Date: 11 October 2016
Validity: **until next update or archiving**
Version 1

MDEP Design-Specific Common Position CP-ABWRWG-01

Related to: ABWR Working Group's activities

COMMON POSITION ADDRESSING ISSUES RELATED TO THE FUKUSHIMA DAIICHI NUCLEAR POWER PLANT ACCIDENT

Participation

Regulators involved in the MDEP working group discussions:	NRA (Japan), SSM (Sweden), ONR (UK) and US NRC (USA)
Regulators which support the present common position:	NRA (Japan), SSM (Sweden), ONR (UK) and US NRC (USA)
Regulators with no objection:	
Regulators which disagree:	

Multinational Design Evaluation Programme

ABWR Working Group

COMMON POSITION ADDRESSING ISSUES RELATED TO THE FUKUSHIMA DAIICHI NUCLEAR POWER PLANT ACCIDENT

INTRODUCTION

The MDEP Advanced Boiling Water Reactor (ABWR) Working Group (ABWRWG) members, referred to herein as "regulators", consist of members of the nuclear regulatory organisations from Japan, Sweden, United Kingdom and the United States. Because not all of these countries have completed regulatory reviews of ABWR applications yet, this paper identifies common preliminary approaches to address potential safety improvements for ABWR plants, as well as common general expectations for new Nuclear Power Plants (NPP), as related to lessons learnt from the Fukushima Daiichi NPP accident or Fukushima-related issues.

As the safety reviews of the ABWR design applications that are currently on-going are progressed, the regulators will consider what additional work is required and may consider the need to update this paper. Otherwise, as additional information becomes available it will be added as further appendices to the paper. The common preliminary approaches are organised into seven sections, namely evolutionary improvements in safety, hazards, reliability of safety functions, accidents with core melt, spent fuel pools, emergency preparedness in design, and safety analysis.

GENERAL CONTEXT AND BACKGROUND

On 11 March 2011 Japan suffered its worst recorded earthquake. The epicentre was 110 miles (180 km) east north east from TEPCO's Fukushima Daiichi NPP which had 6 operating Boiling Water Reactors (BWR). Reactor Units 1, 2 and 3 on this site were operating at power before the event and on detection of the earthquake shut down safely. Reactor Unit 4 was not loaded with any fuel assemblies due to maintenance, including replacement of the core shroud. Reactor Units 5 and 6 were shut down for maintenance. Initially, on-site back-up diesel generators were used to provide the alternating current (AC) electrical supplies to power essential post-trip cooling systems. Within an hour a massive tsunami from the earthquake inundated the site; all AC electrical power to the cooling systems for the reactor and reactor fuel pools was lost, including that from all but one (in Unit 6) back-up diesel generators, as well as a significant amount of direct current (DC) supplies and essential instrumentation. Over the next few hours, and days, the fuel in Reactor Units 1, 2 and 3 heated up and degraded. There were hydrogen explosions which caused considerable damage to the reactor buildings in Units 1, 3 and 4. For over a week the site struggled to put cooling water into the reactors and the reactor fuel pools, by using means untried before and/or unplanned. Electrical supplies were gradually reconnected to the reactor buildings and a degree of control returned. Heavily contaminated water, used to cool the reactors and spent fuel pools, collected in uncontained areas of the site and leaked out to sea. There were also significant releases of radioactivity to the air.

However, to date, the indications are that the public health effects from radiation exposure are not significant.

This was a serious nuclear accident, with an International Nuclear and Radiological Event Scale (INES) rating of Level 7 (the highest level). Tens of thousands of people were evacuated from a zone extending 20 km from the site. Today, there is still a large exclusion zone around the site.

Numerous studies have been performed to better understand the accident progression and detailed technical studies are still in progress in Japan and elsewhere. On-going studies on the behaviour of NPPs in severe situations, similar to the Fukushima Daiichi NPP accident, 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 ABWR plants are engaged in similar activities.

The ABWRWG members have made efforts to ensure that the descriptions of the March 2011 events at the Fukushima Daiichi NPP presented in this paper reflect current knowledge and understanding of the Fukushima Daiichi NPP accident; these have included a comparison with the information in the August 2015 IAEA Director General's Report "The Fukushima Daiichi Accident" (http://www-pub.iaea.org/books/IAEABooks/10962/The-Fukushima-Daiichi-Accident). In addition this paper has undergone factual accuracy checks by ABWR industry stakeholders. The ABWRWG members wish to express their thanks to GE-Hitachi, Hitachi-GE, Toshiba, TEPCO and Horizon Nuclear Power for their contribution.

COMMON POSITION

EVOLUTIONARY IMPROVEMENTS IN SAFETY

Context

The first commercial size BWR, Dresden 1, a BWR/1 model, started operation in 1960. Since then the BWR design has undergone a series of evolutionary changes focused on simplifying the reactor systems and the containment and improving safety.

Fukushima NPP's reactor Units 1, 2 and 3 are BWRs of early generations. Key characteristics are presented in the following table:

	Unit 1	**Unit 2**	**Unit 3**
Reactor model	BWR/3	BWR/4	BWR/4
Containment model	Mark I	Mark I	Mark I
External recirculation loops	Yes	Yes	Yes
AC-independent core cooling features	Isolation condenser and Turbine-driven High Pressure Coolant Injection (HPCI) system	Turbine-driven Reactor Core Isolation Cooling (RCIC) system and Turbine-driven HPCI	Turbine-driven RCIC and Turbine-driven HPCI

	Unit 1	Unit 2	Unit 3
Electrical output (MWe)	460	784	784
Commercial operation	1971	1974	1976

Discussion

The ABWR technology was jointly developed as the next generation BWR based on construction and operating experience in Japan, US and Europe. The ABWR design resulted in enhancement in safety of the systems delivering safety functions. The following are some examples of improvements chosen by different vendors:

- Installation of internal recirculation pumps eliminate all of the jet pumps in the reactor pressure vessel (RPV), all of the large external recirculation loop pumps and piping, the isolation valves and the large diameter nozzles that penetrated the RPV. By eliminating this piping and the associated large vessel nozzles below the top of the active fuel, it became possible to keep the core covered with water during all the design basis loss-of-coolant accidents (LOCA).
- A three division emergency core cooling system (ECCS) was adopted. Each division provides both low pressure and high pressure make-up capability and incorporates its own emergency diesel generator power supply. The safety classification of the turbine driven, AC-independent, reactor core isolation cooling system (RCIC), existing in some models, was raised – the RCIC in the ABWR is a fully-fledged safety (Class-1/Class 1E) system.
- The control rod insertion uses two different method of insertion: an electric motor drive for normal operation and emergency insertion (scram) and a conventional hydraulic drive for scram.

Currently there are differences in the ABWR designs proposed internationally which offer a variety of solutions to provide the fundamental safety functions (discussed below). The key designs considered by the ABWRWG and within this paper are:

- US: US ABWRs offered by GE-Hitachi and Toshiba (design variations between them are not discussed in this paper),
- UK: UK ABWR offered by Hitachi-GE,
- Japan: J ABWRs offered by Hitachi-GE and Toshiba,

Toshiba offers another ABWR design, the EU ABWR. Although none of the ABWRWG members is currently assessing this design, some information on the EU ABWR is provided in this paper for completeness.

Following the Fukushima Daiichi NPP accident, additional design improvements were proposed. The major enhancements are, mainly, further means to prevent extended loss of AC power and/or loss of ultimate heat sink. Moreover, the enhanced functions ensure water supply into the reactor, integrity of the primary containment, and maintenance of the water level in the spent fuel pool (SFP), even during extended periods of loss of AC power, or if the ultimate heat sink has been lost. These enhancements, based on lessons learnt from the Fukushima Daiichi NPP accident, along with provision and maintenance of severe accident management guidelines (SAMG), are aimed at ensuring that the integrity of inherent safety features of the ABWR is retained even in the event of a severe accident.

Overall the ABWR today represents an evolution in safety compared with earlier generation BWR designs.

Common Position

The ABWR today represents an evolution in safety compared with earlier generation BWR designs. Following the Fukushima Daiichi NPP accident, further safety enhancements are being considered, and/or designed and implemented, by the ABWR vendors and licensees to respond to national regulatory requirements and international expectations.

EXTERNAL HAZARDS

Context

The earthquake sequence that affected the Fukushima Daiichi site started with a magnitude 7.3 event on 9 March 2011, which was followed within a few hours by a series of large seismic events. The main shock, of magnitude 9.0 (known as the 2011 off the Pacific Coast of Tohoku Earthquake), occurred on 11 March 2011 at 14:46 local time. There were over 500 aftershocks with a magnitude greater than 6. Although the Tohoku event was the largest in the historical record of Japan, earthquakes of similar magnitude, or greater, occur somewhere in the world on average every 15-20 years. It was the 5th largest recorded in the past 100 years.

This was not the first time the Fukushima plant had been hit by a seismic event. In 1978, the 7.4 magnitude Miyagi earthquake 140 km from the plant resulted in site ground accelerations of 0.125g. The damage levels following this event were minimal and the plant was fully operational within a matter of days.

Similarly, the 2011 earthquake caused loss of off-site power, due to collapse of power lines, but did not compromise the Fukushima reactors' ability to reach a shut-down position. It was the resulting tsunami that led to the loss of post-trip cooling. The first tsunami wave resulting from the main shock arrived at the Fukushima Daiichi site at around 15:27 local time on 11 March 2011, and the second wave at 15:35 local time just under an hour after the earthquake. The estimated height of the tsunami wave was about +14-15m. The height of the flood protection measures was set at +5.7 m. The site was rapidly inundated to depths up to 6 m. The incoming wave completely surrounded the buildings on-site, and entered the buildings via ground level access doors. The extremely long wavelength (and consequently period) of tsunami waves meant that the site remained inundated for a period of between 30 minutes and an hour following the main wave arrival.

Considerable damage was done to ground level structures on the shoreline, including the complete destruction of two large diesel storage tanks to the north of the site. Structures related to the main sea water intake were severely damaged. Emergency diesel generators and power supply boards were flooded.

Discussion

There are a number of different approaches available for the evaluation of external hazards. This is dependent on regulatory requirements in the respective countries. However, the safety assessment should demonstrate that threats from external hazards are either removed, minimised or mitigated. For each type of external hazard identified that is not screened out for a particular site, a design basis event is determined with consideration of the site hazard curves or characteristics, as appropriate depending on the hazard. The severity of the design basis event should correspond to an initiating frequency such that an acceptable overall risk is achieved in accordance with a defined risk target. In the UK, for example, for natural hazards, a design basis event of 1E-4/yr (conservatively defined) is considered reasonable. Due attention should be paid to providing adequate capacity for events beyond the design basis. "Cliff edge" effects should be avoided as far as possible.

For all external hazards, the design should have sufficient robustness to allow shut down and cooling of the reactor from any operating state, and integrity (and cooling as required) of any other facility at the proposed nuclear power plant where significant amounts of radioactive material are expected to be present. Climate change has the potential to affect a number of different external hazards and the foreseeable effects of climate change over the lifetime of the facility are expected to be taken into account; adaptability may be built into the design to accommodate future developments in climate change predictions.

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. The design parameters for these barriers need to be conservative, and may need to be more stringent than those derived from the design basis flooding event, e.g. to take into account required seismic qualification. The barriers should be subject to appropriate safety management arrangements (including periodic inspections, monitoring and maintenance even if their locations mean they are not under the direct responsibility of the operator). In addition, levees, sea walls and bulkheads, etc., should be designed to ensure that water can leave the site when needed and that they do not act as a dam.

The design of structures, systems and components (SSC) needed to deliver the fundamental safety functions in any permitted operational states, could be further augmented by protection from water ingress and waterproofing (as a redundant measure to provide a further barrier in the event of flooding of the site). For further information refer to the 2011 IAEA's Specific Safety Guide on meteorological and hydrological hazards (SSG-18), on which much of the previous discussion is based http://www-pub.iaea.org/MTCD/publications/PDF/Pub1506_web.pdf.

All ABWR SSCs important to safety in the context of seismic hazard are qualified against the design reference level earthquake. A site-specific analysis should be performed in order to ensure that the design reference level earthquake envelops the site-specific earthquake at all points on the hazard spectrum. In determining the effects of a seismic event on the facility, the effects of the 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 access for the control and/or repair of plant, or if they could potentially damage safety systems for example, site/building flood following earthquake from failure of unqualified pipe work.

The range of external hazards to be considered in the design basis for nuclear installations may be wide and diverse. In many cases, careful consideration needs to be given to concurrent hazards, for example wind, ice and snow, and consequential hazards like, in the case of Fukushima Daiichi, tsunami caused by earthquake, or, a flooding event at the NPP induced by seismic failure of a dam in its vicinity. Also, if the frequency of occurrence of some (unrelated) external hazards is high at the site, it may be necessary to consider their random simultaneous occurrence.

Common Position

The accident at the Fukushima Daiichi NPP has reinforced the need to undertake, as part of the safety review process for ABWRs, a comprehensive analysis of external hazards, including consideration of relevant combinations of events. This should include an analysis to address the potential impact of the relevant hazards on all areas of the proposed NPP where significant amounts of radioactive material are expected to be present.

Design basis events are determined with consideration of the site hazard characteristics. The severity of the design basis events should correspond to initiating frequencies such that an acceptable overall risk is achieved in accordance with a defined national risk target, regulatory rule or international expectation.

Due attention should be paid to providing adequate capacity for events beyond the design basis of the NPP.

The foreseeable effects of climate change over the lifetime of the facility are expected to be taken into account when evaluating site hazards.

RELIABILITY OF SAFETY FUNCTIONS

Context

All the Fukushima Daiichi reactor units were based on the concept of defence in depth and had multiple[1] systems to deliver the fundamental safety functions of criticality control, core cooling and containment of radioactive materials. Some of these systems worked as planned, some only partially and others were made ineffective by the earthquake and subsequent tsunami.

<u>Criticality control</u>:

The Fukushima Daiichi reactor units were fitted with an automatic shutdown system linked to ground motion instrumentation. Available data was consistent with the system having worked and that insertion of the control rods was initiated via the seismic trip. BWRs also have a diverse system to shut down the reactor called the standby liquid control (SLC) system. This system injects a "neutron poison" (boron) into the reactor vessel to shut down the chain reaction, independent of the control rods. Had the control rods failed to insert in any of the reactors, the operators could have manually actuated the SLC system.

[1] In the context of this common position the term "multiple" (e.g. "multiple systems" or "multiple means of providing make-up") may imply redundancy, diversity, or both. The ABWRWG is not making an attempt to provide detailed descriptions of the means available to achieve the fundamental safety functions, as they vary among countries and designs.

Core cooling:

Upon loss of off-site power following the 2011 off the Pacific Coast of Tohoku earthquake, reactor Unit 1 was initially cooled with the passive isolation condensers (IC). The system started automatically but the cooling rate had to be maintained by subsequent manual stops and starts. Loss of AC and DC due to the tsunami occurred which resulted in IC cooling being isolated. Thus, the effectiveness of the IC cooling was not upheld beyond the occurrence of the tsunami.

Reactor Units 1, 2 and 3 were equipped with turbine-driven high pressure coolant injection (HPCI) systems. These systems did not start in Units 1 and 2, due to loss of power supplies. Unit 3 HPCI started automatically and ran for several hours until it was manually stopped at low RPV pressure. Attempts to start an alternative water injection or to re-start the HPCI were unsuccessful. In any case, due to loss of ultimate heat sink the HPCI's core cooling capabilities could not have been maintained long term.

Both reactor Units 2 and 3 were equipped with a further turbine-driven cooling system, the RCIC. The RCIC operated in both reactors for a number of hours (longer than expected); the reasons why the RCIC stopped in both units are unclear, however, due to loss of ultimate heat sink, it would not have been possible to maintain core cooling indefinitely.

Alternative water injection measures were available for the three reactors. These required low RPV pressure but it was reported that the operators had significant difficulties in their attempts to depressurise the RPVs in Units 2 and 3. For example, water injection to the Unit 2 RPV using a fire truck started around 20:00 on March 14. After starting the injection, the pressure of the Unit 2 RPV increased and was about 2.3 MPa [gauge] at around 23:00 on March 14 and about 1.6 MPa [gauge] at around 1:00 on March 15 (the operating pressure of the pump on the fire truck was 1.0 MPa [gauge]). Therefore, it appears that the hydrogen generated in the core after water injection exceeded the depressurisation capacity of the safety relief valves (SRV), causing increase in the RPV pressure and preventing continuous injection into the reactor. Thus, the existing alternative water injection measures were either not utilised in time, or not effective, to avoid core damage.

Containment:

The three Fukushima Daiichi Units 1, 2 and 3 had means to cool the atmosphere of the containment and keep the pressure and temperature low enough to maintain its integrity. However, the tsunami damaged the sea water pumps and the heat sink, and thus, the containment cooling capability was lost. After that, the only effective solution available to relieve high pressure from the primary containments and preserve their integrity in the three reactor units, was to vent the containment vessels using hardened containment (drywell and suppression pool) vents. These operations proved to be very challenging and, eventually, pressures and temperatures in the containments reached high values. High pressures and temperatures weakened penetration seals and the gaskets on the flange section of the drywells creating leak paths, which may indicate that containment venting operations had not been effective (or timely) enough to preserve the integrity of the primary containments.

Discussion

The safety of nuclear power systems relies on maintaining of three fundamental safety functions:

- controlling reactor power (criticality control);
- core cooling; and
- containment of radioactive material.

If these fundamental safety functions are preserved then the safety of a nuclear system can be maintained and radioactive materials will not reach people or the environment. These fundamental safety functions can be maintained using different techniques, and diverse methods are generally employed to meet these functions to ensure the safety of a reactor system. The paragraphs below consider each fundamental safety function and describe how these functions are maintained on an ABWR.

Criticality control:

For the ABWR design, criticality control is normally maintained via the control rods. The control rod operation uses two different method of insertion: an electric motor drive for normal operation and emergency insertion (scram) and a conventional hydraulic drive for scram. If a scram is required, it is actuated by both methods; if one of them fails, control rod insertion can still be achieved by the other. These rods have been shown to be able to be inserted under high seismic loads. Insertion of the control rods happens automatically upon loss of electrical power. As an alternative to the control rods the ABWR also employs the SLC system for criticality control. When required the SLC system will inject highly borated water into the reactor system capable of maintaining the reactor subcritical. In the UK, US and EU ABWR designs the SLC system automatically injects upon occurrence of certain signals; in the J ABWR design this system is manually actuated.

Core cooling:

Providing criticality control can be maintained, the aim of the safety cooling systems should be to remove the decay heat. For the ABWR, cooling of the fuel post shutdown is ensured via multiple systems, these systems vary depending on the ABWR design. Key systems for ensuring that reactor cooling can be maintained are the high pressure systems, e.g. high pressure core flooder (HPCF) and reactor core isolation cooling (RCIC), automatic depressurisation system, low pressure systems, e.g. low pressure core flooder (LPCF) and residual heat removal system. The reliability of the depressurisation systems is essential to enable water injection with low pressure injection systems.

The Fukushima Daiichi NPP accident highlighted the importance of cooling systems capable of operating in the absence of all AC power sources. All ABWR designs employ cooling systems capable of operating in the event of loss of all AC electrical power. The RCIC system employed on the UK, US and Japanese ABWRs injects water using steam generated within the core to drive a steam driven turbine which can inject high pressure water from either the suppression pool or the condensate storage tanks (condensate storage pools in some Japanese ABWRs), therefore the operation of this system will be unaffected by loss of AC power. The RCIC was designed to operate for 8 hours after loss of AC power supplies; post Fukushima it was recognised that improvement to the availability of DC power supplies could enable this system to operate much longer to add resilience. The EU ABWR design employs more passive methods of maintaining the cooling such as passive isolation condensers and passive containment cooling. The EU ABWR isolation condensers ensure that the design is capable of maintaining core cooling following complete loss of

AC power supply for at least 72 hours.

The implementation of diverse methods of water injection is a key piece of learning from the events at Fukushima Daiichi NPP. The US ABWR incorporates a seismically designed portion of the fire protection system which can supply cooling water to the reactor, containment or spent fuel pool, as required, using the diesel-driven fire pump; this diverse water addition system is referred to as the AC independent water addition (ACIWA) system. The UK ABWR design employs additional permanently installed safety injection pumps in the so-called "back-up building", which are segregated from the main reactor building in order to enhance reactor cooling capability. All ABWR designs are considering the use of flexible methods of water injection to the core using mobile equipment. One lesson learnt from the Fukushima Daiichi NPP accident is the importance of the ability to control the pressure in the RPV and the containment to enable water injection to the core by mobile, low pressure pumps; the UK ABWR has added the capability to depressurise the RPV and containment from the back-up building.

Despite the resilience of the ABWR against loss of AC power, maintaining the availability of AC power is recognised as critical for the safety of nuclear power plants, hence high reliability of AC power supply is essential. This high reliability is expected to be achieved through an adequate combination of redundancy and diversity. Regarding emergency power supply, diverse AC power sources with adequate electrical and physical isolation provide defence-in-depth to the plant. Other actions for increasing the reliability of back-up AC power supply at nuclear power plants deal with enhanced provisions of long-term diesel fuel, lubricating oil reserves, air and any other necessary supplies, and ensuring the possibility of using mobile power supply units.

All ABWR designs have a minimum of three emergency diesel generators each of which is capable of supplying 100% power requirements to maintain a single train of safety systems. Despite this capability, some ABWR designs have included, or are looking into including, additional emergency generator capacity using diverse technology in order to ensure that electric power supply can be maintained in events beyond the design basis.

The defence-in-depth approach also needs to be applied to the ultimate heat sink. Some ABWR designs are planning to employ alternate heat sink capabilities, such as alternate heat exchanger facilities, eg., once through mobile equipment or other means. When the ultimate heat sink is lost, the final way of removing heat from an ABWR and avoiding core degradation is injecting water to the reactor and venting steam from the containment to the environment in a controlled manner.

<u>Containment of radioactive material</u>:

Provided that adequate core cooling and criticality control can be established, the confinement of most of the radioactive material within the fuel pins should be maintained. However, if radioactive material is released from the fuel it is vital that it is not released to the environment. The ultimate barrier to prevent the release of radioactive material is the reinforced concrete containment vessel (RCCV) and therefore the protection of this barrier is a key piece of learning from the Fukushima Daiichi NPP accident. To protect the containment it is also essential to be able to depressurise the RPV, even in case of total loss of power supply, to avoid high pressure RPV failure which would pose a challenge to the containment.

Additional methods for the protection of the RCCV have been considered post-Fukushima, these include the protection of the drywell head flange, additional methods for injecting water into containment and/or the addition of filtered containment venting to ensure that the containment pressure is maintained below ultimate design pressure. The EU ABWR also employs passive containment cooling capability which reduces the need for containment venting following a severe accident.

The Fukushima Daiichi NPP accident highlighted the importance of ensuring that the drywell head flange sealing capability is protected from the effects of high temperatures and pressures which are created during a core melt event. The Japanese and UK ABWR designs propose to inject water into this volume (referred to as reactor well) during an accident involving possible core degradation to ensure that the structural components remain cool and therefore the drywell flange integrity can be protected. The EU ABWR design has proposed to enlarge the containment volume to reduce peak pressure and fill the reactor well with water during normal operation.

Common Position

The regulators stress the importance of the ABWR reactor design providing ample redundancy and diversity in electrical and cooling capabilities to ensure the fundamental safety function of core cooling.

All ABWR designs should implement measures to ensure that the ABWR plant can fulfil fundamental safety functions without external support for a reasonable time in case of loss of ultimate heat sink – what “reasonable” means may differ in different countries (and for different sites); 24 hours should be the minimum time, although much longer resilience is expected in some countries and encouraged by the regulators. Furthermore, internal AC power sources should be diverse and designed to withstand external hazards.

Maintaining the integrity of the ABWR containment vessel is very important but can be challenging following loss of heat sink. Design solutions should be implemented for this purpose. These may be different depending on national requirements.

ACCIDENTS WITH CORE MELT

Context

The severe accident phenomena that are expected to have happened at the Fukushima Daiichi reactor Units 1, 2 and 3 once the core cooling capabilities were lost, have been widely described. Even though not all these phenomena were directly observable (compounded by the loss of instrumentation on some of the reactor units), at the time of the Fukushima Daiichi NPP accident, there was extensive knowledge of BWR severe accidents. The nuclear industry had considered severe accident phenomena for many years and, using a combination of past events, research, fundamental science and computer analysis, was able to make predictions of what can happen during such accidents.

Once water injection and other means to cool the reactor (such as the Isolation Condenser in Unit 1) stopped, the core cooling capabilities were lost and, eventually, the reactor cores began to uncover and, subsequently, overheat. Increased RPV pressure would have caused the SRVs to open allowing loss of inventory from the reactor circuits. The water level in the reactor pressure vessels would have dropped below the top of the active fuel and would have continued decreasing. Eventually, the capability of transferring heat from the fuel to the coolant would have been severely degraded. When the temperature reached around 1 000°C, the fuel cladding would have started failing and the zirconium in the cladding would have started reacting with the steam in the RPV, oxidising and releasing large amounts of hydrogen and heat. The hydrogen explosions that occurred on the refuelling (sometimes called "operation" or "service") floors of Units 1 and 3 were clear indications of severe degradation of the reactor cores, which, eventually would have lost their geometry and collapsed at the bottom of the RPVs. At some point, the regulators understand that damage and penetration of the three reactor pressure vessels may have occurred and molten core debris known as corium (a mixture of cladding, control rods, material from the reactor internals and fuel) would have relocated to the drywell floor, where they could have attacked the concrete floor releasing non-condensable gases. It is unknown whether this phenomena, called molten core concrete interaction (MCCI) occurred at any of the Fukushima Daiichi damaged units.

BWR severe accident computer models were available and, soon after the accident, used in Japan by the Tokyo Electric Power Company (TEPCO) and Japan's Nuclear and Industrial Safety Agency (NISA) to predict/understand the progression of the severe accidents at the three reactor units. At the time when these analyses were published, their predictions provided the best information on likely progression of the severe accident sequences at the three reactor units. What the predictions suggest would have happened and what actually occurred at the Fukushima Daiichi NPP should converge with time. To achieve this, TEPCO is making continuous efforts, such as the use of robots inside the damage units, to further understand what happened at the Fukushima Daiichi NPP. In February 2015, TEPCO said that they hoped to gain a greater understanding of the location of the molten fuel in Unit 1 of the damaged Fukushima Daiichi NPP with the installation of a muon detection system (http://www.world-nuclear-news.org/RS-Looking-inside-Fukushima-Daiichi-unit-1-1002154.html). In March 2015, TEPCO announced that initial results from using the muon detection system appeared to confirm that most of the fuel had melted and dropped from its original position within the core (http://www.world-nuclear-news.org/RS-Muon-data-confirms-fuel-melt-at-Fukushima-Daiichi-1-2303154.html), as it had been predicted by the analyses. The muon detection system was installed in Unit 2 in March 2016; in July 2016 TEPCO announced that these examinations showed that most of the Unit 2 fuel had melted and dropped from its original position within the core and indicated that most of the debris had fallen to the bottom of the RPV and resolidified (http://www.world-nuclear-news.org/RS-Detectors-confirm-most-fuel-remains-in-unit-2-vessel-2907164.html).

Discussion

The regulators recognise that the different ABWR designs include a variety of measures to mitigate the consequences of release of corium from the bottom of the RPV. Additional methods for water injection into the containment have been identified in all ABWR designs to ensure that cooling of the corium can be maintained. The EU-ABWR design employs a specific device (core catcher) capable of retaining and cooling a molten core outside the RPV. All other ABWR designs look to manage a molten core within the drywell via the addition of water into this volume. In the US Certified ABWR, there is a layer of sacrificial basaltic concrete in the lower drywell to protect the containment boundary. The UK, EU and US ABWR designs employ a passive melt plug which, in the vicinity of corium, will melt with the aim of allowing water from the suppression pool to flow into the drywell, which should cool the molten core slowing core concrete interactions, and therefore protecting the containment basemat. In the J ABWR, water addition to the lower drywell is planned before the molten core is released from the RPV; the water is fed using a newly installed water line. This severe accident management strategy is also being considered in the UK ABWR design.

One of the key phenomena witnessed during the Fukushima Daiichi NPP accident was the effect that hydrogen generated post-accident could have on confining radioactive material. Therefore, adequate means for controlling these phenomena are required. All ABWRs normally operate with an inerted containment which means the risk of a hydrogen explosion within the RCCV is significantly reduced. The addition of passive auto-catalytic recombiners into the refuelling floor of the reactor building (for some designs) will also act to mitigate the leakage of hydrogen from the RCCV into these regions and as such protect these areas of the plant. Other passive measures of hydrogen control have also been proposed for some ABWRs, including the addition of blow-out panels in the refuelling floor which would release hydrogen to the environment and hence prevent it accumulating within the reactor building.

The containment vent in the ABWR designs allows pressure of the containment to be controlled. In the ABWR design the vent line is inerted and, thus, considers the presence of hydrogen. Some ABWRs designs (e.g. in the UK and Japan) have now incorporated filtered venting facilities to enable further reduction of radionuclides released to the environment during venting operations.

Common Position

Although core melt accidents have been considered in the original ABWR designs, further features and enhancements are being considered and implemented, as appropriate, in accordance with the different regulatory requirements and international expectations.

Safety features which ensure the adequate integrity of the containment in case of an accident with core melt need to be included in the design. These features need to have adequate independence from the other provisions of the plant. They should also include: provisions to avoid over pressurisation (relying for example on containment venting and/or containment spray systems); hydrogen management; and consideration of the ultimate pressure strength in accidents with core melt.

SPENT FUEL POOLS

Context

Upon removal from the reactor, spent fuel is placed in the reactor spent fuel pool. These are robust structures that are filled with water to cool the fuel and provide shielding from gamma radiation. The spent fuel pools are designed with cooling systems to maintain water temperatures below 52°C and maintain water levels several metres above the top of the fuel assemblies. After several years, the residual decay heat within the fuel will reduce to a level that would permit the spent fuel to be transferred into other interim storage facilities, for further storage prior to final disposal. Each of the six Fukushima Daiichi reactors had spent fuel pools located at the top of the reactor building to facilitate fuel handling during refuelling.

According to information provided in April 2011 by Japan’s Nuclear and Industrial Safety Agency (NISA), on 11 March 2011 the six nuclear reactors at the Fukushima Daiichi site were in different stages of their operating cycle as follows:

	Unit 1	**Unit 2**	**Unit 3**	**Unit 4**	**Unit 5**	**Unit 6**
Status	Operation at power	Operation at power	Operation at power	Refuelling Outage	Shutdown since January 2011	Shutdown since August 2010
Fuel assemblies in the reactor	400	548	548	0	548	764
Spent Fuel assemblies in the fuel pool	292	587	514	1331	946	876

Following the 11 March 2011 events, the spent fuel pool structures remained essentially intact. However, in the absence of any active cooling of the pools following the loss of the power and the damage to the sea water pumps that occurred with the tsunami, the water temperature in the pools increased.

TEPCO started spraying reactor Unit 3's pool with water cannon from the ground on 17 March 2011, having tried to add water via helicopters earlier in the day. Spraying of Unit 4's pool with water cannon commenced on 20 March 2011. Water cannon/fire trucks were later replaced on Unit 4 with water spray from above via the articulated arm of a concrete pumping truck. Water injection to Unit 2's pool commenced on 20 March 2011. These are examples of TEPCO's efforts to add water aimed at keeping the fuel in the spent fuel pools covered.

Discussion

The Fukushima Daiichi NPP accident highlighted the need to fully consider safety in the design of spent fuel pools. This implies proper consideration of internal initiating events and internal and external hazards.

Both prevention of accidents and defence-in-depth, as well as the possibility of radionuclide releases should be considered in the context of fuel storage pools. The most fundamental and demonstrably effective way to achieve a safe outcome is to ensure the integrity of the spent fuel pools, and to maintain sufficient water level in the pools. The ABWR spent fuel pool is, for all designs, a robust reinforced concrete structure with a liner to prevent leakage; it should retain its integrity even if the water is boiling. Any evaporative losses or small leakages can be mitigated by make-up systems to maintain the spent fuel pool water inventory and keep the fuel covered. Multiple means of providing make-up water are provided including back-up mobile systems with connection points at separate locations. Make-up systems can maintain the required water level by means of sprays or injection lines. Loss of ultimate heat sink is also a challenge that needs to be considered in the design of the spent fuel pools.

Instrumentation and monitoring are maintained even during extended periods of loss of AC power. This is assured by the provision of alternative power sources (e.g. batteries). The purpose is to ensure that the water level and temperature can be monitored. Monitoring of spent fuel pool water level is provided from the control room and other appropriate protected and accessible locations.

Permanently fixed instrumentation for the measurement of water level and temperature is qualified against hazards and is capable of maintaining its design accuracy following a power interruption without recalibration.

The design of the ABWR spent fuel system is such that potential weak points (such as large penetrations) are avoided and defence in depth contributes to the robustness of the design.

Common Position

The Fukushima Daiichi NPP accident highlighted the need to fully consider safety in the design of spent fuel pools and their supporting SSCs. This implies proper consideration of internal initiating events and internal and external hazards.

The structural integrity of the spent fuel pools needs to be ensured with adequate margin in case of external hazards.

It is important that permanently fixed instrumentation, reasonably protected against hazards and qualified for expected conditions, be provided to monitor the conditions in the spent fuel pool.

EMERGENCY PREPAREDNESS IN DESIGN

Context

The 2011 off the Pacific coast of Tohoku earthquake was felt over a significant area of Japan. In some areas, there was extensive ground liquefaction, and severe damage to some petrochemical facilities. In addition, there was extensive disruption to transport systems, both train and roads. Telecommunications were badly affected as a result of direct damage and loss of power systems. External power to the Fukushima Daiichi site was lost as a result of failures of pylons, landslides affecting transmission lines, and damage to circuit breakers and insulators.

In many places the tsunami was more disruptive than the earthquake, with inundation reaching many kilometres inland and affecting an area of up to 600 km^2. The buildings and infrastructure of many towns and villages were completely destroyed, with debris scattered over a large area. The damage and disruption created significant problems in the first few days following the events, which limited access to the Fukushima Daiichi site for specialist equipment and personnel.

At the plant, the tsunami rendered most of the installed instrumentation inoperable and many of the control room facilities were not available – lighting was also lost. Operators established limited control and monitoring facilities using ad hoc techniques such as portable electrical power sources, such as car batteries, to provide power to I&C components. They made use of portable compressors to drive pneumatically operated control equipment. They also had to undertake manual operation of what would normally be electrically driven control equipment. By using such techniques station staff were able to monitor some plant parameters and perform some limited key mitigating actions, such as containment venting. These techniques would be time consuming and laborious under normal conditions; during this event there were additional adverse factors such as poor lighting and restricted access to plant areas due to high radiation levels.

Overall, the conditions at the plant impaired the ability of station staff to make decisions about the best means of mitigating the situation, to effect timely mitigating actions (such as containment venting), and to determine the effectiveness of such mitigation actions.

Discussion

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. IAEA SSR-2/1 requires that an on-site emergency response centre, separate from both the plant control room and the supplementary control room, be provided from which an emergency response can be directed at the nuclear power plant (Requirement 67). The remote shutdown station (or supplementary control room, whichever is the case) must also be adequately protected with sufficient margin to ensure it is available under all credible scenarios, including severe accidents. Suitably shielded and protected spaces to house necessary personnel in severe accident conditions should be considered for ABWR plants.

Dedicated facilities should be provided to support on-site actions including an off-site centre and back-up provision of key services to enable emergency response. SSCs needed for managing and controlling actions in response to an accident, including plant control rooms, on-site emergency control centres and off-site emergency centres, should be capable of operating adequately in the conditions, and for the duration, for which they could be needed, including possible severe accident conditions.

Access to appropriate locations to implement mobile means to recover safety functions should be possible when necessary – access and connection points should be clearly identified.

The reliability and functionality of the on-site and off-site communication systems need to consider conditions relating to internal and external hazards. The Fukushima Daiichi NPP accident also highlighted the need to consider long timescales, widespread on and off-site disruption, and the environment on-site associated with a severe accident. The robustness of necessary off-site communications for severe accidents involving widespread disruption may require provision of equipment with satellite communications capability.

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 release measurements, radiation level measurements, and meteorological measurements may need to be strengthened. Assurance must be provided of the readiness to take samples and analyse them in a laboratory.

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; 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. This should also take into consideration the human resource required to cope with such scenario.

As discussed earlier in this paper, the Fukushima Daiichi NPP accident has emphasised the need for extended autonomy of the plant. Safety functions should be maintained for a reasonable time without requiring off-site supplies or assistance. Some countries, like UK and Japan, expect new nuclear sites to hold essential supplies which will last for at least seven days.

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.

Common Position

An on-site emergency response centre, separate from both the plant control room and the remote shutdown station, should be provided from which an emergency response can be directed at the nuclear power plant.

The control room, the emergency response centre, remote shutdown station, and local control points need to be sufficiently protected against hazards to ensure the plant can be taken to a safe state and remain there.

On-site and off-site communication systems and equipment must be sufficiently robust so that they can be relied upon during an emergency event.

An assessment of the on-site and augmented staffing capability for responding to a multi-unit event should be performed to ensure that adequate resources are available.

SAFETY ANALYSIS

Context

The June 2011 report of the Japanese Government to the IAEA Ministerial Conference on Nuclear Safety "The Accident at TEPCO's Fukushima Nuclear Power Stations" (https://www.iaea.org/newscenter/focus/fukushima/japan-report) made some references to the extent of the safety analyses underpinning the design of the Fukushima Daiichi plants. It stressed the need to undertake a proper evaluation of design basis events and for the effective use of probabilistic safety analysis (PSA).

Discussion

The ABWR design was originally supported by traditional design-basis deterministic analyses complemented by PSA. The past decades have highlighted the need to expand the scope of the traditional deterministic and probabilistic analyses to demonstrate that the plant design is robust and there are no "cliff edge" effects (e.g. small deviations in plant parameters that could give rise to large variations in plant conditions). For example, in Europe, the WENRA safety objectives call for an extension of the safety demonstration for new plants, consistent with reinforcement of defence-in-depth. Some situations for which existing plant did not originally include design provisions, such as multiple failures conditions and core melt accidents, are taken into account in the design of new plants.

The accident at the Fukushima Daiichi NPP highlighted the importance of having robust and comprehensive safety analyses to support the design and operation of a nuclear power station. Different regulatory regimes have different expectations with regard to the boundaries between traditional deterministic and probabilistic analyses as well as their approach to identifying design extension conditions (DEC) and analyses of margins to cliff edge effects. A rigorous approach to the application of modern safety analysis techniques should, however, ensure that all the ABWR designs remain robust against a Fukushima-type event.

The ABWRWG members support the modern IAEA Standards, and, therefore, the following expectations on safety analyses are shared among the ABWR regulators:

- Comprehensive deterministic safety assessments and probabilistic safety assessments shall be carried out throughout the design process for a nuclear power plant to ensure that all safety requirements on the design of the plant are met throughout all stages of the lifetime of the plant, and to confirm that the design, as delivered, meets requirements for manufacture and for construction, and as built, as operated and as modified (IAEA SSR-2/1 Requirement 10).
- A set of DEC shall be derived on the basis of engineering judgement, deterministic assessments and probabilistic assessments for the purpose of further improving the safety of the nuclear power plant by enhancing the plant's capabilities to withstand, without unacceptable radiological consequences, accidents that are either more severe than design basis accidents or those involving additional failures. These design extension conditions shall be used to identify the additional accident scenarios to be addressed in the design and to plan practicable provisions for the prevention of such accidents or mitigation of their consequences if they do occur (IAEA SSR-2/1 Requirement 20).

Common Position

Comprehensive deterministic safety assessments and probabilistic safety assessments carried out throughout the design process for a nuclear power plant will ensure that all safety requirements on the design of the plant are met.

Deterministic and probabilistic assessments combined with engineering judgement can effectively identify further safety improvements, such as enhancing the plant's capabilities to withstand, without unacceptable radiological consequences, accidents that are either more severe than design basis accidents or that involve additional failures.

The ABWR regulators support the effective use of comprehensive safety analyses to improve the safe design and operation of ABWRs.

GLOSSARY

Basemat – Floor of containment below reactor pressure vessel, of concrete construction.

Cliff edge effect[(1)] – In a nuclear power plant, an instance of severely abnormal plant behaviour caused by an abrupt transition from one plant status to another following a small deviation in a plant parameter, and thus a sudden large variation in plant conditions in response to a small variation in an input.

Containment[(1)] – Methods or physical structures designed to prevent or control the release and the dispersion of radioactive substances.

Corium – Molten core debris, comprising a mixture of cladding, control rods, material from the reactor internals and fuel.

Criticality[(1)] – The state of a nuclear chain reacting medium when the chain reaction is just self-sustaining (or critical), i.e. when the reactivity is zero.

Defence-in-depth[(1)] – A hierarchical deployment of different levels of diverse equipment and procedures to prevent the escalation of anticipated operational occurrences and to maintain the effectiveness of physical barriers placed between a radiation source or radioactive material and workers, members of the public or the environment, in operational states and, for some barriers, in accident conditions.

Design basis[(1)] – The range of conditions and events taken explicitly into account in the design of a facility, according to established criteria, such that the facility can withstand them without exceeding authorised limits by the planned operation of safety systems.

Design basis accidents[(1)] – Accident conditions against which a facility is designed according to established design criteria, and for which the damage to the fuel and the release of radioactive material are kept within authorised limits.

Design Extension Conditions – Accident conditions that are not considered for design basis accidents, but that are considered in the design process of the facility in accordance with best estimate methodology, and for which releases of radioactive material are kept within acceptable limits. Design extension conditions could include severe accident conditions.

Deterministic analysis[(1)] – Analysis using, for key parameters, single numerical values (taken to have a probability of 1), leading to a single value for the result. In nuclear safety, for example, this implies focusing on accident types, releases and consequences, without considering the probabilities of different event sequences.

Diversity[(1)] – The presence of two or more independent (redundant) systems or components to perform an identified function, where the different systems or components have different attributes so as to reduce the possibility of common cause failure, including common mode failure.

Drywell – Part of a BWR containment used to accommodate steam and non-condensable gases in the event of an accident.

External hazard (event) [(1)] – Events unconnected with the operation of a facility or the conduct of an activity that could have an effect on the safety of the facility or activity.

Hardened containment vent – A system designed to prevent potential failure of the containment due to over-pressurisation during an accident.

Muon detection system – A system used at the Fukushima Daiichi NPP to determine the post-accident configuration of materials within the RPV. This uses the detection of cosmic ray “muons” to generate 3D images.

Passive (safety) – Providing and maintaining a safety function without the need for an external input such as actuation, mechanical movement, supply of power or operator intervention.

Probabilistic Safety Analysis (Probabilistic Safety Assessment or Probabilistic Risk Assessment)[(1)] – A comprehensive, structured approach to identifying failure scenarios, constituting a conceptual and mathematical tool for deriving numerical estimates of risk.

Redundancy[(1)] – Provision of alternative (identical or diverse) structures, systems and components, so that any single structure, system or component can perform the required function regardless of the state of operation or failure of any other.

Reliability[(1)] – The probability that a system or component will meet its minimum performance requirements when called upon to do so, for a specified period of time and under stated operating conditions.

Safety functions – Functions that are necessary to be performed for the facility or activity to prevent or to mitigate radiological consequences of normal operation, anticipated operational occurrences and accident conditions.

Scram[(1)] – A rapid shutdown of a nuclear reactor in an emergency.

Severe accident[(1)] – Accident more severe than a design basis accident and involving significant core degradation.

Suppression pool – A large mass of water held within a BWR containment vessel, used to provide a source of cooling water and to provide retention of fission products released from the reactor in a severe accident.

Tsunami – A series of travelling waves of long wave length generated by deformation or disturbances of the sea floor (for example, resulting from a seismic event).

Ultimate heat sink[(1)] – A medium into which the transferred residual heat can always be accepted, even if all other means of removing the heat have been lost or are insufficient.

[(1)] *Note: taken from IAEA Safety Glossary: Terminology Used in Nuclear Safety and Radiation Protection: 2016 Edition, IAEA, Vienna (2016): http://www-ns.iaea.org/downloads/standards/glossary/iaea-safety-glossary-rev2016.pdf*

ABREVIATIONS

ABWR - Advanced Boiling Water Reactor

ABWRWG - Advanced Boiling Water Reactor Working Group (of MDEP)

AC - Alternating Current

ACIWA - AC Independent Water Addition

BWR - Boiling Water Reactor

DEC - Design Extension Conditions

DC - Direct Current

ECCS - Emergency Core Cooling System

HPCF - High Pressure Core Flooder

HPCI - High Pressure Coolant Injection

IC - Isolation Condenser

I&C - Instrumentation & Control

INES - International Nuclear and Radiological Event Scale

LOCA - Loss-of-Coolant Accident

LPCF - Low Pressure Core Flooder

MDEP - Multi-national Design Evaluation Programme

MCCI - Molten Core Concrete Interaction

NISA - Nuclear and Industrial Safety Agency (Japan)

NPP - Nuclear Power Plant

PSA - Probabilistic Safety Analysis

RCCV - Reinforced Concrete Containment Vessel

RCIC - Reactor Core Isolation Cooling

RPV - Reactor Pressure Vessel

SAMG - Severe Accident Management Guidelines

SFP - Spent Fuel Pool

SLC - Standby Liquid Control

SRV - Safety Relief Valves

SSC - Structures, Systems and Components

TEPCO - Tokyo Electric Power Company

WENRA - Western European Nuclear Regulators Association