G. Tokmachev and V. Morozov

Lessons learnt from PSA for new and advanced reactors in Russia

Customer requirements to probabilistic safety targets are usually stronger than existing Regulatory or IAEA ones. It appears that industry takes the lead over regulation in this case and forces the designer to find and implement appropriate means to enhance safety, which sometimes have no reference to practical experience. On the other hand, regulatory documents and the existing PSA methodology are mainly oriented to operating plants. This creates problems when developing a PSA as well as performing regulatory reviews. The scope of the PSA may be different depending on a design stage such as the development conceptual, basic or detailed design. In addition, the base case PSA is usually performed for NPP in design. However, a customer may require additional PSA applications to consider, for instance, risk monitoring. In this case the scope of the PSA should be extended to implement special attributes of the application needed that often requires specific information not available at the design stage. Lack of design information affecting PSA development may be associated with incompleteness of the design that is typical for interim design stages and communication problems caused by the involvement of many different companies in the deign activity. To deal with this issue bounding technologies and the iterative PSA development are used. However this sometimes contradicts to the "best estimate" approach recommended by regulatory guides. PSA development for advanced NPPs has raised some issues originated from unknown new components, processes and technologies incorporated into the design of an advanced plant. The paper addresses some issues resolved while carrying out PSAs for advanced NPPs. Some PSA results for new advanced VVER plants under construction and the first lessons learnt from the Fukushima accident are also discussed.

Erfahrungen mit der Durchführung von PSA für neue und fortschrittliche Reaktoren in Russland. *Kundenanforderungen an probabilistische Sicherheitsziele sind in der Regel strenger als bestehende Vorschriften oder IAEA-Empfehlungen. Es scheint, dass die Industrie in diesem Fall die Initiative übernimmt und den Designer zwingt, geeignete Mitte zu finden und umzusetzen, um die Sicherheit zu verbessern, bei denen manchmal ein Bezug zu praktischen Erfahrungen fehlt. Andererseits orientieren sich regulatorische Dokumente und die bestehende PSA-Methodik vor allem an in Betrieb befindliche Anlagen. Das schafft Probleme bei der Entwicklung einer PSA sowie bei der Durchführung von behördlichen Überprüfungen. Der Umfang der PSA kann je nach dem Entwurfsstadium (Konzeption, Basis- oder Ausführungsplanung) unterschiedlich sein. Darüber hinaus wird eine Basis-PSA in der Regel für das KKW in der Ausführungsplanung durchgeführt. Allerdings kann ein Kunde fordern, zusätzliche PSA-Anwendungen zu betrachten, zum Beispiel Risikoüberwachung. In diesem Fall sollte der Umfang der PSA erweitert werden, um zusätzlich benötigte spezielle Attribute der Anwendung zu implementieren. Dabei sind aber häufig die notwendigen spezifischen Informationen zu diesem Zeitpunkt der Planung noch nicht verfügbar. Der Mangel an Information bezüglich der Anlagenauslegung, die die PSA Entwicklung beeinflussen, ist mit der Unvollständigkeit des Designs zu diesem Zeitpunkt der Entwicklungsphase sowie mit Kommunikationsproblemen durch die Beteiligung vieler verschiedener Unternehmen verknüpft. Zur Bewältigung dieses Problems werden Grenzbetrachtungen verwendet und die PSA in einem iterativen Prozess entwickelt. Doch dies steht manchmal im Widerspruch zum „best-estimate"-Ansatz, der in behördlichen Leitfäden empfohlen wird. Die PSA-Entwicklung für fortschrittliche Kernkraftwerke hat einige Fragen aufgeworfen, die dadurch entstehen, dass unbekannte neue Komponenten, Prozesse und Technologien bei der Auslegung einer fortschrittlichen Anlage verwendet werden. Das Papier erörtert einige Probleme, die während der Durchführung der PSA für fortschrittliche Kernkraftwerke gelöst wurden. Einige PSA-Ergebnisse für neue fortschrittliche WWER-Anlagen im Bau sowie erste Lehren aus dem Unfall in Fukushima werden ebenfalls diskutiert.*

1 Introduction

JSC Atomenergoproekt is an engineering company, general designer of nuclear power plants. They belong to different plant generations constructed or planned to construct in Russia, Iran, India, Turkey and Bulgaria including Generation 3+ plants. Now a PSA for a Generation 4 plant is going to be started. The new plants have new inherent safety features that are addressed in terms of their influence on probabilistic safety assessment (PSA) studies which have been performed by Atomenergoproekt since 1988.

One of the new plants under construction is the Kudankulam nuclear power plant (NPP) in India. Its design is developed on the basis of VVER-1000/V-412 advanced reactor unit which is the evolutionary design of serial power units with VVER-1000/V-320 reactor plants operated in Russia and East European countries for many years. The main design features are a unique combination of active and passive safety systems and accommodation to tropical climatic conditions. This design is referred to Generation 3 advanced pressurized water reactors class and complies with international requirements to the nuclear power plants commissioned after the year 2000.

The Kudankulam NPP design developed by Atomenergoproekt has enhanced safety characteristics. The qualitative upgrading of the safety level is attained due to the maximum use of the following passive safety features:

- Eight additional hydraulic accumulators for long-term passive core flooding for 24 h or longer (2^{nd} stage hydroaccumulators system)

- Twelve air cooled heat exchangers for passive decay heat removal via the secondary side for an unlimited time period without operator interference
- New passive fast acting boron injection system to transfer the reactor in a sub-critical state
- Double containment shell of the reactor building with passive filtering of the annulus
- Hydrogen recombiners installed in different compartments inside the containment
- Core melt catcher for catching core debris generated when the core melts and corium penetrates the reactor pressure vessel

The main advantage of the NPP with the new generation reactor compared with Russian designs of previous generations is the use of advanced equipment and introduction of additional passive safety systems in a combination with conventional active systems. Implementation of diversity increases likelihood of safety function fulfillment (see Fig. 1).

Another new plant under construction is the Novovoronezh NPP-2 in Russia. Atomenergoproekt was selected as the general contractor for both designing and construction of this plant. The Novovoronezh NPP-2 is the prototype nuclear power plant of the new generation AES-2006 design with VVER-1200 reactor type. It is based on the technical solutions of the AES-92 design, which is officially certificated for compliance with the European Utility Requirements (EUR). Unique technologies, used in the AES-2006 design not only increase the service life of the main nuclear power plant equipment up to 60 years, but also enhance safety characteristics and competitiveness on the electric power markets. The main design feature is the compliance with modern and prospective safety requirements. The AES-2006 design is characterized by a broad use of passive and active safety systems, which are similar to those at the Kudankulam plant, as well as low sensitivity to human errors. All these features increase safety level and improve the design performance.

For newer plants specific features have been incorporated into the design to provide protection for severe accidents. These pre-planned severe accident management measures includes:

- providing cooling to the core by any means when it is still in the pressure vessel, e. g. using feed-and-bleed procedure
- using depressurisation of the primary circuit to prevent high pressure melt ejection
- removing hydrogen from containment volume by means of passive recombiners that have the capacity to deal with the rate and volume concentration produced during a severe accident
- adding water to the containment to provide a means of heat removal from the molten core material after it has exited the pressure vessel

The planned development of nuclear energy in Russia in the nearest future is going to be mainly based on the AES-2006 design with either VVER-1200 or VVER-1300 reactor (VVER-TOI). Atomenergoproekt is also the general designer of Seversk, Central and South-Ural NPPs in Russia. All three plants are supposed to be constructed as per the AES-2006 design.

Last but not least the company has started the development of a power plant based on module lead-bismuth fast neutron reactor – SVBR-100. Its design has integral layout of the entire primary circuit equipment in a robust casing covered with protective housing. The advantage of this reactor technology is an enhanced safety level and the modular design which allows creating nuclear power plants of different capacity multiple of 100 MW (e) based on a standardized reactor module which is completely manufactured at machinery works and practically ready-made is delivered to the NPP site. At the moment the Atomenergoproekt Company has been performing PSAs for six NPPs in design. The paper is aimed at sharing some issues and experience gained from the PSA development for new and advanced plants.

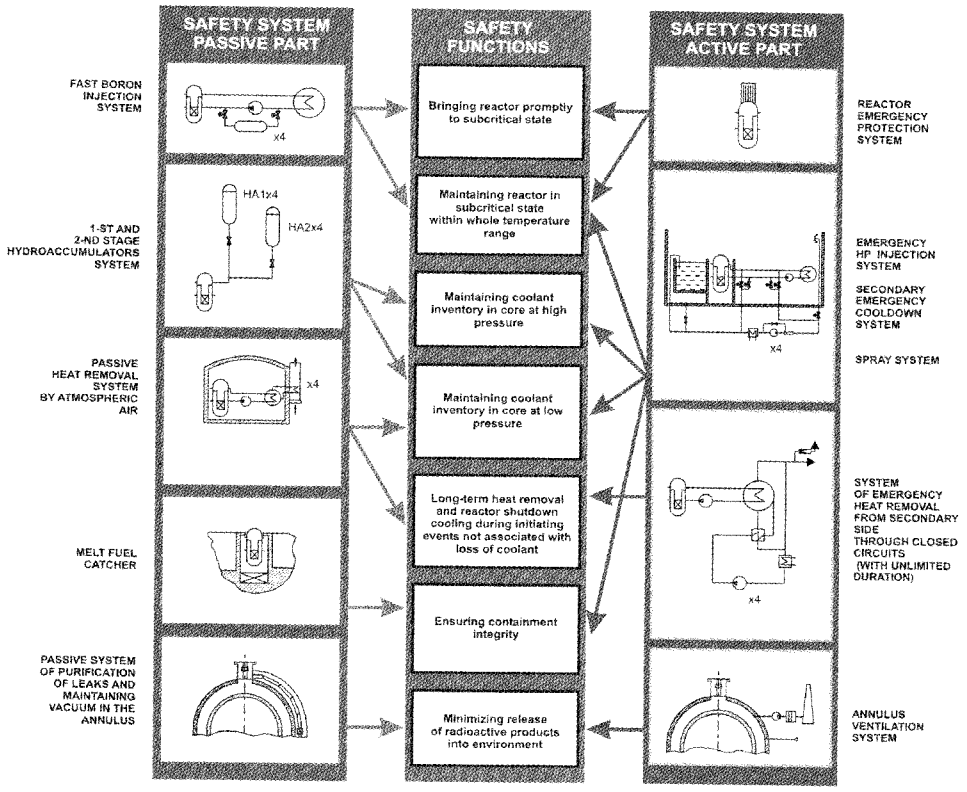

Fig. 1. Diversity in design of new plants

2 Special features of PSA for new plants

2.1 Requirements to probabilistic safety targets

Customer requirements to probabilistic safety targets are usually stronger than existing Regulatory or IAEA ones. It appears that industry takes the lead over regulation in this case and forces the designer to find and implement appropriate means to enhance safety, which sometimes have no reference to practical experience. For example, an industry requirement to the core damage frequency estimated for the AES-2006 family plants is defined as 1E-6 per reactor year taking into account contribution from all plant operating states, internal initiating events, internal and external hazards. This is an order of magnitude stronger that the Russian regulatory requirement [1] and INSAG-12 [2] recommendation.

On the other hand, the existing PSA methodology and regulatory documents are mainly oriented to existing operating plants. This creates problems when developing a PSA as well as performing regulatory and IAEA reviews [3]. For example, according to some national standards NPP shall be designed to sustain safe shutdown earthquake with frequency of 1E-4 per year. In the plant design such a seismic level is associated with the most stringent safety requirements, i.e. the target probability levels defined for the plant. The expected frequency of occurrence of the associated seismic scenarios is too high for input to a seismic probabilistic safety assessment because the nuclear power plant has a very low core damage frequency for innovative plants in relation to both seismic and non-seismic initiating events as it was mentioned above.

Another example is that PSA rules and standards say nothing about the scope and methodology of a preliminary PSA when it is carried out at the conceptual or preliminary basic design stage given lack of important information (equipment location, cable routing, operating procedures, characteristics of specific site, etc.). Our experience from IAEA IPSART missions to review preliminary PSAs shows that any expert initially provides many comments, especially on internal/external hazard PSAs. Following a discussion the expert is usually faced with the necessity of allocating his requirement among design stages (see next Section).

2.2 Scope of PSA

The scope of the PSA may be different depending on a design stage and PSA applications required. The design process can be split into three general phases:

- Conceptual design
- Basic design
- Detailed design

The scope of the PSA depends on what stage of the design the PSA is used for its evaluation. For a new plant, the PSA is usually started during the conceptual design aimed at evaluation whether the level of redundancy and diversity in the safety related systems is adequate. After that, the PSA is improved at the basic design stage to assess more detailed design issues, including evaluation of protection against internal hazards. Finally, the full-scope PSA is used for design verification against probabilistic safety criteria at the detailed design stage.

At the conceptual design phase the PSA usually addresses the contribution to risk arising from all internal initiating events and possibly all the modes (power, low power and shutdown) of operation of the plant.

During the basic design phase the design of the plant may be not site specific. To verify that the plant design complies with the probabilistic safety targets during the basic design phase, the scope of the PSA includes a Level-1 and Level-2 type analyses for internal events and internal/external hazards which are simplified. The last is optional.

The full scope PSA, including a Level-1 and Level-2 type analyses for all plant operating modes, internal initiators, internal and external hazards, needs to be developed during the detailed design phase to provide a basis for demonstrating compliance with quantitative safety targets [4].

When using a PSA as a support to design, making decision about safety features to be incorporated into the design based on the PSA results is an iterative process to ensure that the insights gained from the PSA are fed back into the design process. The designers, based on research results as well as operational experience and PSA results for reference plants, make initial judgment. After that, any modification being incorporated into the plant layout, system diagrams, descriptions, and operating modes, duration of plant operating states, lists of signals, etc. based on the previous version of the PSA requires producing a new version of the PSA, which, in turn, can provide new findings and insights being used as input for new design modifications. The design process can involve several iterations. Therefore, this should be a much more living PSA than a PSA for operating plants.

Actually, the PSA and design are developed in parallel. When performing the next revision of the PSA the plant design can potentially be modified because of the fact that the PSA is a time consuming task. Therefore, special attention is given to these living features of the plant design being developed and PSA being conducted at the stage of the plant design development.

The base case PSA is usually performed for NPP in design. However, a customer may require additional PSA applications to consider, for instance, risk monitoring. In this case the scope of the PSA is extended to implement special attributes of the application needed that often requires specific information not available at the design stage.

2.3 Uncertainty of PSA findings

A specific point that should be addressed for any plant in design is a lack of some design/operating information, especially for a PSA performed during the conceptual or basis design stage. Such a PSA may contain substantial uncertainties.

The lack of design information affecting PSA development may be associated with incompleteness of the design development that is typical for interim design stages and communication problems caused by the involvement of many different companies in the deign activity. The extra uncertainties related to the areas of insufficient information may come from incomplete design information, inapplicable data, rough thermal-hydraulic analyses, lack of operating procedures, engineering judgement, etc. It is important to note that the non-quantifiable uncertainties associated with modelling, assumptions and completeness of the study are much higher when performing a PSA for an advanced plant in design than those for operating plants.

To deal with this issue bounding technologies are used. However this approach sometimes contradicts to the "best estimate" one recommended by regulatory guides.

It is also very important to manage the iterative PSA development. The PSA should address the actual or intended design of the plant that should be clearly identified as a starting point for any revision of the PSA.

Within the design process all necessary systematic actions to provide adequate confidence that the PSA documentation will satisfy given requirements for quality are established, included in the procedures, followed by the PSA team, and controlled from independent experts to exclude root causes of possible discrepancies [5]. These actions include:

- *Coordination of deadlines between the PSA team and different groups of designers both within the design company and with subcontractors.* The establishment of an effective project work control process is very important. The overall work plan that addresses all the efforts required for the performance of activities by all the parties involved in the design process, including PSA development, is developed and carried out for the entire design development.
- *Good information exchange between designers, including deterministic analysts, and the PSA team.* Establishing of an electronic archive of valid design documentation is very useful. A good example is an extensive, detailed 3D computer model being developed for the VVER-TOI nuclear power plant. Although the model is developed over several years, using inputs from a number of design participants from a variety of companies, is labour consuming, it is very useful for the PSA, especially for fire and flood analyses.
- *Internal check and approval of the PSA documentation by designers.* It can help to reveal last changes incorporated into the design of the plant, but not considered in the PSA model.
- *Good communication with manufactory experts responsible for equipment reliability evaluation.* Due to lack of operational experience for new plants, the PSA is often forced to involve manufactory data that should be treated carefully. A typical example is the inconsistency between definitions of the boundaries and failure modes used in system and data analyses, in particular for new components if manufacturer data is applied. The PSA component boundaries in the system analysis typically extend beyond the equipment, failure modes, and failure causes specifically defined by manufacturer. For instance, the PSA boundary for a "pump" typically includes the pump mechanical components, motor, circuit breaker, and local control circuits. The manufacturer's data for "pump" failures may include only the mechanical parts of the pump because other vendors are responsible for the other subcomponents.
- *Coordination between PSA analysts performing different PSA subtasks.* Detailed procedures are developed for each PSA subtask with an emphasis on subtask interfaces, especially when incorporating the design changes into the PSA model and documentation.
- *Tracking changes in the PSA documentation in both paper and electronic form correlating with the actual design status, etc.* A special QA procedure is established to assure that the models and data used are good representation of the actual plant design. It is taken into account that a considerable information exchange is conducted in a paperless form.

In order to succeed in developing a PSA of high quality, an iterative approach to performance, modification, consistent PSA tracking, permanent interaction among PSA team members, and effective communication with designers from organizations involved in the design process are carefully established and maintained.

2.4 New methodological issues

The PSA development for advanced NPPs has raised some issues originated from unknown new components, processes and technologies incorporated into the design of an advanced plant. This is a challenge to PSA developers.

2.4.1 Mission time

Much longer mission times for components of, at least, three days need to be considered in the PSA for a new plant design in comparison with the usual time of 24 h. For instance, Russian advanced VVERs [6] have low pressure passive hydroaccumulators, called the second stage, with capability of more than 24 h depending on a size of a primary leak. During this time the active emergency core cooling is unnecessary. Therefore, in this case a 24 h mission time is inadequate to quantify actual contribution to the core damage frequency from loss-of-coolant-accidents (LOCA). In general, the calculations for accident sequences should be extended beyond the time point when the reactor has been tripped and other safety systems actuated, until a long term stable state has been reached. On the other hand, a greater mission time can be used for recovery actions and repair usually ignored in the PSA for existing plants [7].

2.4.2 Safe end states

A safe end state is a long term stable state when all the safety functions have been fulfilling such as criticality control, residual heat removal from the reactor facility and the containment, and localization of radioactive products within the boundary envisaged in the plant design, plant parameters are well below the design limits for components and structures.

There is a tendency not to consider end states as safe if parameters are not stable and no heat removal from the reactor fuel is maintained via a closed circuit, i.e. actions have to be taken for replenishment of water sources.

2.4.3 Error probabilities for long-term human actions

Safety philosophy for non-power operating modes of new Russian reactors is based on long-term passive residual heat removal using considerable water inventory. In this case a problem of human error probability estimation within a long time window exists because the current methodologies are limited to smaller time values.

2.4.4 Common cause failures

Methodology adopted in the Atomenergoproekt Company distinguishes weak and strong coupling factors [8]. Depending on that common cause failure models are chosen. There are some aspects we would like to discuss:

- The use of diversity in Russian new designs is an effective defense against common cause failures. One of the approaches to minimizing the impact of common causes is to apply diversity in operating modes when some trains are standby and the others are in operation before an accident. That affects common cause failure model parameters.
- The extensive use of digital systems in the design of a new plant poses methodological problems in a PSA since there is less experience in modelling computer based systems. In particular, there seems to be potentially high contribution of common cause failures and software faults (recurrent errors in redundant software modules) [9]. Issues associated with receiving fault data from software developers should also be resolved. The Russian approach is to apply diversity to software based redundant modules. It should be men-

tioned that the main Russian regulatory document [1] prescribes the fulfillment of a software reliability analysis.
- It is usual practice not to model inter-system common cause failures for existing plants because they are believed to be negligible contributors to core damage frequency, large early release frequency, etc. However, for future reactors involving inherent safety features and demonstrating compliance with reduced safety target values special consideration seems to be given to inter-system common cause failures and common cause failures associated with similarity in active subcomponents (motors, circuit breakers, etc.).

2.4.5 Statistical treatment of raw event data coming from reference plants

Using operating failure data from reference plants may lead to extra uncertainties for new ones even if components of similar types are used. This can be explained by differences in age of equipment at different units, maintenance culture, criteria used for event selection as well as modernization performed. All these factors result in inhomogeneity when pooling data in a sample. The issue should be correctly addressed in the methodology and practical analyses.

2.4.6 Reliability estimation for new components

New design decision made for new plants are sometimes based on using new unique equipment. This raises an issue of its reliability estimation because operational experience may be inapplicable. In our opinion the design companies should encourage and press on manufactures to assure a good experimental and scientific support to justify reliability values, including passive equipment, e.g., based on fracture mechanics analysis.

2.4.7 Reliability methods being used for the analysis of natural circulation systems

The development of the reliability assessment methodology for passive systems that utilize natural circulation, including evaluation of an uncertainty range of the system performance, is very important. The existing methods are generally based on Monte-Carlo simulations which require a large number of thermohydraulic calculations. As a result, these calculations can be extremely time consuming ones. To avoid this problem, an internationally accepted methodology should be developed.

3 Interpretation of PSA results for new plants

There are a number of ways how the results of the PSA are used to evaluate the design of a new plant, to identify weaknesses in the design and to assess and rank potential options for improving the design. Generally, these include [10]:

- *Safety metrics/indicators such as safety system reliability, core damage frequency, large early release frequency, etc.* Safety metrics/indicators show whether the overall risk from the plant is low enough to start a license process.
- *Lists of minimal cut-sets.* The integrated list of top minimal cut-sets and lists of minimal cut-sets generated for separate initiating event groups related to different plant operating modes are reviewed. Both internal initiators and hazard-induced initiating events are considered. If a single order minimal cut-set representing an independent failure, e.g. a failure of a common support system component, appears in the list of minimal cut-sets provided within the internal event PSA, then, hence, the single failure criterion is not met, and redundancy of the system concerned has to be increased. If a similar finding is found in the internal hazard (e.g., fires and floods) PSA, then separation and segregation of safety related components is insufficient and needs to be improved.
- *Importance functions for basic events, groups of basic events, safety systems, initiating event groups.* High importance of an independent failure event may indicate insufficient redundancy of the system in some plant operating modes and the need for improvement. In this case, either system redundancy needs to be increased or limiting conditions for operation of the system should become tougher for this particular plant operating mode, if possible. High importance of a common cause failure may indicate insufficient diversity applied to some safety function. In this case a drastic change in the design basis might potentially be required. High importance of a human error may indicate a poor man-machine interface. Increasing automation of the plant can be considered as an additional design measure to resolve the issue.

These results are used to determine whether the design is balanced or additional measures need to be incorporated to reduce risk.

As an example, the history of the AES-92 conceptual design development in Russia can be considered. The concept of this advanced VVER was developed taking into account findings of PSA studies conducted for operating VVERs, for example, it was found that both failure of residual heat removal systems and common cause failures together with human errors have a relatively high contribution to the core damage frequency. Therefore, special measures using passive and diverse technology for residual heat removal were incorporated into the design of new plants in order to reduce their contribution. After that, results of a new PSA showed that a LOCA contribution became relatively high. That required new measures to be applied like long-term operating hydroaccumulators to reduce the LOCA contribution and create a balanced design. It was an iterative design process. Of course, the concept is supported by a large number of research and experimental studies.

Where the PSA has been used to identify weaknesses in the safety systems that prevent core melt or mitigate severe accidents it can also be used to compare options for improvements to remove the weakness. The options for improvement would depend on the origin of the weakness and the stage in the plant design development when the weakness was identified. Our experience shows that the considerable changes are usually possible at the conceptual design stage and might include:

- making significant improvements to safety systems used at a reference plant – for example, by adding redundant trains, incorporating diversity, etc. An example is the replacement of a three-train configuration of safety systems typical for existing VVER-1000 plants by a four-train configuration of VVER-1000 plants being constructed now in several countries [6, 11, 12];
- incorporating additional safety systems – for example, by adding diverse safety systems to prevent core melt, provide protection for a severe accident, etc. For instance, in the design of the Kudankulam plant the emergency residual heat removal is fulfilled by two diversified long-term redundant systems, one of which operates in a passive mode [11, 13];

- incorporating additional fire protection systems, fire barriers, separation, segregation, fire retardant cables, water lubricating in bearings, etc. As it was shown in paper [13], although the numerical results of the fire PSA at the preliminary design stage are associated with high uncertainties, the fire PSA including fire hazard assessment can provide an extremely cost-effective approach to fire protection improvement. The fire PSA performed in a highly iterative manner was recognized as a valuable tool that can provide insights into plant design and identify important fire-induced dependencies;
- incorporating additional flood barriers and drain facilities;
- replacing key old components with similar components of a more modern design. For instance, it is a well known VVER problem related to containment sump plugging by primary pipe thermal insulation in case of a LOCA. That was eliminated by the block structure of primary thermal insulation and a new design of the containment sump filters in the advanced VVERs [14];
- incorporating additional seismic protection;
- applying pre-planned severe accident management measures; etc.

It is important to note that a comprehensive analysis of any option to be incorporated into the design needs to be carried out involving all the parts of the PSA study. It should be done to avoid missing potential negative aspects of the option considered, for instance:

- an additional train connected to the primary circuit may increase a LOCA frequency;
- an additional water-based fire suppression system needs to be considered as an additional flood source;
- any new fluid system should also be considered as a potential flood source;
- any additional system could be dependent on the same support system as the old one that may neglect benefit of the option proposed;
- any new AC/DC powered system needs to be considered as both additional fire load and potential source of fire-induced dependencies; etc.

The results of the PSA are being used as one of the inputs to a risk informed decision making process with respect to the option to be incorporated into the design. The PSA is used to estimate the reduction in the risk for each of the options identified. This information is used together with the costs of applying the change, the deterministic requirement and other factors in decision making.

Integral PSA results for the Novovoronezh-2 plant (new advanced VVER) under construction are presented in Table 1 and discussed below. To bring into adequate comparison the results are given for internal initiating events.

The comparison of PSA results obtained for the last family of operating VVER and advanced VVER in design shows that core damage and large early release frequencies for internal initiating events are approximately two orders of magnitude less at the Novovoronezh-2 NPP. This dramatic reduction in the cumulative frequencies is mainly caused by incorporation of passive systems and diversity principles into the design of the advanced VVER.

It should be noted that the passive systems are also very beneficial in case of internal hazards like fires and floods. These hazards may mainly cause transients, loss of off-site power or blackout. The use of diversity in the design to provide an alternative path of residual heat removal based on a passive mode is a very effective tool to cope with such hazards. That was evaluated when performing PSA for the Kudankulam plant in India. Although the fire PSA was performed in a conservative manner the extremely low value of the core damage frequency obtained shows that passive safety features incorporated into the design of the Kudankulam NPP assure reliable fire resistance of the plant. The overall fire-induced core damage frequency for Kudankulam NPP was quantified to be six times lower than the core damage frequency addressed in the internal event PSA [13].

4 Lessons learnt from the Fukushima accident in Japan

Following the Fukushima accident in Japan the main attention has to be paid to external hazards especially for the plants having safety features. This work has been done before the accident and is extended after that. For example, the Kudankulam NPP is located on the seacoast. Certainly the Kudankulam plant design was checked against the conditions occurred during the Fukushima accident in Japan when the earthquake had caused major damage to the power grid and the subsequent tsunami flooded the plant, knocking out emergency generators needed to run pumps which cool the reactors. It is demonstrated that the Kudankulam plant is designed to cope with the Fokushima like long-term blackout because the passive decay heat removal system can start in a passive mode in case of blackout and run for an unlimited time period removing residual heat from steam generators to atmosphere.

The main task now is to update the PSA methodology, including seismic PSA already applied to analyze the design of new plants constructed in seismic regions like India, Turkey and Bulgaria. For instance, some delayed consequences such as a seismically induced loss of diesel fuel pumps may become important when considering a long-term loss of off-site power. Therefore, long-term accident sequences need to be carefully addressed in order to avoid core damage frequency underestimation.

Other lessons learnt from the Fukushima accident are to direct additional efforts to the following points within the PSA development:

- *Investigation of multi-unit accidents.* Some dependencies such as shared diesels, switchyards, transformers, heat ex-

Table 1. Comparison between PSA results for Novovoronezh-2 and VVER-1000/320 operating unit

Core damage frequency, 1/a		Large early release frequency, 1/a	
VVER-1000/-320	Novovoronezh-2	VVER-1000/V-320	Novovoronezh-2
4.5 E-5[1] 1.5 E-5[2]	6.1 E-7[3]	4.0 E-6[4]	1.8 E-8

[1] Balakovo Unit 4, Russia, internal initiating events, power and shutdown operating states
[2] Temelin NPP, the Czech Republic, internal initiating events, power operation [15]
[3] Internal initiating events, power and shutdown operating states
[4] Temelin NPP, internal initiating events, power operation [15]

changers, etc. are evident and usually analyzed while performing a PSA. Particularly important are subtle interactions that have the potential to result in the simultaneous unavailability of safety systems at adjacent units following a long-term accident. Common cooling water and diesel fuel inventory is of utmost importance. Other important points are manager reliability analysis in case of multiple accidents as well as availability of spare parts and repair staff for several units simultaneously. Allocation of available resources may be a very useful PSA application. For a multi-unit site, the potential spreading of a hazard like seismically induced fire to other units should also be considered in the analysis.

- *Spent fuel pool analysis.* For new designs that provide the features to delay spent fuel damage, consideration of a long-term mission time is necessary. It is clear that following a loss of off-site power spent fuel cooling pumps need to be powered by essential diesel generators even if water inventory is sufficient to remove residual heat for several days by evaporation. Other important items may be resources shared between the spent fuel pool and reactor core or among several units in case of a long-term or/and multi-unit accident.
- *Analysis of combined internal/external events.* Consequences of the Fukushima accident show that combinations of hazards may be significant for risk. As a matter of fact, a multiple hazards analysis should involve a systematic check of the dependencies between all internal and external hazards. It is evident that combinations of hazards may have a significantly higher impact on plant safety than each individual hazard considered separately. On the other hand, the frequency of combined events may be comparable to that of the individual hazards. Regarding experience from Japan accidents, at least, three types of hazard dependencies can be found. First, a seismic hazard induced another one (tsunami). Secondly, a fire (internal hazard) occurred in the turbine section of the Onagawa NPP following the earthquake (external hazard). Thirdly, flooding caused by recovery actions discharging a large amount of water kept safety system pumps disable at the Fukushima plant. The analysis of combined internal/external events is definitely supposed to be extremely time consuming.
- *Availability of an extended list of the procedures for severe accident management.* It is evident that Japanese operators were not trained to cope with the accident occurred.

(Received on 18 July 2011)

References

1 Gosatomnadzor of the Russian Federation. General Rules of Ensuring Nuclear Power Plant Safety. OPB-88/97. PNAE G-01-011-97. Moscow, 1997 (in Russian)

2 International Atomic Energy Agency. Basic Safety Principles for Nuclear Power Plants 75-INSAG-3 Rev.1 INSAG-12, Vienna, 1999

3 *Tokmachev, G. V.*: Special features of development and review of probabilistic safety assessment carried out for new NPP in design. Nuclear and Radiation Safety 58 (2010) 3–10 (in Russian)

4 Federal Authority of Nuclear Regulation of the Russian Federation. Main recommendations for performing PSAs for NPPs, RB-032-02, Moscow, 2004 (in Russian)

5 *Tokmachev, G.; Lyubarskiy, A.*: Lessons Learnt from Review of PSA Studies for VVER-type Reactors. In: Proceedings of PSAM7-ESREL'04 Conference, 14–18 June 2004, Berlin, Germany, Vol. 1, pages 32–38

6 *Svyriaev, Yu. V.; Morozov, V. B.; Tokmachev, G. V.; Baykova, E. V.; Chulukhadze, V. R.; Fedulov, M. V.*: Use of probabilistic analysis in safety validation of AES-2006 designed for the Novovoronezh nuclear power plant site. Atomic Energy 106 (2009) 155–161

7 *Morozov, V. B.; Tokmachev, G. V.; Baykova, E. V.; Chulukhadze, V. R.; Fedulov, M. V.*: Estimation of NPP Probabilistic Safety Characteristics for Long-Term Mission Time. Izvestiya VUZov. Nuclear Power Engineering 2 (2010) 78–89

8 *Morozov, V. B.; Tokmachev, G. V.*: Approach to Common Cause Failure Modeling in Probabilistic Safety Assessments for New Designs of NPPs with VVER-1000 Reactors. Izvestiya VUZov. Nuclear Power Engineering 4 (2008) 31–41

9 *Tokmachev, G. V.; Podkolzina, L. V.; Lobanok, O. I.*: Estimation of Reliability of Information Computing System with Function of Presenting the Safety Parameters of Balakovo NPP. Nuclear Measurement & Information Technologies 4 (2006) 52–63

10 *Tokmachev, G. V.*: Approach to the use of the PSA in designing NPPs with VVER reactors of a new generation. Izvestiya VUZov. Nuclear Power Engineering 1 (2007) 44–53

11 *Mishra, A.; Chauhan, A.*: Probabilistic Safety assessment of KK-NPP. In: Proceedings of International Conference ICRESH05 "Reliability, Safety and Hazard", Ed. *P. V. Varde* et al., pages 339–345, Mumbai, India, 2005

12 *Ershov, G.; Sobolev, A.*: Plant Status and PSA of Tianwan NPP. International Workshop "SAFETY OF VVER-1000 NUCLEAR POWER PLANTS", 7–12 April 2003, Piestany, Slovakia

13 *Tokmachev, G.*: Fire Probabilistic Safety Assessment for Kudankulam NPP in India. In: Proceedings of International Conference ICRESH05 "Reliability, Safety and Hazard", Ed. *P. V. Varde* et al., pages 375–380, Mumbai, India, 2005

14 *Berkovich, V. M.; Kopytov, I. I.; Shvyryaev, Y. V.*: Design Solutions on Safety for NPP Units with WWER Reactors of New Generation – Short Description of NPP Power Units with New Generation WWER Reactors. In: Proceedings of International Conference ICRESH05 "Reliability, Safety and Hazard", Ed. *P. V. Varde* et al., pages 403–409, Mumbai, India, 2005

15 *Kučera, L.*: Temelin PSA Level 2. // IAEA Regional Workshop on Harmonization of Level 2 PSAs for VVER Reactors, Sofia, Bulgaria, 20–24 October 2003

The authors of this contribution

G. Tokmachev, V. Morozov
JSC "Atomenergoproekt", Moscow, Russia
E-mail: tokmach@orc.ru

You will find the article and additional material by entering the document number **KT110182** on our website at *www.nuclear-engineering-journal.com*