Artur V. Lyubarsky
Gennady V. Tokmachev
Mikhail V. Fedulov

Safety Issues of Nuclear Power Plants

LAP LAMBERT Academic Publishing

TABLE OF CONTENTS

GENERAL INTRODUCTION

The book is devoted to the safety assessment of nuclear power plants (NPPs) at the design stage using probabilistic safety assessment (PSA) methodology and Integrated Risk Informed Decision Making (IRIDM) process. Lessons learned from Fukushima accident are also considered.

The book consists of three papers.

The first paper addresses issues of probabilistic safety assessment for reactors of new design in Russia. A great expansion in the number of new advanced nuclear power plants being under design in Russia increases the importance of probabilistic safety assessment carried out during the pre-operational stage and its role in the design process. The paper discusses applications of PSA in the design process of new NPPs. Peculiarities and limitations of PSA conducted during the design stage are discussed. The paper classifies methodological problems related to advanced reactor PSA. Issues, that designers and the Regulatory Authority should resolve in the PSA development and review process (with reference to Russian NPP-2006 design), are discussed. Post-Fukushima PSA issues are also addressed.

The second paper considers how the concept of "fail-safe" design and corresponding "safe" states is being practiced by the designers of NPPs. The main attention is paid to failures of support systems and potential dualism of their consequences from the point of view of overall plant safety. The impact of the actual application of the "fail-safe" design principle on the consequences of the Fukushima Daiichi Unit 1 accident is discussed. Applications of deterministic and probabilistic approaches for defining "safe" states while implementing "fail-safe" design principle are compared. Integrated Risk Informed Decision Making Process is proposed for resolving issues related to "fail-safe" design in the plant systems design phase.

The third paper discusses features of the human reliability analysis conducted at the stage of the development of the preliminary safety analysis report. The differences in the goals of the human reliability analyses for operating plants and plants under design are discussed. The specific features of the human reliability analyses in application to the plants at the design stage are considered including issues related to collection of information, identification of human errors, qualitative and quantitative analyses, integration into the probabilistic safety assessment model. Pre-initiator and post- initiator human errors as well as errors that trigger the initiating event are examined. Analysis of the dependencies between the human failure events is considered. The special attention is paid to the definition of the minimal value of the resulting human failure events probabilities to be used in the PSA at plant design stage.

FEATURES, ISSUES AND APPLICATIONS OF PROBABILISTIC SAFETY ASSESSMENT FOR NEW REACTORS IN RUSSIA

Tokmachev G.V., Lyubarsky A.V.

INTRODUCTION

There are a number of new VVER-type reactors being under design, construction or operation in Russia and other countries. A Russian nuclear renaissance is supported by the Russian Government. The Russian energy strategy set a policy priority for reduction in power supply based on natural gas, aiming to achieve this through an increase in electricity production by nuclear power generation. In total now, two VVER units of advanced designs are under operation and four ones are under construction in Russia. In addition, the basic design of the advanced VVER plants needed for applying a construction license is developed for several new NPPs in Turkey, Bangladesh, India, Belorussia, etc.

A great expansion in the number of new nuclear power plants (NPPs) being designed increased the importance of probabilistic safety assessment (PSA) carried out at the design and pre-operational stages and highlighted the problem of evaluating the adequacy of the PSA. It is the design stage when PSA can provide a valuable contribution to the safety enhancement of the NPP; however, in order to allow PSA to support design applications it should be comprehensive and of adequate quality. The paper discusses the role of PSA at an NPP design stage and considers issues related to PSA for new plants (with reference to Russian NPP-2006 design).

PSA APPLICATIONS AT DESIGN STAGE

Design PSA is the PSA that is developed during the design phase of the NPP lifetime with the goal to support technical and organizational decisions made in the NPP

design process to achieve safe and balanced design. Potential applications of the design PSA are listed below.

Justification that the design is in compliance with the national probabilistic safety targets and/or requirements set by the Nuclear Regulatory Authority

The PSA results are used to demonstrate that target safety values (probabilistic safety indices or metrics) have been achieved for getting better understanding of the NPP design safety concept. PSAs performed for the Novovoronezh-2 NPP and Akkuyu Unit 1 NPP during the design phase are typical examples of such an application [1-3]. The results of the PSA are used to obtain licenses for construction and further operation of the Unit.

Allocation of equipment reliability targets for manufactories

This is responsibility of a plant designer. The reliability parameters for equipment used in the design PSA are limiting values for component reliability that must be satisfied by the manufactures. If a component has a high significance for safety then its reliability target itself may be changed to a higher one to get better assurance in estimated risk indexes for the NPP under consideration.

Equipment qualification

The new Russian regulation [4] allows assigning lower safety qualification to the equipment, not belonging to safety systems, if risk associated with a failure of this equipment is extremely low. PSA is the only tool to evaluate such risks and should be sufficiently detailed and comprehensive to allow such an assessment for all equipment of interest.

Evaluation of alternative design options and optimization of system configurations for different operational states and hazards

PSA is used for choosing the best solution among different design options. It is important to note that a comprehensive analysis of any option to be incorporated into the design needs to be carried out involving the full-scope PSA. This is important

not only from the viewpoint of the completeness of the numbers obtained (e.g., the estimated values of risk metrics, their uncertainty, importance of components, etc.), but also to avoid missing potential negative aspects of the option considered. For instance, the additional train connected to the primary circuit increases reliability of the emergency core cooling system, but at the same time increases Loss-Of-Coolant-Accident (LOCA) frequency, acts as a source of internal fire and flood, etc. Another example is the installation of additional walls acting as fire propagation barriers that may have a negative impact in seismic hazards if not designed adequately.

Optimization of system configurations requires the consideration of various operational states, because in certain shutdown states in some new VVER designs planned maintenance of one safety train is performed. This leads to reduction or even loss of the redundancy in safety systems and may require certain limitations or rescheduling of maintenance activity taking into account risk insights.

Therefore, PSA should be capable to account for all the features of the design for all the operational states and for all the hazards.

Input to cost-benefit analysis

It is difficult to develop a robust procedure for weighting cost and safety factors. However, PSA insights are taking into account in the cost-benefit consideration following so-called Integrated Risk Informed Decision Making process [5].

Input to public relation activity in the pre-licensing process

PSA results are used during public hearings on safety concerns. The hearing process that involves risk insights makes it possible for the public to get more complete understanding of safety matters.

Development of conditions for safe operation

It is usual practice to use PSA for definition of allowed outage times and surveillance test intervals for safety related systems. It is performed in an iterative manner at different design development stages. Justification of on-line maintenance is another

PSA application at the detail design development stage. PSA is also used for developing other operational and design documentation up to the end of the design development.

Identification of R&D works which are necessary to support the design

PSA is used for establishing the list and priority of research activities for new technical issues on advanced reactors, which need to be carried out in support of design options.

Input to development of a list of beyond design basis accidents

Frequencies of combinations of an initiating event group and safety function failures are calculated using PSA models [6]. The technical measures must be implemented for scenarios with multiple failures if risk metrics for NPP exceeds regulatory requirements/targets (core damage frequency $<1.0\ 10^{-5}$/a or/and frequency of large radioactive release $<1.0\ 10^{-7}$/a).

Categorization of postulated initiating events in terms of their frequency

The defence-in-depth concept implies that postulated incidents and accidents leading to anticipated operational occurrences or accident conditions are examined.

When performing deterministic safety analyses all postulated initiating events and their associated transients are grouped into categories enveloping a family of events of the expected frequency.

Design acceptance criteria depend on their frequencies, which can be calculated using PSA tools.

Development and improvement of the emergency operating procedures

The use of best estimate codes and models as well as best estimates of important modelling parameters is essential for adequate modelling of accident scenarios being addressed in the emergency operating procedures. PSA provides valuable information for defining scenarios to be addressed in emergency operating

procedures that also accounts for uncertainties in the models, parameters, operator actions and other important features of accident progression.

Feedback to deterministic analysis to support the evaluation of the adequacy of defence-in-depth

One of essential outcomes of a PSA is a generation of logic model incorporating all the interconnections between systems and equipment, both intra- and inter-system of the plant. Such a logic model analysis with the use of mathematical tool constructed on the basis of Boolean laws enables revelation of minimal combination of failures and human errors, sufficient to entail core damage for the entire spectrum of possible initiating events, including beyond design basis events. Such combinations are usually referred to as "minimal cutsets" (MCSs); they incorporate combinations of initiating events, equipment failures and human errors. Here, if the model is calculated with no cut-off by probability, we can guarantee revelation of all the MCSs containing as a minimum two basic events representing equipment failure and/or human errors and/or unavailability due to maintenance.

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, 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. [7]

Analysis of the degree of defence against assumed terrorist attack scenarios

The use of PSA for terrorism risk analysis has certain limitations. However, PSA tools like event trees, fault trees, and decision trees can be a useful approach for the decomposition of terrorism scenarios and comparison of terrorism risks. Location-

oriented methods used in fire/flood PSA can help to focus on target vulnerability and be used for the evaluation of consequences of a successful attack.

Selection of safe states when applying "fail-safe" design principle

A "fail-safe" design principle is a principle when all equipment is designed to achieve the safest state in case of a loss of support systems. In publication [8] it is shown that wrong implementation of this principle had a significant impact on accident progression during Fukusima Daichi accident. PSA is the valuable tool to define the most balanced safe state for the equipment being used as a part of Integrated Decision Making Process (IRIDM) as discussed in [8].

Other PSA applications

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.

PECULIARITIES OF DESIGN PSA

A designer of a new plant usually considers a range of alternatives in addressing safety issues and reaches a conclusion on the acceptability of the design through a traditional engineering analysis, complemented by insights from the PSA to reduce the risk from severe accidents and make the design safer.

This activity is started from the early stages of the design process involving the development of conceptual, basic and detailed design in a consecutive order.

The design PSA is carried out in a highly iterative manner during different points in the plant design lifecycle. Certain tasks needed refinement after conducting one or more of the subsequent tasks or incorporating changes in the plant design. Actually, the PSA and design are developed in parallel. When performing the next revision of the PSA the plant design is more detailed and can potentially be modified because of the fact that the PSA is a time consuming task and it is not easy to react

immediately on any single change introduced during the design process. 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.

As it was mentioned above, the PSA to be able to support all applications must be full-scope; however, certain insights from some applications can be drawn even from the PSA of a limited scope. It is a practical approach that the scope of the PSA varies depending on a design stage. The typical PSA scope at the different design stages are briefly described below.

- In developing the conceptual design a simplified Level 1 PSA can only be performed based on a representative set of internal initiating events, assumed full power initial conditions. Such a PSA typically is carried out for a plant design independent of site considerations.
- PSA is extended to include various operational states and internal/external hazards as well as Level 2 analysis at the basic design stage to assess more detailed design issues based on a detailed description of the front line safety systems, comprehensive treatment of the initiating events and plant operational states, and simplified treatment of internal and external hazards. At this design stages, however, the information or the data are not fully available concerning the system layout, equipment arrangements, cable tray raceways, and so on. Therefore, the risk perspective is hard to be gained through the PSA of internal hazards (e.g., fire, internal flood, etc.). A bounding approach is usually used in this case to be on the conservative side of risk assessment. Moreover, the basic design of the plant may not be site-specific that is important for the external hazard PSA.
- Finally, the full-scope PSA is used for design verification against probabilistic safety targets/criteria at the detailed design stage. The full scope PSA providing a basis for demonstrating compliance with quantitative safety targets is conducted for a plant design at a specific site with well defined site

characteristics and detailed design description of the entire plant. It includes comprehensive treatment of the internal initiating events and plant operational states, detailed analyses of the internal and external hazards, radiological source terms, and offsite radiological consequences.

At the conceptual and basic design stages there is a lack of the following information:

- data on pipeline layout;
- data on layout of power and control electric cables;
- data on equipment arrangement and details of its anchorage.

  A walkdown approach, widely used in hazard PSA specifically for evaluation of the potential spatial systems interactions, construction quality, anchoring devices, water access from flooding, etc., is impossible to implement in these design stages;

- operation procedures, describing system operation and maintenance, and abnormal operation procedures, describing actions in an accident for the NPP personnel. Many aspects cannot be evaluated in the human reliability analysis given their absence, absence of the NPP itself and the operating staff;
- data on control systems, human-machine interface, main control room design;
- specific data on equipment reliability, leading to the need to use only generic data, which is more ambiguous. For a completely new unique design of the component applicable experience data from reference plants might not be available. Note, that this limitation is also valid for the detailed design stage.

Some new approaches have to be established for the design PSA which are as follows:

- approaches to analysis of potential risk contribution from design errors. Design errors can result in that a plant may enter a mode not accounted for in the design;
- approaches on how to timely evaluate design changes implemented during the design development process;
- concerted approaches to evaluation of specific new technologies (e.g. digital and programmable systems, passive front-line safety systems, etc.).

PSA performed during the conceptual and basic design stages inevitably has certain limitations, which are objective reality. The experience from the development and review of PSAs for NPP in design shows that the scope and level of details of a PSA is always limited by the current level of details in specifying the site, design, and operational features of the plant. There is an evident problem that Russian regulations and IAEA standards [9, 10] do not specify what the PSA scope and level of details are consistent with the design life-cycle stage of interest and how these limitations impact the PSA applications.

In spite of design PSA limitations the effective use of PSA during the basic design stage, when all changes are easy to implement as they affect only drawings and documentation, is extremely higher comparing to the use of PSA for already operating plants. At operating plants apart from changes in documentation, it is necessary to install equipment, erect structural units, etc. in conditions that all structures are already fixed. It is also important that any construction work leads to break in plant operation and losses in electricity generation. As an example, the Russian NPP-2006 design incorporated multiple improvements based on PSA insights, including the following:

- changing the type or normal position of certain valves to improve reliability;

- installing separation valves at the suction part of the residual heat removal pumps to exclude their dependent failures in shutdown modes;
- constructing additional fire barriers or improving their fire resistance;
- replacing zero signals by zero plus ones to eliminate spurious actuations caused by a fire-induced open circuit;
- incorporating an additional line of different diameter into the spent fuel pool cooling system to avoid common cause failures;
- implementing diversified operating modes (standby vs. run) of a redundant safety system train to reduce a common cause failure contribution;
- incorporating changes in the refuelling process that all planned maintenance is performed in states when more than one train of one system is capable to provide residual heat removal, etc.

PSA REVIEW

The advanced VVER design used to be reviewed by the Russian Nuclear and other Regulatory authorities with the involvement of the industry [11]. The Russian Nuclear Regulatory Authority has issued main regulations [4] to establish quantitative safety targets and the administrative regulations to manage the licensing process [12]. PSA must be provided to apply a licence for unit construction or operation. The required PSA scope and quality are defined in several regulatory guides [13-18].

In addition, the Russian Nuclear Regulatory Authority published its probabilistic safety assessment policy statement in 2012 taken into account post-Fukushima reality and past experience [19]. The role of PSA is declared to be of utmost importance.

As a matter of fact, the regulatory documents mentioned above were developed for existing operating plants and do not distinguish early design stages when a plant do

not exist and some information is unavailable. The same approach can be found in IAEA PSA documents. The regulatory review experience shows that uncertainty in the allocation of requirements to the PSA performed at early design stages makes it difficult to perform a consistent review. Such requirements must be created by the PSA society.

Currently, the regulatory review is solely based on the opinion and experience of a particular expert resolving the issues.

The development of the concerted approach of the regulatory body and industry to the question of what exactly a design PSA should be and how it should be implemented in the NPP design is considered to be vital. The PSA technology should be able to address key questions regarding the development and licensing of advanced reactor designs.

PSA ISSUES RELATED TO ADVANCED REACTORS

The main advantage of a new generation of the plants belonging to NPP-2006 family compared with conventional VVER designs is the introduction of additional passive safety systems in the combination with proven active systems. Execution of safety functions can be performed by either active or passive safety systems independently of each other. Application of a complex of active and passive safety systems to cope with design basis accidents and beyond design basis accidents is beneficial because implementation of diversity increases the likelihood of the safety function fulfilment [20].

The most innovative passive system is a passive safety system for decay heat removal from steam generators to the atmosphere that provides a stable, infinite, ultimate heat sink using natural circulation of steam-water mixture and atmospheric air. In addition, following a large LOCA two or three sets of hydroaccumulators in different modifications of the modern VVER design can supply the reactor core with water from one to three days for all design LOCAs. Therefore, the grace period, i.e.

the period of time during which a safety function is ensured without the necessity of personnel actions in the event of an accident, is at least 24 hours in case of LOCAs and infinite in case of transients. In shutdown states huge water inventory in the spent fuel pool and hydroaccumulators can provide residual heat removal for weeks. These periods can be used for recovery of failed active safety systems.

New design features of advanced plants (e.g., long-term passive safety systems, software-based control systems, personnel actions under digital environment) challenge standard, widely-used PSA methodology, models, and data.

The efforts should be aimed at extending the current PSA methodology and data to address new issues. There are a number of potential issues to be resolved posed by the lower risk estimates of new reactors using the current PSA technology and originated from unknown new components, processes and technologies incorporated into the design of an advanced plant [20]. These issues are discussed below.

Mission time

Extended mission time of safety systems beyond the conventional 24-72 hours should be considered to exceed the grace period for new and advanced reactors. For instance, Russian advanced VVERs [20] have low pressure passive hydroaccumulators, called the second stage, with capability of more than 24 hours. During this time the active emergency core cooling is unnecessary. Therefore, in this case a 24-hour mission time is inadequate to quantify the actual contribution to the core damage frequency from a 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 [21]. Therefore, the mission time for new NPPs can be defined as the time period beyond which the changes of plant risk is negligible compared to that during the mission time.

Safe end states

A safe end state is a long term stable state when all the safety functions 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 are maintained and 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 heat removal from the reactor fuel cannot be maintained via a closed circuit (for example, when actions have to be taken for replenishment of water sources).

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 windows. Approaches in the area of human reliability analysis should be refined and extendable to the analysis of new situations (e.g., long time, more than 24 hours, to make decision). Generally the practice of human reliability analyses requires reconsideration in PSA at designs stages. This problem is discussed in details in [22].

Common cause failures

Methodology applied to advanced plants distinguishes weak and strong coupling factors [23]. Depending on those, common cause failure models are chosen. There are some aspects to discuss:

- The use of diversity in Russian new designs is an effective defence 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 decreases common cause failure probabilities.

- The extensive use of digital systems in the design of a new plant poses methodological problems in a PSA since there is a lack of experience in modelling computer based systems. In particular, common cause failures of software (recurrent errors in redundant software modules) and digital systems can be high contributor to overall plant risk [24]. Issue associated with receiving fault data from software developers should be resolved to enable justifiable assessment of such common cause failures. The Russian approach is to apply diversity to redundant software based on redundant modules.
- It is usual practice not to model inter-system common cause failures for existing plants because they are believed to be negligible contributors to the core damage frequency, large early release frequency, etc. However, for future reactors involving inherent safety features and demonstrating compliance with very low probabilistic safety target values, a special consideration might be given to inter-system common cause failures associated with similarity in active subcomponents (motors, circuit breakers, etc.). This become even more important when multi-unit risk considerations are involved [25].

Reliability estimation for new components

New design decisions made for new plants sometimes are based on new unique equipment. This raises an issue of its reliability estimation because an operational experience may be inapplicable.

It is evident that 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 a fracture mechanics analysis or other novel approaches.

Reliability methods for the analysis of passive 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 implementation of passive systems to assure long term decay heat removal safety function raised an issue of process stability depending on the surrounding conditions affecting the passive system behaviour. The PSA study of the Novovoronezh-2 NPP identified a problem associated with freezing water in the passive system given extremely low outside temperatures. Also efficiency of the system in extremely high outside temperature conditions is a concern. An R&D activity was initiated to resolve the issue based on the PSA insights.

The existing methods are generally based on Monte-Carlo simulations which require a large number of thermo-hydraulic calculations. As a result, these calculations can be extremely time consuming ones. To avoid this problem, an internationally accepted methodology should be developed. The passive system reliability assessment is still an open issue [26].

POST-FUKUSHIMA PSA DEVELOPMENT

Correlated hazards events

The impact that the Tohoku earthquake of magnitude 9.0 followed by the Fukushima disaster has on PSA is considerable.

Following the insights from Fukushima Daichi disaster (earthquake, tsunami, and failure of all power supply and cooling systems at the Fukushima NPP) consideration of internal and external hazards in PSAs are in focus of the PSA community. This is also very important for the new Russian plants having inherent safety features. The accident experience in Japan shows that dependencies between different internal/external hazards are of high importance because combinations of hazards may be significant for risk and much higher that risk associated with single

hazard considered individually [27]. The analysis of correlated internal/external hazards is supposed to be extremely important though might require significant efforts.

Gigantic aftershocks

Another issue related to seismic PSA based on lessons learnt from the Fukushima accident is influence of gigantic aftershocks on seismic hazard. Magnitude of the largest aftershock of the Tohoku earthquake was 7.7 and seismic motions of some aftershocks were observed that exceeded the amplitude of the design basis seismic ground motion [28]. Therefore seismic ground motions for gigantic aftershock of magnitude 9 class earthquake and their impact on weakened facilities or equipment should be considered.

Delayed consequences

The seismic PSA methodology already applied to analyse the design of new Russian plants constructed in seismic regions should be elaborated. In particular, 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. This issue is connected to the issue of stable safe state and mission time discussed earlier. Core melt occurs later than 48 hour at unit 3 and after 72 hours at Unit 2 of Fukushima Daichi NPP. This fact again highlights the importance of reconsideration of 24 hours mission time used in a typical PSA.

Multi unit site impact

The PSA methodology for evaluating site-wide risk at a multi unit site should be developed, in particular, multiple plant impacts should be considered in the event sequence development and end state definition. A traditional PSA usually considered shared systems which can be damaged due to an accident or maintenance at the adjacent unit.

However the Fukushima experience shows that external hazards, especially earthquakes, may cause simultaneous multiple nuclear reactor damages in the site for units, which are believed to be independent. For the multi-unit site, the potential spreading of a hazard like seismically induced fire to other units should also be considered in the analysis. It is very important that emergency planning should take into consideration multiple reactor core damage by external hazard, e.g. earthquakes.

Historically some multi-unit accidents and dependency among neighbouring units were considered in Russian PSAs such as a loss of off-site power at several units. Some dependencies like shared diesels, switchyards, transformers, heat exchangers, etc. are evident and usually analysed 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 are of utmost importance. Other important points are human reliability analysis associated with accident management at the site level in case of the multi-unit accidents as well as availability of spare parts and repair staff for several units simultaneously. Allocation of the available resources and defining spare parts requirements may be a very useful PSA application.

However, current probabilistic safety targets both in Russia and internationally are based on individual reactor safety.

There is no regulation for site-wide risk. This regulatory gap should be eliminated.

Spent fuel damage

A current Russian regulation requires consideration of a spent fuel pool in PSA for all hazards and operational modes. For new designs spent fuel damage may occur following loss of a spent fuel pool cooling system (either as a result of random failures or following loss of support systems). In such events level in spent fuel pool drops, resulting in the fuel uncover and damage to fuel assemblies with significant

delay. Typically in such accidents water inventory is sufficient to remove residual heat for several days by evaporation (from 24 hours to 7 days depending on the plant operational states and amount of loaded fuel in the pool). Such consequences may become important when considering long-term stable safe conditions in the PSA. There are two important aspects that have to be taken into account:

- Risk to the integrity of the containment due to overpressure.
- Risk associated with damage of the fuel both in the reactor core and spent fuel pool for the same initiating events affecting systems common for cooling the reactor and fuel pool.

It should be noted that the potential for damaging spent fuel due to leaks from the spent fuel pool or connected pipes or due to accidental drop of any load to spent fuel storage facility should also be quantified. The latter may occur due to a failure of a spent fuel handling or heavy load transfer equipment. All the mentioned above aspects should be modelled in the PSA.

CONCLUSION

PSA is a valuable tool to create a really safe design of advanced plants.

PSA is performed in a highly iterative manner during different stages of the plant design lifecycle and is applied to make decision on various design matters. The limitations of design PSA should be well understood in order to consistently use its results. The development of the Russian advanced plant design with passive safety features and post Fukushima reality raised new PSA issues that should be resolved by the PSA community. The contribution from the IAEA and Regulators is expected to be very important because no requirements for PSA carried out at early design phases and quantitative safety targets for multi-unit plants and spent fuel storages are available now internationally.

REFERENCES

1. Svyriaev, Yu.V., Morozov, V.B., Tokmachev, G.V., et al., 2009, "AES-2006 Design Safety Justification for Novovoronezh Plant-2 Site Using Probabilistic Safety Assessment Methodology," Heavy Engineering Industry, No 11, pp. 2-6.

2. Svyriaev, Yu.V., Morozov, V.B., Tokmachev, G.V., et al., 2009, "Use of Probabilistic Analysis in Safety Validation of AES-2006 Designed for the Novovoronezh Nuclear Power Plant Site," Atomic Energy, 106(3), pp. 155-161, Moscow.

3. Akkuyu Nuclear Joint Stock Company, 2018, "Akkuyu Nuclear Power Plant. Summary Report on Level 1 Probabilistic Safety Assessment", Moscow.

4. Rostechnadzor of the Russian Federation, 2015, "General Rules of Ensuring Nuclear Power Plant Safety. NP-001-15" Moscow.

5. International Atomic Energy Agency, 2011, "A Framework for an Integrated Risk Informed Decision Making Process," INSAG-25, IAEA, Vienna.

6. Lankin, M., 2012, "On Developing Methods of Defining a List of Beyond Design Basis Accidents to Be Taken into Account in a NPP Design," Proc. PSAM11 & ESREL 2012 Conference held in Helsinki, Finland on 25-29 June.

7. Tokmachev, G.V., 2007, "Approach to the Use of the PSA in Designing NPPs with VVER Reactors of a New Generation," Izvestiya VUZov. Nuclear Power Engineering. 3(1), pp. 44-53. Obninsk.

8. Lyubarskiy A.V., Tokmachev G.V., Lankin M.Yu., "Fail-Safe" Design Considerations in Conjunction with Integrated Risk Informed Decision Making", the same publication.

9. International Atomic Energy Agency, 2010, "Development and Application of Level 1 Probabilistic Safety Assessment for Nuclear Power Plants," IAEA Safety Standards, Specific Safety Guide SSG-3, IAEA, Vienna.

10. International Atomic Energy Agency, 2010, “Development and Application of Level 2 Probabilistic Safety Assessment for Nuclear Power Plants,” IAEA Safety Standards, Specific Safety Guide SSG-4, IAEA, Vienna

11. Lankin, M., and Tokmachev, G., 2012, “Interaction between Industry and Regulator to Improve Quality of the PSA,” Proc. PSAM11 & ESREL 2012 Conference held in Helsinki, Finland on 25-29 June.

12. Rostechnadzor of the Russian Federation,2008, “Administrative Regulations for Execution of State Function of Licensing Activities in the Area of Utilization of Nuclear Power by Federal Service for Environmental, Technological and Nuclear Regulation,” Moscow.

13. Rostechnadzor of the Russian Federation, 2015, “Main Requirements to Probabilistic Safety Assessment of Nuclear Power Plant Unit, NP-095-15,” Moscow.

14. Rostechnadzor of the Russian Federation, 2011, “Provisions of Main Recommendations on Conducting Level 1 Probabilistic Safety Assessment for Internal Initiating Events occurring at All Plant Operational Modes. RB-024-11,” Moscow.

15. Rostechnadzor of the Russian Federation, 2009, “Main Recommendations on Level 2 Probabilistic Safety Assessments for Nuclear Plants with VVER-type Reactors, RB-044-09,” Moscow.

16. Rostechnadzor of the Russian Federation, 2012, “Provisions of Main Recommendations on Conducting Level 1 Probabilistic Safety Assessment of Nuclear Power Plant for Initiating Events Caused by Internal Fires and Floods, RB-076-12,” Moscow.

17. Rostechnadzor of the Russian Federation, 2014, “Main Recommendations on Conducting Level 1 Probabilistic Safety Assessment for Nuclear Power Plant Unit for External Natural and Man-Made Initiating Events”, RB-021-14,” Moscow.

18. Rostechnadzor of the Russian Federation, 2017, “Main Recommendations on Conducting Level 1 Probabilistic Safety Assessment for Nuclear Power Plant Unit for Seismic Induced Initiating Events”, RB-123-17, Moscow.

19. Rostechnadzor of the Russian Federation, 2011,” Policy Statement on Application of Probabilistic Safety Assessment and Risk-Informed Methods for Constructing and Operating Nuclear Power Plants,” Moscow.

20. Tokmachev, G., and Morozov, V., 2011, “Lessons Learnt from PSAs for New and Advanced Reactors in Russia,” Kerntechnik, 76(5), pp. 377-383, Munich.

21. Morozov, V.B., Tokmachev, G.V., Baykova, E.V., et al., 2010, ”Estimation of NPP Probabilistic Safety Characteristics for Long-Term Mission Time,” Izvestiya VUZov. Nuclear Power Engineering. No.2, pp. 78-89, Obninsk.

22. Lyubarsky A.V., Tokmachev G.V., Fedulov M.V. Human Reliability Analysis at the Basic Design Stage, the same publication.

23. Morozov, V.B., and Tokmachev, G.V., 2008, “Approach to Common Cause Failure Modelling in Probabilistic Safety Assessments for New Designs of NPPs with VVER-1000 Reactors,” Izvestiya VUZov. Nuclear Power Engineering. No 4, pp. 31-41, Obninsk.

24. Tokmachev, G.V., Podkolzina, L.V., and Lobanok, O.I., 2006, “Estimation of Reliability of Information Computing System with Function of Presenting the Safety Parameters of Balakovo NPP,” Nuclear Measurement & Information Technologies, No 4, pp. 52-63, Moscow.

25. International Atomic Energy Agency, 2018, “Multi-Unit PSA”, Draft Safety Report, IAEA, Vienna.

26. International Atomic Energy Agency, 2014, “Progress in Methodologies for the Assessment of Passive Safety System Reliability in Advanced Reactors”, TECDOC 1752 , IAEA, Vienna.

27. Tokmachev, G., 2012, “Post-Fukushima PSA Development for New Reactors in Russia,” Proc. PSAM11 & ESREL 2012 Conference held in Helsinki, Finland on 25-29 June.

28. Ebisawa, K., Fujita, M., Iwabuchi, Y., and Sugino, H., 2012, “Current Issues on PRA Regarding Seismic and Tsunami Events at Muli Units and Sites Based on Lessons Learned from Tohoku Earthquake/Tsunami,” Nuclear Engineering and Technology, 44(5).

“FAIL-SAFE” DESIGN CONSIDERATIONS IN CONJUNCTION WITH INTEGRATED RISK INFORMED DECISION MAKING

Lyubarsky A.V., Tokmachev G.V.

INTRODUCTION

The concept of ‘fail-safe’ design is being practised by the designers of NPPs since the beginning of the nuclear industry. The requirement to implement the concept for components important to safety is included in IAEA Safety Standards. The concept of the ‘fail-safe’ design covers several aspects, which need to be addressed in an integral manner.

Though the concept of ‘safe-fail design’ is claimed to be satisfied in many NPP designs, a formal detailed guidance on practical application on the fail-safe design principles is relatively rare; this could result in non-optimal design solutions. The accident at the Fukushima NPP provided several lessons to be learned in the area of fail-safe design considerations. Therefore a balanced and systematic approach for ‘fail-safe’ design provisions is very beneficial.

DEFINITION

The IAEA Glossary [1] does not provide the definition of the term “Fail-safe design” though the principle itself is referred in several IAEA safety publications, for example, Requirement 26 of the IAEA safety requirements SSR-2/1 [2] states that*:* *“The concept of fail-safe design shall be incorporated as appropriate into the design of systems and components important to safety.”*

Para 5.41 of SSR-2/1 elucidates: “Systems and components important to safety shall be designed for fail-safe behaviour, as appropriate, so that their failure or the failure of a support feature does not prevent the performance of the intended safety function”.

In accordance with Ref. [2] the following definition could be given to the term: “Fail-safe design” is the concept of the design of systems and components important to safety that their failure or any failure of their support systems does not prevent the performance of the intended safety function”.

There is no clear guidance in the IAEA safety publications on how the requirement cited above should practically be met and, in particular, there is no guidance on when fail states for the system or specific component should be considered as “safe”:

- The state that prevent spurious actuation of the system, even it might decrease the reliability of the performance of the intended function
  OR
- The state that support the performance of the intended function even it might increase probability of inadvertent actuation of the system or inability to turn off the performance of system function when it is no longer needed.

Even through one can have an impression that the answer is already given in para 5.41 [2] – “safe” fail state is the state that “does not prevent the performance of the intended safety function” the correct decision may be less evident in practical applications and requires thorough engineering analysis including risk assessment. A wrong answer to the question and in turn a wrong technical decision taken may lead to severe deficiencies in the design of the system and finally may have significant negative impact or even can be a main cause for a severe accident at NPPs.

In the next sections of the paper it will be shown that the severe consequences of the accident at the Fukushima Daiichi Unit 1 partially if not fully were caused by the wrong application of the “fail-safe” design principle.

“FAIL-SAFE” DESIGN PRINCIPLE AT FUKUSHIMA DAIICHI UNIT 1

The “fail-safe” design obviously was implemented in the design of the Fukushima Daiichi unit 1, but due to the fact that tsunami disabled most of safety systems, the consequences of the particular applications of this principle were highlighted when the attempts to use the isolation condenser and containment venting system were made. The description of these attempts observed at the Fukushima Daiichi unit 1 is provided below. It should be noted that the goal of the description is not to criticize the design of the plant systems or specific actions taken by plant personal, but to analyse the impact of the applied “fail-safe” design principle on the availability of these systems in the accident condition caused by the extreme event occurred at the Fukushima Daiichi NPP.

Isolation Condenser (IC)

Figure 1 shows the technological scheme of Isolation Condenser of the Fukushima Daiichi Unit 1. This scheme is taken from a TEPCO presentation given at the meeting in the IAEA in December 2011 [3]. The description of the attempts to start operation of this system is mainly based on the information provided in the INPO report [4], also other information from the presentation mentioned above [3] and the TEPCO report [5] was used.

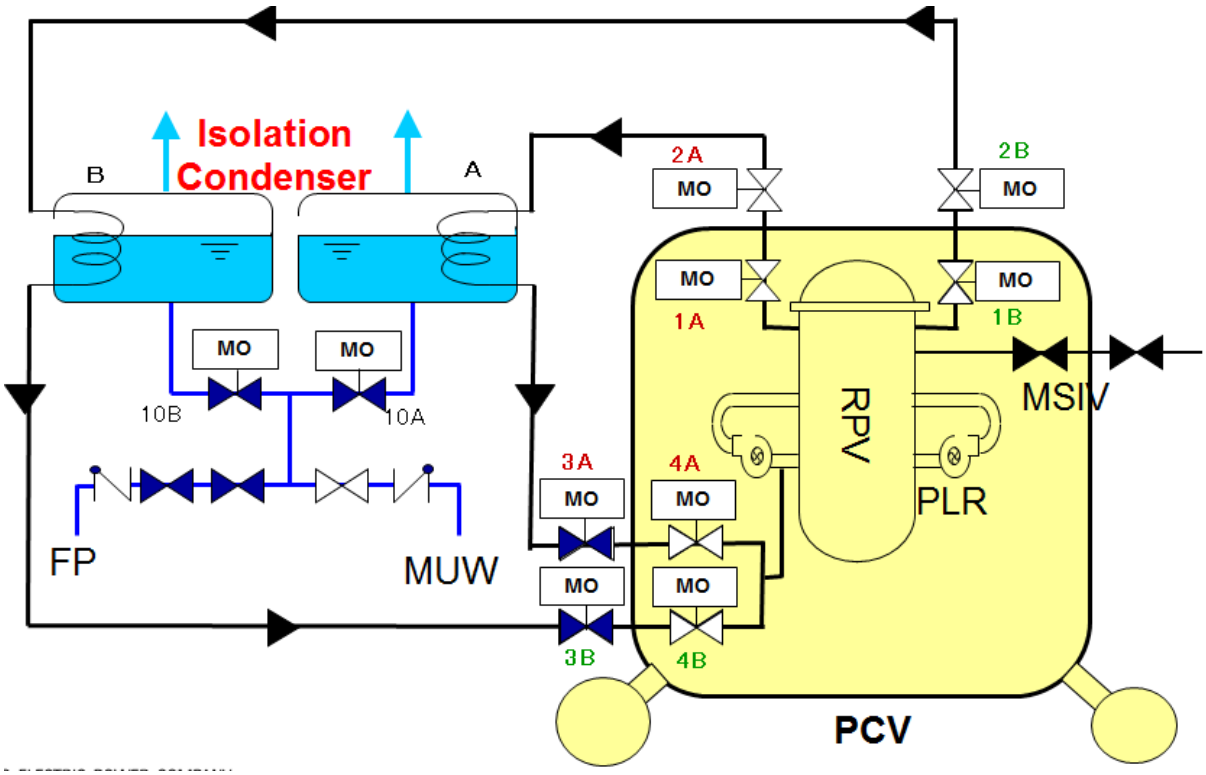

Fig. 1 Technological scheme of isolation condensers

One can see from Figure 1 that initially all valves of the system are opened except for the valves (MO-3A and MO-3B) on the pipeline connected to the cold leg of the recirculation loop. In accident conditions start/disconnection of IC is performed by opening/closure of these valves.

In accordance with the information from [3-5] both ICs started automatically by opening of these valves in 6 min after reactor scram following generation of the "high pressure in the reactor" signal. This led to a sharp pressure decrease in the reactor and violation of the required cooling rate (55 C per hour). Therefore operators turned off both condensers after 17 min of their operation. Later the operators came to the conclusion that to provide decay heat removal one condenser (A) is sufficient and further controlled heat removal was maintained by periodic opening/closure of the valve MO-3A. This operation has been performed three times in the interval between 15:10 and 15:34 (Japanese time).

The last closure of the valve was done exactly at 15:34, practically just before the tsunami wave came and disabled all AC and DC power buses. In the situation with no DC power the valve can be returned to open position only locally and manually. Unfortunately, the operators were not able to enable the system despite of numerous attempts. In accordance with information from Ref. [4] at 18:18 operators succeeded to open both valves MO-3A and MO-3B, but there were no signs of operation of any IC. It should be noted that the fact of failure to enable ICs was confirmed by the measurement of the level in ICs, done by the TEPCO in November 2011 [5]. This measurement shows the water level in IC A to have been 65% and IC B to have been 85% given that a nominal level is usually kept at 80%. The report [5] discusses many potential reasons for the non-efficient operation of the ICs, and one of the reasons (not explicitly mention in Ref. [5]), but believed to be realistic is the following: *valves 1A and 4A located inside the containment, that are designed to be closed by the interlock triggered by loss of an AC power source* ***did perform this action***.[1]

The design related to IC interlocks for the event of a loss of DC power is considered as "fail-safe" from the point of view of decrease of frequencies of the events with spurious actuation of the IC and potential thermal shocks for the reactor vessel. Therefore with certain level of assurance it is possible to state that *it was the "fail-safe" design principle implemented in the design of isolation condensers that has led to the situation when valves inside containment were closed in SBO conditions***.**

In other words these valves were closed and the ICs were disabled in the situation when they were the last possibility to support decay heat removal and delay core damage.

[1] In Ref. [5] literally states the following: «What this meant was, valves 1A and 4A located inside the PCV which were supposed to operate to close by the interlock triggered by loss of DC power source were not fully closed, the opening degree unknown although».

This last strong statement could be supported by information from Ref. [4], that the impossibility to reduce pressure in the reactor did lead to the non-efficiency of the use of fire water pumps that were not able to inject water in the reactor at a high pressure. Therefore, it is clear that "fail-safe" which is considered to be good for some specific objectives may be the cause of unwanted adherent conditions.

Containment venting system

Figure 2 presents the scheme of the containment venting system of the Fukushima Daiichi Unit 1. The scheme as well as further description of the system operation during the accident are based on the information from Ref. [4].

In 9.3 hours after the beginning of the accident the plant superintendent gave an order to operators to start containment venting. As it was clarified later the plant did not have a procedure on how to perform this action in SBO conditions; however, operators were able to define the exact scheme for containment venting and manual actions for specific valves opening. In particular they clarified that motor operated valve MO-210 on the common venting line just before a rupture disk and small air-operated valve AO-90 on the torus venting line (see Fig. 2) technically could be opened manually and locally.

At 09: 03 (18.2 hours after the beginning of the accident) the valve MO-210 (see Fig. 2) was opened, but there was no possibility to manually open the air-operated valve AO-90 due to the high elevation of the valve location. At 10:17 (19.5 hours after the accident) temporary batteries were installed to provide the valve AO-90 with DC power and in total three attempts were made by operators to open valve AO-90 remotely. The intention was that the air pressure remaining in the instrument air system would have been sufficient to open this small valve and keep it opened for the required duration.

The result of radioactive analyses performed later confirms that at least one of these attempts was successful, but the valve closed almost immediately (in the opinion of

the authors of the paper most probably due to decrease of pressure in the instrument air system). Therefore, further efforts were focused on the opening of the large pneumatic valve AO-72 on the torus venting line, even though this valve could not be opened manually and requires both DC power and compressed air[2]. As the result of all these efforts, operators managed to provide both DC power and compressed air (from temporary air compressor) and the large air-operated valve AO-72 was opened at 14: 00 (23.2 hours after the start of the accident), thus providing rupture of the rupture disk as designed and finally containment venting.

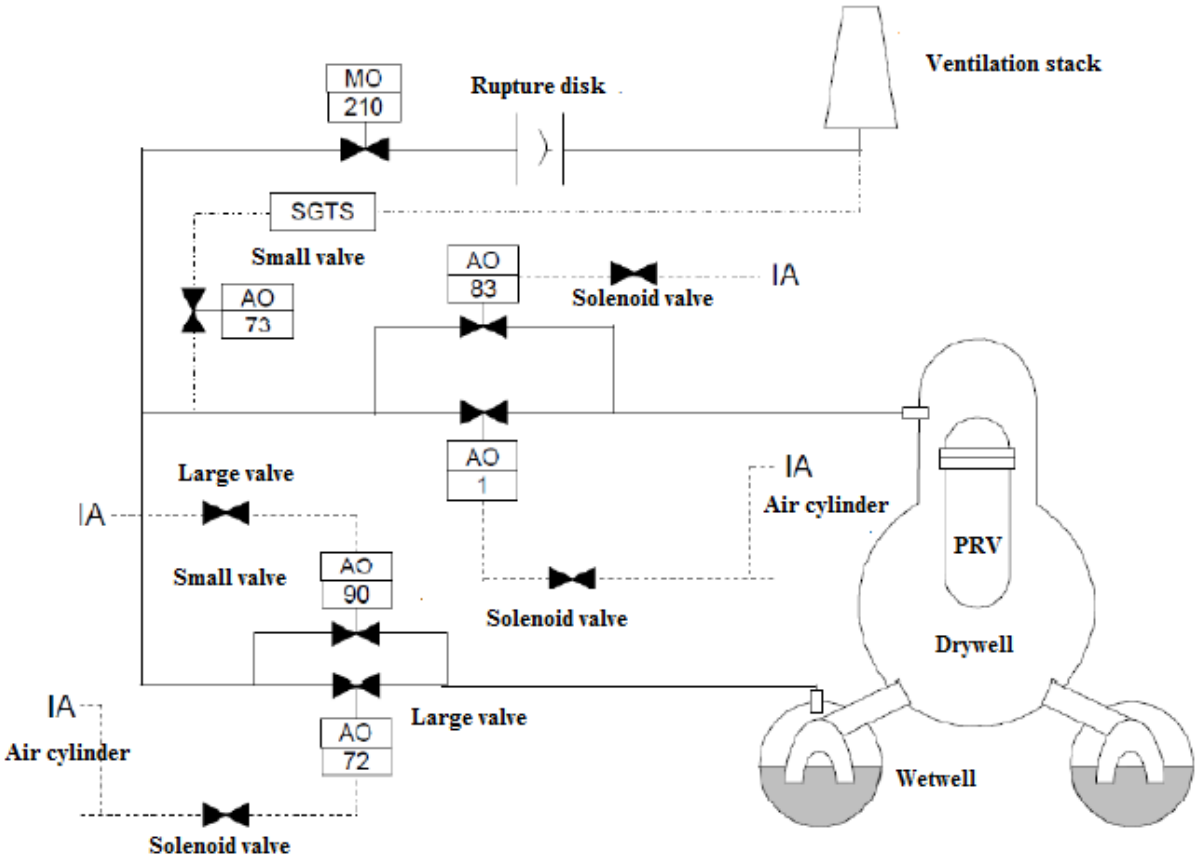

Fig. 2 Containment venting system at Fukushima Daiichi unit 1

It is very likely that until this moment due to high pressure in the containment vessel, large amount of hydrogen was released into the reactor building that led to the

[2] It is not clear whether there were stationary sources of compressed air or not and why they were not used; however, this is not the topic of this paper

hydrogen explosion, to the damage of the reactor building and to the disturbance in the work to provide make up into the reactor. The design of the containment system in the event of loss of DC power is considered as "fail-safe" from the point of view of radiation protection and decrease releases. However, similar to the previous case, it could be suggested that it was the "safe-fail" principle applied to the design of the containment venting system that led to the situation when all the valves remain closed or were closed after opening when support systems were lost. This finally led to 14th hours delay in containment and reactor vessels pressure decrease, to the release of significant amount of hydrogen into the reactor building, hydrogen explosion and meshing of the situation in general.

Security Controlled Gate

In accordance with the information from Ref. [4] after the tsunami only one from three fire trucks remains available for water make-up into the reactor of Unit 1.

This truck was located near Units 3 and 4. Because one of the ways to Unit 1 was blocked by the heavy tank with oil (moved by the tsunami) there was the only way on how the truck can be brought to Unit 1 – through the security controlled gate. However, it appears that loss of power to the electronic lock on the gate blocked it in closed position, and it took several hours [6] to break the lock and provide possibility for the fire truck to reach Unit 1. This also led to a significant delay in providing water make-up into the reactor vessel of Unit 1.

This is one more example of the application of the "fail-safe: design principle, that led to the impossibility to use in critical situation the only available way for transferring the fire truck after security gate blockage due to loss of power.

DEFICIENCIES IN THE CURRENT APPROACHES TO DEFINE "SAFE" FAILED STATE

As it could be seen from the information given in Section 3 the specific application of the "fail-safe" design principle in the design of the systems of the Fukushima

Daiichi Unit 1, have made the accident situation significantly more severe. After the accident at Fukushima Daiichi NPP it seems to be obvious that "fail-safe" position of valves on isolation condenser lines should be taken as "failed-opened" in case of loss of power; that air-operated valves on containment venting lines should be also "failed-opened" after loss of compressed air; that electronic lock on security gates should not be blocked at loss of power. However, this is not absolutely true: the "failed-closed" position of the valves of the IC system was most probably defined with the aim to avoid overcooling transients if specific DC buses failures would occur (for example in case of a local fire); the "failed-closed" position of the containment venting system was aimed to prevent inadvertent containment venting and uncontrolled releases of radioactive materials; and obviously security gates should not provide easy access for terrorists when power is destroyed.

The following section of the paper examines the process on how to define the "safe" state of a system.

Deterministic approach for defining "safe" state

In current practice the decision on what particular state of the system and component is "safe" is mainly defined based on deterministic engineering analysis of the systems (if such an analysis were performed at all). All designs declare application of the "fail-safe" design principle (otherwise the Requirement 26 of Ref. [2] would not be met). A typical example is a reactor protection system, which actuation is triggered when power (or other support system depending on the design) is lost.

However, justification of the consistent and balanced application of the "fail-safe" principle in the design of other systems is complicated and requires consideration of many factors:

- The design of a system considers not only the requirement to perform the intended safety function, but also the requirement to avoid inadvertent

actuations of the system (e.g. loss of support systems of safety valves should not lead to leaks from primary or secondary circuit).

- The design of a system takes into account the different aspects of system operation and post-operation behaviour (e.g. the reliable passive injection into the reactor from hydro accumulators, and their isolation after depletion of the water to prevent nitrogen intrusion in the core).
- The need for multiple starting/turning-off of the system (e.g. the design of isolation condenser at Fukushima Daiichi Unit 1 considered it's multiple connection/disconnection to prevent reactor vessel overcooling). In fact the selection of what state of the system (or specific equipment) is actually considered to be "safe" is usually based on the engineering analysis, bearing in mind challenge to plant safety.

However, there are usually many competing factors:

- The need to perform an intended function, for example:
    a. Inject water in the reactor in a LOCA (Hydro-accumulators system)
    b. Open safety valves at over pressure conditions (Primary pressure protection system)
    c. Passively remove decay heat (Isolation condenser)
    d. Reduce pressure in the containment (Containment venting system)
    e. Isolate the containment (Containment isolation system)

OR

- The need to fulfil requirements to the system after the intended function is completed , for example:
    a. Isolate injection lines to prevent nitrogen intrusion into the core after depletion (Hydro-accumulators system in cooling down process)
    b. Prevent loss of coolant after pressure reduction or spurious opening (Primary pressure protection system)
    c. Prevent reactor overcooling (Isolation condenser)

d. Prevent uncontrolled release from the containment (Containment venting system).
e. Prevent initiating events caused by spurious closure of the isolation system valves (Containment isolation system)

Depending on what is more appropriate to satisfy the safety goals of the whole plant the "safe" fail state is selected either to promote the performance of the intended system function (primary function) or the requirement to the system (secondary function).

As an example for the systems mentioned above the states that are typically accepted as "safe" in case of loss of support systems are shown in Table 1.

Table 1 indicates that not always the selected "safe" failed state leads to the increase of the reliability to perform the intended function, in many cases the decision is such that the intended primary system function is jeopardized, but compliance with the requirements to the systems performance (secondary system function) is better supported (e.g. to prevent spurious actuation or increase the possibility to terminate the system function performance).

Obviously the designer always has reasons for the selected "safe" fail state; however, it is not always the case that these reasons have a comprehensive basis.

Table 1 Typical “safe” states of the systems valves in case of loss of support systems

System/ equipment	**Primary system function**	**Valve position during unit at-power**	**Design valve position given loss of support systems**	**Reasons for selection of the design valve position given loss of support systems**	**Impact of valve transition to design position given loss of support systems**	
					On primary system function	**On secondary system function**
Passive primary injection system at VVER plants	To provide passive water make-up of the core during LOCAs	Open position of fast-acting closing valves at hydro-accumulators injection lines. The valves are intended to isolate hydro-accumulators after depletion to prevent nitrogen ingress in the core	Open position of fast-acting closing valves	Providing reliable performance of the main function - passive water make-up of the core during LOCAs	Increase of system ability to perform the primary function	Increase of the probability of nitrogen ingress into the core

System/ equipment	Primary system function	Valve position during unit at-power	Design valve position given loss of support systems	Reasons for selection of the design valve position given loss of support systems	Impact of valve transition to design position given loss of support systems	
					On primary system function	On secondary system function
Air subsystem of passive heat removal system at VVER plants	To provide residual heat removal and reactor facility cooling down	Closed position of slide gates at air ducts	Open position of slide gates at air ducts	Providing reliable performance of the main function in case of loss of off-site power	Increase of system ability to perform the main function in case of loss of off-site power	Leads to inadvertent system operation in case loss of support systems. As a result, plant efficiency decreases due to partly removal reactor power through passive heat removal system to atmosphere
Pressurizer safety valves at VVER plants	To open in case of	Closed position of pulse valves	Closed position of pulse valves	Prevention of inadvertent actuation	No impact on system ability to perform the main function because it	Decrease of the probability of inadvertent system

System/ equipment	Primary system function	Valve position during unit at-power	Design valve position given loss of support systems	Reasons for selection of the design valve position given loss of support systems	Impact of valve transition to design position given loss of support systems	
					On primary system function	On secondary system function
	primary overpressure	and the whole system	and the whole system	of the valves leading to primary leaks	assures by opening pulse valves by primary pressure even if support systems are lost	operation caused by loss of support systems
Fast-acting main steam isolation valves at PWR plants	To isolate steam generator steam line in case of secondary side breaks or primary to secondary leaks	Closed position of motor operated support valves and open position of steam operated main valves	Closed position of motor operated support valves and open position of steam operated main valves	Fulfilling of the main function is secondary compared with prevention of initiating events caused by inadvertent closure of main valves	Prevention from fulfilment of the main function, i.e. given loss of support systems the fast-acting main steam isolation valves keep open position and cannot isolate steam generators	Prevention from inadvertent closure main valves if support systems are lost. This leads to decreasing frequency of initiating events associated with loss of heat removal through the secondary side

System/ equipment	Primary system function	Valve position during unit at-power	Design valve position given loss of support systems	Reasons for selection of the design valve position given loss of support systems	Impact of valve transition to design position given loss of support systems	
					On primary system function	On secondary system function
Fast-acting main steam isolation valves at BWR plants	To isolate the reactor in case of steam line leak	Closed position of motor operated support valves and open position of main valves	Open position of motor operated support valves resulting in closure of main valves	Fulfilling of the main function is primary compared with prevention of initiating events caused by inadvertent closure of main valves	Promote fulfilment of the main function, i.e. fast-acting main steam isolation valves isolate the reactor from the turbine if support systems are lost	Inadvertent system operation if support systems are lost, as a result, loss of heat removal from the reactor
Containment isolation system at VVER plants	To prevent release from the containment	Different, dependent on pipeline	Not changed (as a rule)	Fulfilling of the main function is secondary compared with prevention of incident caused by inadvertent closure of a valve (e.g., loss of main	Limited fulfilment of the main function related to prevention of radioactive release	Prevention from inadvertent system operation. This leads to increase in NPP economic indicators and decrease of frequency

System/ equipment	Primary system function	Valve position during unit at-power	Design valve position given loss of support systems	Reasons for selection of the design valve position given loss of support systems	Impact of valve transition to design position given loss of support systems	
					On primary system function	On secondary system function
				coolant pump due to loss its cooling pipe)		of initiating events potentially resulting in core damage
Isolation condenser (BWR)	To provide decay heat removal in transients	Open position of valves inside the containment, closed position of valves outside the containment	Closed position of valves inside and outside the containment	Prevention of spurious actuation aimed to avoid overcooling transients and decrease in NPP economic indicators	Impossibility to perform the main function when the valves of the system are in a failed state	Prevention of inadvertent actuation of the system
Isolation condenser (ESBWR) [7]	To provide decay heat removal in transients	Open position of valves inside the containment, closed position of valves	Open position of valves inside and outside the containment	Providing reliable performance of the primary function	Increase of the system ability to perform the primary function	May lead to inadvertent actuation of the system causing overcooling transients and

System/ equipment	Primary system function	Valve position during unit at-power	Design valve position given loss of support systems	Reasons for selection of the design valve position given loss of support systems	Impact of valve transition to design position given loss of support systems	
					On primary system function	On secondary system function
		outside the containment				decrease in NPP economic indicators
Containment venting system (BWR)	To reduce pressure in the containment	Closed position of air operated valves on the line for filtered gas removal from the containment	Closed position of air operated valves on the line for filtered gas removal from the containment	Providing reliable performance of the main function - prevention of uncontrolled releases	Significant decrease of the reliability to perform the main function	Prevention of uncontrolled releases from the containment till it failure due to overpressure during severe accident
Automatic fire suppression system	To suppress a fire in rooms	Closed position of valves on the fire water suppression lines	Open position of valves on the fire water suppression lines	Providing reliable performance of the main function	Assisting performance of the main function	May lead to inadvertent system operation and can cause damage of safety related equipment

Probabilistic approach

Probabilistic safety assessment (PSA) in principle can provide a more systematic approach to answer the question what is the most "safe" failed state of the system in terms of overall probabilistic safety goals for the plant. For some systems (e.g. containment venting system) the answer may depend on the safety goal definition:

- if safety goals are defined in term of core damage frequency (CDF) the containment venting function become more important OR
- if they are defined in terms of large release frequencies (LRF) the possibility to terminate venting could be more important.

However, if full scope (all initiating events, internal and external hazards and all operational modes) Level 1 and 2 PSAs are used it is practically possible to get supportive information for the decision on safe fail states for systems and components modelled in the PSA. The decision process for the particular system can be brought to the modelling of different alternatives of the "safe" failed states and selection of those that better promote the objectives of safety goals. However, there is a very limited experience on the use of the PSA for this purpose, also some important issues are not treated in the PSA (e.g. technical feasibility of the decision made) that limits its use for such purposes. Hence there is a need to apply Integrated Risk Informed Decision Making (IRIDM) process.

"FAIL-SAFE" DESIGN AND INTEGRATED-RISK INFORMED DECISION MAKING

Integrated Risk Informed Decision Making Process

In 2011 the INSAG-25 report "Framework for an integrated risk-informed decision making process" [8] was published under the IAEA umbrella.

The main goal of this report was to promote understanding of different organizations involved in nuclear business (designers, manufacturers, operators, regulators, technical support organizations, etc.) on how the risk concept can be applied in

making balanced and sound decisions on various complex issues**,** including those that have impact on safety. The IRIDM process discussed the INSAG-25 report is aimed at providing transparency and soundness of the complex technical decision that require consideration of different factors. It provides the possibility for the decision-making process to be well structured and documented and it gives clear understanding on how particular factor was actually taken into account in the decision making process.

The ultimate goal of the IRIDM is to get assurance that any decision important to safety is optimized and at the same time does not provide unnecessary burden to operators.

The following key elements that should be considered in the IRIDM process are highlighted in the INSAG-25 report:

- Standards, good practices and operational experience
- Results of deterministic and probabilistic analyses
- Organisational considerations
- Security considerations
- Other factors (e.g. expected radiation doses during and after implementation of the decision option, results of research, economical consideration).

Only considering importance of each factor related to the particular problem it is possible to reach balanced and optimized decision.

It is also important that the IRIDM process provides high transparency and thus the decision will be clear not only to technical experts involved in the specific problem, but to any qualified engineer.

The principle of the IRIDM process implementation is shown at Figure 3 (in particular, the IRIDM process may be applied to “fail safe” failure problem considered above). According to this scheme, it is necessary to take into account

aspects important for both Regulatory Authority and Utility during decision making for any problem (e.g. “safe” state definition).

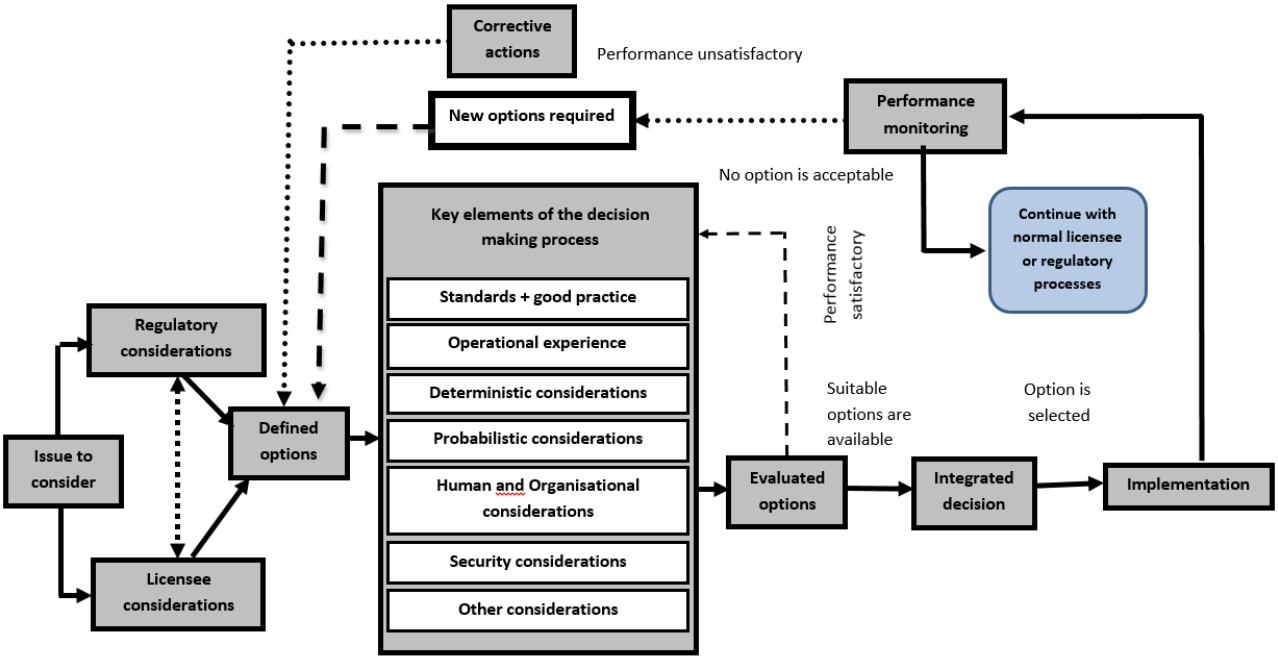

Figure 3 Main Components of the Integrated Risk Informed Decision Making Process (based on INSAG-25)

Based on the consideration of the problem a preliminary list of possible solutions (options) is generated. Each option is checked against the key elements of decision-making process. Because of such a consideration, the variants of decision-making corresponding to the key elements listed above are chosen.

If no preliminary defined options meet corresponding requirements of the key elements then additional options of decision-making are selected.

If several options meet the key elements requirements then the option, which corresponds most closely to all the elements, is chosen.

This option is proposed to be implemented, moreover after its implementation indicators characterized the option are controlled (indicators are determined for key elements, for example, compliance with risk targets, financial costs for its implementation and maintenance, etc.).

The IRIDM allows making such a decision that assure acceptable risk values from one hand (e.g. changes in core damage frequency, large radioactive release frequency and possibly other risk indicators related to the decision made), and adequate implementation of deterministic requirements to structures, systems and components, and NPP as a whole affected by the decision made from the other hand (e.g. assurance of defence-in-depth concept, reliability of barriers and their protection).

It should be noted that in the decision-making process both logistical (difficulty of manufactory, testing and maintenance, operational experience of similar systems, new research in the area of system design, regulatory document requirements, IAEA recommendations, etc.) and other factors (economical, dose rates, etc.) are taken into account.

IRIDM and "fail-safe" design in the plant systems design phase

Existing approaches to the application of the "fail-safe" design principle in system designs are currently lacking transparency and justification. The existing high potential to define a wrong "safe" failed state can lead to severe challenges to plant safety. However, this can be minimized if at the design phase the IRIDM process is used.

It is important to note that the approach utilizing some features of the IRIDM in applying "fail-safe" design principle is practiced in some countries. The example of such an approach is given below and based on the information from Ref. [9].

In accordance with Ref. [9] all faults of the system/component are grouped following features of the fault: "Safe or dangerous" and "Revealed or unrevealed" as shown in Table 2 (extracted from Ref. [9] with reduction).

Table 2 Grouping of Safe, Dangerous, Revealed and Unrevealed faults

Effect	**Mode**	
	Revealed	**Unrevealed**
Safe	**Group I** The failure either has no effect on the safety function or it generates a safety actuation signal	**Group II** Failures in this group do not prevent a safety function from being carried out, but will become evident only when a specific test or operation necessary to reveal its presence is completed. The availability of the system may begin to be affected.
Dangerous	**Group III** Failures in this group will partially or totally inhibit a safety function. A benefit is that operators are made aware of the presence of such a fault soon after its occurrence. A justification on whether the failure mode could be eliminated by redesign and the adequacy of the means of revealing the failure should be sought	**Group IV** Failures in this group will partially or totally inhibit a safety function without providing any indication at the time that this has occurred. Such failures have to be revealed by deliberate measures to exercise the safety function periodically - i.e. proof testing. These failures are considered to be the greatest threat to the safety function

The decision on the acceptance of a safety system design is usually made when the system/components have only group I and II failure modes, whereas a safety system with too many group IV failure modes is likely not to be acceptable. Other points that could be taken into account to consider adequacy of the system design:

- The percentage of "safe failure" rates (e.g. adequate when more than 90% of the total failure rate)

- Overall dangerous failure rate, e.g.:
    a) Adequate when the proportion of safe to total failure rate is considerably less than 90%, but overall dangerous failure rate is low
    b) Non-adequate when too high.
- Overall frequency of fail-safe faults (e.g. excessive frequency can itself become a safety concern).
- However, the comprehensive application of the IRIDM approach requires consideration of organizational and technical factors of different nature in a balanced and weighted manner, e.g.:
    a) difficulties dealing with manufacturing, testing and maintenance, operational experience with similar systems,
    b) recent achievements in the designs of the systems,
    c) requirements of applicable standards (including the IAEA requirements),
    d) economical rational;
    e) reduction of radiation doses to maintenance personal, etc.

IRIDM and security issues

The “fail-safe” design principle applied to different devises and measures providing physical security of NPPs may also deserve attention. The example with security controlled gate at Fukushima Daiichi NPP (see section 2.3), when after the loss of power the path through the gate was blocked, shows that measure important from security perspectives might play exceptionally negative role for NPP safety.

One of the advantages of the IRIDM process is that it provides and actually requires balanced and justified assessment of safety and security interferences with the aim that security measures will not compromise safety and wise versa.

In fact, the option would have been recommended which still allows a blockage of the security gate in case of the loss of power, but at the same time, the effective measures would be available to transfer the lock from the state that is assessed to be "fail safe" to another state.

This possibility can be assured by providing special mechanical devises aimed to timely unlock the gate to the designated staff, for example, fire brigade personnel[3].

Example on the application of the IRIDM for justification of a selected "safe-state"

The illustrative and simplified example of the IRIDM application for the solution of the problem of defining "safe fail" state for the system of fast isolation valves located on steam lines for NPPs of two types: PWR and BWR is provided in Table 3.

Not going in details of the methods recommended in [9], the example applies the simplified approach for integration of information in the decision making process, which is based on assignment of importance (W_i) for each constituent factor I and weights (S_{ij}) for the level of compliance of the decision option J with factor I. The decision option with the highest value of Q, obtained by formulae (1) is estimated to be the selected option.

$$Q= \Sigma W_i S_{ij} \quad (1)$$

The steps and results of the application of the IRIDM process are provided below.

Step 1 Definition of the issue and identification of possible solutions.

The problem has the following definition: "To find the position of Fast Acting Isolation Valve (FAIV) on steam line of an NPP in case of loss of a support system

[3] It is worthwhile to mention that in realization of the "fail-safe" design principle it is always useful to consider as one of the options design solutions when the systems (or equipment) transferred to a safe state could be timely (from the point of view of NPP safety) moved to another state opposite to those defined in the design as "safe". This can help to relax the issue of the "safe" state selection in the NPP design discussed in the paper. In fact, if the Fukushima Daichi Unit 1 would have technical and organizational measures that allow valves in isolation condenser and containment venting systems to open (that were designed to close in case of the loss of power) the accident would progress more gently and severe consequences most probably would have been avoided.

that satisfies the “fail-safe” design principle (for NPP of two types - PWR and BWR).

Possible technical solution options:

Option 1: FAIVs remain open in case of the loss of a support system without possibility to close until the support system is restored.

Option 2: FAIVs close in case of the loss of a support system without possibility to re-open until the support system is restored.

Step 2 Identification of key elements that are important for the decision making for the issue: all the key elements listed in Section 5.1 are considered.

Step 3 Collection of information for each key element and identification of factors to be considered in the IRIDM process. The results of information collection are shown in Table 3. The following constituent factors (CF) to be important for the issue are considered in the IRIDM process:

- CF1 –Probability of accident sequences directly leading to radioactive materials releases outside the containment.
- CF2- Estimated average number of the events with a spurious closure of FAIVs during the plant lifetime.
- CF3 – Estimated average financial losses associated with the FAIVs system.

Step 4a Evaluation of the importance of each constituent factor.

The importance of each CF will be evaluated using the scale from 1 to 10 [10], where 1 is assigned to the CF with the lowest importance for the issue and 10 – with the highest importance.

Table 3 Results of information collection and selected constituent factors

№	Key element	Information required for the review of decision options		Constituent factor	Comment
		Option 1	**Option 2**		
1	Requirements of Norms and Standards	The following regulatory requirements are identified: 1) The frequency of severe accident should not exceed 1.0 10^{-5} 1/a. 2) The frequency of large release should not exceed 1.0 10^{-6} 1/a. 3) The frequency of accident sequences directly leading to radioactive materials release outside the containment should not exceed 10^{-8} 1/a 4) The number of spurious FAIVs closure during the NPP lifetime (40 years) should not exceed 10. No other requirements in the norms and standards related to the issue that can be taken into account in the decision making process have been identified		**CF1**: Frequency of accident sequences directly leading to radioactive materials release outside the containment. **CF2**: Estimated average number of events with spurious FAIVs closure during the plant lifetime	For both decision options it was shown that the frequency of severe accidents is below 1.0 10^{-5} 1/a and frequency of large releases is below 1.0 10^{-6} 1/a. These frequencies are almost identical for both options
2	Operational experience	At NPPs where the Option1 was implemented spurious operations of FAIVs have been observed.	At NPPs where Option 2 was implemented, spurious operation of FAIVs have been observed due to	Frequency of spurious actuation is taken into account in CF2	-

№	Key element	Information required for the review of decision options		Constituent factor	Comment
		Option 1	**Option 2**		
		However, these were not connected to support systems failures, but mainly due to operator errors or a false signal	either support system failures or operator errors or false signals. However, the main cause of spurious closure was an operator error		
3	Results of deterministic analysis and compliance with deterministic principles	Both options satisfy all deterministic principles (defence in depth, single failure criterion, etc.)		There is no need to consider factors related to this key element as both options satisfy the requirements and they will not have impact on decision to be made	Not considered in the further analysis

№	Key element	Information required for the review of decision options		Constituent factor	Comment
		Option 1	Option 2		
4	Results of probabilistic assessment	Frequency of severe accidents: F1 ≅ $2.3 \cdot 10^{-6}$ 1/a		There is no need to consider factors related to this key element as for both options the calculated parameters satisfy safety goals and are very similar for both options	The reduction of frequency of large release in Option 2 for BWR is due to a more reliable isolation of the reactor from the turbine in accidents with severe core damage
		Frequency of large release: F21≅ $7.3 \cdot 10^{-7}$ 1/a (for PWR and BWR).	Frequency of large release: F21≅ $7.3 \cdot 10^{-7}$ 1/a (for PWR); F22≅ $6.6 \cdot 10^{-7}$ 1/year (for BWR)		
		Frequency of a spurious FAIVs actuation: $9.1 \cdot 10^{-2}$ 1/a. Estimated averaged number of events with spurious FAIVs actuation during 40 years of the operation: 3.64 (N_1)	Frequency of a spurious FAIVs actuation: $9.3 \cdot 10^{-2}$ 1/a Estimated averaged number of events with spurious FAIVs actuation during 40 years of the operation: 3.72 (N_2)	Frequency of FAIVs closure is considered in **CF2**	Frequency of a spurious actuation was assessed with account for operational experience and system reliability analyses

№	Key element	Information required for the review of decision options		Constituent factor	Comment
		Option 1	**Option 2**		
		Frequency of accident sequences directly leading to radioactive material release outside the containment due failure of the FAIVs to isolate: $1.3 \cdot 10^{-9}$ 1/a (PWR); $8.2 \cdot 10^{-8}$ 1/a (BWR).	Frequency of accident sequences directly leading to radioactive material release outside the containment due failure of the FAIVs to isolate: $3.7 \cdot 10^{-9}$ 1/a (PWR); $1.8 \cdot 10^{-8}$ 1/a (BWR).	Frequency of accident sequences directly leading to radioactive material release outside the containment is accounted for **CF1**	-
5	Organizational factors	Both technical solutions (options) have no impact on the organizational factors		Consideration of this key element is not needed as both options have no impact on organizational factors	Not considered in the further analysis

№	Key element	Information required for the review of decision options		Constituent factor	Comment
		Option 1	Option 2		
6	Factors associated with security aspects of NPP	Both options has no impact on security aspects		Consideration of this key element is not needed as both options have no impact on security factors	Not considered in the further analysis
7	Other factors	1) Estimation of financial losses due to unit shutdown after the spurious closure of the FAIVs: S1≅ 5.0 10^{+5} conditional units 2) Estimation of losses after core damage: S2≅8.0 10^{+9} conditional units 3) Estimation of losses after large releases: S3≅2.0 10^{+12} conditional units No other factors that might have impact on the decision making process for the issue were identified		**CF3**: Average estimation of financial losses during the plant lifetime	-

№	Key element	Information required for the review of decision options		Constituent factor	Comment
		Option 1	**Option 2**		
		Average estimation of losses during 40 years of the plant lifetime: PWR and BWR: N1*S1+40*F1*S2+F21*40*S3= 3.64*5·10^{-5} + 40*2,3·10^{-6}* 8.0·10^{+9}+ 40*7.3·10^{-7}* 2.0·10^{+12} = 60,956,000 conditional units	Average estimation of losses during 40 years of the plant lifetime: PWR: N2*S1+40*F1*S2+F21*40*S3= 3.72*5·10^{-5}+40*2,3·10^{-6}* 8.0·10^{+9}+40*7.3·10^{-7}* 2.0·10^{+12}=60,996,000 conditional units BWR: N2*S1+40*F1*S2+F22*40*S3= 3.72*5·10^{-5}+40*2,3·10^{-6}* 8.0·10^{+9}+40*6.6·10^{-7}*2.0 10^{+12} = 55,396,000 conditional units		

In the example the following importance indices are assigned to CFs:

- CF1 – 9: This factor is dealing with the safety target stated in regulatory requirements. Typically for the regulatory requirements it has the highest

importance, but in this particular case the importance is slightly lower taking into account that the requirement is given in the form of target, but not the criterion.

- CF2 – 10: This CF has the highest importance as it is related to the regulatory requirement stated in the form of the criterion.
- CF3 – 6: Risk of financial losses is the priority for plant owners, but has a low importance for regulators. For this CF the importance is assigned close to a median value.

Step 4b Assessment of the level of compliance for each potential decision option.

Assessment of level of compliance of each decision option to each CF is performed following recommendations of Ref. [9] and the [-5,5] scale (the weight 0 is assigned for the Option 1). The results of the assessment and explanations are shown in Table 4.

Step 5 Integration of the information and option selection.

Integration of the information was performed utilizing estimated importance values and weights. The results of integration and recommended decision option are given in Table 4.

Table 4 Estimation of weights and integration of the information

Constituent factor CF_i	Weight of the CFi (W_i)	Level of compliance of the option J with factor I (S_{ij})					
		Technical solution options for PWR			Technical solution options for BWR		
		1	2	Comments	1	2	Comments
CF1	**9**	**0**	**0**	Frequency of accident sequences leading directly to large releases outside the containment due to failure to close of FAVs is equal for both options	**0**	**+4**	Frequency of accident sequences leading directly to large releases outside the containment due to failure to close of FAVs is lower than the value recommended by regulations. At the same time this frequency is much lower for the option 1 than for the option 2
CF2	**10**	**0**	**- 1**	Expected number of spurious actuation during the plant lifetime is much lower than the required value for both options, but slightly higher for the option 2	**0**	**-1**	Expected number of spurious actuation during the plant lifetime is much lower than the required value for both options, but slightly higher for the option 2
CF3	**6**	**0**	**-1**	Expected losses in case of implementation	**0**	**+2**	Expected losses in case of implementation of the

Constituent factor CF_i	Weight of the CFi (W_i)	Level of compliance of the option J with factor I (S_{ij})					
		Technical solution options for PWR			Technical solution options for BWR		
		1	2	Comments	1	2	Comments
				of option 2 is slightly higher than for option 1			option 2 is much lower than for option 1
$Q=\Sigma W_i S_{ij}$		0	-16	The option 1 is recommended for PWR NPP	0	38	The option 2 is recommended for BWR NPP

The simplified example presented above illustrates how the IRIDM process can be applied to the issue on what state of the equipment or system is "safe" based on a balanced consideration of all constituent factors. In the example it is shown that typical technical solution for FAIVs (see Table 1) is in line with the recommendation of the IRIDM approach, but for the real IRIDM process it is possible that the solution would be different from those presented in Table 1.

It is important to mention that in the analysis process all potential consequences of the loss of support systems should be taken into account, not only those that relate to the considered equipment. In particular, for the case of the FAIVs the loss of systems supporting the FAIVs operation can lead to changes in the state of other equipment of the plant. In addition, the simultaneous loss of several support systems is also possible as well as some non-evident failure modes of the support systems – for example, voltage and frequency fluctuation in the electrical grid without complete loss of power (such an event was observed at the Russian Kola NPP in year 1993 and at the Swedish NPP Forsmark in year 2006).

CONCLUSION

In many plants the “fail-safe” design principle is declared to be applied to the design of safety related systems; however, there is no clear guidance on how the “fail-safe” state can be defined for particular system and system components. Making a decision during plant design on how the “fail-safe” design principle should be applied in the selection of a state of a system (or equipment) to where the transfer has to be made in case of a support systems failure requires a thorough analysis. When making a decision, various factors should be taken into account, such as the impact on the performance of the main and secondary functions of the system, the issues of security, conformity with the requirements of rules and regulations, compliance with existing operating experience and others.

The use of the IRIDM process allows defining “fail-safe” state in a balanced, justifiable and transparent manner taking into account many aspects associated with the plant safety and security.

ABBREVIATIONS

AC	Alternative Current
BWR	Boiling Water Reactor
CDF	Core Damage Frequency
DC	Direct Current
ECCS	Emergency Core Cooling System
ESBWR	Economic Simplified Boiling Water Reactor
IAEA	International Atomic Energy Agency
IC	Isolation Condenser
INPO	Institute of Nuclear Power Operations
IRIDM	Integrated Risk Informed Decision Making
LOCA	Loss Of Coolant Accident
LRF	Large Release Frequency
NPP	Nuclear Power Plant
PCV	Passive Containment Venting
PSA	Probabilistic Safety Assessment
PWR	Pressurized Water Reactor
SBO	Station Black-Out
TEPCO	Tokyo Electric Power COmpany, Inc.
VVER	Pressurized Water Reactor (Russian abbreviation)

REFERENCES

1. International Atomic Energy Agency, Terminology used in Nuclear Safety and Radiation Protection. Safety Glossary. 7 Edition, Vienna, 2007

2. International Atomic Energy Agency, Safety of Nuclear Power Plants: Design, Safety Requirements No. SSR 2/1 (Revision of Safety Standards Series No. NS-R-1), 2011

3. IAEA Consultancy Meeting in Preparation of the International Experts Meeting (IEM). Safety Measures based on Fukushima Daiichi Accident Additional Safety Measures at Kashiwazaki Kariwa NPS. Hideki Masui, Seismic Research Manager, Nuclear Asset Management Dept., TEPCO, November 29, 2011

4. Special Report on the Nuclear Accident at the Fukushima Daiichi Nuclear Power Station, INPO 11-005, November 2011

5. Evaluation of operating conditions of Isolation Condenser, Unit1, Fukushima Daiichi Nuclear Power Station, TEPCO, 22 November 2011, Evaluation of operating conditions of Isolation Condenser handouts_111122_03-e.pdf

6. Strickland, E. "24 hours at Fukushima", IEEE Spectrum, November 2011

7. IAEA Consultancy Meeting in Preparation of the International Experts Meeting (IEM). Individual Perspectives on Fukushima Accident – Reactor. Larry E Fennern, GE Hitachi Nuclear Energy (GEH), Chief Consulting Engineer, ESBWR, November 29, 2011

8. "A Framework for an Integrated Risk Informed Decision Making Process", INSAG-25, A Report by the International Nuclear Safety Group, Vienna, 2011

9. "Guidance for IRIDM", Working material for the Technical Meeting, 26-30 March 2012, Vienna.

HUMAN RELIABILITY ANALYSIS AT THE BASIC DESIGN STAGE

Lyubarsky A.V., Tokmachev G.V., Fedulov M.V.

INTRODUCTION

The human reliability analysis (HRA) performed for the units under design differs significantly from the HRA performed for the operating units, especially for the modern new generation NPPs that do not have any obvious analogous. These differences are primarily due to the objectives of the HRA, but also due to specific conditions for the HRA performance at design stage of the NPP.

The design process of a nuclear power plant usually is carried out in several stages, depending on the licensing process in a particular country. Nevertheless, three main stages can be distinguished:

- The stage of development of the preliminary safety analysis report (SAR) required to obtain a license for the construction of a nuclear power plant
- The stage of development of the final SAR required in many countries to obtain a license for the operation of a nuclear power plant
- The commissioning stage, on which it is confirmed that all design decisions included in the final SAR, as well as operational documentation (technical specifications, operational and emergency procedures, etc.) are actually implemented as designed. At this stage, typically a refined probabilistic safety assessment (PSA) is performed that takes into account the actual implementation of design and operational solutions.

The availability of the PSA at each stage is usually a prerequisite for obtaining the appropriate license, but in addition to obtaining a license, the results of the PSA are used for a number of purposes that differ depending on the stage of the design.

Accordingly, approaches and requirements for the development of the PSA differ depending both on the objectives of the PSA and on the information available at a particular stage. Especially these differences are manifested in the performance of the human reliability analysis.

Table 1 presents the main objectives and limitations for the development of the HRA for each of the design stages. Table 1 is limited to the consideration of the HRA only for the Level 1 PSA for internal IEs. When PSAs for internal and external hazards or Level 2 PSAs are performed, the objectives of the PSAs do not actually change, but the limitations in the HRA may differ significantly due to the need for information of a specific nature.

As can be seen from Table 1, each design stage has its differences from the point of view of the tasks and conditions of the HRA performance and, consequently, the requirements for the HRA and the HRA development process may differ. The greatest number of particular features has the HRA conducting at the stage of the development of the preliminary SAR. These features are discussed in the paper.

CURRENT STATUS OF THE HUMAN RELIABILITY ANALYSES AT THE STAGE OF THE PRELIMINARY SAR DEVELOPMENT

Collection of information

Table 2 provides a list of typical information sources for the HRA performance and analyses of their availability as well as the need for the HRA performance for various types of human errors during the development of the preliminary SAR.

Table 1 Stages of design and HRA

Design stages	**PSA objectives**	**HRA objectives**	**Specific conditions for HRA performance**
Development of the preliminary SAR	Construction license application (CLA) Optimization of design solutions. Assessment of the compliance with probabilistic safety targets (CDF, LRF, etc.) defined in national safety requirements and in terms of reference to the design of the unit.	Identification of operator actions and possible errors, the most important in terms of meeting the probabilistic safety targets. Optimization of design solutions to achieve reliable performance of human actions: 1) identification of design features aimed at reducing the probability of human errors (introduction of specific alarms, improvement of human-machine interface, etc.) 2) implementation of automation for the most critical human actions, etc.	Only limited information is available on the design of normal operation and safety systems (including I&C). Plant specific human factors operational experience is not available. Operational, emergency, maintenance procedures as well as training programs and full-scope simulators are not available.

Design stages	PSA objectives	HRA objectives	Specific conditions for HRA performance
Development of the final SAR	Operating license application (OLA) Assessment of the compliance with probabilistic safety targets defined in national safety requirements and in terms of reference for the design of the unit.	A realistic as practically possible estimate of the probabilities of human errors.	The plant staff has no working experience specific for the unit. Operational, emergency and maintenance procedures are in the verification phase. Full-scope simulators and training manuals might not be available.

Design stages	PSA objectives	HRA objectives	Specific conditions for HRA performance
Commissioning	Resolution of issues that were not completed in the PSA for OLA (resolution from the OLA-PSA review). Commissioning applications. Assessment of the compliance with probabilistic safety targets defined in national safety requirements and in terms of reference to the design of the unit. Development of basic for a living PSA for operational phase	A realistic as practically possible estimate of the probabilities of human errors.	Operational experience from the plant is very limited. Operational and emergency procedures are available. Training programs for staff are developed and implemented.

Identification of Human Errors

At the stage of the development of the preliminary SAR, the identification of human errors of various types is the most uncertain and important task. The lack of complete information on the systems design (including I&C) as well as the absence of emergency operating procedures, however, should not prevent comprehensive identification of potential human errors. One of the possible ways to comprehend the analysis in such a situation is to introduce an excessive conservatism, considering the possibility of making all possible errors, even though some of them can be further excluded by technical measures. The main goal of this task at the preliminary SAR

development stage is to identify as complete as possible a list of human errors that no human error significant for safety is excluded or omitted.

It should be noted that compilation of the comprehensive list of human errors is particularly essential for the design stage of the preliminary SAR development, because it provides a basis for designers for reducing impact of the human errors on plant safety. This is especially important for modern designs with high safety requirements.

As known, several types of human errors are considered in the HRA [1]:

- Type A errors committed during tests or maintenance of the equipment prior to the onset of the initiating event.
- Type B errors that trigger the initiating event.
- Type C errors committed by personnel in response to the initiating event.

Identification of type A human errors

The greatest difficulty at the stage of the development of the preliminary SAR is the identification of the type A human errors. This is due to the lack of information on how the equipment will be inspected and maintained, and how the check of the equipment operability returned to service after maintenance will be organized.

A common practice in the HRA performance at this stage is the analysis of the design as well as operating and maintenance procedures of the reference plants. All the pre-initiator human errors identified for the reference power units are considered in the PSA of the unit under consideration. In addition, for all the equipment considered in the PSA model, erroneous actions of the operator that can lead to some kind of an equipment failure could be identified (for example, bringing the manual valve to the closed position on the head of the pump after preventive maintenance or repair work, leading to its unavailability to perform its function).

This approach may lead to the identification of a large number of the type A errors that may cause unavailability of each single equipment modelled in the PSA.

Table 2 Typical information sources for HRA at the stage of the development of the preliminary SAR

Information source	**Degree of completeness of information**	**The possibility of accounting for information in the analysis**		
		Type A errors	**Type B errors**	**Type C errors**
Procedures	There are no plant specific procedures. Procedures from referenced plants[4] are the only information source	Procedures from referenced plants allow to some extent compensate for the absence of plant specific procedures. However, procedures from referenced plants might be of little use when the design of the NPP is significantly different	Procedures from referenced plants are of little use	Procedures from referenced plants allow to some extent compensate for the absence of plant specific procedures. However, procedures from referenced plants might be of little use when the design of the NPP is significantly different
Plant walkdown, including visiting main control room and local control centres	There is no possibility of plant walkdown	Visiting referenced plants cannot compensate for the lack of information		

[4] The term "referenced plant" is used for the operating power unit, the closest in characteristics to the unit under design

Information source	**Degree of completeness of information**	**The possibility of accounting for information in the analysis**		
		Type A errors	**Type B errors**	**Type C errors**
Analysis of operational events	Only operating experience from other NPPs (including referenced units) is available	The information from other NPPs (including referenced units) is not fully relevant to the units being analysed, but is useful for determining the causes of potential HFEs		
Interviews and discussions with plant staff	Information can only be obtained from referenced plants	Typically, information from the PSA for referenced units is used		
Collection of information from the simulator, including monitoring the reactions of the shift to simulated accidents	Same as above	Same as above		
Thermohydraulic analyses	Information is usually available, but in a limited amount	Not applicable	Can be used in some cases to estimate the operator's time window	Used in full to estimate the operator's time window
Outputs of other tasks of the PSA for the unit under design (e.g. system analysis and analysis of accident sequences)	This information is developed iteratively in conjunction with the HRA and form the basis for HRA	Used in full to determine possible HFEs		

Therefore, even at the stage of the preliminary SAR development it is possible to perform grouping of those human errors that lead to equipment failures with the same consequences in operation of the systems modelled in the PSA (for example, one can consider a single HFE of type A leading to the unavailability of a train or part of a safety system train).

For modern design with extended use of passive systems, it is essential to identify the type A HFEs that can affect their reliability. However, there is quite a little experience and consensus how reliability of passive systems should be analysed and what HFEs can be associated with them.

Identification of type B human errors

Typically, type B human errors for operating NPPs are only defined for conditions where a significant interaction of the operator with the equipment of the unit is assumed (for example, for shutdown modes the human errors leading to IEs such as overdraining of the reactor or boron dilution are typically considered). For at-power operation of the unit in stationary modes, it is generally considered that these HFEs are already taken into account in the statistics of the frequencies of the IEs (e.g., erroneous reactor or turbine trips, etc.)

For the preliminary SAR development stage, this approach is applicable with constraints for the reasons given below:

- For a number of initiating events for the plant in design there may be no statistical information about events on referenced plants. First of all, this refers to the events caused by failures or spurious actuations of systems, the design of which is either absent on the referenced units or is radically different (for example, the passive heat removal system was first introduced on the improved VVER-1000 and VVER-1200 and is absent on the referenced units with VVER-1000/320 reactors).

- The presence of dependencies and interrelations, which can lead to an equipment spurious actuation due to a failure of support systems that are absent on referenced plants. An example of such dependencies may be the situation when a failure of the support system leads to the operation of the front-line system due to the specific implementation of the fail-safe design principle (see Ref. [1]).

To identify human errors leading to initiating events, it is necessary to perform an analysis of all the systems. It is needed to identify all human errors, leading to false actuation or false shutdown of the system if such consequences disrupt the normal operation of the unit and require the operation of systems important to safety to maintain the safe state of the unit.

All the dependencies between the systems, including the dependencies associated with the implementation of the fail-safe design principle, should be identified.

The performance of such an analysis at the preliminary SAR development stage is hampered by the lack of the accurate information on the interconnections between systems, accurate information on the set-points and interlocks as well as information on the on-line maintenance of systems during power operation. Therefore, in practice, the most conservative approach is typically based on the assumption that operator errors leading to the loss of the support systems cause a failure or false activation of the dependent front-line system, if there is no justification for the absence of such consequences.

It should be also noted that at the stage of development of the preliminary SAR the identification of human errors leading to IEs for the unit in shutdown modes has certain peculiarities, because of the lack of procedures for performing various actions during shutdown.

Therefore, for shutdown modes at the stage of preliminary SAR development all technically possible HFEs are identified and none of the potential errors is excluded from consideration.

Identification of type C human errors

The procedure for identifying post-initiator HFEs, including HFEs in performing recovery actions, is almost the same as the procedure for performing such an analysis for operating units. The only difference for the design stage of the preliminary SAR development is that, due to the absence of emergency procedures, all theoretically possible operator actions aimed to bring the unit to a safe state are postulated. In addition, all technically possible recovery actions are considered, even those for which the technical means in the design are defined at the conceptual level only.

An extended review of type-C actions allows to assess their potential significance and to develop later technical and organizational measures aimed at minimizing the probability of dominant HFEs.

Qualitative analysis

The necessary stage of the qualitative analysis of human errors is the collection, analysis and documentation of the information necessary to understand the specific tasks to be performed by the plant personnel. Such an analysis makes it possible to choose the most suitable method for the error probabilities estimation. As it can be seen from Table 2, the information necessary for the qualitative analysis of HFEs at the stage of the preliminary SAR development (in contrast to the HRA for operating NPPs) is extremely limited and does not allow a detailed analysis for the majority of HFEs. In this regard, typically, at the stage preliminary SAR development, a qualitative analysis of the HFEs is performed in a limited scope.

At the stage of the preliminary SAR development the most important result of a HFEs qualitative analysis is the definition of the operator's time window for performing the actions required (for type C and B human errors) and determination

of the nature and timeline when information that helps to decide on the implementation of the action becomes available. As for type A human errors, the qualitative analysis is limited only to identifying factors that contribute to making an error based on the available information from system analyses and operational documentation of the referenced units.

Quantitative analysis

There are principle differences between quantitative HRA at the stage the development of the preliminary SAR and HRA for the operating units. This is due to the following reasons:

- Limited information required to perform a detailed quantitative analysis (see Table 2).
- Specific objectives of the HRA at the stage of the preliminary SAR development (see Table 1).

The main objectives of the HRA at the stage of preliminary SAR are:

- Evaluation of the lowest justifiable probabilities of human errors that provide:
    a. Compliance with the probabilistic safety goals for the unit
    b. Balanced design aimed to risk associated with the IEs that disproportionally contributing to the overall/total risk of the unit (or units).
- Identification of technical measures to achieve the assessed values of the probability of HFEs. Such measures can be, for example:
    a. Design solutions that reduce the likelihood of type A and B errors, including the elimination of dependencies between systems potentially leading to IEs (e.g. changes in the application of fail-safe design principle).

b. Introduction of new alarms that provide timely information for the operator to make a decision on the need of the action and for the implementation of the action.

- Introduction of automatic interlocks to avoid the need of operator actions if feasible or to reserve operator in case of failure to perform the action (e.g. automatic isolation of the reactor during drainage process in shutdown state).
- Determination of organizational measures to ensure the achievement of the assessed human error probabilities (HEPs) of HFEs. Organizational measures considered at the stage preliminary SAR development may include:

    a. Requirements for inspections, repairs and maintenance of equipment to reduce type A and B errors probabilities in the operating and maintenance procedures.

    b. Specific information to support the operator to make the correct decision on the implementation of a particular post-accident action in the emergency procedures.

    c. The specific requirement for the design of the main and reserve control rooms, as well as the organization of the work of the control crew, which makes it possible to reduce the likelihood of failure to perform the action by introduction of additional signals and by providing a convenient human-machine interface

    d. Introduction of the possibility to monitor the implementation of the action by the other control crew staff of the unit, plant staff outside the control crew or technical support group.

It is the difference in the objectives of the HRA that determines the methodology for performing the quantitative analysis and the choice of HRA models at the stage of

the preliminary SAR development. The applied methodology and models should allow the most practical assessment of both the basic HEPs and the changes in these probabilities in case of implementation of the organizational and technical measures. The main approaches used to quantify the HEPs for the three types of HFEs are described below.

It is important to note that the quantitative analysis at the stage of development of the preliminary SAR is performed iteratively and in conjunction with other HRA tasks. That is, this task is not independent, and its completion is impossible without performing the activities presented in Figure 1.

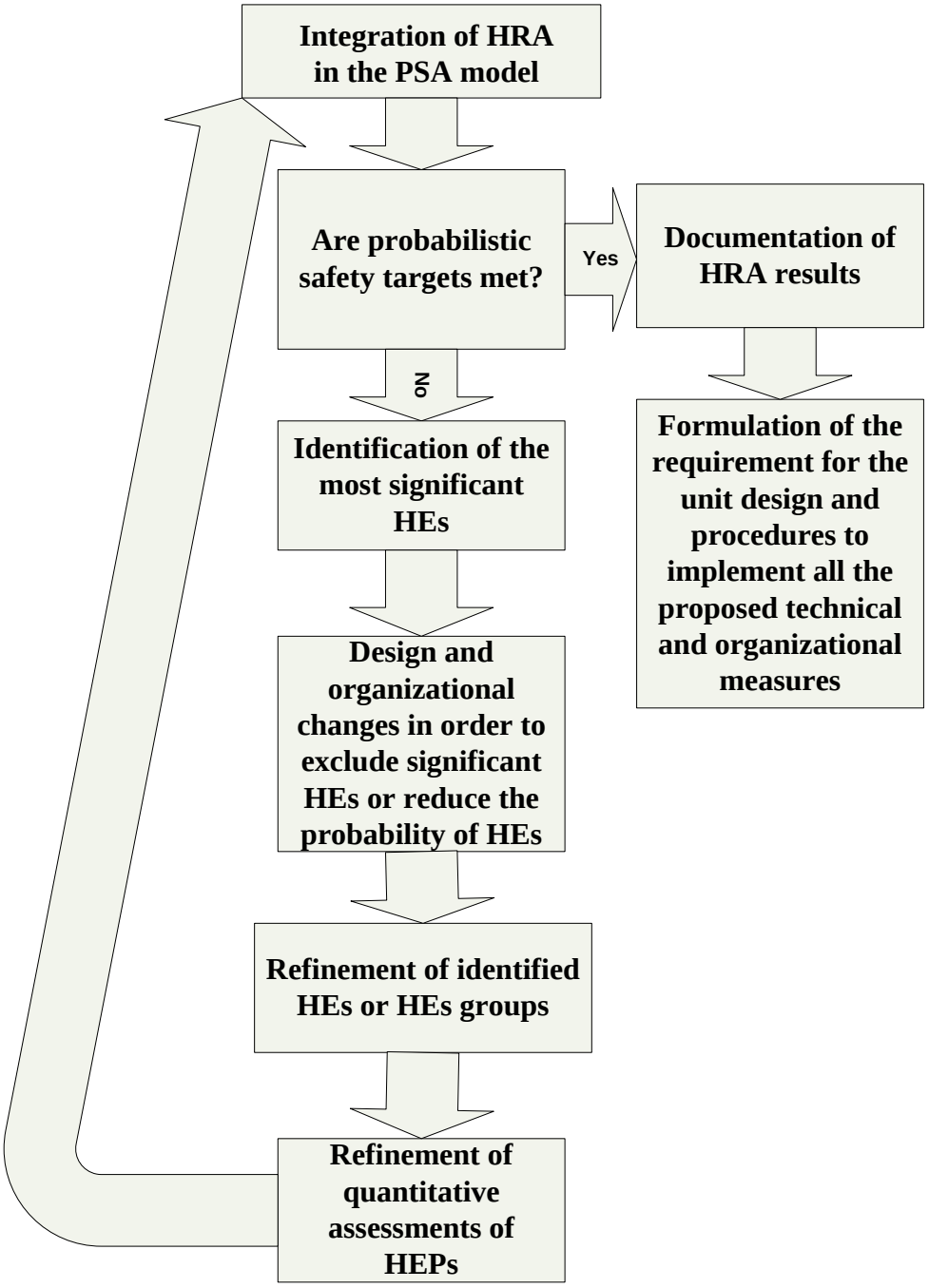

Fig. 1. Quantitative analysis steps

Quantitative analysis of type A human errors

The quantitative analysis is typically performed in several iterations:

- Once all the possible errors of type A have been identified and grouped, screening values can be assigned to HEPs at the first step of the quantitative

analysis. This practice is acceptable, since, as a rule, type A errors do not make a significant contribution to risk and for a number of HFEs screening values can remain in the PSA model without their refinement. More important is the assignment of the conditional probabilities of dependent type A human errors, leading to the failure of several safety system trains. It is important to note that the type A errors are most important in stand-by systems, since they appear only when system operation is required or during testing. For quantification of the type A HFE applicable for passive systems the same approach can be used as for any active system. However, it is important to understand what type of dependencies between HFE for a single passive system train and how these dependencies can be quantified.

- When performing screening, the conditional probability of the dependent HFEs is usually assigned rather high (for example, 0.1 for the HEPs in two trains and 0.05 for HEP in three or more trains).
- The probabilities of the type A human errors, estimated during the screening analysis, are included in the integral PSA model. After the identification of significant type A errors, the conditions and causes of their occurrence are analysed, as well as the possibility for the dependent HFEs.

  In joint discussions with system designers, necessary and possible technical and organizational measures are defined to reduce both the probabilities of the independent type A HFEs and the conditional probabilities of the dependent HFEs.
- A refined analysis is carried out for the dominant HFEs, assuming that all the design and organizational measures are implemented. The probabilities of the type A human errors, estimated during the refined analysis, are included in the integral PSA model. The refined analysis is carried out using the same methods that are used for the type A errors in the PSA for

operating units. When choosing the HRA method, the information available for the analysis is taken into account. This step can be skipped if a safety target is met with the screening HEPs.

- The contribution of the type A human errors to the calculated risk metric/CDF/LRF is estimated and the need for additional measures to reduce the probabilities of the type A HFEs is analysed. In practice, the additional measures are not required if combined Fussell-Vesely importance of all the type A HFEs (including dependent HFEs) is less than 1% of the target safety probability index. If this value is exceeded, it is possible to come back to step 2. However, in practice, after the first iteration, it is more efficient to proceed to other types of human errors and return to step 2 after inclusion of the other types of HFEs in the integral PSA model.
- After the HRA is completed, all the measures identified in the analysis are documented in the HRA report and at the stage of the final SAR during the performance of the PSA it is specified how the measures proposed in the analysis are implemented in the systems design and in the operating and maintenance procedures.

Quantitative analysis of type B human errors

The procedure for performing a quantitative analysis of the type B HFEs does not essentially differ from the one described above for the type A errors.

Some differences between the analysis steps can be for the errors associated with making an erroneous decision to disconnect normally operating systems or erroneous actuation of stand-by systems (as a rule, in the PSA, deliberate malicious actions are not considered). Fundamentally, the analysis scheme does not differ, but in analysing of such HFEs, the dependencies between the type B HFEs are not considered. The absence of the dependencies between the type B HFEs is due to the

nature of such events - typically, it is an error to push the wrong button instead of correct one, or a wrong decision (start the stand-by or disconnect operating system). In both cases there is no reason for dependences between HFEs. Instead, the dependencies between the type B and those type C human errors that associate with the actions aimed at eliminating the consequences caused by the type B HFEs must be analysed.

Quantitative analysis of type C human errors

The greatest difference in the approaches to the quantitative analysis of the HFEs at the stage of the preliminary SAR development and one for operating units is found precisely for the type C HFEs.

At the stage of the development of the preliminary SAR, there is a rather limited information about the processes after the occurrence of the initiating event, obtained in the framework of deterministic safety analyses for both design and beyond design basis accidents. Typically, this information is sufficient for the development of preliminary accident sequence models and determination of the operator's actions necessary to transfer the unit to a stable safe state.

However, in the first stage of the HRA, there is the limited information necessary for a detailed analysis of the type C human errors, such as:

- information on the settings and interlocks for triggering systems is incomplete;
- signals informing the operator about the need to perform the action are not fully defined;
- thermohydraulic calculations that justify time required and time available for operator to perform the action are insufficient to cover all operators actions;
- information about the steps necessary for the operator to perform a specific action and the time available is needed for each step;

- there is limited or even no information about who and how can detect the error of the operator both in the decision making process and in the implementation of the action itself;
- there is no information on the extent to which the specific situation requiring the performance of a particular action is reflected in the emergency procedures and how the operator's training process is organized to perform this action under the specified conditions.

In such conditions, accepting conservative screening HEPs will not lead to a realistic result, since formally the screening values should be extremely high (due to lack of procedures, lack of alarms, etc.).

Therefore, even for the first step of the analysis, such assumptions are made that make it possible to perform more realistically the quantitative estimates of the probabilities.

- based on the available information on the composition of the control room crew, it is determined who and how can detect the operator's error in making a decision on the need for the actions or during the implementation of the action;
- it is assumed that the emergency procedures reflect all the necessary information to perform the action and the operators have been trained in responding to the specified accident conditions.

Quantitative assessment of the HEPs is performed for all identified HFEs (including dependent HFEs) using analysis methods that provide realistic estimates and are able to use all of the above information.

The estimates obtained are used as the screening values for inclusion in the integral PSA model and for the identification of dominant type C human errors.

After identifying the dominant HFEs, steps are carried out in many respects that are similar to those for the type A errors:

- The analysis of the conditions and causes of the dominant HFEs is carried out, in particular, the most important factors influencing the human behavior in the considered accident scenarios are determined. As a rule, such factors are the same factors as those considered in the HRA for the type C human errors for operating units:

  a. Time for decision and action

  b. The quality of the human-machine interface (HMI)

  c. The complexity of decision making

  d. The complexity of the action

  e. The level of preparation of the operator for the implementation of the action in question under the conditions being considered, etc.

- Possible measures to reduce the negative impact of these factors are identified. Examples of the technical and organizational measures for some factors are given in Table 3 below.

- A refined analysis is carried out for dominant HFEs assuming that all the design and organizational measures are implemented.

  The probabilities of the type C human errors (including dependent HFEs), estimated during the refined analysis, are included in the integral PSA model.

  The refined analysis is performed using the same methods as used in the PSA for the operating units. When choosing the HRA method, the information available for the analysis is taken into account. This step can be skipped if a safety target is met with the screening HEPs.

- The contribution of the type C human errors to the calculated risk metric/CDF/LRF is estimated and the need for additional measures to reduce

the probabilities of the type C HFEs is assessed. In practice, additional measures are not required if the combined Fussell-Vesely importance of all the HFEs is less than 1% of the probabilistic safety target. If this value is exceeded, a transition to step 1 is possible.

- However, in practice, after the first iteration, it is more efficient to consider additional technical solutions that reduce the dependence of the results of the PSA on the probability of the considered HEFs of the type C, namely, making changes to the design of the unit that ensure an automatic execution of the function, previously performed by the operator. This step can be also skipped if the safety target is met with the refined HEPs.
- After the HRA is completed, all measures identified in the analysis are documented in the HRA report. In addition, in the PSA performed at the final SAR development stage, it is specified how the recommended measures are implemented in the systems design and system manuals, in the MCR design and control crew organization, in emergency procedures, training programs, etc.

Integration into the PSA model

The integration of HFEs of all types into the PSA model is carried out using the same methods and approaches as in PSAs for operating units.

The only important difference is that the integration process is performed many times and, therefore, methods should be chosen that allows the inclusion of HEPs in the PSA model in a way that maximally supports the possibility of updating both the probability of the HFEs, the dependencies between the HFEs and the nomenclature of the HFEs.

At the stage of the final SAR development the HRA carried out for the preliminary SAR is revised to take into account the differences in the final design from the

preliminary design, the probabilistic model of which was developed during the development of the preliminary SAR.

Table 3 Measures to reduce the negative impact of factors affecting the operator behaviour

Performance shaping factors	**Possible organizational and technical measures**	**Comments**
Time window for making a decision and action implementation	The introduction of earlier alarms, more automated functions, restructuring of EOPs.	-
Quality of HMI	The introduction of additional signals (sound, light). The organization of the main control room crew in such a way as to strengthen the independent control of other members of the shift. The identification of signs, allowing to identify the need for the execution of an action by the personnel of the unit that are not part of the control room crew.	New alarms should be introduced with care as more alarms mean also a higher likelihood for spurious alarms, which in long term are counter-productive and can be disturbing for the operators. An example of such signs may be a high level of radiation detected by radiation monitoring personnel that performs independent monitoring of all radiation-hazardous operations and can identify the need for carrying out a post-initiator action, due to the presence of an elevated level of radiation.

Performance shaping factors	Possible organizational and technical measures	Comments
Complexity of the decision	The inclusion in the emergency procedures of a clear requirement to perform the action in the context of the scenario in question	This is not easy to implement and can be done only for the most significant HFEs.
The complexity of the action	The optimization of the workplace of operators of the control room and local control centres	An example of such an optimization can be the use of control keys located in an accessible place, with a clear identification of the function of each key. The elimination of errors of a false selection of the control key must be ensured.
The level of preparation of the operator for the implementation of the action in question in the conditions under consideration	The inclusion of the analysed action in the training programs under the conditions of the scenario in question	-

ANALYSIS OF DEPENDENCIES BETWEEN HFEs AND THE MINIMAL VALUE OF THE RESULTING HFEs

The results of the PSA, regardless of the stage of the life cycle of the NPPs, are not so dependent on the nominal values of the HEPs of any type, but mainly on how the dependencies between the HFEs included in the same minimal cut set are estimated.

Any optimization of the unit that provides a reduction in the probabilities of the specific HFEs will not provide a significant reduction in the probabilistic safety performance of the unit if:

- there are significant minimum cut sets, which include more than one HFE;
- the degree of dependency between the HFEs included in the minimal cut sets is high.

Therefore, the most important tasks of the HRA during the design PSA performance and especially at the stage of the preliminary SAR development are:

- identification of minimum cut sets that include more than one HFE;
- analysis of the degree of dependency between the HFEs included in the same minimal cut set;
- identification of measures to reduce the degree of dependencies.

These tasks are performed during the entire process of the HRA when performing the PSA at the preliminary SAR development stage and are eventually included in the integrated PSA model used to confirm the compliance with the target probabilistic safety indicators of the NPP.

In itself, the process of analysing the dependencies during the preliminary SAR development stage is not different from the analyses performed for the operating units, but it has certain specificity due to the difference in the objectives of the HRA.

As it was shown earlier, the primary objective of the HRA at the stage of the preliminary SAR development is to optimize the unit by identifying and implementing organizational and technical measures in the design that will ultimately provide the required level of safety for the unit. Therefore, the purpose of analyses of dependencies is, first of all, the identification of factors that affect the degree of dependency between the HFEs, and the identification of the technical and organizational measures that allow it to be significantly reduced.

Table 4 shows the most significant factors, usually determining the degree of dependencies between the HFEs, and examples of the measures that can be implemented to reduce it. For simplicity, which does not affect the general approach, the situation is considered where only two HFEs enter the minimal cut set. Table 4 is applicable for the HRA at any design stage; however, most of the measures listed in the table can be implemented easily only at the preliminary SAR development stage.

Table 4 Factors determining the degree of dependencies between HFEs

Factors determining the degree of dependencies	**Possible organizational and technical measures**	**Comments**
Dependence on the cognitive component of the human actions in the change of actions	-	The cognitive component of the human actions is determined by the purpose of performing the actions and cannot be reduced by organizational and technical measures. In the absence of cognitive dependence, it can be asserted that the HFEs associated with the corresponding actions of the operator are independent
The time between human actions in one minimal cut set.	Changing the settings and interlocks that provide an increase in the time window for the operator to perform the second action when the first one in the minimal cut set fails.	This measure also leads to an increase in the reliability of the performance of the first action in the chain of the operator backup actions. Note that the dependent HEP in most of HRA methods depends on the first HFE in the chain of the redundant actions. Therefore, what action in the chain of the actions can be defined as the first one is extremely important and is discussed after the table.

Factors determining the degree of dependencies	Possible organizational and technical measures	Comments
The commonality of the personnel making the decision to perform the actions	The organization of the main control room crew in such a way as to strengthen the independent control of the other members of the crew. Establishing of signs and alarms that allow the personnel of the unit that is not part of the control crew to timely identify the control crew error.	The measures are almost identical to those proposed for improving the reliability of a single human action, but are also effective for reducing the degree of dependency. If the staff, independent of the staff of the control crew, has the opportunity to identify the HFE made by the control room crew based on signals other than those relied on by the control room crew, then the independence of the recovery actions to eliminate the consequences of the HFEs increases
The load on the operator when performing the actions	The optimization of the workplace of the operators in the main control room and local control centres. Training the operator to practically perform all actions individually and in the chain of the actions.	An example of such an optimization can be the use of control keys located in an accessible place, with a clear identification of the function of each key

One can see from Table 4, that the measures designed to reduce the level of dependencies are similar to the measures designed to improve the reliability of individual actions. A feature of the analysis of dependencies at the stage of the

preliminary SAR development is the very possibility of identifying and implementing in the design those measures that will ensure their overall effectiveness in terms of reducing the contribution of the HFEs in the risk of the nuclear power plants.

It is necessary to note that several features of the dependency analysis are especially important in the analysis of dependencies at the stage of the preliminary SAR development because at this stage it is easy to implement important changes in the plant design aimed at enhancing safety.

Accounting for dependencies between different types of HFEs

When performing the HRA at the preliminary SAR development stage the type C HFEs are analysed for the presence and the degree of their dependency on the type B HFEs. This is in particular important for the type C errors while performing the actions aimed to eliminate the consequences of the type B HFEs. The degree of such dependencies can be high when the same personnel make an error leading to an IE and participates in elimination of the HFE consequences.

Most clearly, such dependencies are manifested when performing operations in shutdown modes. An example of such dependencies is discussed below for the reactor drainage process.

When draining the reactor, the operator can for some reason make a mistake to reduce the level below the permissible level (during mid-loop operation), and he can also make the mistake of preventing dropping the level below the critical level (for example, the cold leg of the reactor) by the same reason.

This dependence can be considered high and, in principle, the most reasonable technical measure is the introduction of a signal to automatically cut the drainage line to prevent from reducing the level below the permissible level. Nevertheless, even without it, there are other possible compensating technical and organizational

measures that make it possible to reduce the overall probability of the HFEs for the reactor over-drainage:

- Introduction of additional signals after the level is lower than permitted, allowing the operator to notice the error made by himself.
- Inclusion in the drainage process of other shift operators, supervising the operator performing the drainage process.
- Use of information from operators controlling the filling of containers into which the water from the reactor is drained.
- Identification of technical measures and their inclusion in the emergency procedures for adding water into the reactor in case of the over draining, but prior of reaching a critical level (for example, the top of the reactor core).

At the stage of the development of the preliminary SAR the analysis and accounting of the HRA dependencies allow to develop an optimal strategy and technical measures to protect against the dependent HFEs of the types B and C.

Selecting the first action in the chain of actions when analysing the dependencies

As a rule, when performing the analysis of the dependencies between HFEs in the HRA for the operating unit the first action in the chain of backup actions is the action that is supposed to be done by the operator according to the emergency procedures. Obviously, if the factors influencing the performance of this action are negative, then the estimation of its probability will be quite high. In such a case if the redundant actions are dependent on the first action, then the overall dependent HFE will also have a high probability, since, based on widely used HRA methods, it is determined by the probability of the first action and then by the degree of the dependency.

When the HRA is performed for a plant in design, the emergency procedures have not been developed yet and the sequence of personnel actions is not defined. It seems consistent to define as the first action a human action that has the least probability of an error and to include in the emergency procedures and training programs the priority execution of this particular action. This allows obtaining lower probabilities for dependent HEPs and lower risk estimates for the facility. However, this approach may be not acceptable as it contradicts to the purpose of such an analysis - to increase the safety of the unit. This is due to the fact that many other aspects should be also considered beyond the scope of the HRA in making such a decision in addition to probabilistic measures. The following example illustrates the issue.

Let us consider the need for reactor cooling down in accident conditions for PWRs. Two possibilities for safe cooling down can be identified. One evident, but relatively complicated path is the cooling down through the secondary side that requires performance of human action having a relatively high probability of an error. For operating plants this action is usually considered in emergency procedures as the first priority action. Another possible cooling down path is associated with opening of a pressurizer power operated relief valve (PORV). An operator error in performing this action is low.

Therefore it seems logical to define at the design stage the action with PORV opening as the first priority action and obtain a low dependent HEP. However, the cooldown path using PORVs cannot be defined as the first priority action, since it is associated with potential negative effects such as radioactive contamination of the plant premises, the occurrence of the initiating event (primary coolant leak), and others. The following question comes to mind – what designer should do to decrease HEPs and at the same time to reduce harm to the plant? It is clear that the answer should not be dependent on the accepted methodology of the HRA.

In the opinion of the paper authors, the dependent HEPs should be not based only on the first action defined in procedures. It might be more fruitful for the designers

that the approach utilizing HEPs for both actions should be used. The dependency between these actions could be accounted for using coefficients that can be calculated based on the influencing factors (time between actions, cognitive connection between actions, common staff performing the actions, workload, etc.) . The example of the approach that utilizes HEPs of both actions could be found in [3]. This allows the designers to provide valuable estimates of the plant risk and at the same time does not push them to assign priorities for operator actions in the emergency procedures following the desire to show lower risk indices.

Restriction on the minimum value of the joint HEP for the chain of backup actions

As indicated in [1], in the practice of performing the HRA for operating units, it is assumed that the total probability of the joint HFE, taking into account the dependencies of HFEs in the chain of actions that enter into one minimal cut set, cannot be less than $1.0\ 10^{-5}$. In practice, this is tantamount to the assertion that there is no possibility to prevent fuel damage with a probability of less than $1.0\ 10^{-5}$ by means of technical measures controlled only by operators. Such an approach is fundamentally unacceptable in the HRA for the units at design stage, as it leads to a global contradiction between the HRA and the design goals, and the HRA acts as a progress-inhibiting factor:

- In practice, the number of signals that contribute to the identification and recovery of the HFEs tends to increase
- In the HRA methodology, even multiple recovery does not allow to obtain the total probability of the HFEs below $1.0\ 10^{-5}$.

In the HRA performed during the development of the preliminary SAR, the dependency analysis is performed using known methodologies, and the assumption that the minimum value is limited is removed. This approach allows to optimize the process of unit control, to reduce the degree of the dependencies between operator

errors in the chain of the actions, to evaluate and reduce the realistic contribution of the HFEs to the unit probabilistic indicators. Therefore, the restriction on the minimum value of $1.0\ 10^{-5}$ of the joint HEP can be removed while performing the HRA at the stage of the development of the preliminary SAR, but only in sequences when it is ensured that all the information available to the operator is correct and does not lead to errors caused by the situation. The specific situations where additional equipment failures can lead to an error due to the incorrect information, such as in case of the accident at the Three Mile Island plant, should be directly included in the PSA[5].

CONCLUSION

The human reliability analysis being performed within the probabilistic safety assessment of new nuclear power plants in design has specific features different from ones of the human reliability analyses carried out for operating plants. It is related to the analysis of all the types of human errors including dependent errors. This difference is caused by both incomplete design information and another main goal on the human reliability analysis at the stage of the plant designing. Such an analysis is a powerful tool for optimizing plant design that is easy to make at this stage of plant lifetime to enhance safety.

[5] It should be noted that there is typical objection to the above considerations, namely: "The assertion that the increase in inspections increases the probability of detecting and recovery from errors is contradictory. It can be seen from the operational experience that despite the checks (mostly several checks) errors can still be found". This statement is not entirely correct, since all known multiple human errors in the chain of the backup actions have the same characteristics: either high, or moderate level of dependency between the actions or a rigid combination of factors that affect the operator behavior, which has led to an increase in the probability of the HFEs. The best example is the multiple human errors in the Three Mile Island accident, where the error to prevent a low level in the reactor was mainly caused by a human error related to stopping the injection. However, this error was made due incorrect understanding of the level in the reactor that was based on the correct information on the level in the pressurizer and wrong information on the status of power operated relief valves. From the point of view of the available information for the operators and the level of knowledge about the development of the accident at the time of the accident, the operators behaved absolutely correctly and they did what they was supposed to do.

ABBREVIATIONS

CDF	Core Damage Frequency
CLA	Construction License Application
EOP	Emergency Operating Procedure
HEP	Human Error Probability
HFE	Human Failure Event
HMI	Human-Machine Interface
HRA	Human Reliability Analysis
IE	Initiating Event
I&C	Instrumentation and Control
LRF	Large Release Frequency
MCR	Main Control Room
NPP	Nuclear Power Plant
OLA	Operating License Application
PORV	Power Operated Relief Valve
PSA	Probabilistic Safety Assessment
SAR	Safety Analysis Report
VVER	Water cooled water moderated reactor (Russian abbreviation)

REFERENCES

1. Development and Application of Level 1 Probabilistic Safety Assessment for Nuclear Power Plants, IAEA Safety Standards Series No.SSG-3, Vienna, 2010.

2. Lankin M.Yu., Lyubarskiy A.V., Kuzmina I.B., Tokmachev G.V. “The application of the fail-safe design principle taking into account information about the risk (following the lessons of the lessons of the accident at the nuclear power plant "Fukushima Daiichi")/ Nuclear and Radiation Safety, 2015, No. 4 (78), pp. 3-18.

3. SWISRUS PROJECT, Novovoronezh Unit 5 PSA. Part I: PSA Level-1 for Internal Initiating events, Main Report, Moscow, December 1999