the NRC "maintenance rule".*

3 *There is in fact a problem with Boolean models if the probabilistic truncation threshold used for the reduction of the models is greater than the contribution threshold adopted to define the equipment requiring a preventive maintenance programme.*

These negative effects of maintenance must be analyzed. By introducing them into a PSA model, they can be compared to the advantages brought about by increased reliability of equipment or its sustained reliability resulting from maintenance.

2.5 RISK MONITOR

2.5.1 Description

PSA can be used for real-time or more or less deferred assessment of the risk run by a unit in a given situation. These assessments can be for a variety of purposes; they are often lumped under the name "Risk Monitor".

One of the most interesting utilizations of the Risk Monitor is to compare different operating strategies (normal, incident status, or accident status). Let us look at some examples :

- control of the residual heat removal system in normal operating conditions (is it better to have one or two trains operating ?)
- control of the residual heat removal system, of long-term safety injection and containment spray after a LOCA (what systems should be used as basic requirements, and what other systems should kept on standby; should the H4 link[4] be used as soon as it is available, or only as a last resort ?, etc.).

Risk Monitor tools can also be used to plan unit shutdown (ORAM, Dial-Cafta, [4]) and, more generally, maintenance. For instance, these tools enable to know whether, for a given unit configuration, an equipment item can be locked out without running too great a risk, or whether it would be more advisable to wait until other equipment is available again, or whether the reactor status should be changed before the equipment is taken off line. If this application is used after unscheduled unavailability, to determine the operating status to be instituted (rather than to know when and how to schedule unavailability), the application becomes a practically real-time calculation of operating technical specifications (cf. ESSM, [5]).

Finally, if the value of the hourly risk determined by the Risk Monitor is integrated over a full year, one can obtain an indicator of the level of safety of the unit. This should be compared to the NRC Safety Index obtained as part of the ASP programme [6] (see also the paper devoted to precursor analysis - topic 4).

---

4 *The H4 link is an arrangement which enables French PWR units to link Containment Spray and Low Pressure Safety Injection pumps. These two systems can thus back each other up, and, in the case of a LOCA, each of them can perform safety injection and discharge residual power from the containment several days after the accident.*

2.5.2 Specific Difficulties

This application has not yet been developed by the EDF. The following comments are therefore only suppositions.

Of all the applications presented here, this is the one that can have the most direct consequences on control (in the broadest sense including maintenance). It therefore has a very great effect on safety. This application is potentially dangerous, particularly since it is "close to" power plant operators who are not adepts of reliability, and is "far from" PSA specialists.

PSA must be thoroughly understood for its results to be properly interpreted. This application must therefore be implemented :

- either with the subsequent (deferred) help of a PSA expert,
- or, possibly with only very slight deferment (cf. ESSM), if the number of cases processed by the tool is restricted and all have been previously tested by a PSA expert (before being set up in the power plant). But the PSA application then loses all its interest : it becomes a PSA result presentation tool rather than a calculation tool.

In addition, it would appear to be prudent to start by setting this type of application up in safety engineering services before considering setting it up in maintenance services or in the control room.

It goes without saying that the use of the Risk Monitor solely for safety level assessment purposes does not raise the same type of problem as for control-support purposes. Questions might nevertheless be asked about the representativity of such an indicator : ESSM measures the supplemental risk over the basic risk (all equipment available) linked to unavailability of equipment; the Safety Index of the ASP programme measures the risk induced by the most significant events (this risk too is supplemental to the basic risk). With the possible exception of simple unavailabilities resulting in non-compliance with operating technical specifications and multiple unavailabilities, no common event is taken into account in these two indicators. Individually therefore, they cannot really represent the safety level of the unit. Yet they seem to be complementary. Furthermore, as the NRC has observed, shutdown states must be taken into account in the estimation of these safety indicators (something ESSM does not do for the moment[5]).

Finally, since Risk Monitor tools are based on an estimate of the hourly risk of the unit, one might ask what purpose this application serves if it does not use :

---

5 *ESSM is used for reactor No. 2 of the Heysham plant. It is an AGR unit. Nuclear Electric experts consider that the risk in shutdown states is negligible with this sort of reactor. Unfortunately this is not so true for PWR reactors.*

- unit-specific data (this is feasible for equipment, but is impracticable for human-factor data); and
- instantaneous data, i.e. which is representative of the current status of equipment and operators, and not averaged data for the entire lifetime of the unit. It is practically impossible to generate such instantaneous data.

3. CONDITIONS FOR USE OF PSA

The conditions for use of PSA pose organizational problems. These problems depend on the type and structure of the entity (designer, operator, etc.; number of units operated, engineering services on site or delocated, etc.). The following applies particularly to entities like EDF (large number of units operated, and highly centralized engineering services).

PSAs are generally performed first of all in connection with a demonstration of safety. They are often ill-suited to applications aimed at providing support for design or operation. They must be "fine tuned" and complemented. In addition, as the number of applications is on the increase, they can no longer be the sole reserve of reliability specialists, and must gradually be made available to "design" or "operation" experts who are not necessarily dependability specialists. It is thus clear that these "comprehensive" and "complex" PSAs developed essentially for safety assessment are not at all "user friendly" for those not previously involved in their development.

It is therefore necessary to find an optimum level of detail. This level must be sufficiently detailed for analysts to find the information they want from a PSA, while being sufficiently limited for the model to remain within the bounds of human understanding and to enable design and operation specialists - who must be able to introduce their expertise (which dependability experts do not have) - to effectively handle the model and use it in their applications. This level of detail must also be uniform : as has been said in paragraph 2.1.2, in the case of processing of a PSA using a probabilistic truncation threshold that varies from one sequence to another, there is a risk of introducing equipment with minor contributions into the minimum cut sets while eliminating other more important contributions. In an RCM programme, poor interpretation of results could result in maintenance being upgraded on equipment with relatively insignificant safety functions, to the detriment of much more vital equipment.

In fact, the essential thing is to ensure that the model is robust, i.e. to ensure that everything that is modelled and quantified is modelled and quantified correctly :

- only the most important equipment failure modes and human errors should be involved,
- the major sequences where these events occur should be modelled and quantified.

It is better for an equipment item not to be modelized at all than to be modelized incorrectly.

In the first case, no conclusions will be drawn from the PSA, and means of decision support other than PSA will have to be used, or a specific model will have to be developed in response to the problem; in the second case, erroneous conclusions could be drawn, with possibly drastic consequences on plant safety, availability, or operating costs.

To minimize the risk of improper use of these studies by persons who did not work on their development, it may be useful to draw up "operating instructions" for the studies (by "operating instructions" we mean any support for the use of a PSA, whether an adaptation of the computerized PSA model or paper documentation). "Operating instructions", as the term is understood at EDF, is based on extensive use of the graphic interfaces of the PSA model. All the basic events, the generic events, and accident sequence probabilities are featured in it and commented on. The main assumptions required for the construction of fault or event trees are specified. A synthesis can also present the architecture of the PSA : the different sets of accident scenarios, the systems involved, the link between the systems and accident sequences (which sequences a given system or item of equipment might be involved in). This document can also specify the scope of validity of the PSA (what data or assumptions can be varied without detracting from the validity of the result ?). This sort of document is undoubtedly difficult to draw up, but it provides PSA users with precious help [7].

For all the applications of PSAs aimed at loosening regulations, one has to start with realistic PSAs that are neither too conservative (in which case nothing at all can be relaxed!) nor too optimistic (in which case the demonstration would not be credible). That is how EDF came to study reactor shutdown statuses (indispensable for determining technical operation specifications or organizing maintenance programmes) and long-term scenarios. The long-term scenarios were particularly valuable, enabling assessment of the benefits of medium-term emergency action between low-pressure safety injection and containment spraying; without this mutual emergency action, the medium-term risk (beyond 14 hours) is far from negligible. These fine features of modelling result in not only a relatively advanced level of detail, but also a varied choice of methods. Apart from fault trees, EDF has used Markovian techniques [8][9] and a method for quantification of event trees automatically taking account of the actual operating time of systems operating in normal-emergency mode and the repair of equipment which can avoid arriving at unacceptable consequences [10]. Moreover, use of Markovian techniques is recommended by the IAEA [11].

However, sequential methods are often more complex to use than Boolean methods, and can give rise to models which are more difficult to use in applications (cf. paper on this subject presented to the Seminar : Topic 1). They do have the advantage of not requiring simplifying assumptions to take account of sequential aspects, and therefore make more robust models with fewer implicit assumptions, so they are more easily traceable, though often less legible[6]. Sequential models must be used appropriately. As for the level of detail, a trade-off must be made between the level of detail of the mathematical model and its ease of use.

---

6 *For the same modelling precision, sequential models like Markov graphs are more traceable than Boolean models if time dependencies are taken into account. However, when a Markov graph is used, the opportunity is taken to model a large number of time dependencies whereas normally, with a Boolean model, the model would be restricted to the most important time dependencies; Boolean models therefore appear to be simpler and more legible than the graph.*

The development of applications implies that there will be a greater number of users on a variety of sites. These applications can be used to enrich PSAs [12]. Precursor analysis, for example, will validate or invalidate the accident scenarios of PSAs by comparing them to actual incidents; it can thus highlight initiating events not taken into account in the PSA or recalculate the probability of occurrence of an event. To facilitate coherence between these applications and to allow them to benefit from information from the others, it is advisable for the applications to be able to communicate with each other. If not the concept of living PSA has no real meaning!

EDF has therefore developed its PSAs on networked work stations, and attributes much importance to the management of the data and models : studies of sensitivity to a change in models or data are performed without "overwriting" the results of the "reference study". This organization makes it possible for each developer to work on his own applications with the same reference model as other developers. The reference model approved by the safety authorities is updated from time to time, taking account of new feedback on experience, amendments to design or operating procedures, and the contribution of the various applications to the PSA models. Such inter-model communication can obviously be achieved in other manners. The fundamental point is to establish communication between the different users of a PSA, and for PSA specialists to be able to guarantee the relevance of the model used in accordance with the development it undergoes.

4. SYNTHESIS OF THE MAIN DIFFICULTIES - OUTSTANDING QUESTIONS

The first limit of PSAs, and one that is common to all applications, concerns their scope of validity :

Questions : How, depending on the application, does one define the scope of validity of a PSA (without testing all cases of application, one by one!) ?
When a PSA is used, how does one ensure that its scope is not overreached ?

A second difficulty associated with PSAs is the uncertainty hanging over the results. PSAs provide results that are more or less precise or relevant to a given criteria : the risk of core melt or of emission of radioactive products. To this criterion are added others related to decision-making (unit availability, cost of the intervention, doses to which operators are subjected, etc.). The safety criterion cannot easily be compared with the others.

Questions : How does one position this criterion given by PSAs relative to others (in the absence of precise regulations) ?
What credit can be given to an imprecise PSA result, even if it does measure a fundamental variable : i.e. safety, as compared to other criteria which are often much more precise but which measure less important variables ?

A third difficulty in the use of PSAs is due to their very complexity. PSAs represent a synthesis of a variety of knowledge :

- theoretical operation (codes)
- feedback (data, operation, operation modes)
- reliability
- human factors.

This makes their use by non PSA specialists problematical. Yet these users are specialists in design and operation (control and maintenance) who need the results provided by PSAs in connection with their applications.

Questions : Should PSA applications be solely the concern of PSA specialists or should they be made available to design and operation engineers ?
If they can be opened up to non-specialists, how can the transfer of know-how from PSA specialists to these engineers be effected ? What sort of training should the engineers be given ? What role should the PSA specialists play in the implementation of PSA applications ?
If they cannot be opened up to non-specialists, what sort of organization should be set up between PSA specialists and design and operations engineers so that PSA applications are really relevant ?

5. CONCLUSIONS

PSAs are one of the rare means of obtaining an overall view of the behaviour of a unit with which one can measure the criticity of phenomena (Seriousness x Probability). Models of thermohydraulic, mechanical, or neutronics codes are restricted to the "consequence" aspect and deal with phenomena on a case-by-case basis.

Furthermore, PSAs create a unique reference tool : it is possible to compare two equipment items, procedures, etc. in terms of the same criterion : core melt (or emission of radioactive products).

PSAs can also provide precious assistance for the design and operation of nuclear power plants.

However they remain tools of great complexity with which their potential users (chiefly among operators) are still relatively unacquainted. One should therefore be relatively cautious in the development of applications. At the same time as an application is developed, its scope of validity should be defined, its methods of use foreseen, work done on the ergonomics of the application in order to minimize the risk of acquisition errors and erroneous interpretation, and plentiful comments made on the models (if the user has access to them).

Although the final result of a PSA may be of relatively little value, all the expertise implemented in PSA is of great interest. It is a powerful tool for questioning a model of reality ("What would the risk be if ... ?"). More than probabilities, it is the scenarios, minimal cut sets, or sequences leading to the loss of a system or to an impaired operating condition which are of interest. The user of the application should therefore be helped to understand and interpret the results.[7]

In the field, in power plants, as well as providing support for the operation of units, the role of computerized PSA is to serve as a means of developing a safety culture among "operators" that will lead them to think about the potential consequences of the actions they intend to carry out or the incidents they have encountered, and which will develop in them some mastery of the operation of the plant, of the way in which it responds to "disturbances" (cf. INSAG 4, [13]). To do this, PSA models have yet to be sufficiently representative of the unit and consequently not instil erroneous knowledge among operators.

Whatever the progress made in reducing uncertainties, the exhaustivity of the situations considered, the quality of data, the user-friendliness and management of PSA, PSA is nevertheless a complex and approximate modelization of reality. It could certainly be a powerful means of analysis, but also a dangerous tool if improperly used. That is why progress must be made in the completeness and robustness of models, in the precise definition of their scope of validity, and in the ease with which users can learn how they work so that correct PSA applications can be implemented. This calls for the level of detail to be optimized, for the use of complex methods to be restricted to just a few cases, and for guides for using the studies to be drawn up. A compromise must be reached between complete but complex models and effectively usable models.

In addition, even complete and detailed PSAs will not answer all questions on safety. New roads that complement PSA must be explored, particularly those associated with human factors (psychological and cognitive aspects) or organizational factors (relative to operation and maintenance), in order to achieve a global approach to safety. Progress must also be made in the knowledge we have of PSA in order to precisely define its pertinent applications and the fields in which it can contribute nothing. These studies have yet to acquire a certain maturity before they can achieve recognized status like thermohydraulics, mechanics, or neutronics.

---

7 *Every time a result is obtained from a PSA, it must be understood and compared with what was predicted. As a good reliability specialist, an expert should mentally calculate the result he is looking for and compare it with the one he then gets with the computer model, and analyze any discrepancies. However, in this there is unfortunately a substantial element of bias, i.e. the representation one has of a nuclear power plant unit, which is limited by Man's intelligence!*

REFERENCES

[1] L. Lederman, F. Niehaus, B. Tomic
"Probabilistic Safety Assessment. Past, Present, and Future"
IAEA document yet to be published.

[2] G. Östberg
"Evaluation of a Design for Inconceivable Event Occurrence"
Materials and Design, vol. 5, April/May, 1984

[3] Nuclear Safety Research in OECD Countries
Report of Senior Group of Experts on Safety research (SESAR)
August, 1993

[4] Richard A. Michel
Using ORAM technology to reduce outage costs, improve safety
Nuclear News / April 94

[5] G.R. Moir
On-Line Use of PSA for Risk-Based Configuration Control
IAEA TCM on "Use of PSA for optimizing NPP operational limits and conditions" - Barcelona, 20-23 September, 1993

[6] J.W. Minarick
The US NRC Accident Sequence Precursor Program : Present Methods and Findings
Reliability Engineering and System Safety 27 (1990) 23-51

[7] F. Bruyère, H. Pesme
Mode d'emploi de l'EPS 1300 : Présentation générale de l'étude
(*EPS 1300 PSA Operating Instructions : General Presentation of the Study*)
EDF-DER - HT51/93/86B - June, 1994 (in French only)

[8] A. Dubreuil Chambardel
"Why Markovian Techniques Were Used in EDF's PSA of Paluel"
PSAM - Beverly Hills - February 4-7, 1991

[9] L. Magne, M. Balmain
"Comparison of Various Methods Used in PSAs : First Lessons"
PSA 93 - Clearwater - January 25-29, 1993

[10] A. Dubreuil Chambardel
"ELSA : un Ensemble de Logiciels quantifiant les Séquences Accidentelles"
(*ELSA : Accident-Sequence-quantifying Software Suite*)
EDF-DER - HT13/4/85 - January 85 (in French only)

[11] Case study on the use of PSA methods : Assessment of technical specifications for the reactor protection system instrumentation
IAEA-TECDOC-669

[12] J. Dewailly, S. Seriot, A. Dubreuil Chambardel, Ph. François, L. Magne
"Living PSA Issues in France on Pressurized Water Reactors"
IAEA TCM on "Use of PSA for optimizing NPP operational limits and conditions" - Barcelona, 20-23 September, 1993

[13] Safety Culture
INSAG 4
IAEA - SAfety Services No. 75 - 1991