EUROSAFE TRIBUNE

#012

APRIL 2008

PROBABILISTIC SAFETY ASSESSMENT

- Risk assessment
- Design & construction
- Maintenance & upgrading
- Ageing management
- Research & development

Published jointly by GRS and IRSN
as a contribution to the EUROSAFE initiative

CONTENTS

TO OUR READERS

Lothar Hahn and Jacques Repussard

The need for going beyond the 'traditional' approach used as the sole safety assessment basis for designing and operating nuclear facilities was largely evidenced by the TMI reactor core melt accident in 1979. Based on the analysis of a limited number of accident sequences with conservative assumptions, deterministic assessments had proved insufficient to give a comprehensive view on the plant's safety.

Another approach, aimed at assessing the frequency of an undesirable event by identifying all the accident sequences conducive to this event and combining the probabilities of the elementary events likely to trigger each sequence, was then implemented to supplement the deterministic assessment method. Called 'probabilistic safety assessment' (PSA), this approach provides an integrated model developed using best-estimate assumptions and gives a balanced view of the relative importance of initiating events, the failure of the structures, systems, components and the human errors modelled in the analysis. Whereas deterministic analysis is a powerful tool to specify the design based on a limited number of transients, PSA aims at covering the whole range of situations and allows to evaluate the weight of uncertainties on the range of the results. The former is thus suited to specify legally binding design requirements when licensing a nuclear power plant, and the latter more appropriate to provide insights into the existing safety margins for event sequences with low probabilities.

The present issue of The EUROSAFE Tribune provides an overview of the implementation of PSA at different stages of the life cycle of nuclear facilities from various perspectives – e.g. regulatory body, TSO, designer, operator… We wish you pleasant reading.

PROBABILISTIC SAFETY ASSESSMENTS:
GOING BEYOND DESIGN LIMITS

By Marina Röwekamp (GRS), Jeanne-Marie Lanore (IRSN), and Pieter De Gelder (AVN)

Developed first in the USA in 1975, Probabilistic Safety Assessments (PSA) are primarily used to determine whether or not there are any relative weaknesses in the design or operation of a nuclear power plant. This is achieved by determining the relative importance of structures, systems, components and human actions with respect to the risk considered. A PSA thus provides insights that are not available from the deterministic analyses, limited to design assumptions.

Dr. Marina Röwekamp
Gesellschaft für Anlagen- und Reaktorsicherheit (GRS), Germany

A non-dissociable part of any safety analysis

Until 1975, when first experience was gained with a Probabilistic Safety Assessment (PSA) and published in the USA, the safety demonstration of nuclear power plants was purely deterministic [1], based on the analysis of a limited number of accident sequences with conservative assumptions.

Originally aimed at comparing the risk associated with nuclear power to other risks, the first PSAs raised real interest after the Three Mile Island reactor core melt accident since they had predicted this type of accident with a non-negligible probability.

Beyond providing overall results, the main benefit of PSAs rests with their ability to identify and rank the possible risk causes, thus giving a comprehensive view on plant safety. This is why PSAs were increasingly developed and used, and are now considered as a useful part of many safety analyses.

Providing a balanced view of risks and weaknesses

Aimed at assessing the frequency of an undesirable event (see box and Fig. 1), a PSA first consists of identifying all the accident sequences conducive to this event and of combining the probabilities of the elementary events likely to trigger each sequence. PSAs complement this way the safety approach based on deterministic analyses and often also on prescriptive requirements.

The deterministic approach relies on conservative assumptions, the analysis of a set of faults that are thought to be bounding and the application of conventional safety criteria. By comparison, the PSA starts with as complete as possible a set of initiating events and hazards, and aims at identifying all the

[1] *See Balance between PSA and Deterministic Approaches*, by H.P. Berg (BfS) on page 7.

accident sequences that could lead to core damage or a release of radioactivity to the environment. The PSA provides an integrated model developed using best-estimate assumptions, and gives a balanced view of the relative importance of initiating events, the failure of the structures, systems, components (SSCs) and the human errors modelled in the analysis.

Relying as far as possible on operating experience

Theoretically, there are a number of ways of carrying out a PSA. The usual approach is to use appropriate logical models called *event trees* and *fault trees* to identify the combinations of failures that can occur, leading to the undesirable events. Although various combinations of fault trees and event trees could be used, all the approaches should produce similar results.

The data used in a PSA (e.g. frequency of initiating events, probability of component and human failures) rely as far as possible on operating experience, on a national and/or international basis. Particular attention should be paid to data – such as common-cause failures and human reliability – which may have a large impact on the results and are difficult to collect or assess.

Uncertainties: making knowledge limitations more visible

Uncertainties are obviously inherent in PSA results and should therefore be considered as highly significant for the credibility of the results and as a support to decision-making. Uncertainty and sensitivity analyses are therefore useful to empower the PSA results.

In this respect, it has to be noted that a large part of PSA uncertainties are in fact due more generally to knowledge limitations. Uncertainties e.g. are growing from Level 1 to Level 3, and uncertainties in a Level 2 PSA correspond to the limits of knowledge relating to severe accidents physics and management. One of the virtues of PSAs is to make these limitations more visible and to stimulate the on-going activities aiming at the reduction of uncertainties in a national or international context.

An enlarged scope of implementation

The safety improvements resulting from the PSA applications lead to its increasing development worldwide for all the nuclear plants, at design or construction stage, and obviously in operation towards a continuous monitoring of safety ("Living PSA"). Moreover, the application of PSAs was, for a long time, restricted mainly to nuclear reactors, but there is a tendency towards using this approach for other nuclear facilities. Due to the large number of existing PSAs, there is also a trend towards a harmonisation of methods by external peer reviews, intercomparisons or set-up of standards, thus enhancing the quality and credibility of the studies.

An increased role in the licensing of future NPPs

The framework of a PSA depends on the country where it is implemented, i.e. whether or not probabilistic safety criteria are available, and whether or not a formal demonstration is required. However, the general trend is to →

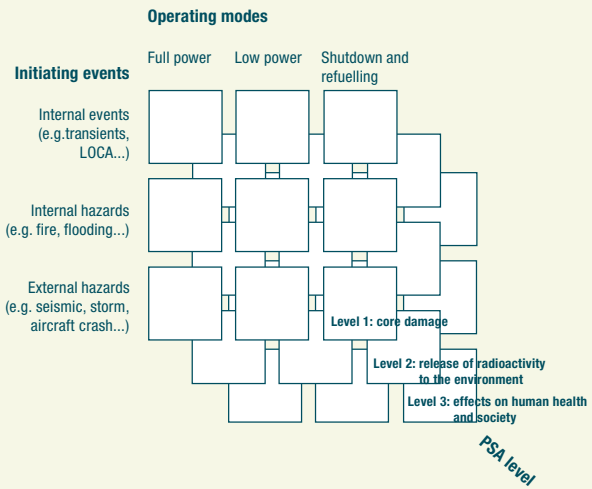
Jeanne-Marie Lanore
Institut de Radioprotection et de Sûreté Nucléaire (IRSN), France

Pieter De Gelder
Association Vinçotte Nuclear (AVN), Belgium

➔ use more and more the PSA insights as a necessary complement to the traditional safety analysis. This combined approach, called "Risk Informed Analysis", is now widespread. The main applications take advantage of the particular strength of the PSA to determine whether or not there are any relative weaknesses in the design or operation of the plant. This is achieved by determining the relative importance of structures, systems, components and human actions with respect to the risk by applying importance functions provided by recent PSA computer codes. This provides insights that are not available from the deterministic analyses.

In recent years, there has been an increase in the use of PSAs by plant designers, operators and regulatory authorities for making decisions on safety and regulatory issues throughout the lifetime of a nuclear power plant. The use of the PSA is likely to increase further and it will be even more prominent in the licensing of future nuclear power plants. ■

Figure 1: The objectives and scope of probabilistic safety assessment



The objective of a nuclear power plant PSA is the assessment of the frequency of an undesirable event. According to the current terminology, the undesirable event can be defined as core damage (referred to as a "Level 1 PSA"), a release of radioactivity to the environment ("Level 2 PSA"), or the effects on human health and society ("Level 3 PSA").

These three levels are in fact three steps of the same study:

- A Level 1 PSA is a systematic analysis of potential accident sequences starting from an initiating event and looking at the performance of the safety systems that need to operate for preventing core damage.
- A Level 2 PSA also considers the performance of the containment and the severe accident management measures in preventing a release of radioactivity to the environment.
- A Level 3 PSA considers the dispersion of any radioactive material released to determine its effect on human health and society.

As shown in the figure, the scope of the PSA is defined by the level of PSA carried out, the range of initiating events, and the modes of operation addressed.

PROBABILISTIC AND DETERMINISTIC APPROACHES:
TAKING ADVANTAGE OF THE RIGHT MIX

By Heinz-Peter Berg (BfS)

What realistic safety margins should be taken to operate a nuclear reactor in an as safe and effective way as possible? Since they are suited to ensure that the design basis events and event sequences used in the deterministic approach have been appropriately selected, probabilistic methods are considered as a useful complement to use the operating experience.

Probabilistic safety assessment: a major shift in safety decision-making

In the past, the safety concept of nuclear power plants as well as licensing decisions by the competent authorities and their experts were mainly based on deterministic principles such as safety features to prevent or control abnormal operating conditions and incidents, passive barriers against radioactivity releases in case of an incident, and redundancy and diversity of safety systems to ensure high reliability.

Safety decision-making at design and licensing stages was essentially based on the verification of compliance with technical requirements as laid down in respective industrial and nuclear safety standards. Boundary conditions for the safety analysis, safety margins with regard to the prevention and control of incidents as well as specific, partially detailed, requirements concerning safety functions are thus deterministically postulated.

Due to improved databases and analysing methods implemented in suitable computer codes, methods based on probabilistic safety assessment (PSA) are now considered to be mature, to be able to check deterministic design assumptions within acceptable limits of confidence and to provide information on plant vulnerabilities and potential weaknesses of operation and design.

Deterministic analysis: a conservative approach to safety based on limited situations

The traditional approach to nuclear safety is deterministic, in a sense where a preselected number of events or postulated event sequences have to be considered. The results of the analysis are then checked against a numerical target, e.g. a dose limit or a set of criteria including optimisation such as the ALARA principle. This approach needs two ingredients, the set of →

Heinz-Peter Berg
German Federal Office for Radiological Protection, Bundesamt für Strahlenschutz (BfS), Germany

→ events to be considered on the one hand and, on the other hand, the physical modelling and the technical data to assess these events. The selection criteria for the events to be considered, however, contain primarily requirements on the maximum loads for systems and components. The use of deterministic reliability principles as specific precautionary design measures, e.g. physical separation and barriers or leak detection and protection features, allows decreasing the likelihood of the design basis accidents.

Probabilistic analysis: taking uncertainty and sensitivity into consideration

A probabilistic analysis starts by defining the detrimental end effects, for which probability estimates are sought. Such effects may include potential plant damage states (e.g. core melting) or potential source terms for radioactive releases to the environment. The next step is to identify relevant initiating events. For each initiating event, potential event sequences are mapped modelling potential paths to the detrimental end effect. Probabilities, e.g. for component failure, are assigned to each step in each sequence. The end result will typically be an estimate of the overall probability of occurrence of the chosen detrimental end effect, and the identification of those initiating events and sequences that are predominant in this outcome.

The main objectives are to check the overall safety level of the plant and whether or not the engineered safeguards designed to cope with safety-relevant incidents are well-balanced. The evaluation has to be performed taking into consideration quantitative as well as qualitative results of the analysis reflecting dependencies and human interaction. Interpretation of the results includes uncertainty, sensitivity and importance analysis in an adequate way.

In search of the right balance

As shown in Table 1, deterministic and probabilistic approaches complement each other in many ways. Both methods having their inherent strengths and weaknesses, they should be used as complementary tools when specifying and assessing the safety of nuclear power plants, e.g. in case of fire safety evaluation (see Table 2).

It has been pointed out that a PSA helps identify possible weaknesses of the plant design but also *provide insights into the existing safety margins for event sequences exceeding the design limits*. A further benefit of a PSA in this context is to show the existing safety margins correlating the original design criteria and boundary conditions and the real operating experience (e.g. by comparing the expected loads on structures, systems and components with the actual situation over several years of operation). In that sense, a PSA is a very useful tool to complement deterministic insights in safety evaluation.

The deterministic approach is typically better suited to *specify legally binding design requirements when licensing a nuclear power plant*. It also provides valuable tools when specifying the robustness of the design,

Comparison of deterministic and probabilistic tools

Table 1: Simplified comparison of the deterministic and probabilistic approaches

	Deterministic approach	Probabilistic approach
Objectives	Analysis of the effectiveness of safety systems to control postulated accidents and covering not explicitly quantified events by additional margins and deterministic principles	Analysis and quantification of the likelihood of initiating events and associated event sequences by using realistic success criteria for safety systems; quantification of uncer-tainties associated with reliability data
Initiating events	Limited to design basis accidents	All potentially important events are included
System reliability	A single-failure criterion is often considered as a design criterion	Multiple failures and common-cause failures are also considered
Operator behaviour	- For t < T: no action is postulated (T = to 30 min) - For t > T: absence of operator errors is postulated	Errors in diagnosis and errors of execution are considered in the accident sequence
Analysis	Conservative assumptions	As realistic as possible

Table 2: Exemplary comparison of the deterministic and probabilistic approaches with respect to fire safety evaluation

Deterministic approach	Probabilistic approach
The train with fire protection features does not fail randomly	The train with fire protection features can fail randomly, with a failure probability based on operating experience
The fire does not propagate between different fire compart-ments	The fire can propagate between different fire compartments, assigning a failure probability to the different barriers
Loss of offsite power is postulated simultaneously with fire	Loss of offsite power simultaneously with fire has not probability one, but can occur randomly

i.e. ensuring that the plant can cope with certain specified events and event sequences with adequate safety margins against unacceptable consequences.

Since probabilistic assessment provides valuable insights into plant vulnerabilities and major contributors to risk, it is used to improve the deterministic approach, e.g. to ensure that the design basis events and event sequences in the deterministic approach have been appropriately selected. Because of these complementary aspects, a combination of both approaches should be applied.■

PROBABILISTIC SAFETY ASSESSMENT: USES WITHIN NUCLEAR REGULATION AND PRACTICE

By François Corenwinder (IRSN)

To which extent are probabilistic safety assessments used from a regulatory perspective in different nuclear countries worldwide and, among others, in France? This article provides an overview of the current situation.

François Corenwinder
Institut de Radioprotection et de Sûreté Nucléaire (IRSN), France

The use of PSA in the regulation of several countries worldwide

Most of the nuclear safety authorities regard the deterministic and probabilistic approaches as complementary, and seek to combine them in as an effective way as possible. However, depending on each particular country, the role played by the PSA in regulation ranges from a very precise legal framework to a very abstract situation. Thus, in some countries such as Finland, the Netherlands or Great Britain, the compliance with several probabilistic objectives must be evidenced, requiring PSAs to be carried out and formally approved, whereas in other countries such as the United States, probabilistic objectives are given as an indication with no legally binding compliance requirement. In the same way, the implementation of a PSA is seldom required, but very often encouraged. A non-exhaustive overview of the respective positions of different nuclear safety authorities is provided below with particular attention paid to the situation in the United States, where the concept of "risk-informed regulation", now used as an element of reflection in most of the other countries, was introduced.

• The United States

The "risk-informed" approach there is aimed at combining the advantages brought by the probabilistic approach with those of the traditional deterministic approach. It is thus a kind of intermediate position between the deterministic approach and a "risk-based" approach which would exclusively build upon probabilistic evaluations. In other words, the "risk-informed" approach incorporates simultaneously the insights from probabilistic assessment and other inputs to establish requirements aimed at focusing the owner's and the nuclear safety authority's attention on those design or operational issues which have the greatest importance for public health and safety.

• The Netherlands

They are the only country where the respect of probabilistic objectives is le-

gally binding. Defined in the Eighties in terms of risk of death among the population, these objectives distinguish between two levels of risk:

- the threshold below which the risk is acceptable;
- the threshold above which the risk is unacceptable.

Although these thresholds originally applied to all hazardous activities (e.g. nuclear, chemical, transport of dangerous goods, airports), it was decided to formulate these objectives in a different way with respect to the industry considered in particular. Concerning nuclear power production for instance, the lower threshold is no longer regarded as the acceptable limit, but as the limit to be reached for future facilities.

PSAs are required both for approving construction and for periodic safety reviews. PSA results are primarily used to check compliance with the probabilistic objectives, but also to justify safety improvements.

The Dutch nuclear safety authority evaluated the PSA simultaneously with their development. Moreover, one external review was requested from the IAEA. Guides were drafted to carry out and assess the studies.

Finland

A legal request, PSA studies are conducted according to a scope of work and acceptable methods specified in a guide issued by STUK, the Finnish nuclear safety authority. Probabilistic criteria, whose demonstration is required, were defined to assess the reliability of systems. Those pertaining to core melt and releases were defined for future nuclear power plants. Since they are required by law, PSAs are systematically reviewed by STUK and become part of an official document describing the requirements related to the performance of PSA studies.

Canada

Probabilistic objectives have been defined concerning the reliability of systems. These are not comprehensive, but the incorporation of probabilistic criteria into the regulation, in a more formal way, is presently considered. The Canadian nuclear safety authority requires that compliance with the probabilistic objectives related to the systems be evidenced and carries out PSA reviews. The first reviews were incorporated into guides issued either by international organisations such as the IAEA or national safety bodies such as HSK, the Swiss nuclear safety authority. Guides drafted in Canada are currently debated. Generally speaking, Canada aims at establishing a more formal process for the use of the probabilistic approach in the regulation.

Japan

The performance of PSAs is not formally required, nor is compliance with probabilistic objectives. Nevertheless, the Japanese nuclear safety authority clearly supports the performance of level 2 PSA studies at all nuclear power plants and scrutinises the results with utmost attention. Internal documents have been drafted for performing or reviewing PSAs, although no formal guide was issued on this matter. →

Belgium

There are no probabilistic objectives whose respect must be evidenced by the operators, nor is the Belgian nuclear safety authority requested by law to perform PSAs. There is rather an incentive to use them, in particular for periodical safety reviews. There are no formal proceedings for PSA approval, but, as studies progress, a comprehensive evaluation process results in a report whose conclusions are then discussed with the owner.

The particular situation in France

Since 1990, probabilistic safety assessments have commonly been used to corroborate or supplement the traditional deterministic safety analyses. ASN, the French Nuclear Safety Authority, consider the PSA as a valuable tool to support safety analysis and recognise their contribution to improving the safety of nuclear power plants. A major advantage of PSA is to provide a more exhaustive consideration of safety problems and to prioritise the issues to be tackled. However, no excessive confidence should be placed in the numerical results (particularly in absolute values), and the uncertainties related to these results have to be considered. Major uncertainties pertain to the data, the assumptions and the lack of exhaustiveness.

In addition, it should be underlined that, besides PSAs, different approaches can be adopted to account for risk in assessing safety: risk can also be allowed for in an implicit or relative way, notably in deterministic safety studies (e.g. defence in depth, safety margins). PSAs allow a specification of the concept of risk and provide quantification for some types of risks. Beyond the difficulty linked to allowing for uncertainties, the use of quantified probabilistic objectives is not advisable, since compliance with such objectives may encourage licensees to consider that the safety level in their facilities is sufficient, whereas the goal of the Nuclear Safety Authority is not only to maintain safety but always to seek to improve it.■

View into the open reactor pressure vessel on the reactor core during maintenance

THE SPECIFIC ROLES OF PSA AND PSR:
A SWEDISH REGULATORY PERSPECTIVE

By Ralph Nyman (SKI)

After the TMI accident, the Swedish Parliament required in 1981 that all NPP operators should submit thorough periodic safety reviews (PSRs) every 8-10 years for each reactor unit. Probabilistic safety assessments (PSAs) have no longer been part of the PSR process since 1998, when the SKIFS 1998:1 regulation went into force. The Swedish Nuclear Power Inspectorate (SKI) considers today that PSRs have to focus on how different regulations are fulfilled and what issues can challenge future operation, whereas, in the past, the flashback into the previous decade's operating experience was considered as important for the understanding of the present situation of the plants.

The Periodic Safety Review (PSR) process described in the Swedish Safety Regulations [1] is based on the "looking-ahead principle" which is a way to provide conditions for the future safe operation of the NPPs. Other aims are to show and verify how the present regulations are fulfilled and how resistant the design and construction are against accidents. The overall aims of PSRs are to provide safety evaluations for 15 specified areas (called SKIQ-15) in the regulation (see Table 1).

The Integrated Safety Assessment process at SKI is structured to follow the SKIQ-15 areas in the annual safety assessment of all regulatory supervision activities, follow-up of operating experience, and reporting to the Government. The PSRs are planned to follow the same structure, to get better uniformity both at licensees and at SKI.

How does SKI "look ahead" with PSRs

SKI reviews the report submitted every 8-10 years by a licensee in the following manner:

- For each of the 15 PSR areas, a judgement is made of the licensee's analyses of the present situation regarding, among others, how regulations are fulfilled, the visions of the future considering planned or actual plant modifications, or fulfilment of new demands;
- Documents from the licensee are reviewed and compared with SKI's own documents (e.g. inspections, reviews, plant visits, investigation reports, operating experience, R&D);
- The plant's safety barriers and levels in the defence-in-depth at present are assessed, and a judgement about the conditions for safe operation over the coming 10 years is derived from this.

Ralph Nyman
Swedish Nuclear Power Inspectorate,
Statens Kärnkraftinspektion (SKI),
Sweden

[1] *SKIFS 2004:1 chap 4 §4.*

The current SKI approaches in a nutshell (according to the latest regulations).

- A PSR report shall still be produced every 8-10 years for all plants.
- Recommendations in the reviewed PSR report of SKI are presented to the Government.
- A PSR report is coupled to the operating licence.
- PSA is separated from the PSR process.
- PSAs have to be regularly updated and actively used in applications.
- Final Safety Analysis Reports (FSAR) have to be updated continuously in rhythm with the modifications performed at the plants.
- FSAR and PSA typically are living documents.

➔ The main focus in a review is placed on assessing the fulfilment of present regulatory decisions and requirements by the licensees.

›PSAs' primary role in Sweden today: optimise the NPP modernisation processes

As stated in the introduction, the PSA activities have been kept separate from the PSR process since 1998 and their role has changed accordingly. In compliance with the *Regulations concerning Safety in Nuclear Facilities* (SKIFS 2004:1), Level-1 and Level-2 PSAs have to be performed by licensees for all operational modes and have to be complemented with area events analyses (fire, flooding) and external events analyses.

The *Regulations concerning the Design and Construction of Nuclear Power Reactors* (SKIFS 2004:2) published by SKI in 2004 encompass new areas such as design principles of defence-in-depth, strongly constructed safety functions against failures and events, resistance to environmental impact, threats to control rooms… To fulfil these regulatory demands, huge plant modernisation processes were launched at all facilities alongside power uprate projects.

Today, PSAs are obviously expected to help verify and optimise, with the most valid or updated models, the planned construction solutions. This implies also to indirectly verify the actual fulfilment of construction and design rules, guides and standards of e.g. structures, systems and components. It is mandatory that the final safety analysis report be kept updated after plant modifications, or if current deterministic safety analyses are updated or new ones are introduced.

In Sweden, PSAs are also used, among others, to:

- verify and evidence the safety impact of changes required in plant-specific technical specifications, of allowed outage time and of test intervals;
- evaluate the risk increase factor resulting from previous incidents;
- identify weak points in a plant and plan for countermeasures.

Supervision by SKI of the PSAs performed by licensees corresponds to the following regulatory activities:

- review of applications to SKI,
- review of the chapter devoted to updated PSA results in the final safety analysis report,
- review of PSA documentation and fault-tree models,
- inspections and plant visits,
- research and development.

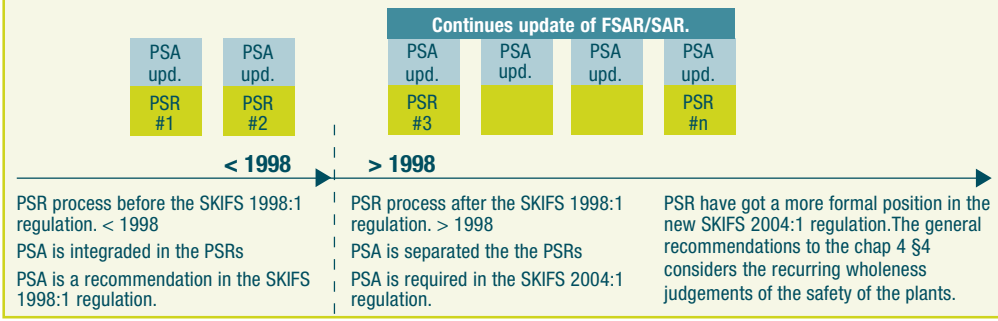
Reviews of PSAs or PSA applications aim at getting knowledge about:

- the representativeness of the PSA-models regarding the correct behaviour of analysed initiators affecting the structures, systems and components,
- the dominating assumptions and simplifications,
- the clarity and readability of documentation (e.g. are the results presented and interpreted in a didactic manner?),
- the eventual plant modifications derived from the PSA results.

›Taking advantage of a "risk-informed" approach

For SKI, it is also very important that the primary and the independent reviews be performed according to process-oriented

Figure 1: The relationship between PSR and PSA in Sweden before and after 1998. (SKIQ-11, PSR area 11 – Safety analyses and safety reporting)



instructions at the licensees and with appropriately chosen reviewing level and depth. A current trend is that SKI puts more pressure on this process to make clear statements about the applicability of the PSA models to different uses. SKI is "risk-informed" to a sense where they are provided with information on the models' content, on how realistic those studies are and how they are used. This background helps SKI review licensee applications. It is therefore of a certain interest to have good knowledge of how well the self-control function operates at the licensees. Moreover, the knowledge about how well a PSA study does fulfil the requirements plays an important part in the overall integrated safety assessment of some of the 15 PSR areas.

As shown in Figure 1, the new respective roles of PSRs and PSAs – providing conditions for the future safe operation of the NPPs thanks to the "looking-ahead principle" on the one hand, and optimising the NPP modernisation processes on the other – provides the Swedish regulatory authorities with complementary perspectives on the safety of the reactor fleet in operation in the country. ■

Table 1: Demands and extent of the PSRs in the regulation.

1	Design and construction of the facility (incl. modifications)	
2	Management, control and organisation of the activity	
3	Competence and staffing of the nuclear activity	
4	Operations, incl. the handling of deficiencies in barriers and defence-in-depth	
5	Core and fuel issues as well as criticality issues	
6	Emergency preparedness	
7	Maintenance, material and in-service inspection issues	
8	Primary and independent safety review	
9	Investigation of events, experience feedback and external reporting	
10	Physical protection	
11	Safety analyses and safety reporting	11 Final Safety Analyses Reports and PSAs
12	Safety programme	
13	Safekeeping of facility documentation	
14	Handling of nuclear material and nuclear waste	
15	Non-proliferation control, export control and transport safety	

PLANT OPTIMISATION AND OPTIMUM MAINTENANCE PLANNING AS A RESULT OF PSA

By Risto Himanen (TVO)

Probabilistic Safety Assessment (PSA) can be used in many ways to support the planning of different maintenance-related activities in nuclear power plants. The first PSA application in the operating units at Olkiluoto NPP during the late 1980s was the optimisation of on-line maintenance of diesel generators and diesel-backed pumps of front-line safety systems. Today's model shows that the impact of the on-line maintenance on the core damage frequency has been decreased from 50% to less than 1%. PSA, in connection with Probabilistic Availability Analysis [1] gives useful insights when planning Reliability Centred Maintenance [2] Programmes, in maintenance priority classification of components according to their safety and availability importance.

Risto Himanen
Teollisuuden Voima Oy (TVO), Finland

Optimisation of maintenance during power operation: the lessons learnt from diesel generators

Since the 1980s, preventive maintenance of diesel generators has been permitted during power operation at the Olkiluoto units 1 and 2 (OL1 and OL2). The maintenance time has been limited to three days per year for each of the eight diesel generators (four per unit). Since it is assumed in the deterministic design basis accident analyses that the connection to the external grid is lost, the diesel-backed safety systems are considered as "unavailable" when the corresponding diesel generator is unavailable due to preventive maintenance. Thus, the conclusion from the deterministic analysis is that all diesel-backed, front-line safety systems in one train can be maintained at the same time as the corresponding diesel generator itself in maintenance packages which are done consecutively for each of the four trains.

The PSA of OL1 and OL2 (which during the 1980s included only internal initiating events) showed that the impact of the diesel packages on the core damage frequency was 17%. Today's model, which also includes common cause initiators such as fires, floods, seismic events and different weather phenomena, shows that the impact of the old-type diesel package would be more than 50%.

Bringing the impact of on-line maintenance on the core damage frequency down from 50% to less than 1%

Because PSA showed that the preventive maintenance of the safety systems was a dominant risk contributor, the diesel packages had to be re-designed in order to minimise the risk impact. In addition, the consecutive mainte-

nance of all trains included potential for repeated maintenance errors, which were not explicitly modelled. Risk-based modifications were thus performed in the diesel packages, and the optimised on-line maintenance made it possible to reduce its impact on the core damage frequency to less than 1%:

- Firstly, the diesel packages were staggered so that only two diesel packages in each unit were scheduled consecutively and the remaining ones only after a longer period.
- Secondly, each diesel package was divided into three consecutive parts:
  a. The diesel generator is maintained simultaneously with the core spray pump and those parts of the intermediate cooling system and circulating water system which are necessary for the diesel generator and the core spray system.
  b. The auxiliary feed water pump (high pressure), which is a separate system for the low pressure core spray system, is maintained in its own package.
  c. The containment spray pump is maintained at the same time as some components in other systems that have no impact on the availability of core cooling systems, i.e. the auxiliary feed water system or the core spray system.
- Thirdly, the maintenance tasks are allocated for each year so that the average of the sum of the three packages during a ten-year period will not exceed three days per year and train. Thus, a ten-day major overhaul is possible every ten years for each diesel generator.

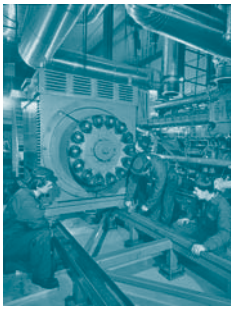
>The Role of PSA in Reliability Centred Maintenance

The purpose of the maintenance activities is to provide the required functionality of Structures, Systems and Components (SSC) to allow safe and reliable power production. The Reliability Centred Maintenance (RCM) method is used for improving and optimising the maintenance program, based mainly on own operating experience of SSC.

In the late 1990s TVO developed an application of the Probabilistic Availability Analysis (PAA) method [1] for the operating BWR units OL1 and OL2. Use of the same modelling method and same computer code in PAA as in PSA allowed the calculation of importance measures for the components and systems. All SSC of OL1 and OL2 were classified according to their maintenance priority into four different classes:

- Components in the highest priority maintenance class should always be operational, and are thus subjected to the most thorough preventive maintenance programmes.
- In the second highest class, limited unavailability of the component is permitted.
- In the third class, preventive maintenance is performed only if economically justified.
- In the lowest priority class no preventive maintenance is carried out.

This maintenance priority classification was based on several economical and safety-related factors. Besides the operating and maintenance experience of the components as well as the preventive and corrective maintenance costs and requirements in Technical Specifications (TS), insights →



Maintenance of diesel generators in Olkiluoto

➔ were drawn from the probabilistic analyses (PSA and PAA). PSA is used to assess the importance of the component failures on the plant safety. The implementation of the insights from PSA in OL1 and OL2 was based on two importance measures: Risk Achievement Worth (RAW [3]) and Fussel-Vesely (F-V [4]) Importance. The limits for the importance measures were chosen after several trials in such a way that the main components of the front line safety systems were clearly distinguished in the highest priority safety class. The following rules were applicable for OL1 and OL2:

- If the Risk Achievement Worth (RAW) is greater than 2, then the highest maintenance priority is always applied because decreased reliability of the component would have a strong effect on the Core Damage Frequency (CDF).
- If the RAW is between 1.1 and 2 and the F-V is greater than 0.005, the maintenance priority is 2 because the effect of decreased reliability of the component on the CDF is moderate (RAW) and the increased reliability would at least slightly decrease the CDF (F-V).
- PSA is not used in the definition of the maintenance priority if the F-V is less than 0.005 and the RAW is less than 1.1, i.e. neither increase nor decrease of the component's reliability has a great impact on CDF.

Defining the initial Preventive Maintenance Plan

RCM is used in the design phase of the EPR-type OL3 unit for the definition of the initial Preventive Maintenance Plan. This plan defines – taking into account risk insights – the maintenance activities of each component, e.g. maintenance priority of the component, effective maintenance activities, and the frequency of the activities.

Usual RCM methods are not well adapted to a new nuclear power plant design because own operating experience is missing. Therefore, a new application of RCM was developed for OL3 to define the initial Preventive Maintenance Plan without own operating experience. The maintenance priority class, which defines the depth of the RCM analysis, is based on the Technical Specifications (TS), PSA, PAA and expert opinion. The experts may also select other SSC that are neither addressed in TS, PSA nor in PAA, but which have to be covered by Preventive Maintenance activities.

The use of risk importance measures in the classification shall be "relative" and "advisory". "Relative" means that plant-specific limits shall be defined because they seem to depend on the risk profile of the plant. "Advisory" means that the expert group shall have the possibility to change the maintenance priority class independently of the results of PSA, if justified.

The PSA model includes a great variety of components, and some of them may have very low importance due to several reasons. Inclusion of a component in the PSA model shall not automatically mean that it should be classified into high maintenance priority. If the PSA importance measures are used to distinguish e.g. between two highest priority classes, a limit shall be set to indicate when the importance is so low that even the second-highest class is not justifiable based on PSA. ■

---

(1) Probabilistic Availability Analysis (PAA) is a method similar to PSA, but it estimates the risk for loss of production (MWh/year) instead of core damage frequency. It is now used also by utilities such as EDF or reactor designers such as Framatome.

(2) Reliability-Centred Maintenance (RCM) is an engineering framework that allows the definition of a complete maintenance regime. This approach is focused on identifying and establishing the operational, maintenance, and capital improvement policies that will manage the risks of equipment failure most effectively. It is defined by the technical standard SAE JA1011, Evaluation Criteria for RCM Processes.

(3) Risk Achievement Worth (RAW) of a modelled plant feature (usually a component, train, or system) is the increase in risk if the feature is assumed to be failed at all times. It is expressed in terms of the ratio of the risk with the event failed to the baseline risk level.

(4) Fussell-Vesely (V-F) Importance of a modelled plant feature (usually a component, train, or system) is defined as the fractional decrease in total risk level (usually Core Damage Frequency, CDF) when the plant feature is assumed perfectly reliable (failure rate = 0.0). If all the sequences comprising the total risk level (e.g. CDF) are minimal, the F-V also equals the fractional contribution to the total risk level of all sequences containing the (failed) feature of interest.

THE SIGNIFICANCE OF PSA FOR LOW-POWER AND SHUTDOWN STATES

An interview with Michael Wenk (EnKK)

The three NPPs located in the Land of Baden-Württemberg – i.e. Neckarwestheim and Philippsburg – are jointly operated by EnBW Kernkraft GmbH (EnKK). EnKK's CEO, Michael Wenk, gives *The EUROSAFE Tribune (TET)* his views on the contribution of probabilistic safety assessments of low-power and shutdown states to an improved understanding of reactors' behaviour beyond normal operation and, subsequently, to the enhancement of safety procedures in nuclear facilities.

***The EUROSAFE Tribune.* Mr. Wenk, what are EnBW's priorities regarding the operation of its reactor fleet?**

Michael Wenk: We are striving to get our NPPs epitomise safety, reliability and competitiveness in the world of power generation. Safety comes first, before profitability. Just like other German nuclear facilities, our power reactors are permanently placed under the independent control of the regulatory authorities, and the stringent inspections performed in this framework are complemented with mandatory safety reviews performed periodically (PSR). Those are aimed at establishing whether or not a given facility offers a sufficient level of safety in view of future operation. For each of our reactors, we therefore draft every ten years a comprehensive safety report taking into account the state of the art in science and technology.

***TET.* In this process, what use does your company make of probabilistic safety assessments?**

Michael Wenk: In compliance with the Federal regulatory requirements on nuclear energy, any PSR includes both a deterministic analysis as well as a probabilistic safety assessment (PSA) of the occurrence of defined events in order to verify whether or not the corresponding safety concept is commensurate to the risk. In this respect, the scope of PSA was extended in 2005 to such operating configurations as low-power and shutdown states. We had carried out such assessment at our Philippsburg and Neckarwestheim NPPs already earlier, as we consider that the contribution to the risk during low-power and shutdown states is not negligible and should therefore be assessed as thoroughly as other states. This is our opinion, although the reactors operated by EnBW enjoy an availability of more than 90% on average, making low-power and shutdown states by far the less frequent operational state.

Michael Wenk
EnBW Kernkraft (EnKK), Germany

***TET.* How are PSAs performed at EnBW?**

Michael Wenk: Based on the official PSA guidelines, comprehensive PSAs were conducted and optimised for →

→ each plant in an iterative process. First of all, the incidents recorded through the Incident Reporting System in Germany were analysed, taking into account as well the Incident Reporting Systems of the OECD and IAEA allowing the scope of potential events to be assessed. Then, scenarios of each plant were built, drawing upon the modelling of such events. Finally, fault trees based on operating states were adapted to low power and shutdown states.

TET. To which extent do probabilistic safety assessments improve your understanding of low-power and shutdown states?

Michael Wenk: The data gained from low-power and shutdown states PSAs contribute not only to the high safety level of our facilities, as shown by international comparisons, but bearing witness to our efforts towards continuous safety improvements, they gave us precious insights into the behaviour of our facilities during such states and into scenarios of possible events as well. Splitting low-power and shutdown states into different phases including transition states for instance, enabled us to perform numerous optimisations in our facilities (e.g. in the planning of work during periodical inspections) conducive to improvements of results using PSAs.

TET. How are identified optimisations implemented?

Michael Wenk: The conclusions obtained are implemented in the operating manuals of our facilities, in chapters dedicated to low-power and shutdown states. We designed event- and protection orientated operating procedures that can be practised by our operators on simulators.

TET. What do you expect from low-power and shutdown states PSAs for the future?

Michael Wenk: As an iterative process drawing upon previously gained results, the low-power and shutdown states PSAs allow on-going development and improvement thanks to the renewal of procedures based on existing knowledge. We therefore intend to continue with such analyses using the method for future improvements and – this is very important – adjusting our highly conservative safety margins accordingly. We also expect PSAs to help us improve further our working processes and to assess even more accurately the status of our facilities, when operated at low power or shut down. The measures derived from PSA results are incorporated into our operating manuals, thus becoming an important part of our know-how. We use them as a tool to raise the safety standards of our facilities, beyond normal operation, to a level comparable to high quality standards recognised worldwide. Again, we regard the PSAs for low-power and shutdown states as a valuable tool for subsequent safety reviews and for process optimisation. They enabled EnBW to gain meaningful information on the management of transition states and, through adequate changes in procedures, to further enhance the safety of its nuclear facilities. The overall goal should be to have a well-balanced PSA including normal operation and low-power and shutdown states, where the main contribution to the resulting risk comes from normal operation. ■

BACKFITTING AND MODIFICATIONS OF NUCLEAR POWER PLANTS – AN IMPORTANT PSA APPLICATION

By Attila Bareith, Elod Hollo (VEIKI), and Jozsef Elter (PAKS NPP)

Probabilistic safety assessments have been used to support safety-related decisions at nuclear power plants for many years. One of the main objectives of PSA applications is to identify the potential backfits and modifications conducive to safety enhancement, and to demonstrate their impact on different risk measures. The frequency/probability of core damage (level 1 PSA) and large radioactivity release (level 2 PSA) is widely used to support this demonstration. An overview of the essential backfits and modifications performed at the Hungarian Paks NPP is provided below, and their impact on plant safety is summarised.

Four VVER 440-213 type reactor units have been operating at the Paks NPP since the early eighties. The first comprehensive level-1, full-power, internal-initiator PSA study was completed in 1994 for Unit 3 of the plant. More recently, the scope of the original PSA has been considerably extended to encompass internal (fires and floods) and external (seismic) hazards, to determine annual refuelling outage risk (including all phases of cooling down, refuelling and restart) as well as determine the frequency of large radioactivity releases and their main contributors (level 2 PSA).

In general, the methodologies followed to perform the different PSAs were based on international (mainly IAEA and NEA) guidelines and practices, namely:

- The small-event-tree/large-fault-tree approach was used to model accident sequences. Functional and physical dependencies are explicitly modelled;
- Common-cause failures, human errors and recovery actions were included. Plant-specific statistics and generic data were both used to set up the input database;
- An efficient computer code (RiskSpectrum® PSA Professional) was implemented for quantification.

>A major safety enhancement programme based on PSA results

A PSA can be used to determine the important contributors to risk measures and, subsequently, to outline the most effective safety upgrading backfits and modifications. As a next step, the →

Attila Bareith
VEIKI Institute for Electric Power Research, Hungary

Elod Hollo
VEIKI Institute for Electric Power Research, Hungary

Jozsef Elter,
PAKS Nuclear Power Plant, Hungary

→ practically applicable changes in design and in operational conditions have to be incorporated into the event sequence model and data base. The results of a quantification using the modified input information will reveal the risk decrease rate induced by the given changes.

At the Paks NPP, the PSA has been used for this purpose since the completion of the first comprehensive study. In 1996, an extensive programme of safety enhancement measures (SEM) was initiated. This programme covered numerous practically feasible modifications and improvements to provide the plant with enhanced capability to prevent and cope with severe accidents. The essential elements of the completed SEM programme are as follows:

- *Relocation of the emergency feed water system (EFWS)*
  A design shortcoming was eliminated by the relocation of the EFWS from the direct vicinity of the main steam and feed water lines to a plant location protected from the effect of high energy pipe breaks. With this relocation, the EFWS is protected from the hazard of high-energy line breaks as well as of fires and floods.
- *Protection of containment sump against clogging*
  New sump strainers prevent the unavailability of the emergency core cooling system under loss-of-coolant-accident (LOCA) conditions.
- *Refurbishment of the reactor protection system (RPS)*
  The replacement of the analogue RPS with digital equipment and software control has been carried out. The new, reliable system has improved the control functionality and provided a better man-machine interface.
- *Replacement of the primary overpressure protection system*
  The new system with its advanced safety and relief valves and control provides appropriate tools to help prevent severe accidents through primary pressure decrease by both automatic and manual operations.
- *Earthquake resistance improvement*
  The measures include the reinforcement of building structures, technological and I&C systems, introduction of new protection signals, and modification of the cool-down technology following a seismic event.
- *Introduction of symptom-orientated emergency operating procedures (EOP)*
  The new procedures offer better support for operators in their emergency operations to identify and execute the most appropriate actions in a timely manner under high stress. In parallel with the EOPs, a state-of-the-art monitoring system for critical safety functions was also installed.
- *Handling primary to secondary leakage in steam generators*
  Several technological and I&C modifications will facilitate the early detection of steam generator failure, terminate the primary leak by decreasing primary circuit pressure, and limit the amount of radioactive releases.
- *Hydrogen management in the containment during a design basis accident*
  Catalytic recombiners were installed

in the containment to prevent the accumulation of hydrogen resulting from a design basis LOCA event.

Further modifications are currently executed in order to mitigate any consequences of potential severe accidents, e.g. to perform hydrogen management in the containment.

Probabilistic indicators: a clear illustration of risk reduction by SEMs

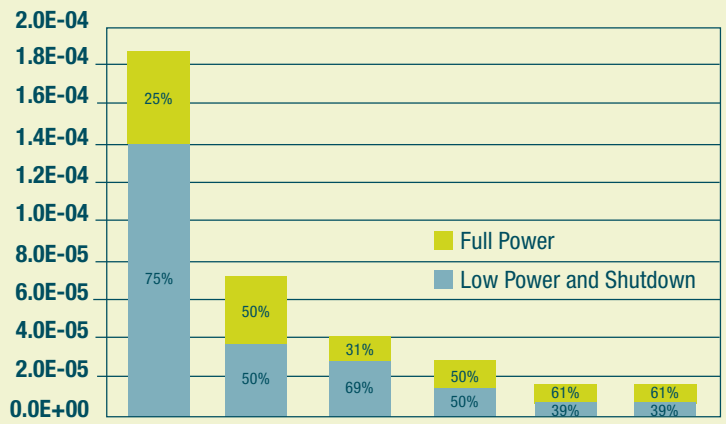
Level 1 PSA was used for evaluating the safety enhancement measures having effect on core damage probability (e.g. introduction of new emergency operating procedures), while the results of level 2 PSA studies supported the identification of the accident mitigation means (e.g. installation of hydrogen recombiners).

Figure 1 shows the changes in the core damage probability of the Paks NPP, Unit 2, during the last decade (the background photo illustrates the construction phase of EFWS pumps relocation). The overall risk figure for internal events has been reduced by an order of magnitude during this period of time.

The individual SEMs can influence the risk level within different plant operating states. It can be seen in the figure that – with a constantly decreasing risk profile – relative contributions from full-power and from low-power and shutdown states vary over time for the Paks NPP: although relatively important, low power has nowadays a small absolute contribution and, similarly, the risk level during planned outages for refuelling has also been reduced. It is nowadays dominated by those plant operating states when the reactor vessel is open for fuel manipulation and the water level in the vessel is low.

From these results, it can be inferred that the safety level of the Paks NPP units has been systematically raised by means of backfits and modifications, and that it now complies with that of plants of the same vintage in other European countries. This is a clear illustration of risk reduction by SEMs.

Figure 1: Evolution of core damage probability at the Paks NPP, Unit 2



APPLYING PSA TO ASSESS NUCLEAR FACILITY AGEING

An interview with Andrei Rodionov (JRC)

As part of the European Commission's Joint Research Centre, the Institute for Energy is focussing on energy issues. Andrei Rodionov, senior researcher in the Institute, co-ordinates the scientific network set up in 2004 to perform research in the field of PSA applied to nuclear facility ageing. He gives *The EUROSAFE Tribune (TET)* an insight into the network's activities and achievements.

Andrei Rodionov
Institute for Energy, European Commission Joint Research Centre (JRC), Netherlands

***The EUROSAFE Tribune*. What is the European Commission's Joint Research Centre (JRC) in charge of?**

Andrei Rodionov: This Centre was originally established under the Euratom treaty signed in 1957. Euratom's role is to promote nuclear safety and security in Europe and the JRC has been contributing to this aim with its research activities ever since. The JRC has, however, at the request of its customers, expanded to also embrace other fields important to policy-making, such as life sciences, energy, security and consumer protection. It has transformed itself from a purely research-driven organisation focussing on nuclear energy to a customer-driven, research-based policy support organisation. Today, the JRC is deeply embedded in the European research area.

***TET*. How is the JRC funded?**

Andrei Rodionov: The JRC, with a staff of around 2700, is allocated an annual budget of around 320 million euros for direct support to EU institutions from the Seventh Framework Programme (FP7). It earns up to a further 15% from such competitive activities as participation in collaborative projects, technology transfer and work for third parties including industry and regional authorities.

***TET*. What is the Institute for Energy tasked with?**

Andrei Rodionov: As part of the JRC, the Institute for Energy (IE) provides scientific and technical support for the conception, development, implementation and monitoring of community policies related to energy. It covers the following key areas: energy techno-economic assessment; energy recovery and production of intermediate fuels from waste and biomass; cleaner fossil fuels, including carbon capture; new energy technologies, including fuel cells and hydrogen; safety of operational and future nuclear reactors; storage and transport of nuclear waste, and new treatment methods in nuclear medicine.

TET. **In the field of nuclear safety, the JRC set up a network specialising in the use of PSA for the evaluation of ageing effects on the safety of energy facilities…**

Andrei Rodionov: Yes, and as a senior researcher in the IE, I am personally tasked with co-ordinating the activities of this network devoted to what we use to call "ageing PSA". Created in 2004 by common initiative of the Institute for Energy and interested European organisations such as research institutes, technical support organisations, regulators and utilities, the network was formally joined by 14 organisations from EU Member States as well as Armenia, Russia, South Korea and Switzerland. CNSC (Canada), Statwood Consulting (USA) and NMRI (Japan) provide active participation.

TET. **What does the network's working programme consist in?**

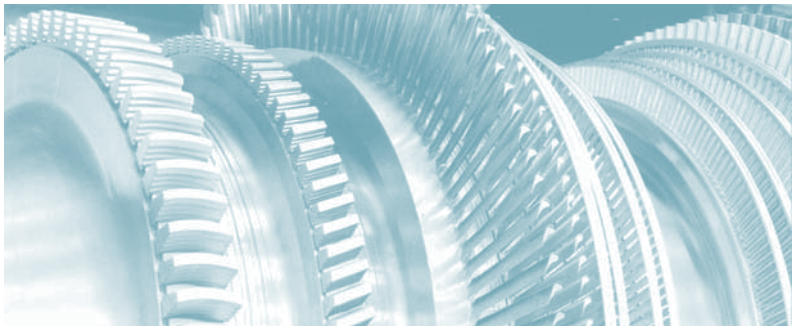
Andrei Rodionov: Its scope of work encompasses eight tasks: **1.** Organisation and co-ordination of network activities; **2.** Analysis of main PSA tasks with regard to Ageing PSA; **3.** Selection of the Structures, Systems and Components (SSC) to be considered in Ageing PSA; **4.** Reliability and data analysis for active components; **5.** Consideration of Common Cause Failures; **6.** Reliability and data analysis for passive components; **7.** Incorporation of age-dependent reliability parameters and data into PSA model. Interpretation of quantification results; **8.** Ageing PSA development and applications. Focus is placed on the PSA application for Long Term Operation of NPPs, but developed approaches and obtained results could be applied as well to research reactors and fuel cycle facilities.

TET. **What are the major issues associated with the ageing of nuclear facilities?**

Andrei Rodionov: Well, if you refer to *The EUROSAFE Tribune* #10, it is clear that the most critical issues are associated with the non-replaceable heavy structures as a reactor or containment for instance. Ageing of major passive components as steam generators, primary and secondary pipes are also considered as very important issues… And since the risk profile is quite sensitive to the failures of passive components considered in PSA models on the level of initiating events (e.g. primary pipe breaks) we are focussing on them. We also address other safety systems that are not considered critical in ageing management, because maintenance is supposed to keep failure rates constant. But this assumption has to be checked and justified when one would like to use PSA for aged NPPs.

TET. **How can PSA be used to help identify and prioritise ageing issues?**

Andrei Rodionov: From a technical perspective, PSA makes it possible to prioritise risk depending on importance factors: if you identify some ageing issue or see some trend towards ageing in a reliability curve, you may decide to perform a sensitivity study to assess the risk more accurately. Let us assume you have some core damage frequency estimated with your PSA code; assessing the sensitivity to the →



Partial view of a turbine rotor

→ ageing parameters included in the model will help you forecast the importance under some boundary conditions in 5 or 10 years.

TET. How would you characterise the JRC Network's achievements at this stage?

Andrei Rodionov: Well, this is a research project, thus we do not pretend to perform any evaluation or judgment of existing facilities. We aim at providing some approaches, models, application examples, etc. For the task titled "Reliability and data analysis for active components" (task #4), for instance, we developed several case studies which demonstrate the statistical methods to identify the ageing trends using some operating experience data. Proposed approaches, models and corresponding software are included into the guidelines for reliability parameters estimation.

As I mentioned earlier, PSA studies consider that failure rates for components are constant because of maintenance. But in reality, if components are not maintained properly, failure rates will increase. So we proposed an approach and method to assess reliability using experience feedback and, as reliability data collection at plants in service do not include such verification, we prepared methodological guidelines to perform it. Moreover, we recognised that reliability data collection has to be improved for long-time operation.

TET. What are the Network's future prospects?

Andrei Rodionov: For future development, concerned by tasks #5 to 8, we shall try to understand:

- how ageing could impact common cause failures;
- whether or not representative reliability models are available to calculate a failure probability of passive components which could be used in PSA; and
- how to apply "ageing PSA" in a risk-informed decision-making process.

From 2008 onwards, we will start with these tasks and should be ready to finalise this stage of the programme within 2 years.

At the end, I would like to invite those *EUROSAFE Tribune* readers who are interested in the subject to visit our web page: http://safelife.jrc.nl/APSA ■

PROBABILISTIC SAFETY ASSESSMENT:
A POWERFUL TOOL TO HONE NEW REACTOR DESIGN

By Reino Virolainen and Ari Julin (STUK)

The Olkiluoto 3 (OL3) NPP is the first unit to be built according to the European Pressurised Water Reactor (EPR) concept. Its planned thermal power is 4,300 MW and net electric power output approximately 1,600 MWe. OL3 has been designed to comply with the current international safety principles, the Finnish regulatory requirements and the European utility requirements, including a management strategy for core melt accidents. Several modifications to the original EPR design were made during the licensing procedure based on the Finnish regulatory requirements and local conditions. Many of those safety-significant design modifications were based on PSA insights.

In Finland, probabilistic safety assessments (PSAs) are formally integrated in the regulatory process of NPPs already in the early design phase and are run throughout the construction, commissioning and operation phases. A plant-specific, design phase level 1 and 2 PSA is required as a prerequisite for issuing the construction license and a complete Level 1 and 2 PSA for issuing the operating license. The plant-specific Level 1 and 2 PSA includes internal initiators, fires, flooding, harsh weather conditions and seismic events for full-power operation mode and for low-power and shutdown mode. In each licensing phase, a PSA has to be used to demonstrate that the following probabilistic design objectives will be met:

- Mean value of the core damage frequency is less than 1.10^{-5}/year;
- Mean value of a large radioactive release frequency (> 100 TBq Cs_{137}) is less than 5.10^{-7}/year.

The design has to be improved in case these objectives are not met.

The plant supplier conducted a design phase PSA for Olkiluoto 3 (OL3). The Level 1 analyses for full-power operation covered internal events, fires, floods and external events. However, there were some shortages in the scope of the analysis (e.g. seismic risks), but PSAs and a qualitative justification together demonstrated that safety objectives will be met.

Weather, seismic risk, severe accidents: the major PSA review findings at Olkiluoto 3

While the design phase PSA was in progress, the detailed design of structures, systems and components (SSCs) was still incomplete. Hence the comprehensive analyses concerning system dependencies and common-cause failures for all systems, particularly →

***Reino Virolainen**, Radiation and Nuclear Safety Authority (STUK), Finland*

***Ari Julin**, Radiation and Nuclear Safety Authority (STUK), Finland*

Construction work at Olkiluoto 3 NPP

→ electrical and instrumentation and control (I&C) systems were lacking. There were also deficiencies in the coverage of plant-specific initiating events, which is understandable at the design stage, where detailed information of SSCs is missing.

The analysis on risk from fire and flooding performed in the design phase demonstrated that their contribution to the total core damage frequency is small and that there are no remarkable flaws left in the plant design that would increase the risk. Not all design details were known at this stage, requiring expert judgment and conservative assumptions to be used. A detailed fire and flooding risk analysis is to be performed at the construction stage of OL3 when the design is finalised.

Weather risks

The design phase PSA has been used to ensure the adequacy of the plant design basis and of the design requirements related to external events (weather phenomena, etc.). The OL3 PSA includes a screening analysis of external phenomena covering weather conditions (wind, temperature, lightning, rain) and seawater-related conditions such as variations in level, temperature, and blockage-causing phenomena (algae, mussels, frazil ice, oil spills). The analysis of external events also covers risks connected with industrial activities, transport and other normal human activities in the vicinity of the plant site, but not activities deliberately aimed at damaging the plant.

Precautions have been taken to withstand a blockage of the essential service water system (loss of ultimate heat sink) and a loss of residual-heat removal and component cooling functions. The plant has been designed to withstand a total loss of the ultimate heat sink for 72 hours. Two safety trains of the emergency feed water and emergency core cooling systems are equipped with air-cooled chillers to ensure cooling also during a loss of seawater cooling. The prevention of a blockage of air intakes with snow has been taken into account while redesigning the diesel generator systems.

Seismic risk

Seismic activity in Finland is quite low. During the construction of the Finnish NPP units currently in operation, there were no specific regulatory requirements on seismic design. Concerning OL3, the plant supplier claimed it would be possible to demonstrate that the plant unit meets probabilistic design objectives with a sufficient safety margin for seismic risks, provided that it is implemented according to the principles of earthquake design stated in the Preliminary Safety Analysis Report. A detailed seismic risk analysis with fragility curves is required to establish that the quantitative risk targets (less than 1.10^{-5}/year for core damage frequency and 5.10^{-7}/year for a large release) will be reached.

Severe reactor accident

A Level 2 PSA analysed the physical progression of sequences leading to a severe reactor accident and the timing of releases in accidents which threaten the structural integrity of the containment or its functional tightness, or in which a release from the primary cir-

cuit occurs through systems located outside the containment building (containment by-pass). The results of the Level 2 PSA indicated that the frequency of exceeding the release limit for a severe accident is less than 5.10^{-7}/year, i.e. the limit set forth as a safety objective in the Regulatory Guide.

Plant design changes resulting from PSA

As a result of the regulatory review of construction license documentation (PSA and PSAR), some changes to the original plant design were required. The design modifications required by STUK were mostly related to the improvement of the reliability of safety-significant systems by adding diversity, redundancy or separation. The most significant changes pertained to:

- the separation requirements of the electrical systems (e.g. safety-classified electrical cables),
- the protection of air intakes of the emergency diesel generator and the cooling systems against snow blocking,
- the separation by fire barriers of redundancies in all safety-critical locations,
- the prevention of flooded conditions spreading through safety buildings and from the service water pumping station between redundant rooms.

Risk informed applications of PSAs

Several PSA applications have been required in Finnish Regulatory Guides for construction and operating licenses, such as:

- Support for safety classification of SSCs: this classification has to be assessed with a PSA also in the construction phase if substantial design modifications are performed;
- Drawing-up of a programme for Technical Specifications, e.g.: testing of safety-significant SSCs, relevance of allowed outage times (AOT) of safety systems, identification of situations in which the plant shutdown may cause a higher risk than that of continuing power operation and fixing the failures;
- Drawing-up of a programme for on-line preventive maintenance;
- Drawing-up and development of piping (RI-ISI) inspection programmes;
- Ensuring the coverage of disturbance and emergency operating procedures: a PSA must be used to determine those situations for which the procedures shall be drawn up;
- Planning of personnel training: the most important accident sequences and significant operator actions in terms of risk have to be practised at least once in the period of three years.

The applicant has submitted to STUK his risk-informed planning methods on the programmes of the technical specifications, RI-IST [1], on-line preventive maintenance, RI-ISI [2] and is drawing up a respective risk-informed programme. ■

Bird's view of Olkiluoto NPP

[1] Risk Informed In-Service Testing
[2] Risk Informed In-Service Inspection

SEISMIC PSA:
A STATE-OF-THE-ART TOOL FOR UPDATING EARTHQUAKE-SPECIFIC REGULATORY GUIDELINES

An interview with Katsumi Ebisawa and Mamoru Fukuda (JNES)

Frequently hit by powerful tremors, Japan developed earthquake-specific regulatory guidelines aimed at reinforcing the design of its nuclear facilities. These texts are revised based on the lessons learnt from major seismic events such as the 1995 Hyôgo-ken Nambu earthquake. Existing plants are now being back-checked according to the new guideline where seismic probabilistic safety assessments play an increased part. The new guideline is put to the test with the 2007 Niigata-ken Chûetsu-oki earthquake.

Katsumi Ebisawa
Japan Nuclear Energy Safety (JNES), Japan

***The EUROSAFE Tribune (TET).* What are the specific implications of earthquakes on nuclear plant design?**

Mamoru Fukuda. Whereas internal events are often attributed to such incidents as random equipment failure, earthquakes are natural phenomena and are therefore difficult to control through human intervention. Damage to structures, systems and components (SSC) resulting from severe seismic ground motions is simultaneous and of different kinds, often rendering multiple protection mechanisms ineffective. The Japanese NPPs have been seismically designed, taking the so-called "design basis ground motion Ss" (DBGM Ss) as a deterministically established reference derived from the records of seismic activity.

***TET.* How can a probabilistic safety assessment (PSA) be applied to seismic events?**

Mamoru Fukuda. First of all, a seismic PSA (SPSA) analyses accident sequences conducive to core damage and estimates their occurrence probabilities and frequencies. Uncertainties associated with earthquake ground motion or responses and fragilities of buildings and components are accounted for, just as earthquakes with extremely small occurrence probabilities, i.e. beyond-design-basis ground motions. Secondly, SPSA can provide information beyond the deterministic approach, as it allows seismic safety to be assessed in a realistic manner. Therefore, SPSA is used to reasonably estimate the "residual risk", to secure the estimation's transparency by providing information of the estimation process, and to define the sequences contributing to core damage as well as the subsequent mitigation systems.

***TET.* How is the SPSA incorporated in the Japanese nuclear plant design regulatory requirements?**

Mamoru Fukuda. Based on such experi-

ences as the Hyôgo-ken Nambu earthquake in 1995, the Nuclear Safety Commission of Japan (NSC) started revising in July 2001 the guideline established in July 1981 and issued the new guideline for the seismic design of nuclear power reactor facilities in September 2006. The new guideline requires to determine the "Design Basis Earthquake Ground Motion Ss" with uncertainties duly considered and to reduce the "Residual Risk", expectedly with probabilistic approaches.

TET. How is the "Design Basis Earthquake Ground Motion Ss" assessed?

Katsumi Ebisawa. Exploration of ground and geographical survey can be performed based on state-of-the-art knowledge. DBGM Ss will be determined for **a.** "Site-specific earthquakes ground motion whose source is identified with the proposed site" and **b.** "Earthquake ground motion whose source is not identified". For the former, a large number of earthquakes which are suspected to have a severe impact on the proposed site will be selected, for which evaluations of ground motion will be conducted. The latter will be determined based on the observation records near the source obtained from past earthquakes. As observation records are limited, probabilistic approaches are used. If uncertainties are properly considered, DBGM Ss can be deterministically assessed. The "Residual Risk" is a function of excess probability of earthquake ground motions over DBMG Ss, in which "Residual Risk" decreases as the excess probability is set small. The Nuclear and Industrial Safety Agency (NISA) of Japan issued instructions in September 2006, calling on those concerned to make back checks on reactors under construction and existing reactors to ensure seismic safety against landslides and tsunamis is included.

TET. What are the limits set for the "Residual Risk"?

Mamoru Fukuda. For the quantitative assessment of the "Residual Risk", the NSC promotes the use of SPSAs to identify seismic-risk-significant scenarios and equipment, and to improve seismic design. The quantitative target of the safety goals is set to less than 1.10^{-6}/year.site, in terms of average fatal risk for individuals living around the facilities. Regarding the performance targets, the core damage frequency is set to 1.10^{-4}/reactor.year while the containment failure frequency is set to 1.10^{-5}/reactor.year.

TET. What happened during the Chûetsu-oki earthquake on July 16th, 2007?

Katsumi Ebisawa. The tremor that occurred near the Kashiwazaki-Kariwa NPP (Niigata-ken) had a magnitude of 6.8 on the Richter scale with a hypo-central distance of 17 km from the NPP. A level of response approximately 2.5 times as high as the value set for the Design Basis Earthquake Ground Motion Ss in the former guideline was observed. However, the plant could maintain the functions of safety-important SSCs, although there were such SSC failures as a fire in a station service transformer.

TET. What are the lessons learnt from this particular earthquake?

Katsumi Ebisawa. On September 28th, vigorous exchanges of views occurred at a special session in the autumn meeting of the Atomic Energy Society →

Mamoru Fukuda
Japan Nuclear Energy Safety (JNES), Japan

→ of Japan (AESJ) devoted to the Chûetsu-oki Earthquake. Those were aimed at finding out whether or not the seismic ground motion could be predictable under the new guideline, whether or not further reinforcements against earthquake motion were needed, and whether or not a revision of the new guideline were needed. Other issues were also debated, such as the reasons why main SSCs did not fail and the way to cope with fire and flooding which are out of scope in the SPSA standard.

***TET*. What do you regard as the main opinions that reached consensus?**

***Katsumi Ebisawa*.** The new guideline requires the establishment of DBGM Ss based on state-of-the-art knowledge for investigation of active faults, analytical techniques, and so on. At present, many seismic specialists are studying the generating mechanisms of the Niigata-ken, Chûetsu-oki earthquake characteristics. In the near future, they will confirm if state-of-the-art technology, including new geological surveys on sea and continental areas, helps accurately establish DBGM Ss based on e.g. earthquake sizes and characteristics. Under the present situation, it is very important to apply and put into practice the new guideline strictly and with sincerity.

***TET*. What do you consider as essential tasks in this respect?**

***Katsumi Ebisawa*.** It is fundamental to establish DBGM Ss in such a way that "Residual Risk" shall be minimised, taking into account uncertainties. Having said that, I think there is no need to revise the basic policy in the new guideline, although there is room for re-categorising SSCs individually with a view to improving prevention, detection and extinction of fire as well as prevention of radioactive material releases out of controlled zones during an earthquake. Even if a NPP does not satisfy the performance targets, a seismic PSA can identify risk-significant accident sequences and seismic safety-critical SSCs, then confirm the efficacy of the improvement. For instance, a seismic PSA can indicate whether or not the reinforcement of support structures by means of e.g. anchor bolts is effective for the structures in case of a DBGM Ss. On its side, AESJ issued a standard for SPSA in March 2007, which utilities are now following to quantify the "Residual Risk" for their NPPs.

***TET*. How does JNES use SPSA to prevent seismic disasters in nuclear facilities?**

***Katsumi Ebisawa*.** First reinforcements for seismically important SSCs identified by the SPSA will be pursued using state-of-the-art technology such as seismic component isolation technology. JNES is developing an information system called *PEES* for "Post-earthquake plant evaluation and evacuation support". This system's aim is to estimate possible damage to the bridges and roads in the neighbourhood and ultimately indicate the evacuation routes, considering the likely behaviour of released radioactive substances, as well as shelters and vehicles.■

REDUCING UNCERTAINTY: HOW FIRE RESEARCH SUPPORTS PSA AND RISK MANAGEMENT

By Nathan Siu, J.S.Hyslop (US NRC), and Steven P.Nowlen (SNL)

As shown by past experience, including the recent transformer fires at the Krümmel (Germany) and Kashiwazaki (Japan) plants, fires can and do occur at NPPs. In a small number of cases [1], they have triggered chains of events that have seriously challenged plant safety systems. Fire PSA provides a mechanism to systematically identify and prioritise potential fire-related vulnerabilities, and to assess potential risk management strategies. Fire PSA is, in turn, improved by fire safety R&D that addresses key areas of uncertainty. Fire safety R&D has supported the development of the fire PSA methods, models, and tools used worldwide. In the future, it can be expected that such R&D will continue to play an important role in the development of improved methods for assessing and managing risk.

Specific aspects of fire PSA

Fire PSA involves the identification and characterisation of potentially significant fire-initiated accident scenarios, as well as a determination of the cumulative risk impact of these scenarios. Similar to the analyses of other initiating events addressed in a PSA study, fire PSA involves the assessment of the likelihood and consequences of failures of plant safety equipment and required operator actions. In general, the fire PSA must:

- identify potentially important fire scenarios;
- estimate the frequency of occurrence of these scenarios;
- estimate the probability that specific fire scenarios will damage key plant equipment (especially electrical cables for instrument, control, and power circuits);
- estimate the probability of important equipment failure modes (including spurious operations); and
- estimate the probability that, under scenario-specific conditions (including the possibility of heat, smoke, loss of lighting, and confusing indications, as well as fire-induced equipment failures), operators fail to perform required actions to achieve a safe and stable plant state.

The benefits of past R&D: an improved understanding of key issues and the development of fire PSA methods

With the U.S. Nuclear Regulatory Commission's (NRC) enacting of a →

Nathan Siu
United States Nuclear Regulatory Commission, (US NRC), USA

J. S. Hyslop
United States Nuclear Regulatory Commission (US NRC), USA

Steven P. Nowlen
Sandia National Laboratories (SNL), USA

→ risk-informed, performance-based fire protection rule in 2004, and with ongoing activities to develop a fire PSA standard, our current ability to perform fire PSA might be taken for granted. However, fire safety R&D, initiated after the 1975 Browns Ferry fire, was needed to develop the basic framework used in current detailed fire PSAs, as well as initial versions of the elements of that framework. This R&D supported the realistic treatment of room-specific features (including cable locations) through the use of fire models. More recent R&D has led to an improved understanding of key issues (notably the likelihood and potential consequences of fire-induced short circuits in electrical cables) and the development of associated fire PSA methods and data. These efforts have demonstrated that, despite the inherent complexity of fire as a phenomenon, a risk-informed approach to fire safety is technically feasible.

>The aims of current efforts: facilitate the performance of high quality fire PSAs and reduce key uncertainties

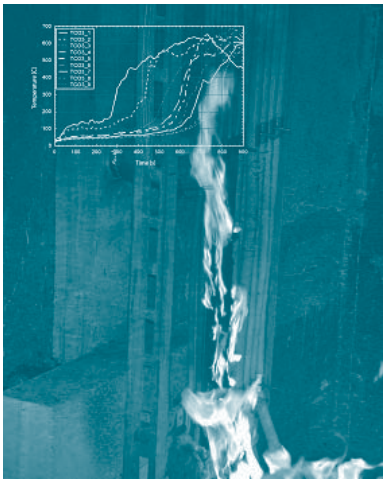
At present, fire PSA is being used in many countries to better understand and manage fire risk. Within the U.S., for example, several utilities have notified the NRC of their intention to modify their fire protection programs using the new risk-informed, performance-based fire protection rule. The modification, which will likely involve upgrades to the plants' fire PSAs, is expected to help resolve complex, long-standing questions associated with possible operator actions performed during challenging fire events, and with potential fire-induced spurious actuations.

Fire PSA is also playing a significant role in the NRC's Reactor Oversight Program where fire PSA results are used to prioritise areas for inspection, and fire PSA tools are used to assess the significance of inspection findings. To support these and other applications, current NRC fire safety R&D and related activities are aimed at: **a.** facilitating the performance of high quality fire PSAs, and **b.** reducing key uncertainties.

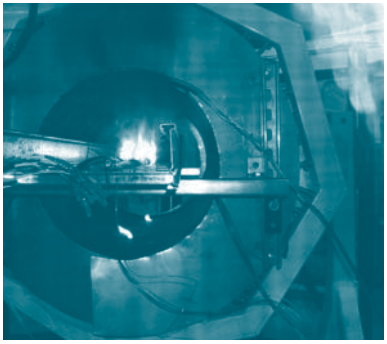
Some notable activities are as follows:

- *Fire risk requantification study*. The purpose of this cooperative activity by the Electric Power Research Institute (EPRI) and the NRC's Office of Nuclear Regulatory Research (RES) is to develop improved fire PSA methods, tools, and data to support more realistic assessments for risk-informed regulation. To date, the program has resulted in a fire PSA guidance document. Ongoing efforts involve the application of the guidance document in two pilot plant studies.
- *Fire model verification and validation*. The purpose of this EPRI/RES cooperative activity is to verify and validate five fire-modelling tools commonly used by the nuclear industry. The approach involved the comparison of model predictions with data from a set of fire experiments, some of which were performed specifically for the study. The results to date, summarised in the form of a simple colour-coded chart, indicate areas of strengths and weakness for each of the tools. In future work, the uncertainties in model predictions will be quantitatively assessed in a probabilistic framework.

- *Electrical cable response fire tests*. The primary objective of the NRC's Cable Response to Live Fire Project (CAROLFIRE) is to assess the importance of a number of potential fire scenarios involving fire-induced short circuits. A secondary objective is to foster the development of cable thermal response and electrical failure fire modelling tools, which can be used in fire PSAs. The preliminary results of the project are documented in a draft report issued for public comment.
- *International fire event data base*. The OECD's Nuclear Energy Agency (NEA) is currently administering a Fire Incident Records Exchange (FIRE) project. The purpose of this international project is to collect and analyse fire events to support the determination of fire frequencies and fire scenario attributes, generate insights into the causes of fires to enable their prevention or mitigation, and establish a mechanism for feedback of fire experience.



Cable tray fire experiment with time-temperature curves (figure courtesy of GRS).



Fire-induced circuit failure testing apparatus and insulation resistance measurements.

New technologies raising new challenges

The R&D activities discussed previously are focused on addressing the needs of current reactors. New technologies introduced through reactor upgrades or new reactor designs can raise new fire PSA questions, including:

- The effects of fires on digital instrumentation and control systems (including the effects of smoke, and the behaviour of fibre optic cables exposed to fire);
- The risks of fires involving new materials (e.g. liquid metals);
- The fire risk associated with co-located hydrogen facilities; and
- The effects of fire on operator performance under operational schemes being considered for advanced designs (e.g. involving reduced control room crew staffing).

In some areas, past R&D efforts (e.g. on the effects of smoke on electrical circuits, and on the characteristics of liquid metal fires) may be useful. In other cases, new R&D may be needed.■

(1) e.g., 1975: Browns Ferry, 1989: Vandellos, and 1993: Narora.

THE BENEFITS OF RISK-BASED, COMPUTERISED DIAGNOSTIC TOOLS IN THE VERIFICATION OF THE INDUSTRY'S SAFETY ASSESSMENTS

By José M. Izquierdo and Miguel Sánchez (CSN)

The growing computational capabilities of information systems allow regulators, supported by TSOs', to develop increasingly refined risk-based diagnostic tools appropriate for an integrated approach of safety assessment. Yet, such developments, necessary to assess the highly complex safety cases provided by the industry, require considerable resources, calling for a co-operative effort among national TSOs. *A regulator's view.*

José M. Izquierdo
Consejo de Seguridad Nuclear (CSN), Spain

Miguel Sánchez
Consejo de Seguridad Nuclear (CSN), Spain

>Ever more sophisticated safety cases from the industry…

The safety cases provided by operators within the framework of licensing processes include safety analyses that rely more and more frequently on computational tools capable of simulating transients as well as accidents and processing the complex models used for probabilistic safety assessments. Such an assessment capability, even if reduced to its analytical aspects, is a huge effort requiring considerable resources.

The ever larger demand for computerised safety case analyses is fuelled by the increasing trend towards Risk Informed Regulation (RIR [1]) and the recent interest in methods that are independent of the diversity of existing nuclear technologies. It is further fostered by:

- new nuclear power plant designs;
- the need to confirm the present applicability of old, "generic" safety analyses;
- the wish to extend the life of existing plants, with associated challenges in terms of potential reductions in safety margins.

>…challenging the regulators' and TSOs' computational resources

This trend makes it mandatory for regulatory bodies to increase their technical expertise and capabilities in computerised diagnostic tools. Technical Safety Organisations (TSOs) have become an essential player in the regulatory process, providing a substantial part of the technical and scientific basis of computerised safety analyses based on available knowledge and analytical methods/tools.

TSO tasks cannot have the same scope as those of their industry counterparts, nor is it reasonable to expect the same level of resources. Therefore, in providing their technical expertise, they shall focus on:

- Reviewing and approving methods and results of licensees; and
- Performing their own analyses/calculations to verify the quality, consist-

ency and conclusions of day-to-day industry assessments.

Plea for a jointly developed, integrated approach

The latter is a highly complex and particular regulatory task requiring specific TSO diagnostic tools to independently check the validity and consistency of the many assumptions used and conclusions obtained by the licensees in their safety assessments. Efficiency is enhanced by increasing the international co-operation among national TSOs with a view to developing jointly methods and tools. Those shall be independent of domestic technology and adaptable to the facilities reviewed by each TSO.

The assessment approach shall include a sound combination of deterministic and probabilistic single checks which, at the same time, are part of an integral safety assessment method suitable for addressing all relevant risk factors associated with decision-making and ensuring that the decision ingredients are properly and consistently weighed.

In recent years, different organisations have undertaken initiatives with claims such as the need for an integration of probabilistic safety analyses in the safety assessment, up to the approach of a risk-informed decision-making process, as well as for proposals of verification methods for application that are in compliance with the state of the art in science and technology. It is our opinion that these initiatives should progressively evolve into a sound and efficient interpretation of the regulations that may be confirmed by means of computerised analyses. It is not so much a question of new regulations from the risk assessment viewpoint, the aim being rather to ensure compliance with the existing rules in a new context by verifying the consistency of individual plant assessment results through a comprehensive set of checks. This can be considered as a key and novel research topic within nuclear regulatory agencies and TSOs [2].

More precisely, issues that require an integrated approach arise when considering:

- The process by which the insights from these complementary safety analyses are combined, and
- Their relationships when addressing high level requirements such as defence in depth and safety margins.

Extending the probabilistic safety metrics used for consistency checks

Establishing the mutual consistency of PSA success criteria on one hand and operating technical specifications on the other is an important issue, as both of them are often derived from potentially outdated base calculations performed in older times, in a different context, and with a different spectrum of applications in mind. This is an important chapter of the optimisation of the protection system design, which encompasses, for instance, such problems as:

- *Ensuring that the protection system is able to cope with all accident scenarios* and not only with a predetermined set. This umbrella character is hard to establish, particularly in a context of reduced safety margins. It requires the regulator's careful attention to the historic evolution of the deterministic assessments and is a source of potential conflicts when different techniques are combined to assess risk. →

- *Verifying the adequacy of critical and sensitive success criteria*. Many studies aimed at demonstrating the umbrella conditions are outdated and potentially unsuitable under these more restrictive circumstances. Verification of emergency procedures for instance is worth mentioning, as it implies to consider longer time scales than those of automatic design accident analyses as well as important uncertainties in the timing of interventions, both potentially altering the umbrella conditions of the deterministic design.
- *The need to consider degraded core situations to ensure acceptable residual risks*. Again consistency issues appear requiring regulatory checks.

These consistency checks call for an appropriate extension of the probabilistic safety metrics used, in terms of exceedance frequencies of safety limit indicators, additional to the widely used severe core damage frequency (CDF) and large early radioactivity release frequency (LERF). This impacts on the basis of the operating technical specifications that so much affect the daily regulatory plant life and goes beyond the design phase of licensing activities.

Together with design-based checks, there is also room for improvements in the analysis of operating events, the associated lessons learned, and the correct focus on the various aspects mentioned above. They may or may not be confirmed in real-life incidents, accounting for more aspects than the present approaches almost exclusively focused on event–tree/fault-tree quantification of CDF and LERF safety metrics.

CSN developments towards an integrated approach

Just as an example of existing projects in the domain of risk-based, computerised diagnostics, CSN has developed its own Integrated Safety Assessment methodology (ISA) in the area of Modelling and Simulation (MOSI [3]). This diagnostic method was designed as a regulatory tool, able to compute the frequency of exceeding selected safety limits by quantifying the contribution of PSA sequences and to check in an independent way the results and assumptions of the industry's PSAs, including their extensions/applications to Risk Informed Regulation. The approach harmonises the probabilistic and deterministic safety assessment aspects via a consistent, unified and suitable computational simulation framework called System of Codes for Integrated Safety Assessment (SCAIS).

Conclusion: EUROSAFE, an important contribution to the development of risk-based, computerised diagnostic methods and tools

We have argued in favour of an international co-operative effort among national TSOs, much in line with EUROSAFE goals: the joint development of TSO diagnosis tools and methods to perform their own computerised analysis to verify quality, consistency, and conclusions of day-to-day safety assessments performed by industrial operators, in such a way that asserts consistency of probabilistic and deterministic aspects. ■

[1] Risk-informed regulation (RIR) is defined by the US NRC as: "incorporating an assessment of safety significance or relative risk in regulatory actions. Making sure that the regulatory burden imposed by individual regulations or processes is commensurate with the importance of that regulation or process to protecting public health and safety and the environment."

[2] The idea of a European platform of safety codes is the basis of such European programs as SARNET. The new aspects we are focusing on pertain to methods for checking consistency by means of probabilistic and deterministic techniques, which, in practice, amount to procedures on how to use these tools for regulatory purposes.

[3] "An integrated PSA approach to independent regulatory evaluations of nuclear safety assessments of Spanish nuclear power stations", J. M. Izquierdo et al. (CSN). EUROSAFE Forum 2003, Paris.

UPCOMING EVENTS

- *17-18 April 2008 – Mannheim, Germany*
  Probabilistische Sicherheitsanalysen in der Kerntechnik – Erfahrungen, Erkenntnisse, Entwicklungen
  TÜV SÜD Akademie GmbH

- *25-29 May 2008 – Dubrovnik, Croatia*
  7th International Conference on Nuclear Option in Countries with Small and Medium Electricity Grids
  Organised by the Croatian Nuclear Society in co-operation with IAEA and Sponsorship from the European Nuclear Society

- *8-12 June 2008 – Anaheim (California), USA*
  2008 Annual Meeting on Nuclear Science and Technology: Now Arriving on Main Street + 2008 International Congress on Advances in Nuclear Power Plants (ICAPP '08), embedded International Topical Meeting
  Organised by the American Nuclear Society

- *1-3 October 2008 – Dubrovnik, Croatia,*
  TOPSAFE 2008
  Organised by the European Nuclear Society

- *17-21 November 2008 – Mumbai, India*
  International Conference on Topical Issues in Nuclear Installation Safety: Ensuring Safety for Sustainable Nuclear Development
  Organised by the International Atomic Energy Agency and hosted by the Government of India through the Atomic Energy Regulatory Board of India

The EUROSAFE Forum 2008 organised in Paris (at Cité Internationale) on 3 & 4 November will be devoted to "The role of TSOs in the context of an increasing demand for safety expertise".

EUROSAFE Tribune is a periodical from the EUROSAFE Forum. **Editorial Committee:** Benoît De Boeck, AVN – Ulrich Erven, GRS – Gustaf Löwenhielm, SKI – Antonio Munuera Bassols, CSN – Edouard Scott de Martinville, IRSN – Peter Storey, HSE – Seppo Vuori, VTT.
Coordination: Horst May, GRS – Emmanuelle Mur, IRSN. **Credits:** GRS Archiv, DR, Thomas Gogny, Seignette/Lafontan. **Writer:** Jean-Christophe Hédouin.
DTP: Regina Knoll, GRS. **Printing:** Moeker Merkur Druck.
ISSN: 1634-7676. **Legal deposit:** April 2008.
The EUROSAFE Tribune will be available on the **Website:** www.eurosafe-forum.org

INSTITUT DE RADIOPROTECTION
ET DE SÛRETÉ NUCLÉAIRE (IRSN)
B.P.17
F-92260 FONTENAY-AUX-ROSES
CEDEX

GESELLSCHAFT FÜR ANLAGEN-
UND REAKTORSICHERHEIT (GRS) mbH,
SCHWERTNERGASSE 1
D-50667 KÖLN

FOR FURTHER INFORMATION:
www.eurosafe-forum.org

E U R O S A F E

Towards Convergence of
Technical Nuclear Safety Practices in Europe