MDEP Design-Specific Common Position CP-APR1400WG-01

APR1400 Working Group's activities

COMMON POSITION ADDRESSING FUKUSHIMA-RELATED ISSUES

Participation

Regulators involved in the MDEP working group discussions:	Republic of Korea, United Arab Emirates, United States
Regulators which support the present common position:	Republic of Korea, United Arab Emirates, United States
Countries with no objection:	All
Countries which disagree:	None

Multi-National Design Evaluation Programme

APR1400 Working Group

COMMON POSITION ADDRESSING FUKUSHIMA-RELATED ISSUES

Introduction:

The MDEP APR1400 Working Group (APR1400WG) members, referred to herein as "regulators," consist of members from Republic of Korea, United Arab Emirates, and the United States. A main objective of MDEP is to encourage convergence of code, standard and safety goals with exploring the opportunities for harmonization of regulatory practice and cooperation on safety review of APR-1400 specific designs. This common position addressing is aimed at sharing knowledge, information and experience on safety improvement related to lessons learned from the Fukushima Daiichi accident or Fukushima-related issues amongst APR-1400 WG member states to achieve the MEDP goal.

Because not all of these countries have completed the regulatory review of their APR1400 applications yet, this paper identifies common preliminary approaches to address potential safety improvements for APR1400 plants, as well as common general expectations for new nuclear power plants, as related to lessons learned from the Fukushima Daiichi accident or Fukushima-related issues. While some asymmetry exists among those of three countries in terms of design, regulatory practice and licensing milestone sharing information and common understanding on post-Fukushima enhancement would be promote resilient design for countering beyond design extreme external event like Fukushima nuclear disaster.

This common position paper aims at identifying characteristics of post-Fukushima enhancements putting in place by each countries and setting common position to achieve balanced and harmonized APR-1400 design. After the safety reviews of the APR1400 design applications that are currently in review are completed, the regulators will update this paper to reflect their safety conclusions regarding the APR1400 design and how the design could be enhanced to address Fukushima-related issues. The common preliminary approaches are organised into five sections, namely, external hazards, reliability of safety functions, accidents with core melt, spent fuel pools, and emergency preparedness in design, supplemented by appendices related to areas where further studies were identified as necessary.

Context:

It is generally understood that Fukushima Daiichi catastrophic events caused the failure of consecutive layers of defence concurrently, which has not taken into account in design and safety management process of nuclear power due to extremely low frequency of occurrence. Fukushima Daiichi accident became a wakeup call for enhancing situation awareness of countering Fukushima typed beyond design basis external events.

After the Fukushima Daiichi accident, each country has made much efforts to identify vulnerabilities, to develop the strategic plan for enhancing resilience against severe accidents induced from beyond design basis external event through the full spectrum of design, operation and institutional arrangement including to establish regulatory provisions, education and training program, and physical and hardware enhancement.

A severe accident involving several units took place in Japan at Fukushima Daiichi nuclear power plant (NPP) in March 2011. The immediate cause of the accident was an earthquake followed by a tsunami coupled with inadequate provisions against the consequences of such events in the design. Opportunities to improve protection against a realistic design basis tsunami were not taken.

As a consequence of the tsunami, safety equipment and the related safety functions were lost at the plant, leading to core damage in three units and subsequently to large radioactive releases (INES 7).

Several studies have already been performed to better understand the accident progression and detailed technical studies are still in progress in Japan and elsewhere. In the meantime, on-going studies on the behaviour of NPPs in very severe situations, similar to Fukushima, seek to identify potential vulnerabilities in plant design and operation; to suggest reasonably practicable upgrades; or to recommend enhanced regulatory requirements and guidance to address such situations. Likewise, agencies around the world that are responsible for regulating the design, construction and operation of APR1400 plants are engaged in similar activities.

Background information:

The Fukushima Daiichi accident demonstrates the importance of reinforcing the Defence-in-Depth principle, correctly identifying the external hazards, their magnitude, their credible combinations and the design provisions to protect the installation. This should be reflected in licensing requirements, detailed in the installation safety case and 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 safety factors. In the safety assessment, specific consideration needs to be given to both multi-unit sites and to address long-term measures protecting the plant.

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 indeed any other industrial facility). However, a robust design based on Defence-in-Depth 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 licensing basis).

The design, construction, manufacturing and installation of structures, systems and components should rely on state of the art engineering measures and sufficient margin beyond the design criteria required for a design basis accident to avoid **cliff edge effects**[1]. Such an approach will help to ensure an appropriate response, should a beyond design basis accident occur. Provisions aiming at facilitating the repair/recovery of impaired safety functions should also be considered.

[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:

EVOLUTIONARY IMPROVEMENTS IN SAFETY

I. The Fukushima Daiichi accident confirms the relevance of the general safety objectives that have been considered for Generation III reactors, such as the APR1400 (lower probability of core melt, limitation of releases, management of severe accident situations…).

As compared to most current operating reactors, the APR1400 reactor contains additional safety measures. For example, there are four redundant and independent trains of safety injection systems to which two emergency diesel generators are equipped, including one alternate AC diesel generator and one mobile generator. For the Barakah 1&2, Barakah 3&4 and SKN 3&4 APR 1400 plants, one alternate AC diesel generator and one mobile generator are shared between two units. There are also systems to provide for severe accident management and protection against external events such as earthquakes and flooding. Total loss of main heat sink is also one of the design bases of the plant.

HAZARDS

II. While acknowledging 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, to date regulators who have made safety findings in the review of their APR1400 design applications, find that the safety systems of the generic APR1400 are designed to cope with design basis external and internal events, mostly by applying adequate physical separation and protection against dynamic loads.

The accident at Fukushima Daiichi has reinforced the need to undertake, as part of the safety review process for APR1400 nuclear power plant applications, a comprehensive analysis of external hazards, including consideration of relevant combination of events.

RELIABILITY OF SAFETY FUNCTIONS

III. It is observed to date, from those regulators who have made safety findings in the review of their APR1400 design application, that since most APR1400 safety functions depend on electric power that the APR1400 reactors could suffer cliff-edge effects after a few hours following a Fukushima-type beyond design basis external hazard, with accompanying common cause failures. Those regulators acknowledge that safety improvements have been proposed to address those situations. Continued discussions, detailed design, and analysis will be needed to make final approvals of these improvements.

The key safety functions that should be protected are reactivity control, reactor and spent fuel pool cooling and confinement of radioactive material. Most safety functions of APR1400 depend on electrical power, hence high reliability of power supplies is essential. This high reliability is expected to be achieved through an adequate combination of redundancy and diversity.

Ensuring adequate protection, through appropriate design, plant layout, electrical and physical separation and segregation, electrical isolation, etc. of the power supplies against infrequent and severe external hazards is a lesson from the Fukushima Daiichi accident.

Other actions for increasing the reliability of AC power supply at an APR1400 plant should be considered such as provisions of long-term fuel and lubricating oil reserves for all emergency power units at the site and ensuring the possibility of using mobile power supply units.

In spite of the reliability of the power supplies, as part of the Defence-in-Depth approach for APR1400 plants, a mitigation strategy for long term loss of electrical power is needed for all reactor states for an adequate length of time. Example of arrangements used in such strategies are enhanced capacity of some critical power sources, the possibility of providing sufficient electrical power through mobile means and/or the use of permanently installed power sources sufficiently independent and adequately protected from external and internal hazards, including infrequent and severe external hazards. The fail-safe status of safety related equipment in case of loss of power supply should be considered in the design taking into account possibly contradicting requirements.

The Defence-in-Depth approach needs to be applied also to the ultimate heat sink. The design of new nuclear power plants needs to provide diverse means to ensure reactor and spent fuel cooling. The use of a secondary ultimate cooling water system is an example of diverse means to provide reactor and spent fuel cooling for decay heat removal in case of unavailability of the primary cooling chain. Other ways of strengthening Defence-in-Depth are e.g. by providing portable means to inject water into the steam generators, reactor coolant system, and make-up water into the spent fuel pool.

ACCIDENTS WITH CORE MELT

The Fukushima Dai-ichi accident confirms the lesson learnt already from earlier NPP accidents that potential accidents leading to a core melt need to be considered in the design of NPPs. Safety features which ensure the adequate integrity of the containment in case of an accident leading to a core melt need to be included in the design. These features need to have adequate independence from the other provisions of the plant and they should also be effective in case of external or internal hazards. Essential containment design principles related to the Fukushima accident deal with provisions to avoid over pressurisation (relying for example on containment venting and/or containment spray systems), hydrogen management and ultimate pressure strength in such accidents. Consideration should also be given to the possibility of hydrogen combustion outside the containment.

IV. The regulators recognise that the generic APR1400 design includes measures to mitigate the consequences of severe accidents. The APR1400 design benefits from reinforced measures to prevent accident situations such as high pressure core melt, direct containment heating, steam explosions, molten corium concrete interaction, and hydrogen detonation. Nevertheless, as some severe accident management systems rely on AC and direct current (DC) power, at least after a few hours, regulators recognise the need to reinforce existing or proposed provisions to increase the time *available before cliff-edge effect. Due consideration to those cliff edge effects is to be given while tailoring long term loss of electrical power mitigation strategies.*

Spent fuel pools

The Fukushima Dai-chi accident also highlighted the need to fully consider safety in the design of spent fuel pools. This implies that single initiating events, multiple failure events, internal hazards as well as external hazards should be properly addressed. In particular, the structural integrity of the spent fuel pools needs to be ensured with adequate margin in case of external hazards.

Both the Defence-in-Depth approach and the prevention of accidents with early or large releases are fully applicable for fuel storage pools. To achieve a safe outcome, it is essential to ensure the integrity of the spent fuel pools, and to maintain sufficient water level in the pools by establishing makeup water in adequate time in order to prevent fuel failure.

Emergency preparedness in design

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 APR1400 plants.

In addition to the structures and fixed equipment ensuring the safety functions, consideration should be given to utilisation of mobile means for restoring safety functions. 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.

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

Instrumentation and controls should be designed and installed in the reactor building and the spent fuel pools to enable and support the accident management measures (refer to appendix 2).

Severe environmental conditions and possible degradation of the regional emergency response 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.

As these topics 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.

AREAS FOR FUTHER STUDIES BY APR1400WG

Based on the issues explained above, the APR1400WG decided to consider some areas in APR1400 design in greater depth to gain a better understanding on what are possible differences, if any, between different APR1400 evolutions (like Shinkori 3 & 4, Barakah 1 & 2, Shin Hanul 1 & 2, US-APR1400) in these particular areas of design and to highlight possible recommended practices.

The following areas for further studies were also identified:

- arrangements for long-term loss of electrical power (supplies and distribution systems) to ensure long term decay heat removal (Appendix 1);
- reliability and qualification of severe accident management instrumentation (Appendix 2);
- management of pressure in containment during severe accidents (Appendix 3);
- long-term cooling of spent fuel pool; reliability of cooling and makeup water systems, instrumentation and hydrogen management (Appendix 4);
- management of primary circuit residual heat removal and sub-criticality (Appendix 5).

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

APPENDIX 1: LONG-TERM LOSS OF ELECTRICAL POWER

Definition

Long-Term Loss of Electrical Power (LTLEP) - A prolonged loss of all alternating current (AC) and/or direct current (DC) power sources in nuclear power plants which are used to help provide the safety functions of reactor core cooling, sub-criticality, containment, and spent fuel pool cooling.

Discussion

On March 11, 2011, the Fukushima Daiichi nuclear power plant experienced a large seismic event followed by a significant tsunami. The tsunami inundated many of the facilities at the plant, including many of the electrical power systems. As a result of the earthquake and tsunami, Fukushima Daiichi experienced a loss of all AC power for all units except Unit 6, which had one air-cooled diesel generator still available. DC power was lost at Units 1 and 2 due to the tsunami, and it was subsequently lost at Units 3 and 4 at a later time due to the inability to recharge the batteries. As a result of the LTLEP, core damage was experienced in Units 1, 2, and 3. The Unit 4 reactor core was off-loaded into the spent fuel pool, which maintained its integrity, and sufficient cooling was provided to the spent fuel pool due to the existing volume of water and water addition by emergency responders.

While nuclear power plants typically have redundant and multiple sources of electric power, the LTLEP at Fukushima Daiichi illustrates the consequences when a CCF of electrical power supplies occurs. Regulators around the world are currently looking at means to update requirements and guidance to ensure LTLEP conditions are sufficiently planned and mitigated. The design is actively being reviewed in the Republic of Korea, United Arab Emirates, and the United States.

Addressing requirements and guidance to address LTLEP requires expertise from various technical disciplines, expertise from regulators and the industry, and careful consideration of all aspects of plant safety. The common positions, recommendations, and comments are primarily applicable to the APR1400 new reactor design, but the information is also applicable to other new reactor designs, and to a lesser extent, operating reactors. Specific common positions for the APR1400 design are identified within this document.

New APR1400 Reactor Common Positions for LTLEP

I. Defence against LTLEP should maintain the following key safety functions: (1) reactor core cooling, (2) reactivity control, (3) confinement of radioactive material, and (4) spent fuel pool cooling.

In the event of an LTLEP, it is critical that decay heat from the reactor core be removed, the reactor remains sub-critical, containment integrity is maintained (including necessary heat removal and pressure reduction) in the event radiological material is released from the core, and the spent fuel pool continues to be cooled. The highest priority will be reactor cooling at the onset of an event since containment is not critical so long as fuel clad and reactor coolant system integrity is maintained. Spent fuel pool cooling will not become critical for several hours after initiation of an LTLEP due to the volume of water in the pool (provided spent fuel pool structural integrity is maintained).

II. New reactor designs should incorporate multiple layers of defence-in-depth to protect against an LTLEP for all modes of operation. Layers of defence against an LTLEP will typically involve robust, permanently-installed equipment, robust and separately located mobile equipment, and adequately trained personnel and resources to implement defence in a timely manner. New reactor designs should have an assessment of the levels of defence-in-depth for an LTLEP. Such an assessment should consider (1) permanent and mobile equipment relied upon, (2) protection of such equipment against external and internal events, (3) capability of the equipment to provide key safety functions, (4) capability of personnel to utilise the equipment in the time required, and (5) transition to other layers of defence when one layer of defence is not available.

An LTLEP may be a result of an external or internal event, whose cause, duration, and extent may be difficult to predict and measure. It is important for new reactor designs to incorporate, to the extent practical, design features and procedural actions to provide multiple layers of defence against an LTLEP. These provisions should address LTLEP common-cause failure sources such as flooding, failures of electrical switchgear, or fires. Design, planning, and preparation for an LTLEP will greatly assist responders in the unlikely occurrence of such an event. The value of planning and preparing for an LTLEP is for plant operators to consider factors that would affect their ability to maintain key safety functions. Response to an LTLEP will require a combination of installed plant features, procedures, knowledgeable plant personnel, additional equipment onsite and/or offsite, and offsite resources. It is important for plant operators to understand the capabilities of their equipment and personnel, means to access reliable plant status/information, required timing for actions, potential impediments to perform the actions, and how to coordinate multiple activities.

III. The design of the plant against external and internal events is critical to protect against LTLEP.

Proper siting and design of the nuclear power plants against external events such as earthquakes and floods will greatly improve their capability to avoid an LTLEP. As demonstrated by other nuclear power plants in Japan that experienced the same tsunami but did not experience an LTLEP, the siting, design, and construction of a facility greatly affects the outcome of such an external event. Similar conclusions can be drawn for internal events as well.

IV. Equipment that is used in the various layers of defence should be adequately protected and qualified against potential hazards and events, including provisions for sufficient testing and maintenance.

Various hazards and events could disable multiple sources of electrical power such as flooding, fires, and explosions resulting from internal or external events. NPPs are designed to withstand such events but there remains a remote likelihood that such events could exceed the design of one or more safety systems within the plant. To protect equipment against events that are beyond the design basis of the plant, it is important to design and locate additional equipment such that a single event would not disable multiple layers of defence. Qualification should consist of in-depth design, testing, and operational follow-up to demonstrate the ability of the equipment to provide high confidence that they will operate effectively when required under design basis conditions. Equipment should at least be protected to the same degree as main line safety systems, but depending on strategy taken (types and location of equipment) additional protection may be necessary.

V. The LTLEP mitigation strategy (including layers of defence and protection of equipment) is dependent on generic design aspects as well as site dependent variables based on types of external events that may occur.

The mitigation strategy should be tailored to capability of the generic design coupled with site specific characteristics. For example, a plant located in a desert region and not near any large water sources is less likely to experience significant flooding as compared to a plant near a coast that has a history of tsunamis. However, the plant located in the desert may experience other events such as sandstorms or extreme heat that the coastal plant is not expected to encounter.

VI. New reactors should consider support capability that could assist the LTLEP mitigation strategy.

Support for personnel and equipment include access to plant areas (including adequate lighting), spare parts, and communication (including capability to charge portable communication devices). For example, mitigation strategies should consider access through security doors, ability to obtain spare parts from storage systems that normally use electronic means of access and retrieval, and mobile means of communicating across the plant site as well as with external resources. Consideration for personnel protection should be included in the mitigation strategy.

VII. The balance of plant safety should be maintained when addressing LTLEP mitigation.

As mentioned earlier, NPPs are designed to withstand external and internal events that could lead to an LTLEP. The likelihood of a new reactor experiencing an LTLEP should be very low when compared to other events and hazards. Any mitigation strategies for LTLEP should be weighed against the mitigation of other events and hazards within the plant design to ensure that the balance of plant safety is not impacted by any design features, procedures, or training used to address LTLEP.

APR1400 Common Positions for LTLEP

I. To date, regulators[2] who have made safety findings on LTLEP have found that the APR1400 design appropriately accounts for external and internal events to make the likelihood of an LTLEP extremely low.

The original design of the APR1400 is robust against external events such as earthquakes, floods, and high winds, making the likelihood of an LTLEP from these events to be very low. The APR1400 design incorporates principles such as physical separation, barriers, and design margin to reduce the impact of internal events. Regulators and vendors and its customers have discussed the design capabilities of the APR1400 and additional design margin and features have been added to enhance the capability to mitigate Fukushima-like events.

II. To date, regulators that have made safety findings on LTLEP have found the approach of permanently installed and mobile means in the APR1400 design to address LTLEP to be acceptable. Continued discussions, detailed design, and analysis will be needed to make final approvals.

[2] NRC has not made this finding as the design is still under review as part of the design certification application review – as of April 1, 2016

Regulators[3] have reviewed the initial proposals by KHNP/KEPCO and its customers to address LTLEP for the APR1400 design. The proposals use permanently installed equipment and mobile means to provide multiple layers of defense against an LTLEP. Regulators will continue to review the proposals as licensing documentation, detailed design, equipment, and procedures are available. Regulators may require some changes to mitigating strategies.

[3] NRC has not made this finding as the design is still under review as part of the design certification application review– as of April 1, 2016

APPENDIX 2: RELIABILITY AND QUALIFICATION OF SEVERE ACCIDENT MANAGEMENT INSTRUMENTATION

General expectations regarding severe accident management instrumentation

The main objective of severe accident management is to maintain containment integrity and avoid containment bypass in order to limit, as far as possible, releases of radioactive material into the environment and consequences for the population. Several phenomena may indeed threaten containment integrity in case of core melt accident. In order to prevent these phenomena, particular safety features such as Passive Autocatalytic Recombiner (PAR) and Emergency Containment Spray Backup (ECSBS) have been implemented in APR1400 reactors. Nevertheless, these features are not sufficient to totally eliminate the risk of such phenomenon and operator actions have a key role in the management of the situation. Operating strategies should be adapted according to the accident progression. Therefore, instrumentation in severe accident is of the utmost importance to support the management for limiting releases into the environment. It is necessary to follow the accident progression in order to be able to predict possible future developments and to determine if the situation can be considered as stabilised.

It is expected that any instrumentation required to inform on decision making related to countermeasures shall be included in the design. Instrumentation shall be appropriately classified, adequately qualified for environmental conditions and it shall have reliability commensurate with the function that it is required to fulfil.
Severe accident instrumentation should be qualified to perform adequately for specified severe accident conditions and mission time.
Safety classification should be commensurate with the categorization of the function to be performed.

Overview of APR1400 severe accident I&C design

All APR1400 I&C designs have severe accident management functions which are considered beyond design basis or as design extension conditions in some member countries. The severe accident instrumentation and controls (SA I&C) are implemented in separate I&C systems for all APR1400 I&C designs, except the US APR1400 design. SA I&C functional requirements depend on the regulatory expectations in each member country. The SA I&C system performs monitoring and control functions required for severe accident management. Inputs are acquired directly from field sensors or from isolated outputs of the safety I&C systems. Outputs are sent to the drive control modules or the priority actuation and control system for component actuation. The drive control modules are provided to interface with the non-safety actuated equipment used for severe accident mitigation. The monitoring and service interfaces provide a communication path between the SA I&C and other I&C systems. Redundant gateways are provided to interface with the plant data network or bus.

APR1400 Common Position

The duty of the instrumentation is described in the APR1400 severe accident management guidelines:

The generic APR1400 design utilizes core exit temperature for entering severe accident management procedure.

- Severe accident monitoring variables include containment pressure and hydrogen concentration in the containment.
- Generic APR1400 design utilizes core exit temperature for entering severe accident management procedure.

The regulators recognize that all APR1400 designs include measures to prevent and mitigate the consequences of severe accidents. APR1400 designs employ a range of instrumentation to inform entry into a severe accident, monitor the accident progression, and support the management of the severe accident including assessment of threat to the containment. The instrumentation also provides information to support decisions for both on-site and off-site emergency response actions.

The licensees have made commitments to meet the regulators' expectations that the severe accident instrumentation and controls necessary to stay on the mitigation path, including their support systems, will be appropriately designed, qualified and protected for severe accident conditions.

The national regulators are currently considering their licensees' solutions and have yet to finalise their respective positions.

APPENDIX 3: PRESSURE MANAGEMENT OF CONTAINMENT DURING SEVERE ACCIDENTS

General expectations regarding containment integrity and reduction of radioactive releases in case of a severe accident

The importance of the integrity of the containment as a fundamental barrier to protect the people and environment against the effects of a nuclear accident is well established. In this regard, an essential objective is that the necessity for off-site counter-measures to reduce radiological consequences be limited or even eliminated. The design should provide engineering means to address those sequences which would otherwise lead to large or early releases[4], even in case of severe external hazards.

The plant shall be designed so that it can be brought into a controlled and stable state and the containment function can be maintained, under accident conditions in which there is a significant amount of radioactive material in the containment, i.e. resulting from severe degradation of the reactor core. It is expected that due consideration to these requirements is to be given while tailoring long term loss of electrical power mitigation strategies.

In order to reliably maintain the containment barrier, the regulators believe that:

- Safety features specifically designed for fulfilling safety functions required in core melt accidents shall be independent to the extent reasonably practicable from the SSCs of the other levels of defence;
- Safety features specifically designed for fulfilling safety functions required in core melt accidents shall be safety classified and or be able to survive for the core melt accident environmental conditions for the time frame for which they are required to operate. In light of the Fukushima Daiichi accident, the regulators believe that those safety features shall be designed with an adequate margin as compared to the levels of natural hazards considered for the site hazard evaluation;
- The systems and components necessary for ensuring the containment function in a core melt accident shall have reliability commensurate with the function that they are required to fulfil. This may require redundancy of the active parts;
- Containment heat removal, including corium cooling, during core melt accidents shall be provided;
- It shall be possible to reduce containment pressure in a controlled manner in the long term taking into account the impact of non-condensable gases;
- The strength of the containment including the access openings, penetrations and isolation valves shall be high enough to withstand, with sufficient margins to consider uncertainties, static and dynamic loads during core melt accidents (pressure, temperature, radiation, missile impacts, reaction forces). There shall be appropriate provisions to prevent the failure of the containment due to combustion of hydrogen.

[4] “**Large radioactive release**”: a release for which off-site protective measures limited in terms of times and areas of application are insufficient to protect people and the environment. “**Early radioactive release**”: release for which off-site protective measures are necessary but are unlikely to be fully effective in due time.

In order to reduce the release of radioactive substances, the regulators believe that the primary means should rely on provisions to minimise the amount of fission products in the containment atmosphere and to reduce the pressure inside the containment.

Main APR1400 design characteristics

The generic APR1400 design includes measures to mitigate the consequences of severe accidents. The APR1400 design includes measures to prevent accident situations such as high pressure core melt ejection, global hydrogen detonations, containment bypass, which would lead to large or early releases. The containment is designed to face a global hydrogen combustion taking into account the implementation of hydrogen recombiners that limit the hydrogen risk.

Nevertheless, as some severe accident management systems rely on AC and DC power, regulators recognise the need to reinforce existing or proposed provisions to increase the time available before loss of power would occur . Due consideration to this is to be given while tailoring long term loss of electrical power mitigation strategies (refer to appendix 1).

APR1400 Common Position

The regulators acknowledge that, following Fukushima accident, in case of extended loss of AC power and loss of ultimate heat sink, all vendors/utilities have provided measures to manage the pressure within the containment. Presently, the following solution has been proposed:

- Emergency Containment Spray Backup System (ECSBS) have been implemented to reduce the containment pressure with the external water supply and mobile pumps.

This proposed solution proposed is deemed as safety improvement to address severe accident situations combined with long term loss of electrical power. The solution is currently being considered by the national regulators who have yet to finalise their respective positions.

APPENDIX 4: LONG-TERM COOLING OF THE SPENT FUEL POOLS

Discussion

On 11 March 2011, the Fukushima Dai-ichi nuclear power plant experienced a large seismic event followed by a significant tsunami. The tsunami inundated many of the facilities at the plant, including many of the electrical power systems. As a result of the earthquake and tsunami, Fukushima Dai-ichi experienced a loss of all AC power for all units except Unit 6, which had one air-cooled diesel generator still available. DC power was lost at Units 1 and 2 due to the tsunami, and it was subsequently lost at units 3 and 4 at a later time due to the inability to recharge the batteries. As a result of the extended loss of electrical power, core damage was experienced in Units 1, 2, and 3.

The Unit 4 spent fuel pool contained the highest heat load of the six units with the full core present in the spent fuel pool and the refueling gates installed. However, because Unit 4 had been shut down for more than 3 months, the heat load was low relative to that present in spent fuel pools immediately following shutdown for reactor refueling. Following the earthquake and tsunami, the operators in the Units 3 and 4 control room focused their efforts on stabilising the Unit 3 reactor. During the event, concern grew that the spent fuel was overheating, causing a high-temperature reaction of steam and zirconium fuel cladding generating hydrogen gas. This concern persisted primarily due to a lack of readily available and reliable information on water levels in the spent fuel pools. Helicopter water drops, water cannons, and cement delivery vehicles with articulating booms were used to refill the pools, which diverted resources and attention from other efforts. Subsequent analysis determined that the water level in the Unit 4 spent fuel pool did not drop below the top of the stored fuel and no significant fuel damage occurred. The lack of information on the condition of the spent fuel pools contributed to a poor understanding of possible radiation releases and adversely impacted effective prioritisation of emergency response actions by decision makers. The Fukushima Dai-ichi nuclear power plant accident also highlighted the importance of appropriate safety in the design of the spent fuel pool and its associated systems, which should ensure their system structural integrity, subcriticality of the spent fuel under all conditions, adequate long-term cooling, and sufficient water level in the pools.

Addressing requirements and guidance for the SFP systems requires expertise from various technical disciplines, expertise from regulators and the industry, and careful consideration of all aspects of plant safety. The common positions, recommendations, and comments are primarily applicable to the APR1400 reactor design, but the information is also applicable to other new reactor designs, and to a lesser extent, operating reactors. Specific common positions for the APR1400 design are identified within this document.

New Reactor Common Positions for SFP

I. *The SFP should be designed to maintain the stored fuel covered following the effects of such natural phenomena as earthquake, tornado, hurricane, flood, tsunami, and seiches.*

   In the event of a natural phenomenon, the spent fuel pool must maintain its structural integrity in order to ensure the stored fuel coverage. The design of the SFP system should maintain the minimum water level which is needed to ensure radiation shielding and SFP cooling. The seismic design of the fluid retaining components should provide assurance that the SFP will maintain this minimum water inventory following an SSE. The fluid retaining components should be protected from internally and externally generated missiles.

II. *The SFP should be designed with adequate cooling capability to ensure the safe-storage of spent fuel.*

Under all conditions (normal operation or accident scenario) the stored fuel will continue to generate decay heat that must be removed. The SFP should have the capability to remove the decay heat and prevent fuel uncovery.

III. *The design should have the capability to provide make up water to the SFP.*

During normal operation and following an accident scenario, the decay heat generated from the stored spent fuel causes the SFP water to evaporate, even while the cooling system is in operation. The rate of evaporative losses increases when the cooling system is not in operation. Eventually, makeup water will be required, until cooling is restored. The SFP system should have the capability of providing makeup water to the SFP, the makeup water source, and the equipment necessary to transfer the makeup water should be of the proper design criteria in order to ensure its availability following all relevant external phenomena.

IV. *SFP shall have reliable water level indication*

During and following an accident scenario, the SFP should retain sufficient water inventory to ensure proper radiation shielding and SFP cooling such that no immediate action is required. In the early phase of most accident scenarios, the operator’s attention should focus on core cooling, assessing the scenario and taking the proper steps to stabilise the unit. If there is no reliable water level indications, like what happened during the Fukushima event, uncertainty of the SFP water level could divert attention and resources from critical operations to the SFP in order to verify pool levels.

The design of the SFP system should provide sufficiently reliable instrumentation to monitor the spent fuel pool water level from above the cooling suction elevation to the top of the stored fuel, which should include a primary instrument channel and a backup one. Both instrument channels should be independent from each other. The permanently installed instrument channels should be powered by a separate power supply. The installation of the water level instruments should be protected from falling debris. The instruments should be capable of withstanding design-basis natural phenomena and should also be reliable at temperature, humidity, and radiation levels consistent with the spent fuel pool water at saturation conditions for an extended period. The instrument shall be provided with backup power capability until outside power can be restored.

APR1400 Reactor Common Positions for SFP

I. *The SFP should be designed to maintain the stored fuel covered following the effects of such natural phenomena as earthquake, tornado, hurricane, flood, tsunami, and seiches.*

In the design of the APR1400 reactor system, the SFP is located inside the fuel building (FB). The FB is designed to provide protection against natural phenomenon including seismic events. In the design of the APR1400 reactor, the water level needed to operate the SFP cooling system is identified as the minimum safety water level[5]. The SFP fluid retaining surfaces are designed as seismic category I[6], in order to ensure that the SFP will maintain sufficient water inventory. Piping systems that connect to the pool above the minimum water level but reach below this level are designed as seismic category I, or are provided with an anti-siphon device to preclude SFP drain down. The SFP cooling system is designed as a safety related system, which means that the system is designed to remain operational following a seismic event. The system includes isolation capabilities at the boundaries between seismic classifications.

II. *The SFP should be designed with adequate cooling capability to ensure the safe storage of spent fuel.*

The APR1400 SFP cooling system (SFPCS) has been classified as a safety related system. The system is powered from safety related sources, which include diesel backup power generators. The seismic classification of the fluid retaining components ensures that sufficient water inventory is retained in the SFP to provide a means to cool the fuel in the event the SFPCS is not immediately available. The amount of time it would take to heat up the SFP water inventory is dependent on the heat load of the spent fuel stored in the pool. At maximum heat load conditions (full core offload) the reactor core is empty of fuel, therefore the protection of the SFP should be a priority.

III. *The design should have the capability to provide make up water to the SFP.*

The APR1400 SFP has several make up paths and water sources available, depending on the scenario, to replenish the SFP water inventory. These sources include both seismic and non-seismic qualified sources, with full seismic/safety related and non-seismic/safety related paths. Additionally, the fire protection system is also a possible makeup water source. The design of the APR1400 reactor also incorporates external cooling water hose connections, located at grade elevation level on the exterior of the fuel building, on opposite sides of the building, to attach a pumper truck or portable pump in order to provide make up water for the SFP.

IV. *SFP shall have reliable instrumentation*

The APR1400 SFP system design has two permanently installed, seismically qualified, safety-related wide range water level instruments which provide indication and warning to alert the operators in the main control room. Each level instrument has a range that spans from the top of the normal operating level to below the top of the spent fuel. These instruments are powered from safety related power and provided with backup battery power, in the event that safety related power is not available. The SFP level indication can be read at the control room and at the remote shutdown panel. The low-low SFP level signal will trip the SFP cooling system pumps to preclude unacceptable loss of water or damage to the pumps. In addition, the design of the

[5] For undergoing NRC design certification review, this minimum safety limit has not yet been identified. NRC staff is awaiting RAI response that should identify the limit – as of April 1, 2016.

[6] For undergoing NRC design certification review, the applicant has proposed to credit seismic II components to retain fluid boundary on the SFP. A request for additional information has been issued to resolve this matter – as of April 1, 2016.

APR1400 SFP system also includes instrumentation to monitor the SFP water temperature and the SFP area radiation level.

Overall, the design of the APR1400 SFP system has instrumentation to monitor the pool water level, water temperature, and area radiation level to provide indication of the degradation of decay heat removal capability and to warn personnel of potentially unsafe conditions in the SFP area.

APPENDIX 5:

MANAGEMENT OF PRIMARY CIRCUIT RESIDUAL HEAT REMOVAL AND SUB-CRITICALITY

Common Positions agreed on the APR1400 Reactor for the management of primary circuit residual heat removal and sub-criticality

Residual heat removal

In the context of this discussion, the scenario considered includes extensive loss of active safety systems, but does not include catastrophic failure of the major primary circuit pipework. It may include a small loss of coolant accident caused, for example, by failure of the reactor coolant pump seals or a break due to a small pipe connected to the reactor coolant system.

I. Maintenance of adequate primary circuit inventory is a key safety function that needs to be ensured on the APR1400 following an extreme event such as occurred at Fukushima.

Following a Fukushima-type event at the site of any APR1400 power plant, it is essential that decay heat from the reactor core should continue to be removed and that following a leak in the primary circuit, sufficient means remains available to ensure an adequate make-up capacity to the primary circuit.

II. It is essential that a means (either installed or mobile) is provided on the APR1400 to ensure adequate cooling and inventory make-up to the primary circuit.

There is a consensus amongst the regulators that at least one means needs to be provided to ensure adequate cooling and make-up in the APR1400 following the long-term loss of off-site power together with failure of the Emergency Diesel Generators (EDGs) and that it will be necessary to demonstrate that this means is functionally capable of achieving the key safety functions, even in case of severe and rare external hazards.

In the APR1400 design, there are potentially a number of options for ensuring adequate levels of cooling and inventory make-up of the primary circuit following the loss of off-site power together with failure of the EDGs. This includes:

External water source and mobile pumps are provided to inject cooling water into reactor coolant system and secondary system of APR1400.

UAE APR1400

For the UAE design, the license applicant was requested to provide an evaluation of lessons learned from the March 2011 accident in Japan’s Fukushima Nuclear Power Plant to determine the Barakah plant’s robustness to cope with extreme natural events, including events that might affect multiple facilities on the same site and to identify if any modification is necessary to strengthen safety.

The assessment resulted in 17 design and process enhancements including the following that relate to the mitigation of loss of primary circuit residual heat removal:

- Channel C & D, Class 1E, Battery Duty Extension from 8 hours to 16 hours
- EDGs and AAC DGs cross tie between Units,
- Installation of Mobile DG Connection on the outside of the Auxiliary Building
- Extension of Fuel Capacity of AAC DG Fuel Oil Storage Tank from 8 hours to 24 hours
- External Water Injection for Steam Generators
- External Water Injection for Reactor Coolant System

The conceptual designs for these enhancements and all others arising from the Fukushima lessons learned assessments were approved by FANR. In the case of the electrical cross tie enhancements, despite that the concept was approved some regulatory reviews is still remaining pending applicant's additional details submission

The key events and provisions in the plant design for loss of UHS and SBO described in the license applicant's assessment are as follows:

1. Reactor is shutdown manually or automatically by the BNPP plant protection system. The timing of subsequent events is not significantly affected by the timing of the trip.
2. The primary side residual heat is removed by natural circulation heat transfer to steam generators, and the secondary side heat is removed by steam dump to the atmosphere via MSSVs or ADVs.
3. The secondary cooling water is provided to the steam generators by the turbine-driven AFWS.
4. The AAC DG can supply electric power to the safety equipment and it has fuel capacity for 24 hours.
5. RCP seal leakage can occur if AAC DG is not available or fails.
6. If AAC is not available, Class 1E battery of channel C&D provides the DC power to the TDAFW pump valves for 16 hours. Moreover, if one EDG on one unaffected Unit is available, EDG cross tie between unit can be implemented
7. If needed, a mobile DG can also be connected to supply electric power to the safety equipment including AFWPs, ADVs, ACP, etc.
8. Cooling water into the secondary system from external sources will be initiated, if the main feedwater system and the AFWS are not functional.
9. Cooling water into the primary system from external sources will be initiated, in preparation for mitigating long-term loss of core cooling.

The license applicant has committed to provide EOPs, SAMGs and Extended Damage Mitigation Guidelines (EDMGs) that provide procedures or guidance to implement the internal and external mitigation measures. FANR will review this material when it is provided.

Korean APR1400

Korean APR-1400 deployed the mitigation strategies to maintain core cooling and inventory of primary coolant, and to prevent criticality similar to US APR-1400. In case of loss of offsite power and loss of diesel generator concurrently, turbine driven auxiliary feed water pump makes up cooling capability. In case of the aforementioned situation, AAC provides electricity for IE-Class systems including cooling pump and necessitated equipment. If AAC would not be available, diesel driven mobile pumps can provide cooling water into primary and secondary system with taking suction from the seismic 1 class water source.

US APR1400

For the US APR1400 design, KHNP proposed to employ a three phase approach for mitigating beyond design basis external event that results in extended loss of AC power. The initial phase (Phase 1) requires the use of installed equipment and resources to maintain or restore core cooling, containment, and spent fuel pool (SFP) cooling capabilities. The transition phase (Phase 2) requires providing sufficient, portable onsite equipment and consumables to maintain or restore these functions. The final phase (Phase 3) requires obtaining sufficient offsite resources to sustain core cooling, containment, and SFP cooling indefinitely.

The APR1400 FLEX strategy can be divided into two sets of operational strategies, as follows:
a) FLEX strategy for Modes 1 through 4 (full-power operation, startup, hot standby, hot shutdown) and Mode 5 operation (cold shutdown) with steam generators (SGs) available
b) FLEX strategy for Modes 5 and 6 operations with SGs not available. Supporting analysis is performed to demonstrate the APR1400 baseline coping capability based on both of the FLEX strategies.
Supporting analysis is performed to demonstrate the APR1400 baseline coping capability based on both of the FLEX strategies.

The actual submittal of US APR1400 is under review by US NRC following the NRC issued interim staff guidance, JLD-ISG-2012-01, "Compliance with Order EA-12-049, Order Modifying Licenses with Regard to Requirements for Mitigation Strategies for Beyond-Design-Basis External Events," (ML12229A174). JLD-ISG-2012-01 endorsed with clarification the methodologies described in the industry guidance document Nuclear Energy Institute (NEI) 12–06, Revision 0, "Diverse and Flexible Coping Strategies (FLEX) Implementation Guide," issued August 21, 2012 (ML12242A378). The guidance in JLD-ISG-2012-01 describes one acceptable approach for satisfying the Commission directives regarding BDBEE mitigation strategies.

Sub-Criticality

III. Effectiveness of the scram of the reactor is a vital function that needs to be ensured on the APR1400 following an extreme event such as occurred at Fukushima.

It should be demonstrated that, in Fukushima-type extreme external event at the site of any APR1400 power plant, either automatic or timely manual shutdown would be available to achieve sub-criticality. Due consideration should be given to deformations of the fuel assemblies and/or control rods induced by an earthquake exceeding the design bases magnitude. In the case of an extreme event with significant ground motion or vibration of the reactor building, the selection of the shutdown mechanism, either automatic or manual, may be based on the site specific conditions. In Korea, an automatic seismic trip system has been installed whereas in US and UAE a manual scram based on seismic alarm is proposed or implemented together with specific operating procedures.

IV. Maintenance of adequate long-term control of sub-criticality is a key safety function that needs to be ensured on the APR1400 following an extreme event such as occurred at Fukushima.

Following every reactor trip, there is an eventual reduction in the shutdown margin of the reactor core due to the cool down of the reactor core (given the moderator density reactivity coefficient of the core) and the decay of xenon. In the case of an extreme event at the site of any APR1400 power plant, it is essential that sufficient shutdown reactivity margin is maintained, by appropriate use of borated water injection despite reactor cool down.

V. It is essential that at least one measure should be provided on the APR1400 design to ensure adequate long-term reactivity control.

Although there are different implementation practices on long term reactivity control, a consensus has been made that at least one measure should be provided to ensure the long-term control of reactivity on the APR1400 following the long-term loss of off-site power together with failure of the EDGs. In addition, it will be necessary to demonstrate that these measures are functionally capable of achieving the key safety function.

On the APR1400 design there are potentially a number of options for ensuring adequate long-term control of reactivity following the loss of off-site power together with failure of the EDGs. These are:

a. The make-up water taken from the IRWST is borated and so provides a measure of ensuring the long-term control of reactivity as long as SBO DG, mobile DG or when applicable electrical cross tie between units are available,

b. Otherwise, it is proposed to use fire protection pumps or mobile pumps to inject borated water directly into the primary circuit via external injection line to RCS.