MDEP Design-Specific Common Position CP-VVERWG-01

VVER Working Group's activities

COMMON POSITION ADDRESSING FUKUSHIMA-RELATED ISSUES

Participation

Regulators involved in the MDEP working group discussions:	AERB, HAEA, NNSA, Rostechnadzor, STUK and TAEK
Regulators which support the present common position:	AERB, HAEA, NNSA, Rostechnadzor, STUK and TAEK
Regulators with no objection:	-
Regulators which disagree:	-

Multi-National Design Evaluation Programme

VVER Working Group

COMMON POSITION ADDRESSING FUKUSHIMA-RELATED ISSUES

Introduction

The MDEP VVER Working Group (VVERWG) members, referred to herein as "regulators", consist of members from the Russian Federation (Rostechnadzor), Finland (STUK), India (AERB), Turkey (TAEK), China (NNSA) and Hungary (HAEA).

It is important to note that not all of these countries have yet completed the regulatory review of their VVER applications against lessons learned from the Fukushima Daiichi accident and other Fukushima-related issues. Thus this paper identifies common preliminary approaches to address potential safety improvements for VVER plants, as well as common general expectations for new nuclear power plants.

These common preliminary approaches are based on their national regulatory requirements and those safety assessments of design documentation that have been completed to date. Consequently, some technical details presented in VVER design features have not been evaluated yet by some member countries and they may in the future differ from those presented.

The following safety reviews of the VVER design applications are currently under consideration:

- VVER-1000/AES-91and 92,
- VVER-1200/AES-2006-M,
- VVER-1200/AES-2006-P,
- VVER-TOI.

When these are completed, the regulators will update this paper to reflect their safety conclusions regarding the VVER designs and how the designs could be enhanced to address Fukushima-related issues.

The common preliminary approaches are organised into four sections, namely:

I. Accounting for external events in the design,

II. Design solutions for specific beyond design basis accident (BDBA) or design extension conditions (DEC) - e.g. station blackout (SBO) or loss of heat removal to ultimate heat sink (UHS),

III. Emergency preparedness and response,

IV. Reliability of safety functions.

Additionally, there are appendices related to areas where further studies were identified as necessary.

Background information

The severe accident directly involving three operating reactor units and their related spent fuel pools, and indirectly other facilities on the site, took place in Japan at the Fukushima Daiichi nuclear power plant (F-D NPP) in March 2011. The immediate cause of the accident was the Great East Japan Earthquake with a magnitude of 9.0 followed by a tsunami waves with a maximum height of 14-15 m that inundated the F-D NPP site. It caused damage to the electric power supply lines to the site and substantial destruction of the operational and safety infrastructure on the site (electrical and mechanical equipment including the emergency diesel generators, DC batteries, associated power panels or connections etc.).

As a consequence there was a loss of both off-site and on-site electrical power (station blackout) and the loss of the residual heat cooling function at the plant. These resulted in the core damage of three units and subsequently large radioactive releases to the environment (INES 7).

Several studies have already been performed in Japan and elsewhere to better understand the F-D NPP accident progression and further detailed technical studies are still in progress. Additionally, there are on-going studies on the behaviour of NPPs, in general, under very severe F-D like conditions, seeking to identify potential vulnerabilities in plant design and operation. Likewise, those international regulatory bodies responsible for regulating the design, construction, commissioning and operation of NPP with VVER type reactors are engaged in similar activities. All of the above aim to suggest reasonably practicable upgrades to the NPPs; or to recommend enhanced regulatory requirements and guidance to address such severe accident conditions.

General context

The Fukushima Daiichi NPP accident demonstrates the importance of reinforcing the Defence-in-Depth (DiD) concept. This includes:

- Adequately identifying the external hazards (including low frequency extreme events),
- Characterising the hazards and effects,

- Examining credible combinations of hazards,
- Making the design provisions to
    - (a) protect the installation against these hazards,
    - (b) prevent the significant radioactive releases.

The outcomes should be:

- reflected in safety requirements and regulatory guidelines,
- reflected in the licensing procedure,
- detailed in the installation safety case
- properly reviewed by an independent regulatory body.

The accident also reinforced the need to have a comprehensive safety analysis using both deterministic and probabilistic methods in a complementary manner to provide a comprehensive coverage of all issues important to the NPP safety. In the safety analysis, specific consideration needs to be given to both multi-unit events and a long duration accident assumed to occur with both the site and surroundings in a devastated condition.

One has to bear in mind that the specific nature of individual events and challenges can never be completely taken into account in design and operation of a nuclear power plant or other nuclear installation. However, a robust design based on the DiD concept with sizeable safety margins and diverse means for delivering critical safety functions as well as flexible, symptom-based operator response plans will help to address accidents beyond current design basis (i.e. latest periodic safety review).

The design, construction, manufacturing and installation of structures, systems and components should rely on state-of-the-art engineering decisions and sufficient margin beyond the design criteria required for a design basis accident to avoid **cliff edge effects**[1]. Such an approach along with proper mitigating arrangements will help to ensure an appropriate response, should a beyond design basis accident or as design extension conditions (DEC) in some member countries occur. Provisions aimed at facilitating the repair/recovery of impaired safety functions should also be foreseen.

[1] **Cliff edge effects** are the effects of those hazards for which a minimal increase in the hazard's magnitude can have a much higher impact. For example, the external flooding hazard may have little to no impact to a nuclear power plant below a prescribed flood level. However, a small increase beyond that prescribed flooding level could impact many of the nuclear power plant's functions and lead to a severe accident.

COMMON POSITION

I. ACCOUNTING OF EXTERNAL EVENTS IN THE DESIGN

Context

Fukushima Accident stressed the fact that the effects of external hazards on a nuclear power plant site may have a major impact on the safety of the plant and these effects should be carefully taken into account in the plant safety analysis. External hazards such as seismic and flood may cause common cause failure (CCF) for safety related systems, with the associated possibility of degradation or loss of some fundamental safety functions that could result in a large amount of radioactive material release.

Although it is acknowledged that external hazards are primarily site dependent and that the adequacy of the design has to be reviewed on a case-by-case basis considering the site characteristics. Up until now regulators who have made safety findings in the review of their VVER design applications, find that the safety related structures, systems and components of the generic VVER-type NPPs are designed and protected to tolerate external and internal events by applying adequate technical measures. These measures include physical separation, redundancy, diversity and protection against dynamic loads, etc.

Discussion

1.1. Site specific characteristics

There are other past examples of external events which have exceeded the design basis than the BDBA earthquake and ensuing tsunami in Fukushima accident. For example, two units of Blayais Nuclear Power Plant in France were flooded in December 1999. The Niigataken-Chuetsu Oki earthquake on July 16, 2007 exceeded the design basis of the Kashiwazaki-Kariwa NPP in Japan. Five months later just after Fukushima accident, on August 23, 2011, an earthquake on the East Coast of the United States also exceeded the design basis of the North Anna Nuclear Generating Station in USA [1, 2, 3].

In all of these examples the units were brought successfully into the safe shutdown state. Similarly, in the Fukushima case, just after the earthquake of magnitude 9.0, all operating units were shut down safely, the structures, systems and components (SSCs) important to safety withstood this extreme earthquake, and also the emergency systems were properly activated and fulfilled their functions until, however in the Fukushima case, the destroying inundation of the tsunami [4, 5].

This illustrates that for the beyond-design basis external events, the safety margins play an indispensable role in the design of NPPs. This, also, reveals that although a sufficient margin with necessary consideration to the beyond design basis earthquake was taken into account in the Fukushima NPP seismic design. The consideration for the specific subsequent tsunami was not

incorporated, which consequently led to a cliff-edge effect when the tsunami height exceeded a certain level, causing the functional failure of many safety systems.

Therefore, the site specific characteristics and parameters should be investigated comprehensively and taken into account while developing the detailed NPP design. These include all aspects of the anticipated external events, i.e. not only earthquakes but also the accompanying events such as tsunami, fire, avalanche, volcanoes, freezing, high and low temperatures, storm, etc., after which those that impact on overall plant safety should be taken account of and reflected in the design of VVERs, with sufficient safety margins incorporated in order to avoid cliff-edge effects.

It should be noted, that in accordance with p.1.5 of SSG-35 [8]: «The siting process, from the beginning, has to be guided by a clearly established set of criteria consistent with the relevant regulatory requirements. Such criteria are of particular importance for those factors for which sites can be excluded. A balance has to be established between the characteristics of a site and specific design features, site protection measures and administrative procedures».

1.2. Adequate protection against extreme hazards and their credible combinations

In the Fukushima accident, the main initiating events were not only the tsunami, but also the earthquake. The earthquake made the accident mitigation more difficult by delaying the recovery of the off-site power and other help from off-site [5]. The combined hazards also may happen in various ways such as heavy rain fall combined with a land slide, earthquake or aircraft-crash combined with the fire, etc. Therefore, such combinations and their risk should be considered in the NPP design, even if their probabilities of occurrence are not high.

1.3. Multi-unit consideration

Close spacing of Units 1-4 in the layout and the extensive impacts of the tsunami and earthquake to the all NPP site also hindered the accident response. In particular, harbor-side tsunami damage, earthquake damage to water storage tanks and water-supply piping, displacement of road surfaces, landslides, and blockage of roads and building access by debris are examples of common damage to Units 1-4 at the site. This damage impeded efforts to establish alternative cooling water and the electrical power [5].

Therefore, for the NPP sites where the building of multi-units is being planned, due consideration at the beginning of the design stage of the NPP should be taken of:

- the inter-dependencies between the units,
- physical separation of units to prevent unit-to-unit spreading of problems caused by both external and internal events,
- shared equipment (e.g., ventilation systems),
- impact of multiple-unit cooling,

- access to each unit and also to the NPP site should be taken into account at.

With a view to providing the solutions or minimizing the risks in the proposed layout.

It is also noted that in determining the effects of an external event on the NPP, the effects of this event on other facilities or installations in the vicinity, and on the safety of any system or service at the facility, should also be taken into account.

The effects of failure of non-nuclear safety related SSCs should be taken into account if this could affect the NPP safety such as access for the control and/or repair of the plant, or if they could potentially damage the safety systems.

1.4. Hazard assessments

One of the most important issues in the Fukushima Daiichi NPP accident is that the design basis tsunami height was not appropriately determined and indeed was underestimated at the Fukushima site [5].

For the determination of the design basis tsunami, only deterministic approaches were used and the studies and their results for the probabilistic tsunami hazard assessments (e.g. those performed in 2006) were not considered [6].

Before the Fukushima accident, compliance with the probabilistic approach for the determination of the design basis earthquake was voluntary in Japan. However, most Japanese NPPs focused on the seismic probabilistic safety assessment (PSA), considering the specific site conditions. Although the seismic PSA was performed for the Fukushima Daiichi NPP, PSAs of other external events such as floods were not developed and consequently the risk associated with tsunami was not taken into account.

In hazard assessments the deterministic approach for the external events implicitly considers historical events and the uncertainties of using these events, coupled with a margin of safety to compensate for the incomplete knowledge.

Conversely, probabilistic approaches allow explicit treatment of uncertainties and their propagation through the various stages of the hazard assessment process. This entails the development of design basis as well as beyond design basis parameters for the external events, together with the specified confidence levels.

Therefore, it is important to conduct both deterministic and probabilistic studies for the NPP site in order to understand the different ways of quantifying uncertainties, as well as provide better compensation for incomplete knowledge.

In this context, the deterministic and probabilistic approaches should complement each other and the results of these two approaches should be reflected in the design of the NPPs and they should be utilised within the substantiation of the NPP safety against the external events.

1.5. Periodic re-evaluation of external hazards

During the construction permits of Fukushima Daiichi NPP units in the 1960s, the original design basis tsunami for Fukushima Daiichi was based on the Chilean tsunami of 1960, which resulted in a historic high water level of 3.122 m. Following the publishing of Tsunami Assessment Methods for Nuclear Power Plants in Japan by the Japan Society of Civil Engineers in 2002 [7], the tsunami design basis was voluntarily reassessed by the licensee (TEPCO).

Using these new deterministic evaluation techniques, the design basis tsunami was determined as a maximum water level of 5.7 m. As these changes were done voluntarily and not at the direction of the regulator, the licensing basis did not change. Nevertheless, some measures were taken to maintain functions such as elevating the seawater pump motors.

Another study, taking into account the latest submarine topography and observed tidal level data was finalized in February 2009, based on the Tsunami Assessment Methodology that revealed the tsunami water level as 6.1 m. In this context, additional measures were taken for the pump motor seals recognising the new height of the tsunami.

One interesting point for the re-evaluation of the design basis tsunami is that a study for the probabilistic tsunami hazard was conducted in 2006, taking the Fukushima site as one example with the aim of improving the methodology and confirming the applicability of the probabilistic tsunami hazards analysis method. The result of this study showed a maximum tsunami height of 10.2m at the front of the intake point and a maximum flood height of 15.7m on the south side of the premises for major buildings of Units 1 – 4 at the Fukushima Daiichi [5]. However, this study on the probabilistic tsunami assessment was not taken into account in the Fukushima Daiichi NPP.

Fukushima accident showed that any changes in external hazards or understanding of them should be periodically reviewed for their impact on the NPP design and the plant configuration. When periodic reviews or new information indicates the potential for conditions that could significantly reduce safety margins or exceed current design assumptions, a timely, formal, and comprehensive assessment of the potential for substantial consequences should be conducted.

An independent and functional safety review should be conducted to fully understand the nuclear safety implications. If the consequences could include common-mode failures of important safety systems, compensatory actions or countermeasures must be established without delay.

Fukushima accident also demonstrated that licensees and the regulators should continually seek out new scientific information about external hazards and their methodologies for estimating their magnitudes, frequencies, and potential impacts. These new information and methodologies as they become available should be incorporated in the safety assessments of the NPP design as well as throughout the plant lifetime. Licensees and the regulators should also take timely actions to implement countermeasures when such new information results in substantial changes to risk profiles at the NPPs.

VVER Design Features Accounting for External Events

The new VVERs are designed taking into account detailed site specific characteristics and parameters related to overall NPP safety (such as earthquake, flooding, aircraft crash, etc.) in accordance with country specific regulations and in line with IAEA standards. Some examples of the external events accounted for in new VVER designs are given in the following topics:

Seismic hazards

The design of the new VVERs and their protection against seismic hazards is provided by taking into account the site specific seismic conditions.

Civil constructions and structures, as well as equipment, process pipelines, other lines and structures of VVER-TOI-based NPPs are designed to resist seismic impacts up to 8 points on the MSK 64 scale.

To encompass the possibility of NPP construction at sites with higher seismic parameters, resistance to seismic impacts up to 9 points, MSK 64 scale, is ensured, with no essential reconsideration of volumetric, planning, routing and other underlying design solutions [12].

For example, at Akkuyu NPP with VVER-TOI in Turkey, both the deterministic and probabilistic approaches including the sufficient margin are used to determine design basis earthquake level and the VVER units to be constructed at this site are designed against a value of about 0.39 g peak ground acceleration (PGA). Another example is the Paks NPP site, where the submitted site license application contains the value of 0.34g PGA for design basis earthquake for the two planned VVER-1200 (AES-2006) units.

External Flood

New facilities may be protected against design basis flood and tsunami by adopting a layout based on maintaining the "dry site concept", where all vulnerable structures, systems and components are located above the level of the design basis flood, together with an appropriate margin. Where it is not practical to adopt the dry site concept, the design must include permanent external barriers such as levees, sea walls and bulkheads against the wave effect. So, the design flood level for new VVERs is specified to be below plant grade level with sufficient margin and demonstration of no cliff edge effects. For example, in Tianwan NPP-2 with VVER-1000 in China (including permanent external barriers), the design basis flood (DBF) is about 7.18m while the plant grade level is 7.85 m, and for Akkuyu NPP with VVER-TOI in Turkey (applied to dry site concept), design basis tsunami parameters including the safety margins are about 10.5 m. In the case of the VVER-1200 units of the Hungarian Paks NPP, it is also planned to apply the

dry site concept.

Other External Events (High wind and tornados hazards, extreme low/high temperature, external explosions, etc.)

A wide range of extreme environmental conditions are demonstrated to be covered by the VVER designs. As a result of the conservatisms that are incorporated into the selection of the standard site environmental conditions, they are expected to bound the most extreme site-specific values or they will be designed for. For example, in Russia, new VVERs safety related components are designed taking into account a wind velocity of 30 m/s (at 10 m above ground) and tornados of class 3.60 according to the Fujita scale [13]. Conversely, due to the fact that almost all design basis wind speeds for sites in China are higher than 30m/s, Tianwan NPP-2 with VVER-1000 in China is designed, regarding with site specific conditions.

Common Position

The regulators agreed that the following issues are important with regards to accounting for the external events in the VVER design in order to protect the plant against these hazards and prevent the significant radioactive releases:

- The site specific characteristics and parameters related to overall plant safety should be investigated comprehensively, with the aim of taking them into account in the design basis, with sufficient safety margins available in order to avoid potential cliff-edge effects.
- The adequate protection against extreme hazards and credible combinations of them (including low frequency extreme events) should be provided in the design of NPP.
- Beyond design basis external events should also be addressed in the design to ensure the practical elimination of large or early radioactivity release by the same or complementary measures as those derived for the above issue.
- Specific technical and organisational measures should be foreseen in the design to address the effects of external events on multi-unit sites.
- Both deterministic and probabilistic approaches should be applied for substantiation of the NPP safety against the external events including their combinations.
- Periodic re-evaluation of external events, their characteristics and of the plant responses to such hazards is important based on state-of-the-art information (knowledge) during the plant lifetime.

II. RELIABILITY OF SAFETY FUNCTIONS IMPLEMENTATION

Context

Lessons learned from the Fukushima Daiichi NPP accident show the importance of proper implementation of the DiD concept including a need for adequate protection of the plants against rare and extreme events (such as external hazards).

Proper implementation of DiD means that NPP design shall have several reliable and independent (as much as practicable) layers of defense aimed to fulfill the following fundamental safety functions: reactivity control, residual heat removal from both the reactor and spent fuel pools to ultimate heat sink, and confining of the radioactivity.

Discussion

The NPP design shall incorporate effective engineering means and organisational measures with the purpose of ensuring the realisation of the fundamental safety functions [9]:

- control of reactivity;
- removal of heat from the reactor and from the fuel store;
- confinement of radioactive material, shielding against radiation and control of planned radioactive releases, as well as limitation of accidental radioactive releases.

Incorporating 'Effective engineering means' at any specific level of DiD implies that such means have adequate reliability.

The 'reliability requirements' are applicable to the safety group (see [10]) accomplishing the specific safety function. So, when establishing the reliability requirements, the means designed to fulfil fundamental safety functions should be considered jointly with necessary support systems (such as electrical power supply, HVAC, etc.)

The 'means' included in the safety groups mentioned above should be considered safety related SSCs in the design. This implies that a set of quality requirements shall be required to cover processes of designing, manufacturing, supplying, and operating these means.

While assessing adequacy of safety group reliability level both deterministic and probabilistic considerations shall be taken into account. For example:

A deterministic consideration would be conformity with single failure criterion when such criterion is applicable.

A probabilistic consideration would be the necessity to achieve a reliability level sufficient to fulfil high level regulatory probabilistic targets (such as CDF or LRF targets).

Special attention should be paid to mechanisms which can potentially lead to common cause failure of the safety groups under analysis. Such mechanisms can be associated with impacts from external or internal hazards or sometimes with normal plant operation.

Measures which reduce likelihood of common cause failures of 'the means' shall be investigated. Such measures include application of separation, redundancy and diversity safety principles. Also special attention should be directed to the hazards which can affect 'the means' belonging to several levels of DiD and also to possible influence on the analysed 'means' by failures of 'the means' designed to maintain the same function at another level of DiD.

While estimating reliability level of safety groups, all relevant human-machine aspects should be analysed and quantified as necessary.

'Innovative technical means' ("first of a kind") are point of special attention in estimating safety group reliability. The necessary prerequisite for implementation of such 'means' is existence of sufficient underpinning which implies there is sufficient substantiation of their operability by calculations, experimental studies and (or) operational experience.

VVER Design Features for the Reliability of safety functions implementation

Safety of the new VVER design is ensured by consistent implementation of the DiD. For example, at the first level of DiD in AES-2006 design (in particular, units of Novovoronezh NPP-2) the following measures are provided:

- robustness of NPP towards external impacts;
- minimization of size of the potential radiation impact zones of NPP on the population during normal operation and accidents;
- development of the design by basing it on a conservative approach with mature intrinsic safety of the reactor installation . Including:-
    - self-control of reactor power
    - maintaining primary pressure at the expense of negative reactivity and pressure feedback,
    - Ability to remove heat from the core of the shutdown reactor to the ultimate heat sink by natural circulation
    - large inventory of water in horizontal steam generators and other vessels;

and

- effective system of maintenance and repair.

As part of the second level of DiD, the new VVER designs provide for engineered features (means of diagnostics, automatic controllers, interlocks, automatic protection features and others) which allow timely identification of and correction to departures from normal operation,

as well as exercise control in case of such departures.

At the third level of DiD, the AES-2006 design has a balanced combination of active and passive safety systems. Such a combination ensures both quick (due to active part) and reliable (due to passive part) mitigation of design basis accidents and BDBAs that may occur.

The active safety systems include the emergency reactor protection system, protection systems of the primary and secondary circuit against overpressure (these systems remain functional when the power is lost), a system for emergency and scheduled cooldown of the primary circuit and cooling of spent fuel pool, an emergency boron injection system, an emergency steam generator cooldown system, an emergency power supply system, a spray system, an emergency gas evacuation system and others. Active safety systems are of a 2-train configuration with internal redundancy (Novovoronezh NPP-2) or a 4-train configuration (Leningrad NPP-2).

The passive safety systems include a passive heat removal system from the SGs and a passive core flooding system (hydro accumulators), etc. Safety functions can be provided both by active systems and passive systems independently of each other.

The passive safety systems in the AES-2006 design also include a double-walled containment which prevents or restricts release of radioactive substances into environment. The inner containment is made of pre-stressed reinforced concrete with a sealing steel liner; it is designed for DBAs and BDBAs in combination with a safe shutdown earthquake. The outer containment is made of non-pre-stressed reinforced concrete and is intended to protect systems and elements of the reactor compartment against natural external and man-made hazards including aircraft crash. The outer containment ensures the leak-tightness of the annulus. An integral leak through the containment is not more than 0.3% of the volume per day at a pressure equal to the design emergency pressure.

The spray system is intended in the event of an accident to reduce pressure and temperature inside the containment and bind radioactive iodine which will be present in the steam and air of the containment. This system ensures automatic injection of borated water into the air of the containment when pressure within the containment exceeds a certain value and ceases when it decreases down to a certain value.

To manage beyond design basis accidents (including severe accidents - Level 4 DiD) the VVER designs include the following engineered features and organizational measures in addition to that used at Level 3:

- passive heat removal system;
- containment hydrogen removal system;
- corium retention and cooling system (core catcher);
- mobile devices (packaged fan cooling tower with necessary piping, mobile diesel generator and others) which help make up the primary circuit and spent fuel pool, as well as heat removal from the reactor and SFP; and

- instrumentation and controls for emergency monitoring.

The use of various engineered features at different levels of DiD facilitates independence of DiD levels from each other.

The passive heat removal system (PHRS) is designed for a prolonged removal of residual heat of the reactor to the ultimate heat sink (for the description of the different water- or air-cooled designs of PHRS, see section III).

The passive core flooding system (hydro accumulators) for Novovoronezh NPP-2 consist of 4 accumulator tanks (AT) of the 1st stage and 8 ATs of the 2nd stage. The operation of the system provides for cooling of the core during, as a minimum, 24 hours when active safety systems fully fail and the primary pipeline suffers a guillotine break.

The emergency hydrogen removal system prevents accumulation of explosive concentrations of hydrogen in the containment. The emergency hydrogen removal system uses passive catalytic hydrogen recombiners, which are located at places of possible accumulation of hydrogen. This arrangement does not require mixing in the containment to create a homogenous atmosphere.

The hydrogen concentration monitoring system consists of the primary and secondary equipment (probes, information processing and display units), communication lines and equipment for metrological qualification, certification and adjustment of instruments. The hydrogen concentration monitoring system can measure a hydrogen concentration in vapor-air-hydrogen mixture, and continuously monitors the parameters.

The core catcher (CC) in the AES-2006 design is intended to localize corium constituents and core fragments, to ensure cooling of molten corium and its subcriticality, and to minimize release of radioactive substances and hydrogen inside the containment. The heat removal from CC is by passive heat transfer to cooling water surrounding the “core melt pot” and is capable of ensuring long term cooling and solidification of the molten core. The sacrificial material of the CC includes gadolinium oxide to ensure subcriticality of molten core. The hydrogen generation decreases significantly (about factor 4) in the CC due to the hot metal capturing oxygen from the aluminum oxide in the pot instead of from water. A crust formed on top of the melt surface minimizes release of radionuclides into the containment.

Common Position

With the aim of guaranteeing a robust DiD, the 'technical means' designed for maintenance of three fundamental safety functions should conform the following principles:

- When establishing the reliability requirements, the 'means' designed to fulfil fundamental safety functions should be considered jointly with associated necessary support systems (such as electrical power supply, HVAC etc.);
- deterministic criteria and probabilistic targets should be established in the design to determine adequate reliability level of safety functions and corresponding 'technical means';
- the 'means' should be considered as safety related SSCs in the design which implies that a set of quality management requirements cover processes of designing, manufacturing, supplying, and operation for such means;
- measures should be taken in the plant design to reduce likelihood of common cause failures of the 'means' fulfilling fundamental safety function at specific level of DiD. Such measures includes application of separation, redundancy and diversity principles;
- the 'means' designed to fulfil specific safety functions at one level of DiD should be (to the extent practicable) functionally and physically independent from the 'means' designed to maintain the same function at another level of DiD;
- the 'technical means' which require human interaction for their start-up or operation shall be checked for appropriateness of human-machine interface issues, possible human errors affected on the 'technical means' operability should be carefully checked and necessary countermeasures should be taken;
- possible delays in the actuation or operation of the 'technical means' due to a variety of likely reasons should be taken into account in the design of NPP;
- 'innovative technical means' can be allowed in plant design if there is sufficient substantiation from necessary calculations, experimental studies and operational experience;
- potential negative interactions of 'technical means' which can be foreseen to operate simultaneously should be considered in the design. (i.e. interactions worsening their reliability).

III. DESIGN SOLUTIONS TO COVER SPECIFIC BDBA/DEC (SBO, LOSS OF UHS)

Context

Learning from the Fukushima Daiichi NPP accident confirms that the defense-in-depth concept remains the backbone of nuclear plants safety provision. However, reviewing the lessons learned has emphasised the need to strengthen the requirements with respect to each of the separate levels in the DiD concept and, in particular, to the level related to accidents that are not assigned to severe accidents but at the same time were not included into the earlier NPP design bases.

Accident scenarios with total station blackout (loss of all onsite and offsite power supplies including emergency power supply from diesel generators) along with an emergency scenario with loss of nuclear fuel residual heat removal systems to the ultimate heat sink (weakness of normal operation systems as well as safety system envisaged by NPP design) are important scenario types subject to consideration in the NPP design.

Hereafter, these accident scenarios are analysed from the point of view of their propagation at non-severe stage (since severe accident management for VVER-type reactors are considered by another subgroup of VVER WG).

Discussion

If accident scenarios with total station blackout or loss of systems on heat removal to the ultimate heat sink leading to common cause failure of both normal operation components and safety systems components can be envisaged to occur, through internal or external impacts, it is necessary to have adequate NPP protection against them. This protection can be realised by two types of measures.

The first type are measures directed to reduce probability of SBO or loss of UHS scenarios (for instance via strengthening of external electrical power network capability to withstand extreme impacts or increasing of reliability of safety systems devoted to respond to loss of offsite power or loss of normal operation heat removal systems – see Chapter II of the common position).

The second type are measures devoted to increasing plant capability to respond to SBO or loss of UHS scenarios. Existence of technical and organizational measures of the second type in plant design is essential. These measures must ensure fulfilment of the fundamental safety functions (listed in Chapter II).

However, it should be noted that the reactor subcriticality is, as a rule, guaranteed within the SBO (loss of UHS) accident scenarios in new VVER designs, because after reactor scram actuation (automatically or performed by operator and never depending on power supply sources status), the provided subcriticality value is considered sufficient to continue to keep reactor against gaining the critical state even with taking into account its reactivity released in the course

of RI cooldown. Fuel subcriticality in fuel cooling pools is reliably guaranteed and does not require additional management measures.

Further, in the non-severe accident stage of SBO (loss of UHS) scenarios the physical barriers remain intact, thus no special measures are required to maintain the third fundamental safety function.

So, the point of interest for SBO (loss of UHS) scenarios is the 'technical and organisational means' which provide removal of heat from the reactor core and from the fuel storage.

Provision of heat removal from reactor core at the initial stage of SBO (loss of UHS) is achieved through heat transfer (usually, under natural circulation conditions) to steam generator (SG) boiler water. As the SG water boils off, the SG level decreases leading to reduction of heat removal from primary circuit and heating of the last one. In case where it is impossible to continue the heat removal through steam generators, the heat removal from core is carried out by primary medium discharging via pressurised relief valve. The overarching purpose of the accident management before accident evolves into severe stage is recovering of the means for core heat removal via SGs; in case of total station blackout the second and the most important goal is to maintain (recover) control over NPP parameters, which demonstrates delivery of the first fundamental safety functions condition.

The tasks performed when systems to provide heat removal from spent fuel pool (SFP) to the ultimate heat sink are inoperable are substantially more inertial when compared to the situation with the reactor installation; and NPP personnel have much more time to recover the heat removal capability(compared to reactor).

VVER Design features to cover specific BDBA/DEC

The following technical solutions can be used to overcome SBO (loss of UHS) scenarios:

- passive heat removal systems;
- specially designated batteries with large discharging period, specially designated hydro-electric power stations, gas-turbine power stations, etc.;
- mobile engineering means for accident management.

For example, the following technical solutions to overcome SBO (loss of UHS) scenarios are used in different VVER designs.

a) Reactor

The distinctive feature of the new VVER designs is application of passive heat removal systems (PHRS) to provide for basic safety functions at the initial period of BDBA with SBO (loss of UHS). There are two types of steam generator PHRSs: air-cooled (Novovoronezh-2 NPP with AES-2006-M and VVER-TOI in Russia, Kudankulam NPP with VVER-1000 in India) and water-cooled (Leningrad-2 NPP with AES-2006-P).

The air-cooled PHRS uses air as the UHS. The reactor residual heat is transferred through steam generators to steam-external air heat exchangers of the PHRS where the steam is condensed and returned to the steam generators. Cold air intake is in the lower part of the reactor building. Heated air conveys through air ducts on the dome of the containment to discharge deflector. If primary circuit is intact, the heat can be removed for considerable time without external water makeup. In case of leaky primary circuit, the heat removal is secured by joint operation of PHRS and 2nd stage hydro accumulators (2^{nd} stage hydro accumulators in case of Kudankulam VVER-1000 and AES-2006-M design and 2nd and 3rd stages hydro accumulators in case of VVER-TOI design).

The water-cooled PHRS in AES-2006-P design uses water stored in tanks on the top part of the containment. The evaporating water from the tanks to the atmosphere removes reactor residual heat in case of SBO. Heat removing capacity depends on the water inventory in the tanks (estimated time varies from 24 up to 72 hours, after that PHRS tanks need to be refilled by external source).

Regardless of passive system existence, mobile equipment is used to fulfil the safety functions in later accident stages. The AES-2006-M (Novovoronezh-2 NPP) design is complemented with the following additional engineering means on BDBA management: alternative air-cooled diesel-generator; alternative intermediate circuit with air cooling tower (closed type modular air-type cooling tower with fans); mobile pump unit for water supply from external sources; cables; additional pipelines for mobile equipment connection to and for coolant circulation organization.

The equipment mentioned above is used in accompany with active safety systems equipment: fuel pond cooling system pump; emergency boron injection system pumps; fuel pond cooling system heat exchanger; ECCS heat exchanger; their related systems pipelines.

In AES-2006-P (Leningrad-2 NPP) the I&C power supply design, in the event of SBO, is provided with a separate power supply system for BDBA management which includes 2 trains. In each train, there is the same set of equipment: 24 hours batteries; mobile diesel-generator (up to 72 hours or more providing fuel supply is secured).

During normal operation, this system is connected to two of the four trains of emergency power supply system. Also, these additional devices to backup the makeup function of the spent fuel pool, emergency heat removal tanks and primary circuit are envisaged in AES-2006-P design: mobile high-pressure diesel and pumping units to be connected to special pipelines cut in bypass of the existing safety systems.

All of the above mentioned mobile equipment is located at the designated place on-site that is protected from external events. In both air and water cooled designs the normal power supply diesel-generators could be used to overcome SBO (as a BDBA ‘technical means’).

b) Spent fuel pool

In new VVER designs (Novovoronezh-2 NPP, Leningrad-2 NPP, etc.) passive systems for spent fuel pool heat removal are not envisaged. In case of SBO initially heat removal can be conducted via warming up and evaporation of the pool water inventory. Afterwards heat removal from SFP can be delivered by usage of mobile technical means.

The following considerations should be taken into account in regard of such systems:

a. The 'technical means' intended to overcome SBO (or loss of UHS) scenarios shall be as independent as possible from the normal operation systems and safety systems delivering power supply and heat removal during normal operation and design basis accidents;
b. Length of actuation period acceptance criteria for systems envisaged for BDBAs/DECs management of SBO or loss of UHS types. The time interval shall not exceed the time period that the natural processes related to coolant heating and boiling-off (in SGs, in primary circuit and spent fuel cooling pools) can prevent the accidents to evolve into the severe condition. Usually, such period of time shall not exceed a few hours in situations where reactor installations are concerned and a significant number of hours in situations with spent fuel cooling pools (available time is determined in accordance with the relevant calculations of different BDBA's before the fuel damage in the reactor and in the spent fuel pool exceeds the prescribed limit). During calculation of time for the systems (equipment) actuation, the time interval required for organization of personnel transfer to the location of the mentioned systems (equipment), the necessity to clear the transportation routes and the time period for equipment transportation to the deployment and connection place is to be taken into consideration;
c. The anticipated technical means and organisational measures should be sufficient to provide for the function of heat removal from the fuel with no time limitation (for water consuming systems – such as watery PHRS – the measures on inventory make-up are to be envisaged; for fuel-operated systems – such as diesel generators and power-driven pumps – the measures on compensation of the fuel reserves are to be introduced). The potential measures aiming to counter the negative effects arising at the prolonged periods of time only are to be addressed. For example, under the incapacity of reactor coolant pump (RCP) sealing for long-term (above 24 hours) retaining of leak tightness in case of high temperatures at primary circuit, the measures on RCP sealing cooling or measures on primary circuit temperature reducing are to be considered.

Introduction of redundancy for the ultimate heat sink should be considered in the NPP design.

Common Position

The member-states consider as principal the following aspects of the 'engineering means' and organisational measures envisaged by NPP's designs and directed at management of accidents with total SBO or in case of loss of systems on heat removal to the ultimate heat sink:

1. The engineering means, which are applied to the management of the BDBAs/DECs of SBO type or loss of UHS type, should be independent as much as practicable from normal operation systems and safety systems. This means they are:

   a) functionally and physically isolated from the normal operation systems and safety systems (as far as this practically possible) with the purpose of ensuring that failure of the least ones never results in failure of engineering means applied for management of accidents with SBO or loss of UHS;

   b) protected from external impacts, including the secondary effects of such external impacts. For instance an earthquake may lead to collapse of non-seismic structures and, consequently, 'engineering means' on BDBAs/DECs management are to be located in a place protected from potential influence of the mentioned destruction fragments. The bunker placement or allocation over a distance from buildings and building structures can be considered;

2. Actuation period for systems envisaged for BDBAs/DECs management of SBO or loss of UHS types should take into account the time interval required for organization of personnel transfer to the location of the mentioned systems (equipment), the necessity to clear the transportation routes and time period for equipment transportation to the deployment and connection place and should not exceed the critical value to be defined in the design;
3. The number of 'engineering means' and organisational measures for management with BDBAs/DECs of SBO or loss of UHS type should be sufficient at multi-unit NPP to cover these types of accidents occurring at all NPP units simultaneously, since the plant states considered for each unit may be different;
4. The anticipated 'engineering means' and organisational measures should be sufficient to provide the long term heat removal from nuclear fuel. The potential measures aimed to counter the negative effects arising from prolonged time periods should be addressed in the NPP design;
5. The 'engineering means' for BDBAs/DECs management should be considered as safety related systems, structures and components in the NPP design;
6. The points for connection of the 'engineering means' provided for BDBAs/DECs management with the operating equipment should be defined in the NPP design. It is important to demonstrate that the specified places are protected from hazards

initiating the necessity of its use.

The following design solutions contribute to achieving the high level of NPP safety in case of emergency scenarios of SBO type or loss of UHS type:

1. Application of passive heat removal systems should be considered as 'engineering means' for the delivery of reactor fuel heat removal;
2. Application of specially designated batteries with large discharging period should provide the additional possibility for monitoring the status of the fundamental safety functions along with the implementation of some accident management actions (etc., power restoration);
3. 'Measures' facilitating the restoration of offsite power (hydro-electric power stations, gas-turbine power stations, etc.) should be considered in the NPP design;
4. Introduction of redundancy for the ultimate heat sink should be considered in the NPP design.
5. Application of mobile engineering means for accident management should be considered as a 'measure' to ensure NPP safety in course of SBO or loss of UHS scenarios.

IV. EMERGENCY PREPAREDNESS AND RESPONSE

Context

The Fukushima Daiichi NPP accident demonstrated the vulnerabilities in emergency management. The releases of radioactive materials contaminated extensive regions around the Fukushima. The accident also resulted in the widespread evacuation of the local population, restricted the use of large areas of land for food production, fishing and put other restrictions on industrial activity in the local community.

The Fukushima Daiichi NPP accident revealed that all aspects of emergency preparedness and response should be properly considered at the design stage of NPP. Also, severe environmental conditions and possible degradation of the regional infrastructure that may occur in a Fukushima-like accident may impact the emergency preparedness and response.

Discussion

The initial mitigation actions were taken according to TEPCO's abnormal operating procedures and an Emergency Response Centre (ERC) was established at Fukushima Daiichi around 15 minutes after the earthquake took place. The ERC was located in a seismically isolated building, which was equipped with an autonomous electrical supply and ventilation systems with filtration devices. The building was constructed as a result of lessons learned from the experience of the Kashiwaziki-Kariwa NPP following the Niigata-Chuetsu-Oki earthquake in 2007. The ERC enabled the mitigation actions to continue at the site during the response to the accident [11].

Emergency plans should take into account all type of hazards on the site that may be encountered an accident situation, not only those limited to reactor installations but also including spent fuel pools, on-site spent fuel storage facilities and radioactive waste management and storage processes and other nuclear facilities as well as dangerous radioactive transport operations.

Emergency plans need to consider all harsh on-site environmental conditions including high radiation levels under which the response actions should be implemented. The accessibility and habitability of the control room, the emergency response centre, and the local control points (locations for necessary manual actions, sampling and possible repair works) need to be adequately protected against internal and external hazards. Suitably shielded and protected spaces to house necessary personnel in severe accident conditions should be considered for VVER plants.

In addition to the structures and fixed equipment ensuring the safety functions, the design of the reactor and the spent fuel pool should allow for the recovery of fundamental safety functions by mobile means in case of loss of safety functions in most of the reactor and spent fuel pool states. The implementation of these measures should be independent, as far as practicable, from non-mobile means, and the access to appropriate locations to implement these measures should be possible in due time.

In the first days after the Fukushima Daiichi NPP accident, there was an absence of real time information on the plant conditions and the environmental monitoring system failed due to damage caused by earthquake and tsunami indicating the need for hardened instrumentation, communication to provide necessary information for on-site and off-site response and for early off-site monitoring capability [11].

Instrumentation and controls should be designed and installed in the reactor building and the spent fuel pools to survive accident conditions. The reliability and functionality of releases measurements, radiation level measurements and meteorological measurements should be strengthened in the design. Power supply to these instruments should be made available for long term during prolonged SBO conditions. Assurance of the readiness to take samples and to analyse them in a laboratory should be considered.

Extensive damage of the transport infrastructure occurred due to the earthquake and tsunami, in addition there was insufficient pre-planning affecting the effectiveness of mitigation activities

and emergency response. Access to outside resources and off-site communications dependent on the local telecommunication network were also severely disrupted, although the TEPCO in-house communications network between the site and headquarters had mostly been intact [3, 11].

The reliability and functionality of the on-site and off-site communication systems need to consider conditions relating to internal and external hazards.

There were no coordinated arrangements for responding to a nuclear emergency and a natural disaster occurring simultaneously. Consequently, this was also not addressed in relevant training and exercise programmes. These simultaneous circumstances were not considered in the emergency plans, with a consequence that the emergency response organization became overwhelmed, and many mitigatory actions could not be carried out in a timely manner [3, 11].

During their training and exercises the response personnel had not been faced with such severe conditions in terms of environmental conditions and other circumstances (multi-unit issue, lack of technical resources) or such a difficult technical scenario in the reactor units.

Some of these issues could be better exercised with severe accident simulation capabilities, which could provide insights into the management of some of such situations.

The delivery of equipment, resources and supplies to the site was hampered due to many problems. Fear of contamination from radioactive material deposited on vehicles impeded the transport of supplies necessary for the response. On-site emergency workers encountered problems in obtaining authorization from the police to travel on roads leading to and from the site [11].

Severe environmental conditions and possible degradation of the regional infrastructure that may occur in a Fukushima-like accident may impact the emergency preparedness and should be considered in the emergency planning. On multi-unit sites, the plant should be considered as a whole in safety assessments and emergency management and interactions between different units need to be analysed. External events that may affect several units should be identified and included in the analysis. Events that may simultaneously affect several units should be explicitly considered in the emergency preparedness.

In Fukushima the response actions were hindered by the inappropriate quality and number of protective means and measures for emergency workers. There were insufficient personal protective equipment and personal dosimeters to carry out the response actions. The strategy for sheltering the emergency workers was not detailed in the plant procedures and the on-site emergency centre had to be used for that purpose, which also hampered the coordination and direction of response activities.

VVER Design Features for Emergency preparedness and response

As the topics discussed above involve both design aspects and site-specific/licensee-specific provisions, the regulators are still evaluating the design and organisational provisions which are normally part of the arrangements for commissioning of the plant.

Common Position

The following items on emergency preparedness and response related to the Fukushima Daiichi NPP accident should be taken into account for VVER plants:

- The emergency plans should be comprehensively prepared and also their practical implementation should be periodically demonstrated via full-scope exercises.
- Training facilities should be extended to cover severe accident scenarios in order to support the preparedness of the personnel and improve the realistic character of emergency exercises.
- The roles and responsibilities of all organizations involved in emergency management and response should be clearly identified and periodically checked during drills and exercises with special regard to interfaces and coordination between the on-site and off-site planning and organization issues.
- The accessibility and habitability of the control room, the emergency response centre, and the local control points (locations for necessary manual actions, sampling and possible repair works) need to be adequately protected against internal and external hazards. Suitably shielded, protected and habitable spaces to house necessary personnel in severe accident conditions should be considered for VVER plants. The accessibility of the local connected point for the mobile facility that used to mitigation the accident in environmental extremes should be considered.
- In the emergency plans and procedures more emphasis should be provided on the protection of emergency workers in terms of provision of protective equipment and emergency dosimeters in appropriate number and of relevant strategies and procedures to avoid any unjustified risks during the response.
- Instrumentation and controls qualified for accident conditions should be designed and installed to support the accident management measures by controlling the reactor and the spent fuel pools status.
- The reliability and functionality of the on-site and off-site communication systems, equipment measuring radioactive releases, radiation levels and meteorological conditions need to be ensured, taking into account conditions related to extreme internal and external

hazards.

- On-site emergency plan, procedures and guidelines should cover long term and multi-unit aspects.
- Severe environmental conditions and possible degradation of the regional infrastructure that may occur in a Fukushima-like accident may impact the emergency preparedness and should be considered in the emergency planning.
- For multi-unit sites, the plant should be considered as a whole in safety assessments and emergency management and interactions between different units need to be analysed. External events that may simultaneously affect several / all units should be explicitly considered in the emergency preparedness.

REFERENCES

1. J. M. Mattéi, E. Vial, V. Rebour, H. Liemersdorf, M. Türschmann, "Generic Results and Conclusions of Re-evaluating the Flooding in French and German Nuclear Power Plants, Eurosafe Forum 2001.

2. IAEA, "Mission Report: Preliminary Findings and Lessons Learned From The 16 July 2007 Earthquake at Kashiwazaki-Kariwa NPP", 6-10 August 2007.

3. IAEA, "The Great East Japan Earthquake Expert Mission, IAEA International Fact Finding Expert Mission of the Fukushima Dai-Ichi NPP Accident Following The Great East Japan Earthquake and Tsunami," 24 May-2 June 2011.

4. North Anna Earthquake Summary, USNRC web page http://www.nrc.gov/about-nrc/emerg-preparedness/virginia-quake-info/va-quake-summary.pdf

5. TEPCO, "Fukushima Accident Analysis Report," June 2012.

6. Toshiaki SAKAI et al, "Development of a Probabilistic Tsunami Hazard Analysis in Japan," ICONE 14, Florida, USA, July 2006.

7. Japan Society of Civil Engineers, "Tsunami Assessment Method for Nuclear Power Plants in Japan," 2002.

8. Site Survey and Site Selection for Nuclear Installations, IAEA, № SSG-35, 2015.

9. Safety of Nuclear Power Plants: Design, Specific Safety Requirements No SSR-2/1. Vienna, IAEA, 2012.

10. IAEA Safety Glossary: Terminology Used in Nuclear Safety and Radiation Protection, 2007 Edition. Vienna, IAEA, 2007.

11. IAEA: "The Fukushima Daiichi Accident Technical Volume 3/5 Emergency Preparedness and Response," August 2015.

12 ROSATOM web page http://www.rosatom.ru/upload/iblock/4c2/4c287b01028620e7f17ee1b50f8c93af.pdf (booklet ATOMENERGOPROECT "VVER-TOI Design")

13. ROSATOM web page http://www.rosatom.ru/upload/iblock/0be/0be1220af25741375138ecd1afb18743.pdf (booklet ROSATOM overseas "The VVER today")

AREAS FOR FUTHER STUDIES BY VVERWG

Based on the issues explained above, the VVERWG will consider some technical issues in VVER designs in greater depth to gain a better understanding on what are possible differences between different VVER evolutions (VVER-1000/AES-92, VVER-1200/AES-2006-M, VVER-1200/AES-2006-P, VVER-TOI) in light of their influence to the safety and to highlight possible recommended practices.

The appendices will be published as they are finalised by technical experts' subgroups in charge of them respectively.

LIST OF ACRONYMS AND ABBREVIATIONS

AERB	**:**	Nuclear Regulatory Body in India
AT	**:**	Accumulator Tank
BDBA	**:**	Beyond Design Basis Accident
DBA	**:**	Design Basis Accident
DC	**:**	Direct Current
DEC	**:**	Design Extension Condition
DiD	**:**	Defense in Depth
CC	**:**	Core Catcher
CCF	**:**	Common Cause Failure
CDF	**:**	Core Damage Frequency
ECCS	**:**	Emergency Core Cooling System
ERC	**:**	Emergency Response Centre
HAEA	:	Nuclear Regulatory Body in Hungary
HVAC	:	Heating, Ventilation and Air Condition
INES	:	International Nuclear and Radiological Event Scale
I&C	:	Instrumentation and Control
LRF	:	Large Release Frequency
NNSA	:	Nuclear Regulatory Body in China
NPP	:	Nuclear Power Plant
PGA	:	Peak Ground Acceleration
PSA	:	Probabilistic Safety Assessment
PHRS	:	Passive Heat Removal System
RCP	:	Reactor Coolant Pump
RI	:	Reactor Installation
Rostechnadzor	:	Nuclear Regulatory Body in Russian Federation
SSC	:	Structures, Systems and Components

SBO	:	Station Blackout
SFP	:	Spent Fuel Pool
SG	:	Steam Generator
STUK	:	Nuclear Regulatory Body in Finland
TAEK	:	Nuclear Regulatory Body in Turkey
TEPCO	:	Tokyo Electric Power Company
UHS	:	Ultimate Heat Sink
VVER	:	Water Moderated, Water Cooled Power Reactor

CONTRIBUTORS TO DRAFTING AND REVIEW

Zhou J.	NNSA, China
Kavimandan S.	AERB, India
Köse S.	TAEK, Turkey
Lankin M.	SEC NRS, Russian Federation
Neretin V.	OECD/NEA
Petőfi G.	HAEA, Hungary
Rogatov D.	SEC NRS, Russian Federation
Salo P.	STUK, Finland