MDEP

Common Position

CP-STC-02

Common Position Addressing Fukushima Daiichi Nuclear Power Accident

Participation

Regulators involved in the MDEP STC discussions:	All MDEP members
Regulators which support the present report:	All MDEP members
Compatible with existing IAEA related documents:	Yes

Introduction:

The MDEP Steering Technical Committee members, referred to herein as "regulators", consist of members from:

- Canada (CNSC – Canadian Nuclear Safety Commission)
- People's Republic of China (NNSA – National Nuclear Safety Administration)
- Finland (STUK – Radiation and Nuclear Safety Authority)
- France (ASN – Nuclear Safety Authority)
- Hungary (HAEA – Hungarian Atomic Energy Authority)
- India (AERB – Atomic Energy Regulatory Board)
- Japan (NRA – Nuclear Regulatory Authority)
- Korea (NSSC – Nuclear Safety and Security Commission)
- Russian Federation (Rostechnadzor)
- South Africa (NNR – National Nuclear Regulator)
- Sweden (SSM – Swedish Radiation Safety Authority)
- Turkey (TAEK – Turkish Atomic Energy Authority)
- United Arab Emirates (FANR – Federal Authority for Nuclear Regulation)
- United Kingdom (ONR – Office for Nuclear Regulation)
- United States (NRC – Nuclear Regulatory Commission)

Following the nuclear accident in Japan as a consequence of the earthquake and tsunami, the MDEP Members provide the following information, based on initial information available, to ensure adequate safety of new reactor design activities being undertaken pursuant to the MDEP programme of work. Due to the extensive nature of the magnitude and duration of the Fukushima Daiichi NPP accident, it is important to consider lessons learnt at an early stage of the design. In this context, the extensive work done by the IAEA, the International Atomic Energy Agency, is also acknowledged[1].

Vendors, licensees and applicants involved in New Design activities should examine the implications of the Fukushima Daiichi NPP accident and identify relevant issues to be taken into account to strengthen defence in depth. Those lessons learnt should include, but not be limited to, plans to assess the following:

- Provisions taken in the design basis concerning flooding, earthquake, other extreme natural phenomena and combinations of external event hazards appropriate to each country,
- The robustness of the plant to maintain its safety functions beyond the design basis hazards,
- The capability of the plant to withstand extended loss of all electrical power supplies as well as prolonged loss of ultimate heat sink and other essential supplies, and
- The capability of the plant to cope with such extreme situations, including provisions to manage severe accidents (such as combustible gas management).

In assessing these areas, the effect of multiple units and nuclear fuel storages should be considered.

The MDEP regulators will strive to harmonize approaches to incorporate lessons learnt in their ongoing national safety reviews of new reactors. Based on the design-specific common positions, this paper identifies the approaches to address potential safety improvements for several designs as related to lessons learned from the Fukushima Daiichi NPP accident or related issues. Designs being considered are:

[1] The Fukushima Daiichi Accident, Report by the Director General; IAEA GC(59)/14; 2015

- EPR – the EPR is a 1650 MWe pressurized water reactor
- AP1000 – the AP1000 is a 1110 MWe pressurized water reactor
- APR1400 – the AP1400 is a 1400 MWe pressurized water reactor
- VVER – the VVER is a 1200 MWe pressurized water reactor
- ABWR – the ABWR is a boiling water reactor with a power output in the 1350 to 1460 MWe range

The designs were assessed in the following five areas:

- external hazards
- reliability of safety functions (addressing station black-out and ultimate heat sinks),
- accidents with core melt,
- spent fuel pools, and
- emergency preparedness in design.

Mitigation of extreme external hazards often implies improving the robustness of an NPP. While the MDEP focus in addressing issues related to the Fukushima Daiichi NPP accident has been on safety, it should be noted that improved NPP robustness will also improve the capability of the plant to withstand security related challenges.

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 such as taking into account analyses providing frequency/magnitude information on tsunamis in the region, 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 out of the four 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 that experienced at Fukushima Daiichi NPP during and after the 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 new plants are engaged in similar activities.

Lessons Learned from the Fukushima Daiichi Accident:

The Fukushima Daiichi NPP 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. The accident also reinforced the need to have a comprehensive safety analysis using both deterministic and probabilistic methods in a complementary manner to provide 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, 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 (SSCs) 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**[2]. 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.

Common Position:

EVOLUTIONARY IMPROVEMENTS IN SAFETY

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

As compared to most current operating reactors, these new reactors contain additional safety measures. For example, there are several (typically four) redundant and independent trains of safety systems, including emergency diesel generator in each of the trains and additionally typically two diverse station black-out diesel generators. There are also means to provide for severe accident management and protection against external hazards such as earthquakes and flooding. Total loss of main heat sink is also accounted for in the designs.

Some designs have a greater emphasis on passive features which have the inherent capability to cool the core, containment, and spent fuel pool for at least 72 hours without the need for AC power or pumps. 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.

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 reactors are designed and protected to tolerate external hazards and internal events , mostly by applying adequate physical separation and protection against dynamic loads.

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

There are a number of different approaches available for the evaluation of external hazards. This is dependent on site characteristics as well as 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

[2] **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.

site, a design basis event is determined with consideration of the site hazard curves. 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 potentially relevant external hazards (single or in combinations), 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 the frequency and/or magnitude of 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.

Protection against Floods and Tsunamis

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 SSCs 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 SSCs 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, it would be useful to refer to the 2011 IAEA's Specific Safety Guide on meteorological and hydrological hazards (SSG-9), on which much of the previous discussion is based[3].

All SSCs important to safety 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.

[3] http://www-pub.iaea.org/MTCD/publications/PDF/Pub1506_web.pdf

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 the Fukushima Daiichi NPP, 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.

RELIABILITY OF SAFETY FUNCTIONS

III. It is observed to date, from those regulators who have made safety findings in the review of their design applications, that since most safety functions depend on electric power that the reactors could suffer cliff-edge effects after a limited period of time following infrequent and severe external hazards, particularly those involving a common-cause failure that results in long-term loss of power and cooling. 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 cooling and confinement of radioactive material. Most safety functions of a reactor 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 NPP accident.

Other actions for increasing the reliability of AC power supply at a reactor 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.

Although the reliability of the power supplies is acceptable, as part of the Defence-in-Depth approach for plants, a mitigation strategy for long term loss of electrical power is needed for all reactor states for an adequate length of time. Examples 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 by providing portable means to inject water into the steam generators, reactor coolant system, and make-up water into the spent fuel pool. Passive designs may also be used for residual heat removal.

ACCIDENTS WITH CORE MELT

IV. The regulators recognise that the generic design includes measures to mitigate the consequences of severe accidents. The design benefits from reinforced measures to prevent accident situations such as high pressure core melt, global hydrogen detonations and in-vessel and ex-vessel steam explosions, which would lead to large or early releases. 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.

The Fukushima Daiichi NPP accident confirms the lesson learnt already from earlier NPP accidents that potential accidents likely to lead 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 safety 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 Daiichi NPP accident deal with provisions to avoid over pressurisation (relying for example on containment venting and/or containment spray systems), hydrogen management and ultimate containment pressure strength in such accidents. Consideration should also be given to the possibility of hydrogen combustion outside of the containment.

SPENT FUEL POOLS

V. The Fukushima Daiichi NPP 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 cooling and 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 spent fuel pools (SFP). Once spent fuel in a pool is overheated, it is very difficult to predict how the accident develops, at what time significant fuel melt starts to occur, and how the molten fuel finally behaves. 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. 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 a safe shutdown earthquake (SSE). The fluid retaining surfaces should be protected from internally and externally generated missiles.

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 loses increases when the cooling system is not in operation. 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. Back-up mobile systems with connection points at separate locations are provided. Make-up systems can maintain the required water level by means of sprays or injection lines.

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 focused 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 NPP accident, 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. Water level instruments should be protected from falling debris and should be capable of withstanding design-basis conditions for an extended period. Backup power capability should also be provided.

EMERGENCY PREPAREDNESS IN DESIGN

VI. The accident at the 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, and to ensure that the design of the installation will minimize any radiological consequences. Additional review should consider the need for additional emergency staff and the power requirements of emergency response equipment.

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.

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.

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 within the required timeframe.

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 enable and support the accident management measures.

Severe environmental conditions and possible degradation of the regional infrastructure that may occur in an accident like the one at Fukushima Daiichi NPP 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.

STATEMENT REGARDING THE VIENNA DECLARATION ON NUCLEAR SAFETY

On the 9th February 2015 the Vienna Declaration on Nuclear Safety was adopted at the Diplomatic Conference of the Convention on Nuclear Safety. The declaration states a number of principles related to the design, operation and regulation of new and existing nuclear power plants. Out of these principles, the following one is relevant in view of the MDEP objectives:

> *New nuclear power plants are to be designed, sited, and constructed, consistent with the objective of preventing accidents in the commissioning and operation and, should an accident occur, mitigating possible releases of radionuclides causing long-term off site contamination and avoiding early radioactive releases or radioactive releases large enough to require long-term protective measures and actions.*

The reactor designs considered by the MDEP programme are designed with the aim of preventing events that might lead to early radioactive releases or radioactive releases large enough to require long-term

protective measures and actions. Part of the activities of the MDEP DSWGs is to consider, from a regulatory perspective, how these objectives are adequately addressed.