Multinational Design Evaluation Programme Design Specific Common Position CP-AP1000WG-02 – PUBLIC USE	Date: September 2016 Validity: until next update or archiving Version 0

MDEP AP1000WG Design-Specific Common Position

CP-AP1000WG-02

Related to: AP1000 Working Group's activities

COMMON POSITION ADDRESSING FUKUSHIMA DAIICHI NPP ACCIDENT-RELATED ISSUES

Participation

Regulators involved in the MDEP working group discussions:	Canada, China, U.K. and the U.S.
Regulators which support the present common position:	Canada, China, U.K. and the U.S.
Regulators with no objection:	N/A
Regulators which disagree:	None

Multi-National Design Evaluation Programme

AP1000 Working Group

COMMON POSITION ADDRESSING FUKUSHIMA DAIICHI NPP ACCIDENT-RELATED ISSUES

Context:

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 had not been 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 release.

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 nuclear power plants in very severe situations, similar to Fukushima Daiichi, 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 AP1000® plants are engaged in similar activities.

The MDEP AP1000® Working Group (AP1000 WG) members, referred to herein as "regulators", consist of members from Canada, China, the United Kingdom and the United States. Since the regulatory review of their AP1000® applications have not been completed by all of these Countries yet, this paper identifies common preliminary approaches to address potential safety improvements for AP1000® plants as related to lessons learned from the Fukushima Daiichi accident or Fukushima Daiichi-related issues. In seeking common position, regulators will provide input to this paper to reflect their safety conclusions regarding the AP1000® design and how the design could be enhanced to address Fukushima Daiichi issues. The common preliminary approaches are organized into five sections, namely, **new reactors and improvements in safety, external hazards**, **spent fuel pools**, **emergency preparedness in design, mitigation strategies**.

Background information:

The Fukushima Daiichi NPP accident demonstrates the importance of reinforcing the Defence-in-Depth (DiD) 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 reliance on passive design principles with sizeable safety margins and diverse means for delivering critical safety functions as well as flexible, symptom-based operator response plans will help the nuclear power plants ability to manage accidents beyond latest licensing basis.

The design, construction, manufacturing and installation of structures, systems and components important to safety should rely on state of the art engineering measures and sufficient margin beyond the design criteria in order to avoid **cliff edge effects**[1]. Such an approach will help to ensure an appropriate response, should an accident not foreseen in the design or license occur. Provisions aiming at facilitating the repair/recovery of impaired safety functions should also be considered.

Common Position:

NEW REACTORS AND IMPROVEMENTS IN SAFETY

I. The Fukushima Daiichi accident confirms the relevance of passive safety features that have been considered in the AP1000® reactor design, and the importance of these features operating properly.

As compared to most current operating reactors, the *AP1000*® pressurized water reactor has safety systems using mainly passive features, which have the inherent capability to cool the core, containment, and spent fuel pool for 72 hours without the need for ac power or pumps. Instead of relying on active components such as diesel generators and pumps, the *AP1000*® design relies on the natural forces of gravity, natural circulation and compressed gases to keep the core and containment from overheating. As designed, the AP1000® design does not have the same level of vulnerability for loss of ultimate heat sink as active plants. The benefits depend on the demonstration of reliability and effectiveness of the passive systems such as emergency core cooling systems, passive containment cooling system, Automatic Depressurization System (ADS) etc.

[1] **A "cliff edge effect", in a nuclear power plant, is 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. In the context of this Fukushima Daiichi Common Position paper, it is the effects of 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 severe accidents.**

The regulators of the AP1000WG emphasize the importance of proper operation of automatic triggers such as squib valves to actuate the passive safety systems. Even with the reliance on passive systems, for DiD, proper regulatory attention remains important for the active systems.

EXTERNAL 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, it is important that the safety systems of AP1000® are designed and protected to tolerate external hazards.

The accident at Fukushima Daiichi has reinforced the need to undertake a comprehensive analysis of external hazards, including consideration of relevant combinations of events. This should be considered to include an analysis that addresses how these hazards could impact areas of the proposed NPP where significant amounts of radioactive material are expected to be present.

The passive safety systems can provide protection against some types of extreme external events, such as those which occurred at Fukushima Daiichi. While these systems do not need ac power or access to cooling water, they still require actuation; therefore, it is important to protect safety systems including the dc power supply and the protection systems that initiate passive core and containment cooling.

External events could exceed the assumptions used in the design and licensing of a plant, as demonstrated by the events at Fukushima Daiichi. Additional diverse and flexible strategies (see section V) that address the potential consequences of these "beyond-design basis external events" enhance safety at each site. Extreme external events (e.g., seismic events and external flooding) beyond those accounted for in the design basis are highly unlikely but could present challenges to nuclear power plants. In order to address these challenges, licensees need to define and deploy strategies that will enhance their ability to cope with conditions resulting from beyond-design-basis external events.

The regulators of AP1000WG acknowledge the following assessments undertaken by Westinghouse for the standard AP1000® design:

1) Seismic Hazard Assessment

For the AP1000® standard design, the seismic margin assessment (SMA) demonstrates the robustness of the passive safety systems and the associated structures to beyond-design-basis conditions and is already included in the AP1000® licensing basis for design certification. The SMA demonstrates margin over the safe shutdown earthquake (SSE) of 0.3g Peak ground acceleration (PGA) through confirmation that the plant high confidence, low probability of failure (HCLPF) is at least 0.5g pga. The SMA for the AP1000® design is discussed further in the Westinghouse AP1000® design documentation.

2) External Flood Assessment

The standard AP1000® design flood level is specified to be below plant grade level with sufficient margin and demonstration of no cliff edge effects.

3) Extreme Cold, High Wind Hazard, and Extreme High Temperature Assessment

The AP1000® design demonstrates a wide range of extreme environmental conditions covered by the design. Because of the conservatisms that are incorporated into the selection of these site environmental conditions, they are expected to bound most extreme site-specific values.

SPENT FUEL POOLS

III. *The Fukushima Daiichi accident 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 need to be ensured with adequate margin in case of external hazards.*

A. The SFP maintains 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 surfaces should provide assurance that the SFP will maintain this minimum water inventory following an SSE. The fluid retaining surfaces should be protected from internally and externally generated missiles.

The regulators of the AP1000WG are satisfied that the AP1000® has a spent fuel pool which is robustly designed consistent modern standards for design basis internal and external hazards. The AP1000® design documents state that the facility is protected from the effects of natural phenomena such as earthquakes, wind and tornados, floods, and external missiles. The facility is designed to maintain its structural integrity following a safe shutdown earthquake (0.3g pga).

Site specific considerations and the requirements of different regulatory regimes for beyond design basis and margin analysis need to be addressed by licensees and vendors as appropriate.

B. The design has the capability to provide sufficient make up water to the SFP.

During normal operation, natural humidity differences cause the SFP water to evaporate, even while the cooling system is in operation. During an accident scenario, the decay heat generated from the stored spent fuel can lead to inventory losses due to boiling when the cooling system is not in operation. Eventually, makeup water will be required. 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 seismic design criteria in order to ensure its availability following a seismic event.

As a result of its passive design concept, the AP1000® makes limited claims on its active spent pool cooling system in accident scenarios. The regulators of the AP1000WG recognise that the AP1000® can safely manage the consequences of a prolonged loss of spent fuel pool cooling for at least 72 hours through “safety related” seismically qualified makeup water sources. These safety related sources remain available in the event of loss of ac power (off-site power and both standby diesel generators) because they rely on gravity and manual valves.

The provision of makeup water can be extended beyond 72 hours, notably from the passive containment cooling ancillary water storage tank. This does require some active pumping, either to get the water to the passive containment cooling water storage tank at the top of the containment building (from where it can be gravity fed to the spent fuel pool) or directly to the spent fuel pool. However, the regulators of the AP1000WG consider this to be a reasonable, pragmatic and modest claim on active systems given the time available to take the appropriate actions.

The regulators of the AP1000WG also recognise the AP1000® design applies the defence-in-depth principle to the provision of makeup water, with a range of alternative water sources and makeup systems provided. These can be used instead of, or in preference to, the safety related means highlighted in the safety submissions, depending on the situation and the availability of services. The SFP Spray lines can be used to get water to the spent fuel pool, including from (but not limited to) outside water sources connected by a temporary line or hose.

In addition to providing makeup water to compensate for evaporative and small leakages, the SFP Spray Lines provide an engineered capability to cool the fuel following the most extreme events where water is not being retained by the SFP.

C. The SFP is 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.

There are differences in the detailed design and safety case claims made on the AP1000® SFP cooling system submitted to the various regulators of the AP1000WG. However, there are some commonalities, notably that it is a two train system designed to remove heat from the SFP such that the water temperature is ≤120°F (≤49°C) in normal operation (non-accident scenario). In most operating modes, including when the reactor is at power, a single train of equipment is operating to cool the SFP. This means there is redundancy in the design, which can be further supplemented by a single train of the normal residual heat removal system (RNS) if required. During refuelling modes with a full or partial core offload, both trains of the SFP cooling system and a single train of RNS may be required to achieve the ≤120°F (≤49°C).

The regulators of the AP1000WG accept that the claims made for the AP1000® SFP cooling system in an accident scenario are different to those of "traditional" active plant designs. The SFP cooling system (and the RNS) is not designated as safety-related and does not feature prominently in justifications of the AP1000®'s resilience against Fukushima Daiichi-type events (for example, prolonged loss of power or ultimate heat sink). However:

- It is important that the SFP cooling system (and its supporting systems) is reliable, robust and fault tolerant to minimise the frequency of loss of SFP (active) cooling events. While the fuel will be safe in the SFP for a prolonged period of time even with the water boiling as long as sufficient makeup water is provided to keep it covered, it will be desirable to return the water temperature to a more typical range as soon as is practicable to terminate the event. To achieve this, the water in the SFP will need to be recovered to the level of the SFP suction connections and the SFP pumps restarted.

D. SFP has 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 be focus on core cooling, assessing the scenario and taking the proper steps to stabilize the unit. If there are no reliable water level indications, like what happened during the Fukushima Daiichi event, uncertainty of the SFP water level could divert attention and resources from critical operations to the SFP in order to verify pool levels.

In addition to narrow range indications of the SFP water level for normal operation, the AP1000® has three safety-related spent fuel pool level instrument channels which measure the water level from the top of the spent fuel pool to the top of the fuel racks. This extended range is a long standing requirement that follows from the passive design concept of accepting that evaporative and boiling water losses are acceptable providing makeup water is supplied to keep the spent fuel in the racks covered. The safety related classification provides for the following additional design features:

- Seismic and environmental qualification of the instruments
- Independent power supplies
- Electrical isolation and physical separation between instrument channels
- Display in the control room as part of the post-accident monitoring instrumentation
- Routine calibration and testing

In addition, safety-related spent fuel pool level instruments and associated instrument tubing lines are located below the fuel handling area operating deck and the cask wash down pit. This location provides protection from missiles that may result from damage to the structure over the spent fuel pool.

The regulators of the AP1000WG recognise that the AP1000® SFP water level indication is robust for design basis events, and has many features which could be of benefit to the operators during an extreme event.

EMERGENCY PREPAREDNESS IN DESIGN

IV. The accident at Fukushima Daiichi NPP highlighted how complicated emergency response can be if multiple reactors on the same site are affected at the same time and electrical power is unavailable. For such large accident scenarios there is a need to ensure that all reasonably practical measures are in place to mitigate accident consequences; to ensure with a high level of confidence that the design of the installation will minimize any radiological consequences; and review the consideration for the need of additional emergency staff and the power requirements of emergency response equipment.

The emergency preparedness aspects of the AP1000 design has taken into account the following causal factors. The Tohoku earthquake was felt over a significant area of Japan. In some areas, there was extensive 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 600km2. 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 for access to the Fukushima Daiichi NPP site for specialist equipment and personnel.

At the Fukushima Daiichi NPP, the tsunami rendered most of the 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 also 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 was 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 on the Fukushima Daiichi site 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.

Therefore, a key lesson is that the severe environmental conditions and possible degradation of the regional infrastructure that would occur in a Fukushima Daiichi-like accident could impact emergency preparedness on an AP1000® site and should be considered in the emergency planning. On multi-unit AP1000® sites, the site 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 arrangements.

Means of monitoring the status of the units is vital for ensuring that the required safety functions are fulfilled. The regulators of the AP1000WG are satisfied that consideration of severe accident conditions has been given to the design and installation of instrumentation and controls in both the reactor building and the spent fuel pools. However, the reliability and functionality of release measurements, radiation level measurements and meteorological measurements may need to be strengthened on a site by site basis. The readiness to take samples and analyse them in a laboratory should also be considered.

The regulators of the AP1000WG recognise the importance of the main control room for managing the response to an extreme event on an individual AP1000® unit and acknowledge the design provision already included. However, other facilities are required to support plant operating staff responding to emergencies, with appropriate consideration given to accessibility and habitability. The "standard" AP1000® design is provided with an Emergency Response Facility which provides both a place to work and resources for personnel providing plant management and technical support to the plant operating staff during emergency evolutions. It is also intended to relieve operators of peripheral duties and communications not directly related to reactor system manipulations and prevents congestion in the control room.

The regulators of the AP1000WG welcome this provision but expect that the main control room, Emergency Response Facility, and any identified local control points (locations for necessary manual

actions, sampling and possible repair works) are shown for each site to be adequately protected against applicable internal and external hazards. Changes to the provision provided at each site and its locations are therefore to be expected, depending on the challenges faced at each site.

As part of this, the reliability and functionality of the on-site and off-site communication systems provided on an AP1000® facility should be reviewed so that it can deliver the emergency arrangement requirements and strategy identified for the site, with consideration given to the conditions that could result from internal and external hazards.

MITIGATIVE STRATEGIES

V. *Strategies to deal with Fukushima Daiichi NPP type events should be in place prior to operation. The AP1000® pressurized water reactor has passive safety systems, which have the capability to cool the core, containment, and spent fuel pool for 72 hours without the need for ac power or pumps. After 72 hours, mitigation strategies need to be implemented to allow the AP1000® plants to cope without their normal electrical power sources. These, strategies must keep the reactor core and spent fuel pool cool, as well as protect the containment building. The mitigation strategies are expected to use a combination of currently installed equipment, additional portable equipment that is stored on-site, and equipment that can be brought in from support centers. Hence, the design shall include features to enable the safe use of non-permanent equipment for restoring the essential safety function capability including removal of heat from the containment.*

The underlying strategies for coping with beyond-design-basis conditions resulting from an extended loss of ac power and loss of access to the normal heat sink for AP1000® plants involve a three-phase approach as follows:

1. Initial coping through installed plant equipment without ac power or makeup to the passive containment cooling system (PCS). From 0 to 72 hours, the AP1000® design includes passive systems that should provide core cooling, containment, and SFP cooling.

2. Following the 72-hour passive system coping time, support is necessary to continue passive system cooling. From 3 to 7 days, this support should be provided by installed plant ancillary equipment or by offsite equipment installed to connections provided in the AP1000® design.

3. To extend the passive system cooling time beyond 7 days to an indefinite time, offsite assistance is necessary, such as the delivery of diesel fuel oil.

The regulators of AP1000WG recognize these strategies are a fundamental part of the AP1000® reactor design and are consistent with the Fukushima Daiichi accident lessons learnt. By providing multiple and diverse means of power and water supply to support key safety functions, these strategies can mitigate the consequences of beyond-design-basis external events. Connections are provided for generators and pumping equipment that can be brought to the site to back up the installed equipment. Additional review should consider the need for onsite and offsite equipment and its compatibility with AP1000® standard equipment.