Multinational Design Evaluation Programme (MDEP)

Technical Report

TR- HPR1000WG-03

Related to: HPR1000 Working Group's activities

Technical Report: HPR1000 HAZARDS

Participation

Countries involved in the MDEP working group discussions:	China, U.K., South Africa and Argentina
Countries which support the present common position	N/A
Countries with no objection:	-
Countries which disagree	-
Compatible with existing IAEA related documents	Yes

Contents

No table of contents entries found.

Contents

I. INTRODUCTION

During the second HPR1000 Working Group (HPR1000WG) meeting [Ref. 1], the participants expressed an interest in understanding the similarities and differences in regulatory approaches to hazards assessment of the member countries, and the potential implications of these regulatory approaches on the design of the HPR1000 technologies. A hazards technical expert's subgroup (TESG) was subsequently established to engage on hazards-related topics, and to identify common positions, where applicable.

This technical report is based on engagements between representatives of the Hazards TESG, and the responses provided to a questionnaire that was developed to capture the regulatory approaches used in relation to identifying, characterising, screening, and assessing hazards in each member country. The questionnaire developed by the Hazards TESG, with each country's responses, is provided in the appendix to this document.

The purpose of this report is to identify the similarities and differences in regulatory approaches, and where applicable, to identify common positions for safety in relation to hazards and/or the conclusions of the safety analysis for the HPR1000 design. This report provides a high-level summary of each country's regulatory philosophy (Section II) and then due to the broad nature of hazards provides several pertinent, example hazards that illustrate how these regulatory approaches are applied in practice. These examples are used to highlight similarities and differences in regulatory approaches, and to identify any implications such as the expectation for additional analyses. The report concludes by explicitly highlighting common practice and summarising any potential implications of differences in regulatory practice.

The scope of this report is limited due to the varying status of each participating nation's regulatory assessment of the HPR1000 reactor technologies. This report does not provide commentary on the implications of any differences in regulatory approaches/expectations for hazards on the design of the HPR1000 plant and its structures, systems, and components.

II. OVERVIEW OF APPROACHES TO HAZARDS

SUMMARY

The first meeting of the Hazards TESG took place at the third HPR1000 WG meeting [Ref. 2]. At this meeting the hazard-related topics of interest were discussed and agreed by the members of the Hazards TESG. The regulatory approaches to certain topics were identified as being significantly different between members, such that it was considered unlikely that a common position could be achieved. For example, the design basis event expectations for external hazards vary significantly between members of the Hazards TESG, and in some instances the expectations for derivation of a design basis event also varies between different external hazards (e.g. return periods). These topics were therefore excluded from further consideration. It was noted that there were more comparable expectations for internal hazard design basis events. Further, following the events at Fukushima-Daiichi all regulators have moved to a position where designs are expected to include resilience against rare and severe hazards, which are additional to design basis events, and represent less frequent events and more challenging accident conditions.

As a result of these discussions, the following topics were identified for further consideration through the development of a questionnaire. The associated questions agreed by the TESG are listed in Annex 1 along with each member response. The topics included in the questionnaire are outlined below:

- High Energy Pipe Failure
- Dropped Loads
- Internal missiles
- Combined hazards in areas of high risk
- Multi-hazard barriers
- Expectations on layout (including exceptions to segregation)
- Fire modeling (including validation and verification of the analysis)
- Beyond design basis events
- Maximum credible events

The approach of each Regulator to these hazard topics and the questionnaire responses were discussed during the fourth HPR1000 WG meeting [Ref. 3]. The vendor[1] for the HPR1000 reactor technology provided a presentation that described the hazards considered in the HPR1000 design, and the associated design bases [Ref. 4], based on the relevant Chinese codes and standards. The vendor and NNSA consider the standards that have been applied to be consistent with the guidance provided in IAEA safety standards.

All national regulators participating in the HPR1000 WG ensure their national guidance documents are aligned with IAEA documentation relevant to hazards. Therefore, at a principles level, the regulatory expectations for the selected hazards are similar between the members of the Hazards TESG. For example, all regulators expect a range of analysis approaches to be used to evaluate hazards and their effects on a design including: deterministic approaches, design basis analysis, analysis of design extension conditions without significant fuel degradation (including demonstrating an absence of cliff edge effects), probabilistic safety analysis and severe accident analysis. The technical discussions also demonstrated that there are differences in the application of these high-level expectations for most hazards, and in particular where detailed methodologies were discussed for internal hazards. These differences are relevant to the assumptions used in the identification, screening, and characterisation of each hazards (including combinations), and also the analysis methods employed.

The appendix provides a detailed summary of the Regulatory expectations and relevant good practice that is adopted for specific hazards in response to the questionnaire developed by the Hazards TESG. This table provides a clear overview of commonality and differences between each member nation and forms the basis for this report.

Using the detailed information from the appendix, the remainder of this section presents the general approach of each Regulator to hazards. In the following sections (III – V) several pertinent hazards are reviewed as examples of how the various regulatory approaches are applied in practice. These examples highlight similarities and differences

1 The Vendor is a representative of the two design authorities for HPR1000 reactor technology; China General Nuclear, the designer of option 1, and China National Nuclear Corporation, the designer of option 2.

in regulatory approaches to identify any implications for the HPR1000 design, such as the expectation for additional analyses.

CHINA

The Chinese nuclear Regulator (NNSA) operates a prescriptive regulatory approach. High-level requirements are provided in the HAF documents (safety requirements), with the detailed technical requirements provided in the supporting HAD documents (safety guides). Consideration of hazards (and combinations) is a requirement. The standards relevant to hazards are:

- HAF101-1991 Safety Regulation for Nuclear Power Plant Siting
    - HAD101/01-1994 Earthquake Problems in Relation to Nuclear Power Plant Sitting
    - HAD101/03-1987 Site Selection and Evaluation for Nuclear Power Plants with Respect to Population Distribution
    - HAD101/04-1989 External Human Induced Events in Relation to Nuclear Power Plant Siting
    - HAD101/06-1991 Relationship between Nuclear Power Plant Siting and Hydrological Geology
    - HAD101/09-1990 Determination of design basis Flood for Nuclear Power Plant Sited by Coast
    - HAD101/10-1991 Extreme Meteorological Events in Nuclear Power Plant Siting (Excluding Tropical Cyclone)
    - HAD101/11-1991 design basis Tropical Cyclone for Nuclear Power Plants
    - HAD101/12-1990 Foundation Safety Problems of Nuclear Power Plants
- HAF102-2016 Safety regulation for design of nuclear power plants
    - HAD102/04-2019 Protection Design against Internal Hazards (other than Fire and Explosion) in Nuclear Power Plants
    - HAD102/05-1989 External Man-Induced Events in Relation to NPP Design

- HAD102/11-2019 Protection Design against Fire and Explosion in Nuclear Power Plants

Chinese standards are benchmarked with IAEA documentation to ensure consistency of approach.

UNITED KINGDOM

In the UK, the Office for Nuclear Regulation (ONR) regulates nuclear safety, security, safeguards, transport, and conventional health and safety on licensed sites according to the UK goal setting regulatory framework. In line with that framework ONR applies a goal setting regulatory philosophy that is consistent with the UK's health and safety law. Fundamental to this approach is the legal duty for duty holders to reduce risks so far as is reasonably practicable (SFAIRP). As part of this, ONR looks for operators of licensed nuclear installations to demonstrate that the normal requirements of good practice in engineering, operation and safety management are met and that risks in operation are reduced to be As Low As Reasonably Practicable (ALARP). This places duties on both the design organisations and on future licensees and operators.

ONR publishes its high-level expectations for nuclear safety in the Safety Assessment Principles (SAPs). Expectations for hazards are explicitly covered by a total of 19 SAPs; EHA.1 – EHA.19, but there are many other related and relevant SAPs. The ONR SAPs are considered fully in line with IAEA guidance and standards. The SAPs cannot reflect the breadth and depth of the entire suite of IAEA publications and so ONR explicitly identify those documents as relevant good practice within technical assessment guides (TAGs). The TAGs provide more specific, technical guidance on a range of safety topics. These provide guidance to ONR's inspectors in making judgements on the adequacy of a dutyholder's safety documentation against the ALARP principle. Relevant technical assessment guides for hazards include:

- NS-TAST-GD-013 for External Hazards
- NS-TAST-GD-014 for Internal Hazards

In addition to the SAPs and technical assessment guides, ONR has also published additional technical guidance for new reactor designs wishing to be assessed through the UK's Generic Design Assessment (GDA) process.

- ONR-GDA-GD-007 - New Nuclear Power Plants: Generic Design Assessment Technical Guidance

The GDA process enables ONR and other regulators to assess the safety, security, and environmental implications of new reactor designs, separately from applications to build them at specific sites. GDA is a stepwise process, with the assessment getting increasingly detailed at each step following the claims, arguments, and evidence (CAE) to safety documentation. At the time of writing the generic UK HPR1000 design is being assessed by ONR through its GDA process, to determine if a Design Acceptance Certificate (DAC) can be issued. A nuclear site licence would still need to be obtained by any operator of HPR1000 technology before the reactor design could be deployed on a specific site in Great Britain.

Demonstrating that risks related to hazards are reduced to be ALARP does not require in all cases an analytical quantification of risk and benefits, but operators of licensed installations use relevant good practice (RGP) to demonstrate the adequacy of their approach against the ONR SAPs, including those relevant to hazards. RGP is the minimum requirement by which the operator can demonstrate the legal requirement of reducing safety risks to be ALARP. The ONR SAPs recognise IAEA publications as RGP via the TAGs. The use of both a goal setting approach and RGP provides operators of licensed sites the flexibility to adopt the most relevant guidance for any specific scenario, so long as this is adequately justified in their safety documentation.

SOUTH AFRICA

The South African nuclear Regulator's (NNR) approach to the regulation of nuclear safety and security takes into consideration:

- the potential hazards associated with the facility or activity;
- the need for the authorisation holder to establish safety related programmes commensurate with nuclear and radiation risks; and
- the requirement to exercise regulatory control over technical aspects such as the design and operation of a nuclear facility.

The approach highlights the fundamental principle that the authorisation holder retains the primary responsibility for safety of its facilities and activities. The regulatory philosophy adopted by the NNR is a hybrid employing methodologies and principles based on the approach taken in the regulatory framework, the maturity of the authorisation holder, and international developments related to regulation and emerging safety standards and issues.

The NNR has adopted a process-based approach in regulating facilities and activities. This entails identifying key processes to manage nuclear and radiation safety for facilities and activities. This approach is supported by the NNR requiring the use of a risk analysis which is used for regulatory decision making related to events that impact adversely on nuclear and radiation safety.

The authorisation holder is required to demonstrate that safety related aspects such as ALARA are applied to the satisfaction of the NNR. The NNR requires authorisation holders to demonstrate application of good engineering practice and justify the use of codes and standards.

The NNR's Regulatory Framework consists of legally binding requirements by International Safety Conventions, laws passed by Parliament that govern the regulation of South Africa's nuclear industry, regulations, authorisations, conditions of authorisations, requirements, and guidance documents that the NNR uses to regulate the industry. Requirements are developed in conjunction with the applicable authorised action and effectively cover all the relevant requirements on the holder.

The NNR enforces these requirements on all applicants and authorisation holders. Certain requirements in the legislation are prescriptive to the extent that no further elaboration is necessary. Other requirements are broad in nature.

The NNR establishes additional requirements based on international best practices. These requirements are registered either directly in the authorisations or in "Requirements Documents".

The NNR Safety Standards are premised on international standards such as the IAEA Safety Standards, the UK NII Safety Principles and the WENRA Reference levels. The safety standards provide the principal safety criteria relating to risk criteria, and dose limits for normal operating conditions, applicable to members of the public and workers.

The safety standards further lay down principal radiation and nuclear safety requirements which are applied to all nuclear installations and other regulated actions, and include the following:

- Defense-in-depth
- ALARA
- Good engineering practice
- Quality management
- Accident management and Emergency Preparedness
- Safety Culture
- Graded approach

The radiological dose and risk limits for the public and workers relate directly to the objectives of nuclear and radiation safety and are therefore considered the most fundamental yardsticks against which to assess nuclear safety, contributing towards a more consistent and transparent basis for regulatory decision making. The dose limits are consistent with the IAEA Basic Safety Standards.

For the existing Koeberg nuclear power station, the applicable laws, regulations, codes, and standards that were used in its design, construction and manufacture were basically those used in French reference stations. Whenever French safety rules did not cover the scope of South African or US rules, the US rules, according to how they were interpreted for the reference station, and the South African rules were applied. Where other international regulations apply for Koeberg, they are referenced in the Koeberg SAR.

Amongst the many general nuclear and radiation safety principles that underpin and form the basis of the NNR Safety Standards, the following one is of relevance to the topic of this report:

The authorisation holder must demonstrate effective understanding of the hazards and their control for an action or facility through a comprehensive and systematic process of safety assessment. The safety assessment must incorporate both deterministic and probabilistic approaches where appropriate.

ARGENTINA

The Argentinian nuclear Regulator (ARN) operates a goal setting regulatory approach. High-level regulatory requirements and expectations are established in the "AR" regulations which are harmonised with the IAEA safety standards. AR regulations have a "performance" based character by which the way of achievement of safety objectives, is based on the appropriate licensee's decision making. Licensee has flexibility in adopting additional guidance for development of submissions as long as they demonstrate to be adequate and its implementation justified.

The relevant AR regulations include the following:

- AR 10.10.1 Site Evaluation for Nuclear Power Plants,
- AR 3.1.3 Radiological Criteria for Accident Conditions in Nuclear Power Plants,
- AR 3.2.1 General Safety Criteria for Design of Nuclear Power Plants,
- AR 3.10.1 Protection against Earthquakes in Nuclear Power Plants.

III. PIPE BREAKS

This section compares the regulatory approaches of the HPR1000 Hazards TESG with respect to pipe breaks, to identify areas of common practice and key differences. The implications of these differences in regulatory approach are considered with respect to the design of the HPR1000.

The pipe breaks hazard includes high, medium and low energy pipe systems. Of these, high energy pipe failures are the most energetic and usually associated with bounding load cases and consequential hazards. Consequently, the remainder of this section describes each member nation's regulatory expectations relating to high energy pipe failures. It should be noted that other (medium and low) energised pipe systems may need to be analysed under different regulatory regimes, to evaluate the consequences of consequential hazards, such as internal flooding.

SCOPE: EXCLUSIONS AND SCREENING CRITERIA

All regulators in the Hazards TESG consider IAEA guidance [Ref. 5] provides a suitable definition of a high energy system. This guidance defines a system as being high energy if it operates at a pressure equal or greater than 2.0 MPa and/or the operating temperature is 100°C or greater in the case of water or equivalent in line (other limits may apply for other fluids). Some nations may choose more conservative parameters that will lead to additional systems being screened-in for assessment (e.g. US NRC NUREG 0800 defines high energy pipelines as having a pressure equal or greater than 1.9 MPa and/or the operating temperature is 95°C), but it is unlikely that any screening criteria will be more optimistic than the IAEA guidance. Furthermore, most regulators require all energised systems (i.e. both low and medium energy systems) to be assessed, albeit, the level of detail may vary depending on the nature of the hazard, design detail and use of bounding hazard scenarios.

Exclusions and screening criteria are used to bound the scope of the HEPF and represent a significant difference between the approaches of the Hazards TESG members. There are clear differences between the regulatory approaches for exclusionary criteria, with the Chinese Regulator allowing for exclusions to be identified and the UK Regulator not applying any exclusion for HEPF.

For example, the acceptability of leak-before-break arguments as an exclusionary criterion varies between Hazards TESG members. Similar debate has been held by other MDEP WGs [e.g. Ref. 6]. There are also differences between regulators on the acceptability of time at risk, utilisation, and geometry arguments for exclusions. Those regulators that do not accept exclusionary arguments as primary safety claims would expect an assessment of the consequences of HEPF for relevant systems from the HPR1000, assuming a full pipe break, unless an alternative justification could be provided for their continued exclusion or they are screened from further consideration based on appropriate screening criteria. It is noted that IAEA SSG-64 [Ref. 5] considers the undertaking of consequence analysis of a full pipe break as good practice to demonstrate the robustness of a design.

With regards to screening, the regulators agree that both deterministic and probabilistic screening criteria are appropriate for use. In applying the screening criteria consideration should be given to the plant configuration, geometry, and location of SSCs important to safety. Potential consequential internal hazards should also be identified for consideration in the analysis. Hazard combinations may be screened out when the probability of occurrence is below a threshold (typically 10^{-7} per annum or lower) but such approaches should be sufficiently justified. However, good practice is moving beyond simple frequency screening. For example, Appendix 1 of SSG-64 (Ref. 5) highlights multiplying numbers together should be treated with caution and reminds the reader that the first hazard may affect the frequency or damage potential of a second hazard. Furthermore, it may still be reasonable to enhance robustness of a design even for a particular combination of hazards with low frequency if the potential consequences warrant such design enhancements.

The screening process can be used to identify appropriate bounding scenarios, which can then be applied in the subsequent analysis to ensure that the design is robust against the HEPF hazard (and associated combinations).

One topic discussed by the Hazards TESG, is that the UK Regulator allows for identification of highest integrity components (HIC); items whose failure is considered to be less frequent than 10^{-7}. However, this is not an exclusionary criterion in the normal sense. To satisfy the HIC claim items are subject to robust assessment of detailed evidence, over and above what is considered relevant good practice and including evaluation of the consequences of failure. Only once all necessary evidence has been provided and assessed will a claim of HIC be accepted; and the items can then be screened out of further analysis as a hazard contributor.

Irrespective of the HIC designation the expectations of internal hazards remain, and any hazards that could impact the HIC should be identified and assessed. It is the UK's expectation that a new nuclear power plant (NPP) design should demonstrate that the plant layouts are optimised to eliminate all potential hazards to HICs, so far as is reasonably practicable. Where this is not practicable through the optimisation of the layout, then robust safety measures should be adopted to protect against and/or mitigate any hazard effects. Any hazards that remain, are within the design basis threshold and still provide a challenge to the HIC should be quantified and consequences conservatively assessed to demonstrate that the integrity of the HIC remains and the risks are demonstrated to be ALARP.

All regulators agree that safety trains should be segregated where practicable or protected, to prevent consequential failures resulting from hazards, including pipe failures. Where divisional barriers are included for protection of safety trains then these should be designed to withstand bounding load cases, which should include consideration of combined hazard loadings.

ANALYSIS METHODS

Following the application of exclusionary and screening criteria, the remaining HEPF hazards screened-in to the assessment should be analysed. The HPR1000 design has been analysed for several HEPF hazards.

All regulators agree that it is for the designer / vendor to demonstrate that the specific deterministic safety analysis methods used as part of the design basis analysis are suitable and sufficient. It is expected that both global and local effects should be considered, including combined consequential effects. In doing so the designer / vendor should provide appropriate characterisation of the event sequences to identify all simultaneous loads on the protective barriers, safety measures and SSCs. For SSC substantiation (the generation of evidence that demonstrates a claim on SSCs can be achieved, such as by calculation, modelling or research) the design basis analysis should consider consequential hazards resulting from pipe interactions. The response of both SSCs and barriers to combined loads (e.g. pipe whip, jet impact, steam release and flooding etc.) should be evaluated. The analysis should be suitably conservative, use appropriate codes and tools, supported by robust justification of their relevance, and appropriately verified and validated for the application applied.

With respect to the detailed analysis, there exist some similarities and differences between regulatory approaches and how conservatism is included in the design basis analyses. It is generally accepted that the initiating hazard and associated faults should be assumed to occur in the most onerous, normally permitted operating conditions and where appropriate, the bounding unmitigated fault scenarios identified via the screening process should be applied. However, arguments relating to leak-before-break are not accepted as primary safety claims by some members of the Hazards TESG.

Deterministic safety analysis for design extension conditions without significant fuel degradation should also be provided to demonstrate the absence of cliff edge effects and identify the margins available before loss of safety functions. The Chinese Regulator has satisfied themselves that the HPR1000 design considers cliff edge effects. The UK Regulator would expect for hazards with a frequency below the design basis threshold, analysis to be undertaken on a best estimate basis. The UK Regulator would also expect sensitivity analysis to be provided for systems with operating limits and conditions near the initial screening criteria to demonstrate the absence of cliff edge effects on other SSCs.

SUMMARY OF DESIGN AND POTENTIAL IMPACT

The analysis provided for HEPF in the HPR1000 design conservatively assumes any SSCs present in the room where the hazard occurs are lost, and a range of hazard combinations are considered. Other protective, defense-in-depth measures include barriers, anti-whip devices and restraints. However, due to the differences in regulatory approaches it is recognised that additional analysis may be required to satisfy the specific expectations of the different regulators.

IV. DROPPED LOADS

This section compares the regulatory approaches of the HPR1000 Hazards TESG with respect to dropped loads to identify areas of common practice and key differences. The implications of these differences in regulatory approach are considered with respect to the design of the HPR1000.

SCOPE: EXCLUSIONS AND SCREENING CRITERIA

Unlike the HEPF hazard, there is less agreement on the scope of the dropped loads hazard between members of the Hazards TESG. It is generally accepted that consequences of dropped loads for lifting equipment should be considered, as well as other falling objects that may occur consequentially as a result of structural failures caused by external and/or internal hazards, or human error (such as incorrect operation, slinging or attachment of a load to lifting equipment). Dropped loads can impact SSCs providing safety functions and should therefore be considered as a potential initiator of fault sequences with nuclear safety consequences. HAD102/04 provides the requirements considered for the HPR1000 design and there has been some consideration of dropped loads in the design.

All regulators expect potential dropped load hazards to be suitably identified and characterised. However, there is clear difference between the regulatory approaches for exclusionary criteria of dropped loads and screening criteria. The Chinese Regulator requires vendors / designers to postulate dropped loads for every lifting or handling device. However, it is generally expected that the vendors / designers will be able to demonstrate that the reliability of the lifting equipment is such that the hazard can be effectively discounted. This is because the Chinese Regulator permits the use of single failure proof cranes arguments to exclude cranes, and associated drop load hazards from further analysis. Defense-in-depth is expected to be provided including via the configuration of handling equipment avoiding SSCs and the integrity of items being lifted, such as fuel casks.

In comparison the UK Regulator expects consideration of the consequences from dropped loads for all lifting operations that occur in the vicinity of nuclear safety significant SSCs that would be susceptible to failure in the event of a dropped load occurring. This includes, for example swing loads and crane collapse. For that lifting equipment not analysed for dropped loads in the HPR1000 design, the UK Regulator would expect them to be considered in the GDA, and if necessary additional analysis to be undertaken to demonstrate that the risks from dropped load are reduced to be as low as reasonably practicable.

Those cranes and objects that could potentially fall and are not excluded from the assessment, depending on the regulatory jurisdiction and approach, should then enter the screening process. Regulators agree that both deterministic and probabilistic screening criteria are appropriate for application. For example, dropped loads can be screened from the analysis if the consequences can be shown to be negligible, or if the frequency of occurrence is below a threshold (typically an event frequency or a fault sequence frequency below once in ten million years (10^{-7})). The screening process is expected to retain all faults associated with both types of hazard (dropped loads and falling objects) that have the potential to make a significant contribution to the overall risks from the facility and then analyse the potential consequence of these faults.

ANALYSIS METHODS

Following the application of exclusionary and screening criteria, the analysis of the remaining dropped loads and falling objects should be analysed. The HPR1000 has analysed a number of dropped loads, associated with cranes, and falling objects. It is also noteworthy that the Chinese Regulator has specifically undertaken additional analysis of dropped loads in the fuel building [Ref. 7] to show that the risks are tolerable.

It is generally agreed that deterministic analysis should be used for those screened-in dropped loads. There are varying expectations as to how this analysis should be undertaken and how conservatism is included. In general, the Chinese Regulator would typically expect that vendors / designers demonstrate that lifting equipment is sufficiently reliable to claim single failure proof criterion, and therefore the safety case will focus on defense-in-depth claims. In comparison the UK Regulator will expect analysis of the worst-case, unmitigated, fault condition, (i.e. a drop from the maximum height) with effects considered for all SSCs that could potentially be impacted. This includes potential effects of dropped loads on barriers such as penetration, spalling, cone cracking and perforation.

All regulators expect defense-in-depth to be demonstrated against dropped loads. This can include, but not be limited to:

- A consideration of whether the lift can be practicably eliminated.
- Movement plans that avoid, where reasonably practicable to do so, the lifting over/near safety significant SSCs, and the height of the lift minimised.
- Measures taken to prevent the lifting of excessive loads.
- Items / packages containing nuclear matter / radioactive materials are designed to retain their integrity following an impact resulting from a dropped load.
- Lifting equipment can only be used in permitted states.

All regulators in the Hazards TESG agree that the analysis of dropped loads should result in the determination of the limits and conditions of operation of, for example, the lifting equipment, detailed load paths, and systems and administrative controls that need to be in place to control the lifts. Such limits and conditions would need to be followed by the plant operator.

SUMMARY OF DESIGN AND POTENTIAL IMPACT

The HPR1000 considers dropped loads and falling objects and has considered these hazards in the defense-in-depth of the plant. However, it is recognised that the due to the different regulatory expectations in relation to exclusionary criteria that additional analysis may be required to satisfy the expectations of the different regulators.

V. COMBINED HAZARDS

This section compares the regulatory approaches of the HPR1000 Hazards TESG with respect to hazard combinations to identify areas of common practice and key differences. The implications of these differences in regulatory approach are considered with respect to the design of the HPR1000.

SCOPE: EXCLUSIONS AND SCREENING CRITERIA

The identification, screening and analysis of combined hazards is a multidisciplinary subject that requires a detailed understanding of the layout and hazards within the NPP design. One of the key sources of multi-hazards is the failure of high energy pipes (see HEPF section above) that can result in a number of consequential hazards including: pipe whip, jet loads, steam release, blast effects and internal flooding. Therefore, the NPP design needs to demonstrate capacity to withstand the combined effects from the combined hazard loads particularly for those areas of highest risk, such as areas where HIC exist.

All regulators involved with the HPR1000 MDEP WG recognise the importance of assessing the combination of events that could impact SSCs important to safety. For the HPR1000 design this is captured in the Chinese guidance HAF-102-2016 and sets out the expectation that where analysis identifies combination of events that can lead to operational, or accident condition the event shall be considered in the design basis of the plant. This guide prescribes specific regulatory expectations on the methodology of combined hazards and there are also related requirements in the Safety Guide HAD102/17-2006 "Evaluation and verification of the Safety of Nuclear Power Plants".

The UK Regulator has specific guidance on the expectations for assessment of combination hazards, where it defines the following classifications, which are consistent with those adopted in Ref. 5:

- **Unrelated (independent) hazards**: when more than one internal and/or external hazard applies simultaneously. This can be the case, for example, of nominally frequent events such as internal fire and flooding when there is no causation link between them.
- **Consequential Hazards**: an internal or external hazard directly poses one or more additional hazards to plant and structures (e.g. seismic hazard leads to an internal fire that activates a water-based fire suppression system leading to water spray and flooding effects).
- **Correlated Hazards**: A common cause results in multiple hazard(s) that occur simultaneously. An example of this would be pressure part failure giving rise to pipe whip impact and flooding.

All regulators recognise the importance of adequate screening highlighting the reliance of deterministic and probabilistic methods. The UK Regulator provides specific guidance on screening techniques to demonstrate the NPP design considers relevant hazard combinations.

All regulators agree on the adoption of redundancy and segregation to ensure that hazards cannot lead to the loss of multiple safety trains. To achieve this, all regulators strive to ensure that the plant design meets the guidance in IAEA SSG-64 (Ref. 5) and national design practices ensuring that hazards are considered in the design, and optimisation of plant layout minimises the effects of hazards.

For the optimisation of layout and hazard protection all regulators recognise the importance of civil barriers (including protecting penetrations through those barriers) for the provision of passive means to provide protection against the maximum credible loads. There is a general regulatory requirement / expectation that barriers required for nuclear safety should be demonstrated to maintain their integrity under all hazard conditions (including combinations) and deliver their safety functions. This sets out the need for barriers to be substantiated to withstand multiple hazards.

ANALYSIS METHODS

All regulators expect hazard analysis and the identification of combined hazards via a combination of deterministic and probabilistic approaches. The assessment of combined loads is universally agreed to be essential in demonstrating the safety of a NPP design. Bounding load cases are considered suitable for use in the analysis, including those resulting from hazard combinations, so long as they are suitably justified.

For example, the UK Regulator recommends considering the worst-case unmitigated hazard conditions, (e.g. most onerous loads including combinations of loads), as a starting point for the assessment. Doing so (e.g. by assuming safety measures are absent or fail to operate) can reveal the most onerous event consequences and hence ensure that the nuclear safety significance of measures and assumptions on which the design depends are appropriately recognised. Where gaps / weaknesses are identified in the design additional measures (engineering or procedural) may be required to reduce the hazard loads or effects. ONR SAPs paragraph 155 provides a hierarchy of safety measures, with a preference for those towards the top of the hierarchy (e.g. passive safety measures compared with mitigative measures). It should be noted that this hierarchy does not prevent other measures being implemented as part of the plant's defense-in-depth. It is the UK Regulator's expectation that the safety case clearly presents the full range of options considered as part of optioneering process to demonstrate that the measures adopted reduce the risks to be as low as reasonably practicable. This stepwise approach provides a basis to understand the hazards and associated risks to nuclear safety for the NPP design and to enable proportionate assessment of the safety case claims, arguments and evidence (as provided by duty holders to demonstrate that the risks from hazards have been reduced to ALARP).

Analysis of the plant against the derived load cases should be undertaken to enable assessment of the tolerability of the NPP design. Consideration of loads resulting from hazard combinations is important in ensuring that the design of passive, multi-hazard barriers is adequate. It is expected that these barriers should be substantiated to be tolerant of bounding hazard loads including combination of hazards. Furthermore, the analysis should underpin the identification and the importance of functional requirements of safety measures that address the hazard.

The regulators expect that the design layout should in the first instance be optimised to eliminate hazards. Where this is not reasonably practicable the design should demonstrate an iterative approach for reducing hazard risks applying a hierarchy of safety measures and defense-in-depth. This approach should adequately demonstrate that hazard effects have been considered and priority given to ensuring segregation of key safety systems through the provision of passive barriers. The analysis should ultimately demonstrate that the layout is optimised such that the risks to SSCs from hazards and hazard combinations are as low as is reasonably practicable. Any areas of exception (i.e. where multiple safety trains pass through a single room) need to be identified and suitably justified to show that there is no significant increase in risk.

SUMMARY OF DESIGN AND POTENTIAL IMPACT

The HPR1000 design considers hazard combinations based on the relevant HAF and HAD codes. The design includes the provision of passive barriers to protect SSCs against the effects of hazards and hazard combinations. This includes segregation of the various safety trains where reasonably practicable to do so. However, due to the differences in regulatory approaches it is recognised that additional analysis may be required to satisfy the specific expectations of the different regulators.

VI. CONCLUSIONS

This technical report presents a summary of the regulatory approaches relevant to hazards of the members of the HPR1000 Hazards TESG. It is based on the detailed information provided by members of the Hazards TESG in response to the questionnaire provided in the appendix. The responses to the questionnaire have been compared to identify areas of common regulatory approach and differences.

Overall, all member countries ensure that their national guidance documents are aligned with IAEA guidance relevant to hazards. Therefore, at a principal level, the regulatory expectations for hazards are similar between the members of the Hazards TESG. However, there are some notable differences in the application of these high-level principles with respect to identification, screening, and characterisation of hazards and in the detailed application of regulatory approaches for assessment purposes.

The differences between regulatory approaches have been explored for a number of pertinent, typical hazards and the potential impact of these differences for the design of the HPR1000 reactor discussed. Given the varying status of each member's regulatory assessment of the HPR1000 reactor design it has not been possible to identify any specific design changes that may result from different regulatory expectations relevant to hazards. However, it is possible to identify where additional analysis may be required to ensure the design meets national expectations. For example, the UK Regulator does not accept leak-before-break arguments as a principal means of demonstrating adequate safety. Consequently, additional analysis is needed to demonstrate that the consequences of a HEPF have been adequately accounted for and that the risks for the design are as low as reasonably practicable.

With respect to common practice, all members agree that:

I. IAEA guidance is considered good practice and each member's guidance is aligned with IAEA documentation relevant to hazards.
II. Identification, characterisation, and screening of hazards (including combinations) is good practice.
III. Individual hazards and combinations of hazards are considered in the design of the HPR1000 design, albeit individual national regulators may expect some additional hazards / combinations to be considered.
IV. Application of bounding hazard scenarios is an appropriate approach.

V. Application of suitable screening criteria to bound the hazards analysis is considered appropriate.

VI. Various approaches should be used to analyse hazards at different annual probability of exceedance including: deterministic approaches, design basis analysis, beyond design basis analysis (including demonstrating an absence of cliff edge effects), probabilistic safety analysis and severe accident analysis.

REFERENCES

1 Minutes of second meeting of HPR1000 WG

2 Minutes of third meeting of HPR1000 WG / first meeting of Hazards TESG

3 Minutes of fourth meeting of Hazards TESG

4 Vendor Presentation at fourth meeting of Hazards TESG

5 IAEA Safety Standards:

SSG-64: Protection against Internal Hazards in the Design of Nuclear Power Plants.

SSR 2/1: Safety of Nuclear Power Plants: Design, Rev 1.

TecDoc 1791: Considerations on the Application of the IAEA Safety Requirements for the Design of Nuclear Power Plants.

SSG-67: Seismic Design for Nuclear Installations

SSG-68: Design of Nuclear Installations Against External Events Excluding Earthquakes

6 MDEP Technical Report TR-VVERWG-02, Regulatory approaches and oversight practices related to reactor pressure vessel and primary components

7 NNSA, Presentation on Fuel Building Dropped Loads Assessment, Presented during the 5th Meeting of the Hazards TESG.

APPENDIX FOR SPECIFIC GUIDANCE

Hazards TESG Technical Report

The following questionnaire was developed by members of the hazards TESG following the 3rd meeting of the HPR1000 WG and the responses were discussed during the 4th HPR1000 WG meeting held at Fangchenggang, China in September 2019.

The Hazards TR is based on the detailed information contained in the table below.

Hazard	NNSA Response	ONR Response	NNR Response	ARN Response
High energy pressure failure	**How is the scope of hazards analysis defined?** a. Pipes containing water or steam @ pressure ≥ **2MPa** (g) during normal operation; or pipes is not less than **100℃** b. Gas **pipes pressurised above atmospheric** pressure. **Are there any exclusions and what is the reason?** a. Pipes using **Leak-Before-Break** (LBB) technology. b. Pipes covered by **2% criterion** (2% criterion: the safety classified piping system with a nominal diameter no less than 50 mm which are in operation as high energy piping systems less than or equal to 2% of the plant life are considered as moderate energy piping system). c. **Pipes within Containment Penetrations** Area meeting appropriate provisions, **according to SRP BTP3-4**. d. Pipes with a **nominal diameter less than 25 mm**. **What are the regulatory expectations for**: The **methodologies** used in the deterministic analysis by vendors? **NNSA does not specify a detailed analysis methodology**. However, vendors should **demonstrate** the methodologies are **reasonable** and feasible. **The process for identification, screening and quantification of credible bounding events (including credible combined hazards) within the DBA**? A full range of screening is conducted according to the above mentioned scope of hazards analysis defined. **Quantitative analysis is conducted if the exclusion requirements are not met**. The assessment of High energy pipe failures includes the following steps: ➢ Data collection: the high energy pipe failure sources are identified according to the criteria mentioned above.	**How is the scope of hazards analysis defined?** For high energy criteria we agree with the same initial criteria, but expect that HE system near these values are considered in sensitivity analysis to determine cliff edge effects. **Are there any exclusions and what is the reason?** ONR does not apply any exclusions for HEPF and all pipes (Medium & Low energy) should be included in the assessment. For example: • Leak-before-break - Not generally accepted as primary safety claim in UK Safety Cases. • Exclusions due to low utilisation or time at risk assumptions would not be accepted as the basis not to provide visibility of the hazard consequences (e.g. 1% or 2% criteria). **What are the regulatory expectations for**: **The methodologies used in the deterministic analysis?** ONR expects HEPF methodologies to include: Assessment of the Dynamic effects / Local Loads on Reinforced Concrete / Steel from hazards including: • Pipe whip; • Jet impingement; • Missiles; • Blast. Assessment of the Global / Environmental Loads on Reinforced Concrete / Steel from hazards including: • Pressure effects due to hot gas or steam release; • Temperature effects due to hot gas or steam release; • Flooding; • Other - moisture/ condensation, toxicity. Use of appropriate codes and tools should be supported by robust justification of their relevance and are	**How is the scope of hazards analysis defined?** For the existing nuclear power plant, plant piping systems or portions of systems that are pressurised above atmospheric pressure during normal plant conditions are classified as either high or moderate energy piping. High energy piping includes those systems or portions of systems in which the maximum operating temperature exceeds 93°C or the maximum operating pressure exceeds 1.9 MPa for more than 2% of the time during normal plant operation. Moderate energy piping includes those piping systems or portions of systems pressurised above atmospheric pressure during normal plant conditions and not identified as high energy piping. For possible new nuclear power plants, the NNR may be guided by the latest guidance from IAEA SSG-64 "Protection against Internal Hazards in the Design of Nuclear Power Plants" on Pipe Breaks (for example, Para. 4.110 and its footnote) or by appropriately justified submissions from the authorisation applicant. More information on the regulatory framework for pressure equipment appears in NNR Position Paper PP-0012 Manufacturing of Components for Nuclear Installations. **Are there any exclusions and what is the reason?** The following text from Section 5 of NNR Draft Specific Nuclear Safety Regulations: Nuclear Facilities implies that all categories of pipes should be included in the assessment: "(2) Internal and external hazards (a) Internal and external events shall be identified based on a comprehensive hazard analysis. (b) All foreseeable internal hazards and external hazards, including the potential for human induced events directly or indirectly to affect the safety shall be identified and their effects shall be evaluated. Hazards	**How is the scope of hazards analysis defined?** **Are there any exclusions and what is the reason?** Depending on the characteristics of the pipes under consideration (internal parameters, diameter, stress values, fatigue factors), the following types of failure should be considered: (a) High energy pipes (except for those qualified for leak-before-break, break preclusion or for low probability of failure) can suffer from circumferential rupture or longitudinal through wall crack, or both. The high energy of the contained fluid means that dynamic effects, such as pipe whip, or jets is more important. (b) Low energy pipes can also suffer through wall cracks, either longitudinal or circumferential, although cracks would in some cases be more stable, given the energy of the fluid, and dynamic effects would be less significant. By exception, for low energy pipes, it could be possible to justify limiting the break size to that of a leak with limited area. For ARN, high energy pipe is defined as a pipe with an internal operating pressure equal to or exceeding 2.0 MPa or an operating temperature equal to or exceeding 100°C in the case of water. It is accepted to postulate only a limited leak (and not a break) if it can be demonstrated that the piping system considered is operated under 'high energy' parameters for a short period of time (e.g. less than 2% of the total operating time) or if its nominal stress is reasonably low (e.g. a pressure of less than 50 MPa). A pipe break need not be assumed if a successful qualification for leak-before-break, for break preclusion or for low probability of failure has been

Hazard	NNSA Response	ONR Response	NNR Response	ARN Response
	➢ Consequence analysis: Impact on the delivery of fundamental safety functions after HEPF is performed comprehensively. ➢ If the consequence is not acceptable, the safety measures will be applied, such as pipe whip restrain. **Combining correlated, consequential and independent hazards (i.e. on a frequency basis, and positively and negatively related external hazards)?** For HEPF, combined consequential effects are identified and analysed based on detailed system and layout design. For example, the SSCs affected by combination of pipe whip and jet impingement are identified and evaluated in design. **The process for identification and quantification of hazard combinations for beyond design basis?** According to domestic and international regulations or RGP, combined internal hazards for beyond design basis have not been considered in design. But the assessment of independent internal hazards combination for beyond design basis analysis could be performed as cliff edge analysis. HPR1000 considered the beyond design basis external hazards as well as Fukushima accident experience feedback. The beyond design basis external flooding (design basis flooding level combines with the once in a thousand year rainfall) is considered. **Ensuring conservatism in the analysis and the various sources of uncertainties (e.g. assumptions, design information or analytical model)?** Adopt the methodology consist with the wildly recognised practice, and used the conservative assumptions in the analysis. **The use of probabilistic analysis?** The frequency of internal hazard has been used to judge the possibility of independent hazard combination. In combined internal hazards definition, two independent hazard combinations are not considered because of low frequency of internal hazard in HPR1000.	appropriately verified and validated for the application applied. Appropriate codes and standards include: • Use of the ANSI/ANS 58.2-1988 and NUREG 0800 rules generally OK as a starting position but additional expectations are documented in NS-TAST-GD-14 (e.g. failures to be postulated at any location which would give rise to bounding consequences) and the responses to the following questions. • Impact on concrete barriers (local and global) should be evaluated using appropriate analytical models (e.g. LS-DYNA) and design codes (e.g. ACI 349-13). **The process for identification, screening and quantification of credible bounding events (including credible combined hazards) within the DBA**? ONR expects that relevant and proportionate screening criteria are applied, within the expectations of design basis analysis. The analysis will be based on pipework layouts and room dimensions, geometry and SSC layouts. Simplification and assumptions may be made for ease of analysis depending on the stage at which the design is (e.g. assuming longest length of unrestrained pipe equal to room dimensions etc.) This can be applied through: Deterministic Screening • Hazard sequences can be either grouped based on the challenges to specific protection features e.g. each individual multi-hazard barrier; or • Hazard sequences can be grouped based on the combined challenge to each safety function. Probabilistic screening • Hazard combinations may be screened out because the frequency of occurrence is considered to be extremely low; below 1 in 10 million years (10^{-7} per annum). • Whilst it may be acceptable to consider that two independent, low frequency hazards in the design basis have a very low probability of occurrence during each other's plant mission time, the combined consequential effects should be checked for cliff edge effects not otherwise captured in the safety case. **Combining correlated, consequential and independent hazards (i.e. on a frequency basis, and positively and negatively related external hazards)?**	shall be considered for determination of the postulated initiating events and generated loadings for use in the design of relevant items important to nuclear safety. (c) …" For possible new nuclear power plants, the NNR may be guided by the latest guidance from IAEA SSG-64 "Protection against Internal Hazards in the Design of Nuclear Power Plants", for example: "4.111. It may be acceptable to postulate only a limited leak (and not a break), if it can be demonstrated that the piping system considered is operated under 'high energy' parameters for a short period of time (e.g. less than 2% of the total operating time). Some States have identified criteria for excluding certain pipe segments from break analysis (see para. 4.136). Alternatively, an assessment of the consequences assuming a full pipe break can be viewed as a good practice to demonstrate the robustness of the design." **What are the regulatory expectations for**: **The methodologies used in the deterministic analysis?** From Section 7.1.1 of NNR RG-0019 "Interim Guidance on Safety Assessments of Nuclear Facilities": '4) Deterministic safety analysis should be used to analyse AOO's, DBA's and DBEC's. 5) For AOO's and DBAs the safety analyses should be demonstrably conservative with respect to the figures of merit or safety criteria. 6) For DBECs, best estimate analyses plus uncertainty or sensitivity analyses, may be justified. 7) Guidance on "Deterministic Safety Analysis for Nuclear Power Plants" can be found in the IAEA Specific Safety Guide, SSG-2."' From Section 7.1.2 of NNR RG-0019: "(8) Deterministic safety analysis (a) Deterministic safety analysis shall be included in the safety assessment, covering both operational states and accident conditions. (b) The objective of the deterministic safety analysis shall be to: (i) Demonstrate compliance with safety requirements such as the requirement for ensuring the integrity of barriers against the	performed for the piping under consideration, resulting in a sufficiently low frequency of the occurrence of a spontaneous break. In general, a fracture mechanics analysis should be performed to calculate the leak size. In lieu of such an analysis, a subcritical crack corresponding to a leak size of 10% of the flow cross-section should be postulated. **What are the regulatory expectations for**: The **methodologies** used in the deterministic analysis by vendors? ARN does not specify a detailed analysis methodology. However it is required that the vendors apply a conservative methodology for AOO's and DBAs while a best estimate analysis plus uncertainty approach must be used for DECs. In addition, deterministic analysis shall mainly provide: (a) Establishment and confirmation of the design bases for all items important to safety; (b) Characterisation of the postulated initiating events that are appropriate for the site and the design of the plant; (c) Analysis and evaluation of event sequences that result from postulated initiating events, to confirm the qualification requirements; (d) Comparison of the results of the analysis with acceptance criteria, design limits, dose limits and acceptable limits for purposes of radiation protection; (e) Demonstration that the management of anticipated operational occurrences and design basis accidents is possible by safety actions for the automatic actuation of safety systems in combination with prescribed actions by the operator; (f) Demonstration that the management of design extension conditions is possible by the automatic actuation of safety systems and the use of safety features in combination with expected actions by the operator. **The process for identification, screening and quantification of credible bounding events**

Hazard	NNSA Response	ONR Response	NNR Response	ARN Response
		As part of HEPF analysis ONR expects that analysis of dynamic and global effects includes assessment of: • Combined consequential effects due to domino effect / pipe to pipe interactions. • Combined consequential effects due to single pipe failure on barriers and SSCs (e.g. pipe whip and steam release or pipe whip, jet and flood). For SSC substantiation the following should be considered: • The barrier response to combined loads (e.g. pipe whip, jet impact, hydrostatic load and etc.) requires appropriate characterisation of the event sequences and duration to identify all simultaneous loads on barriers. • Consequential pipe to pipe interactions should be evaluated and the combined effects on barriers and / or safety classified SSCs should be evaluated. Appropriate design criteria should be made available. • Impact on safety classified SSCs should be evaluated, as appropriate. Decision making on appropriate engineering protection should be make in accordance with the ALARP principle, where accepted good practice is considered as well as residual levels of risk. **The process for identification and quantification of hazard combinations for beyond design basis?** Fault sequences initiated by internal and external hazards beyond the design basis should be analysed applying an appropriate combination of engineering, deterministic and probabilistic assessments. Analysis of beyond design basis events should: • Confirm the absence of 'cliff edge' effects just beyond the design basis. • Identify the hazard level at which safety functions could be lost (i.e. determine the beyond design basis margin) (non-discrete hazards only). • Provide an input to probabilistic safety analysis of whether risks targets are met. • Ensure that safety is balanced so that no single type of hazard makes a disproportionate contribution to overall risk. • Provide an input to severe accident analysis (non-discrete hazards only). **Ensuring conservatism in the analysis and the various sources of uncertainties (e.g. assumptions, design information or analytical model)?**	release of radioactive material and various other acceptance criteria; (ii) Determine whether there are adequate safety margin in the design and operation of a facility, or in the conduct of an activity; (iii) Derive or confirm operational limits and conditions that are consistent with the design and safety requirements for the facility; (iv) Assist in establishing and validating emergency operating procedures and accident management procedures and guidelines; and (v) Confirm that modifications to the design or operation of the reactor facility have no significant adverse impact on safety. (c) The selected events shall be categorised, based on the results of probabilistic safety assessment and engineering judgement. From Section 7.4 of NNR RG-0019: "4) The applicant should begin the safety analysis with an identification of all hazards (chemicals, radiological materials, fissile materials, etc.) that may present a potential threat to the public, facility workers, or the environment (Appendix 1). 5) Based on a systematic analysis of each plant process, the safety analysis process hazard analysis (PHA) identifies a set of individual accident sequences or process upsets that could result from the hazards. The applicant's safety analysis methodology should therefore generally address: b) Hazard identification; c) PHA (accident identification); d) Initiating event identification; e) Accident sequence construction and evaluation; f) Consequence determination; and g) Likelihood categorisation for determining compliance." **Combining correlated, consequential and independent hazards (i.e. on a frequency basis, and positively and negatively related external hazards)?** Design bases should be derived for each credible event and credible combination of events by adopting appropriate methodologies.	**(including credible combined hazards) within the DBA**? ARN does not specify any specific criteria for identification, screening and quantification of events within DBA. It is an applicant decision to submit the process methodology for review and acceptance. However it is expected that the process include both, deterministic and probabilistic approach. When using probabilistic approach, the frequency of occurrence lower than 10-7 per year is mainly used as cut-off value for screening out. For deterministic approach, consideration of layout, room dimensions are taken into consideration. **Combining correlated, consequential and independent hazards (i.e. on a frequency basis, and positively and negatively related external hazards)?** For ARN, it is not feasible to identify a priori a set of hazard combinations that should be required in the design of a plant. Instead, a performance-based approach in this regard is expected from the applicant. This approach, regardless of the specific methods or criteria being used, should be comprehensive and systematic. The objective is to identify which hazard combinations need to be considered and what design features are necessary to address them. Hazard identification processes could lead to long lists of potential combinations and therefore pragmatic approaches should be utilised. While combinations involving two (or even more) simultaneous hazards could be postulated, screening criteria should be developed to ensure that the list represents a credible and reasonable set of plant challenges. The screening criteria can be deterministic or probabilistic. Examples of screening criteria include: (a) The event combination is not credible;

Hazard	NNSA Response	ONR Response	NNR Response	ARN Response
		To demonstrate a conservative analysis ONR expects the following: • Double ended guillotine failure should be assumed (gross failure). • Break location – Both terminal ends and intermediate points should be considered (e.g. high stress/ fatigue areas, weld points), and also other locations representing bounding consequences e.g. potential impact on HIC, or other SSCs. • Failure of plant occurs at its most onerous state, e.g. Analysis in highest energy mode. • Impact on barrier penetrations (cable, pipework, doors, relief panels and etc.) should be evaluated. • The barrier response to combined loads (e.g. pipe whip, jet impact, hydrostatic load and etc.) requires appropriate characterisation of the event sequences and duration to identify all simultaneous loads on barriers. **The use of probabilistic analysis?** ONR expects that the analysis should apply an appropriate combination of engineering, deterministic and probabilistic methods in order to: • Understand the behaviour of the facility in response to the hazard; and • Confirm high confidence in the adequacy of the design basis definition and the associated fault tolerance of the facility.	See also the response to the next question about how unreasonable or not credible combinations of hazards might be excluded. **The process for identification, screening and quantification of credible bounding events (including credible combined hazards) within the DBA**? From Section 7.2 of NNR Position Paper PP-0014 Considerations of External Events for New Nuclear Installations: "The following criteria could be used to eliminate postulated hazards being included in the safety assessment: (1) A phenomenon which occurs slowly or with adequate warning with respect to the time required to take appropriate protective action. (2) A phenomenon which in itself has no significant impact on the operation of a nuclear power plant and its safety assessment. (3) A phenomenon which by itself has a probability of occurrence less than the 10-8 per year (event sequence frequency). (4) Locate the nuclear power plant sufficiently distant from the postulated phenomenon to mitigate its effects. (5) A phenomenon which is included or enveloped by design for another phenomenon. For example, storm surge and seiche are included in lake flooding; toxic gas is included in pipeline accident or industrial or military facility accident. Alternative screening methods prescribed in PRA standards can be used provided they are demonstrated to be compatible with the NNR licensing criteria as well as having a sound technical and defensible basis." **The process for identification and quantification of hazard combinations for beyond design basis?** From Section 3 of NNR Draft General Nuclear Safety Regulations: "(4) The safety analysis shall include (f) External events and credible combination of events which lead to radiological exposure;" From p.26 of IAEA SSR-2/1 (Rev. 1) Safety of Nuclear Power Plants: Design, 2016:	(b) The event combination, even if credible, would not lead to conditions beyond what has already been assumed in the design. **The process for identification and quantification of hazard combinations for beyond design basis?** For ARN, it is not feasible to identify a priori a set of hazard combinations that should be required for beyond design basis. A set of DECs should be derived and justified as representative, based on a combination of deterministic and probabilistic assessments as well as engineering judgement. **Ensuring conservatism in the analysis and the various sources of uncertainties (e.g. assumptions, design information or analytical model)?** ARN expectation includes but is not limited to the following: - The frequency of a double ended guillotine break of high energy piping should be derived from operating experience or fracture mechanics calculations. This frequency might also be available from evaluations made for the purposes of probabilistic safety assessment. - A large longitudinal through wall crack in high energy piping resulting in a break or large leakage area should be considered if longitudinal welds are present. - Complete instantaneous breaks of high energy pipes should be postulated. - For small diameter piping systems, breaks should be postulated at all locations because they are sensitive to vibration-induced failure. **The use of probabilistic analysis?** ARN expects deterministic and probabilistic assessments as well as engineering judgement.

Hazard	NNSA Response	ONR Response	NNR Response	ARN Response
			"Combinations of events and failures 5.32. Where the results of engineering judgement, deterministic safety assessments and probabilistic safety assessments indicate that combinations of events could lead to anticipated operational occurrences or to accident conditions, such combinations of events shall be considered to be design basis accidents or shall be included as part of design extension conditions, depending mainly on their likelihood of occurrence. Certain events might be consequences of other events, such as a flood following an earthquake. Such consequential effects shall be considered to be part of the original postulated initiating event." **Ensuring conservatism in the analysis and the various sources of uncertainties (e.g. assumptions, design information or analytical model)?** From Section 5 of NNR Draft Specific Nuclear Safety Regulations: Nuclear Facilities: "(5) Uncertainty analysis (a) An uncertainty and sensitivity analysis shall be performed and taken into account in the deterministic and probabilistic safety analysis and conclusions drawn from it. (b) Uncertainties in the various safety analyses shall be characterised with respect to their source, nature and degree, using quantitative methods, professional judgement or both. (c) Design base accident analyses shall be demonstrably conservative with respect to the acceptance criteria or safety requirement being analysed against." From Section 7.1.1 of NNR RG-0019: '5) For AOO's and DBAs the safety analyses should be demonstrably conservative with respect to the figures of merit or safety criteria.' From Section 7.2.1 of NNR RG-0019: "7.2.1 Conservative Analysis 1) A conservative (enveloping) analysis should be performed for design basis accidents. 2) In instances where the conservative analysis shows noncompliance with the safety criteria, a best estimate analysis may be performed for	

Hazard	NNSA Response	ONR Response	NNR Response	ARN Response
			those specific factors, which contribute significantly to noncompliance. 3) The level of confidence in the best estimate analysis for such factors must be justified by means of an uncertainty analysis and sensitivity analysis." **The use of probabilistic analysis?** From Section 7.1.2 of NNR Draft General Nuclear Safety Regulations: "(9) Probabilistic safety analysis (a) A probabilistic safety analysis shall be conducted to demonstrate compliance with numerical risk criteria unless it can be justified that no credible accident conditions exist. (10) All activities with regard to safety analysis and risk management shall be conducted in accordance with recognised industry standards and practices as agreed with the Regulator." From Section 7.1.2 "Probabilistic safety analysis" of NNR RG-0019: "5) Either a best estimate analysis, with uncertainties, or a conservative analysis may be performed." From Section 7.1 "General approach for External Events" of NNR RG-0011 "Interim Guidance for the Siting of Nuclear Facilities": "… 6) Appropriate methodologies should be adopted for establishing the hazards from important external phenomena. 7) The methodologies used should be the current and state of the art, and should be justified as being compatible with the characteristics of the region. 8) Preferential consideration should be given to applicable probabilistic methodologies. 9) It should be noted that probabilistic hazard curves are generally required to conduct external event PSAs. …"	
Dropped loads	**How is the scope of hazards analysis defined?** **Are there any exclusions and what is the reason?**	**How is the scope of hazards analysis defined?**	**How is the scope of hazards analysis defined?**	**How is the scope of hazards analysis defined?** **Are there any exclusions and what is the reason?**

Hazard	NNSA Response	ONR Response	NNR Response	ARN Response

	No. NS-G-1.11 *Protection against Internal Hazards other than Fires and Explosions in the Design of Nuclear Power Plants*
	
	2.18. In this systematic analysis, among the important secondary effects the following should be evaluated:
	
	Falling objects. There may be circumstances in which a pipe whip or a missile can damage the supporting structure of a heavy object located above a safety system such that an object falls, possibly causing further damage. It may in certain cases be possible to show that the falling object cannot cause unacceptable damage. If not, either the supporting structure should be modified to withstand the missile impact or means should be provided to prevent such an impact.
	HAD102-04 3.2.2 Dropping of heavy equipment.
	If heavy items of plant equipment are located at significant heights, an evaluation should be made of the possible hazards associated with dropping such equipment, **if the probability of this event is not negligible**.
	
	Scope of Analysis
	
	Dropped loads assumed to occur as a result of a lifting device failure if the lifting devices can no longer control the loads;
	
	Dropped loads are postulated from every lifting or handling device except the ones which are satisfied with 'single failure proof'.
	
	Exclusions during Dropped Loads safety evaluation
	
	The **reliability** of the lifting equipment **should be such** that **dropping of the load can be effectively discounted**, for example, by the use of single failure proof cranes.
	
	Dropped loads of spent fuel **cask are mainly considered** in the design (PSAR 3.5.1.1.3).
	
	The **design of spent fuel cask crane** takes into account **single failure** and **redundancy design**, and is equipped with necessary safety devices, which has high safety reliability. The lifting mechanism of spent fuel cask crane adopts a double wire rope winding system and multiple brakes as redundancy protection measures. The design of the double wire rope winding system can ensure that the
		ONR expects the assessment of the consequences of dropped loads, from all lifting operations on susceptible nuclear safety significant SSCs. In general the scope of assessment should consider:
		
		• Whether as a result of lifting operations specifically, or intended or unintended drop of plant from height have been identified and considered.
		• The analysis of dropped loads results in the determination of the limits and conditions of operation of, for example, the lifting equipment, detailed load paths, and systems and administrative controls that need to be in place.
		• Claims on "high integrity cranes" without the requisite consequences analysis of the dropped loads are not accepted.
		• The maximum fault condition height e.g. double blocking height and mass should be assumed.
		• The various potential effects of dropped loads on barriers should include penetration, spalling, cone cracking and perforation.
		
		Are there any exclusions and what is the reason?
		
		There are no exclusions from assessment.
		
		What are the regulatory expectations for:
		
		The methodologies used in the deterministic analysis by vendors?
		
		• The worst-case unmitigated maximum fault condition height e.g. double blocking height and mass should be assumed.
		• Effects to all interacting SSCs should be assessed e.g.:
		  o The various potential effects of dropped loads on barriers should include penetration, spalling, cone cracking and perforation.
		  o Demonstration Items / packages containing nuclear matter are designed to retain their integrity following the worst-case impact.
		• Demonstration that Optioneering has been undertaken to identify whether the lifting activity is actually necessary, and to identify the preferred method and equipment for undertaking the lift.
		• Assessment to determine if lifting over/near safety significant SSC's can be avoided, and the height of the lift minimised so far as is reasonably practicable.
		
		The process for identification, screening and quantification of credible bounding events (including credible combined hazards) within the DBA?
			The following text from Section 5 of NNR Draft Specific Nuclear Safety Regulations: Nuclear Facilities mentions falling objects:
			"(2) Internal and external hazards
			…
			(c) The design of a facility shall take due account of internal hazards such as fire, explosion, flooding, missile generation, collapse of structures and falling objects, pipe whip, jet impact and release of fluid from failed systems or from other facilities on the site. Appropriate features for prevention and mitigation shall be provided to ensure that safety is not compromised."
			
			For further guidance, the NNR considers that the recommendations of the following IAEA publications, address the hazard of dropping heavy equipment as a result of internally initiated events:
			
			IAEA SSG-64 "Protection against Internal Hazards in the Design of Nuclear Power Plants,
			The section on heavy load drop starting at para. 4.173 of IAEA SSG-62, "Design of Auxiliary Systems and Supporting Systems for Nuclear Power Plants",
			IAEA SSG-63, "Design of Fuel Handling and Storage Systems for Nuclear Power Plants".
			
			Furthermore, IAEA SSG-67, "Seismic Design for Nuclear Installations", and IAEA SSG-74, "Maintenance, Testing, Surveillance and Inspection in Nuclear Power Plants", provide recommendations on seismic design and qualification, and on maintenance, surveillance and in-service inspection, respectively, that together will lead to high integrity lifting systems in operation.
			
			Are there any exclusions and what is the reason?
			
			The following text from Section 5 of NNR Draft Specific Nuclear Safety Regulations: Nuclear Facilities implies that in principle all categories of dropped loads should be considered in the assessment:
			
			"(2) Internal and external hazards
			(a) Internal and external events shall be identified based on a comprehensive hazard analysis.
			(b) All foreseeable internal hazards and external hazards, including the potential for human induced events directly or indirectly to affect the safety shall be identified and their effects shall be evaluated. Hazards shall be considered for determination of the postulated initiating events and generated loadings for use in the design of relevant items important to nuclear safety.
			(c) …"
				ARN's expectations are aligned with IAEA safety standards. With respect to hazards analysis, it is expected that the applicant assess the consequences of the dropped loads on items important to safety.
				For ARN is acceptable that drops are more likely to occur from the handling of plant equipment or from fuel handling lifts. Also, if heavy items of plant equipment are located at significant heights, an evaluation should be made of the possible hazards associated with dropping such equipment. In all cases, exclusion from assessment has to be justified based on the fact that the probability of such event is negligible.
				
				What are the regulatory expectations for:
				
				The methodologies used in the deterministic analysis by vendors?
				
				ARN does not specify a detailed analysis methodology. However, based on NUREG 0612 expects that the analyses of postulated load drops should as a minimum include the following considerations:
				• The load is dropped in an orientation that causes the most severe consequences.
				• The load may be dropped at any location in the crane travel area where movement is not restricted by mechanical stops or electrical interlock.
				• The analysis should postulate the "maximum damage" that could result, i.e., the analysis should consider that all energy is absorbed by the structure and/or equipment that is impacted.
				• Credit may not be taken for equipment to operate that may mitigate the effects of the load drop if the equipment is not required to be operable by the technical specifications when the load could be dropped.
				
				The process for identification, screening and quantification of credible bounding events (including credible combined hazards) within the DBA?
				
				ARN does not specify any specific criteria for identification, screening and quantification of events within DBA. It is an applicant decision to

Hazard	NNSA Response	ONR Response	NNR Response	ARN Response
	loads evenly distribute in the two wire ropes and when one wire rope is broken, the other one is able to maintain the rated load and maintain the balance of the pulley block. Nevertheless, the following defence-in-depth safety measures have been taken in equipment layout and building structure: **The crane layout does not operate above the spent fuel pool**, and, the autoclaved aerated concrete is located at the bottom of loading and cleaning well and loading well. **What are the regulatory expectations for:** **The methodologies used in the deterministic analysis by vendors?** Deterministic analysis: 1. **Measures** are taken to **prevent** the lifting of **excessive** loads; 2. **Conservative design** measures are applied to **prevent** any **unintentional dropping of loads** that could affect items important to safety; 3. The **plant layout permits safe movemen**t of the overhead lifting equipment and of items being transported; 4. **lifting** equipment can be used **only** in **specified plant states** (by means of safety interlocks on the crane); 5. **Lifting equipment** for use in areas where items important to safety are located is **seismically qualified**. **The process for identification, screening and quantification of credible bounding events (including credible combined hazards) within the DBA?** **All** the lifting devices **except** the ones which are satisfied with **single failure proof** are carried out for dropped loads evaluation. **HAD102-04 3.2.2** Dropping of heavy equipment If **heavy items** of plant equipment **are located at significant heights**, an **evaluation should** be **made** of the possible hazards associated with dropping such equipment, **if the probability of this event is not negligible**. **Combining correlated, consequential and independent hazards (i.e. on a frequency basis, and positively and negatively related external hazards)?** **HAD102-04 3.2.2** Dropping of heavy equipment	An effective process should be applied to identify and characterise all external and internal hazards that could affect the safety of the facility. Hazards should be identified in terms of their severity and frequency of occurrence and characterised as having either a discrete frequency of occurrence (discrete hazards), or a continuous frequency-severity relation (non-discrete hazards). All hazards should be treated as initiating events in the fault analysis. The identification process should include reasonably foreseeable combinations of independently occurring hazards, causally-related hazards and consequential events resulting from a common initiating event. Screening criteria should be defined in terms of frequency of occurrence and potential consequences as follows. Discrete hazards may be excluded that: (a) have no significant identified consequential effect on the safety of the facility; or (b) Have a total initiating event frequency that is demonstrably below once in ten million years per annum. Non-discrete hazards may be excluded where: (a) their associated faults have no significant consequential effect on the safety of the facility; or (b) Their frequency of exceedance on their hazard curve is below once in ten million years. Screening should retain all faults associated with both types of hazard that have the potential to make a significant contribution to the overall risks from the facility. **For each internal or external hazard which cannot be excluded on the basis of either low frequency or insignificant consequence, a design basis event should be derived.** For external hazards, the design basis event should be derived conservatively to take account of data and model uncertainties. The thresholds set for design basis events are 1 in 10 000 years for external hazards and 1 in 100 000 years for internal hazards. For non-discrete hazards, consideration may be given to arguments to derive design basis events from a higher	Similar to a previous response, the following criteria could be used to eliminate postulated hazards being included in the safety assessment: (1) A hazard which occurs slowly or with adequate warning with respect to the time required to take appropriate protective action. (2) A hazard which in itself has no significant impact on the operation of a nuclear power plant and its safety assessment. (3) A hazard which by itself has a probability of occurrence less than the 10-8 per year (event sequence frequency). (4) A hazard which is included or enveloped by design for another hazard. Alternative screening methods prescribed in PRA standards can be used provided they are demonstrated to be compatible with the NNR licensing criteria as well as having a sound technical and defensible basis. **What are the regulatory expectations for:** **The methodologies used in the deterministic analysis by vendors?** Similar principles are expected to be adhered to as mentioned in the response to the same question in the section above on high energy pressure failure. **The process for identification, screening and quantification of credible bounding events (including credible combined hazards) within the DBA?** Similar principles are expected to be adhered to as mentioned in the response to the same question in the section above on high energy pressure failure. **Combining correlated, consequential and independent hazards (i.e. on a frequency basis, and positively and negatively related external hazards)?** Similar principles are expected to be adhered to as mentioned in the response to the same question in the section above on high energy pressure failure. **The process for identification and quantification of hazard combinations for beyond design basis?**	submit the process methodology for review and acceptance. Following IAEA DS 494, during plant design, internal hazards should be identified on the basis of a combination of engineering judgement, lessons learnt from similar plant designs and operational experience, deterministic and probabilistic considerations. The identification and the characterisation include the consideration of hazard initial conditions (e.g. plant shutdown modes), the definition of the magnitude and the likelihood of the hazards, the locations of their sources, the environmental conditions produced and the possible impacts on SSCs important to safety. The hazard identification and characterisation process should be rigorous, supported by plant walk-down for verification, and well documented. **Combining correlated, consequential and independent hazards (i.e. on a frequency basis, and positively and negatively related external hazards)?** **The process for identification and quantification of hazard combinations for beyond design basis?** **Ensuring conservatism in the analysis and the various sources of uncertainties (e.g. assumptions, design information or analytical model)?** As stated in IAEA DS 494, assessment is required to be made to demonstrate that those internal hazards relevant to the design of the nuclear power plant are considered, that provisions for prevention and mitigation are designed with sufficient safety margins to cover the uncertainties in the identification and characterisation of internal hazard effects, as well as for avoidance of cliff edge effects. **The use of probabilistic analysis?** ARN expects deterministic and probabilistic assessments as well as engineering judgement.

Hazard	NNSA Response	ONR Response	NNR Response	ARN Response
	Generally, **the cause** of the dropping of heavy equipment **would be an external** phenomenon such as an earthquake or an aircraft impact, **but it may also be human error**. For dropping of heavy equipment: **At present**, **dropping of heavy equipment** is considered as a **single or independent** load condition, and **no combination** with other external event s. **The process for identification and quantification of hazard combinations for beyond design basis?** At present, there is no regulatory requirement for dropping of heavy equipment to consider beyond design basis. **Ensuring conservatism in the analysis and the various sources of uncertainties (e.g. assumptions, design information or analytical model)?** The **identification** of **hazards** sources is based on **actual design** and all sources have been considered in evaluation. The methodology of evaluation including assumption and formula is conservative. **The use of probabilistic analysis?** N/A	frequency of exceedance if the facility (or the relevant parts of it) cannot give rise to significant unmitigated consequences. **Combining correlated, consequential and independent hazards (i.e. on a frequency basis, and positively and negatively related external hazards)?** Hazards should be identified in terms of their severity and frequency of occurrence and characterised as having either a discrete frequency of occurrence (discrete hazards), or a continuous frequency-severity relation (non-discrete hazards). **All hazards should be treated as initiating events in the fault analysis**. The identification process should **include reasonably foreseeable combinations** of independently occurring hazards, causally-related hazards and consequential events resulting from a common initiating event. **The process for identification and quantification of hazard combinations for beyond design basis?** See Comments in HEPF section. **Ensuring conservatism in the analysis and the various sources of uncertainties (e.g. assumptions, design information or analytical model)?** Analysis of design basis fault sequences should use appropriate tools and techniques, and be performed on a conservative basis (as defined in the methodology section above) to demonstrate that consequences are ALARP. The fault sequence analysis should demonstrate, so far as is reasonably practicable, that the correct performance of the claimed passive and active safety systems ensures that: a) None of the physical barriers to prevent the escape or relocation of a significant quantity of radioactive material is breached or, if any are, then at least one barrier remains intact and without a threat to its integrity; b) There is no release of radioactivity; and c) No person receives a significant dose of radiation. In addition to the inclusion of conservative assumptions, it should be demonstrated that a small change in a DBA	At present, there is no regulatory requirement for dropping of heavy equipment to consider for beyond design basis. **Ensuring conservatism in the analysis and the various sources of uncertainties (e.g. assumptions, design information or analytical model)?** Similar principles are expected to be adhered to as mentioned in the response to the same question in the section above on high energy pressure failure.	

Hazard	NNSA Response	ONR Response	NNR Response	ARN Response
		parameter will not lead to a disproportionate increase in radiological consequences, ie there should be no cliff edge effect. The severity and frequency of the initiating event should be amongst the parameters considered. The aim is to be conservative without being overly pessimistic. **The use of probabilistic analysis?** ONR expects that the analysis should apply an appropriate combination of engineering, deterministic and probabilistic methods in order to: • Understand the behaviour of the facility in response to the hazard; and • Confirm high confidence in the adequacy of the design basis definition and the associated fault tolerance of the facility.		
Internal missiles	**Missiles analysis (such as from valves and turbine disintegration) How is the scope of hazards analysis defined?** (HAD102/04, SRP3.5.1.1) a. Missiles from component over speed failures; b. Missiles generating from high energy fluid system failures; c. Missiles caused by or as a consequence of gravitational effects. **(managed in dropped load)** **Are there any exclusions and what is the reason?** a. The **probability** of **generating missiles** is **small** enough to be accepted **without** considering the consequences. b. Although the probability of generating missiles is slightly higher, the **comprehensive consequences** can be **accepted** from the view of safety. Through using the appropriate design standards, specification of materials and equipment, carrying out strict quality assurance requirements, quality control inspection during manufacture, operation and maintenance, equipment and components apply nuclear related standards (e.g., RCC-M 1,2,3,or ASME 1,2,3), probability of occurrence of internal missiles can be exclude from the creditable missile source list. **What are the regulatory expectations for:** **The methodologies used in the deterministic analysis by vendors?**	**Missiles analysis (such as from valves and turbine disintegration) How is the scope of hazards analysis defined?** ONR expectations for missile analysis include: • All possible internal missiles sources should be identified: from pressurised vessels, pipework and components, rotating machinery and systems which contain explosive mixtures. • All assumptions should be made explicit. The consequences depend on key assumptions made in the evaluation of the missile energy such as size and geometry of the fragments ejected, the trajectory of the missiles and any credited loss of energy through interaction with equipment or structures (e.g. rotating machinery casing, walls). • Trajectory of missiles is subject to high levels of uncertainty as a result of the uncertainty inherent to the missile fragment formation, therefore appropriate sensitivity analysis should be undertaken to demonstrate there are no cliff edge effects. • Bounding arguments should be presented e.g. consider that damage from internal missiles may occur in any direction from the source / loss of SSCs in the same location. • Probabilistic arguments alone are not accepted to exclude assessment of missile sources or impacts/ strike on SSCs or nuclear safety significant plant. ONR expectations for Turbine disintegration: • Failure conservatively postulated e.g. disk ruptures to result in several fragments which would impact	**Missiles analysis (such as from valves and turbine disintegration) How is the scope of hazards analysis defined?** The following text from Section 5 of NNR Draft Specific Nuclear Safety Regulations: Nuclear Facilities mentions missile generation: "(2) Internal and external hazards … (c) The design of a facility shall take due account of internal hazards such as fire, explosion, flooding, missile generation, collapse of structures and falling objects, pipe whip, jet impact and release of fluid from failed systems or from other facilities on the site. Appropriate features for prevention and mitigation shall be provided to ensure that safety is not compromised." For further guidance, the NNR considers that the recommendations of the following IAEA publication address the hazard of internal missiles as a result of internally initiated events: The section on internal missiles starting at para. 4.78 of IAEA SSG-64 "Protection against Internal Hazards in the Design of Nuclear Power Plants". **Are there any exclusions and what is the reason?** See comments in Drop load section above. **What are the regulatory expectations for:**	**Missiles analysis (such as from valves and turbine disintegration) How is the scope of hazards analysis defined?** ARN's expectations are aligned with IAEA: • Sources of possible missiles should be identified, included but not limited to: - Valves in fluid systems that operate at high internal energy should be evaluated as potential sources of missiles - Failure of high speed rotating equipment include: (a) Fan blades; (b) Turbine disc fragments or blades; (c) Pump impellers; (d) Flanges; (e) Coupling bolts. - Failure of pressure vessels • The frequency, the possible magnitude of kinetic energy and the likely size and trajectory of missiles should be estimated. The possible targets and their effects on items important to safety should be assessed. **Are there any exclusions and what is the reason?** ARN does not have any criteria for exclusions. It is up to the applicant to justify exclusions from assessment. **What are the regulatory expectations for:**

Hazard	NNSA Response	ONR Response	NNR Response	ARN Response
	NNSA **focuses** on the **adequate protections** from **missiles**, and **do not specify** a detailed analysis methodology. Since the methodologies used in the deterministic analysis by vendors are not the same, NNSA **require vendor demonstrate** the **methodologies are reasonable and feasible**. The assessment of internal missiles mainly includes the following steps: ➢ Data collection: the missile sources are identified according to the screening criteria mentioned above. ➢ Consequence analysis: Impact on the delivery of fundamental safety functions after internal missile is performed comprehensively. If the consequence is not acceptable, the safety measures will be applied, such as enhancement the building structure or modifying the layout, etc. **The process for identification, screening and quantification of credible bounding events (including credible combined hazards) within the DBA?** A full range of screening is conducted according to the above mentioned scope of hazards analysis defined. **Quantitative** analysis **is conducted** if the **two exclusion requirements** are **not met**. **Combining correlated, consequential and independent hazards (i.e. on a frequency basis, and positively and negatively related external hazards)?** N/A **The process for identification and quantification of hazard combinations for beyond design basis?** N/A **Ensuring conservatism in the analysis and the various sources of uncertainties (e.g. assumptions, design information or analytical model)?** **Screening range** of the **missile sources** is **broad enough** to **cover all possibilities. Conservatism exists** in the **calculation** of missile characteristic parameters, and in the empirical formulas of shield design. In conclusion, there are **considerations of conservative margin** and **reducing uncertainty** at every stage of the design. **The use of probabilistic analysis?**	adjacent disks resulting in a number of missiles ejected from the turbine cases. Both high and low trajectory missiles should be postulated. • The number and velocity of turbine missile fragments ejected is specific to the design and fabrication of the specific turbine under consideration. • A probabilistic argument alone e.g. to support unfavourable layouts and lack of design provision against turbine disintegration is not acceptable and risk should be demonstrated to be ALARP. • ONR expects consideration of impact angles wider than 25° generally assumed. • Demonstration that the design provides sufficient redundant equipment that will survive a turbine disintegration to deliver the Fundamental Safety Functions. **Are there any exclusions and what is the reason?** There are no exclusions from assessment. **Combining correlated, consequential and independent hazards (i.e. on a frequency basis, and positively and negatively related external hazards)?** See comments in Drop load section above. **The process for identification and quantification of hazard combinations for beyond design basis?** See Comments in HEPF section. **Ensuring conservatism in the analysis and the various sources of uncertainties (e.g. assumptions, design information or analytical model)?** See comments in Drop load section above. **The use of probabilistic analysis?** See comments in Drop load section above.	**The methodologies used in the deterministic analysis by vendors?** Similar principles are expected to be adhered to as mentioned in the response to the same question in the section above on high energy pressure failure. **The process for identification, screening and quantification of credible bounding events (including credible combined hazards) within the DBA?** Similar principles are expected to be adhered to as mentioned in the response to the same question in the section above on high energy pressure failure. **Combining correlated, consequential and independent hazards (i.e. on a frequency basis, and positively and negatively related external hazards)?** Similar principles are expected to be adhered to as mentioned in the response to the same question in the section above on high energy pressure failure. **The process for identification and quantification of hazard combinations for beyond design basis?** Similar principles are expected to be adhered to as mentioned in the response to the same question in the section above on high energy pressure failure. **Ensuring conservatism in the analysis and the various sources of uncertainties (e.g. assumptions, design information or analytical model)?** Similar principles are expected to be adhered to as mentioned in the response to the same question in the section above on high energy pressure failure. **The use of probabilistic analysis?** Similar principles are expected to be adhered to as mentioned in the response to the same question in the section above on high energy pressure failure.	**The methodologies used in the deterministic analysis by vendors?** ARN does not specify a detailed analysis methodology.

Hazard	NNSA Response	ONR Response	NNR Response	ARN Response
	Probabilistic analysis is mainly used for turbine missiles.			

Combined hazards in areas of high risk (e.g. highest integrity components and areas with no segregation)	**What are the regulatory expectations for: the methodologies used in the deterministic analysis by vendors?**
	
	Combinations of events and failures **(HAF102-2016)**
	
	5.32. Where **the results of** engineering judgement, deterministic safety assessments and probabilistic **safety assessments indicate** that **combinations of events could lead** to **anticipated operational occurrences** or to **accident conditions**, **such combinations** of events **shall be considered to be design basis accidents** or shall be included as part of design extension conditions, depending mainly on their likelihood of occurrence.
	
	Certain events might be consequences of other events, **such as a flood following an earthquake**. Such consequential effects shall be considered to be part of the original postulated initiating event. **No specific regulatory expectations for methodology of combined hazards.**
	
	The design details are as follows :
	HPR1000: Special methodology of combined hazards has not been published in HPR1000. **But in HPR1000 design, some combined hazards have been considered**, such as the flooding caused by the fire.
	
	The process for identification, screening and quantification of credible bounding events (including credible combined hazards) within the DBA?
	
	Screen of external hazards
	
	Effect of **external hazards** on plant to be **evaluated on the scale of hazards**, **frequency of occurrence** and **distance from the plant**; Hazards to be selected based on the screen distance value /frequency of occurrence; **design basis** to be **defined for the remaining hazards after screening** taking into account of the impact on the structure of plant ;
	
	In the NNSA **Guide HAD102/17**, the **following requirements** are set **for** the "**hazards combination**" and "**load combination**".
		What are the regulatory expectations for: the methodologies used in the deterministic analysis by vendors?
		
		ONR expects demonstration that SSCs with **highest reliability claims are not challenged by internal hazards.** These are items for which failure cannot be conceded in the design due to highly undesirable consequences and therefore require highly robust materials and care in the design, fabrication and inspection. This is expected as per ONR SAP. EMC.3 *Evidence should be provided to demonstrate that the necessary level of integrity has been achieved for the most demanding situations identified in the safety case.*
		
		A highest reliability claim is an onerous route to a safety case because the low failure frequency expected goes beyond what may be inferred from the actuarial statistics relating to the failure frequencies for the gross failure of pressure vessels and piping designed and constructed to high standards.
		
		ONR therefore expects a demonstration of integrity based on sound engineering provision with measures over and above normal practice defined in nuclear codes and standards. Taken together these measures provide conceptual defence-in-depth. In addition, these structures and components need to be monitored, inspected and maintained through-life to maintain confidence that gross failure can be discounted.
		
		The analysis of HIC components should include:
		
		• A comprehensive and systematic hazard identification process covering internal hazards which may challenge HICs, considering those hazards individually and also in combination with consequential, concurrent or independent hazards and/or faults which may arise.
		    ○ **Consequential Hazards**: The consequences of an internal hazard induce one or more additional hazards – e.g. an exploding gas bottle generating fragmentation and fire.
		    ○ **Concurrent Hazards**: A common initiating event (including external hazards) results in multiple internal hazard(s) occurring – e.g. seismic event leading to both fire and flood challenges.
		    ○ **Independent Hazards**: Non-casually linked. An initiating event (including hazards) occurs independently from, but simultaneously with an internal hazard, e.g., a fire on a standby diesel when responding to a plant-trip
			What are the regulatory expectations for: the methodologies used in the deterministic analysis by vendors?
			
			Similar principles are expected to be adhered to as mentioned in the response to the same question in the section above on high energy pressure failure.
			
			The process for identification, screening and quantification of credible bounding events (including credible combined hazards) within the DBA?
			Similar principles are expected to be adhered to as mentioned in the response to the same question in the section above on high energy pressure failure.
			
			Combining correlated, consequential and independent hazards (i.e. on a frequency basis, and positively and negatively related external hazards)?
			
			Similar principles are expected to be adhered to as mentioned in the response to the same question in the section above on high energy pressure failure.
			
			The process for identification and quantification of hazard combinations for beyond design basis?
			
			Similar principles are expected to be adhered to as mentioned in the response to the same question in the section above on high energy pressure failure.
			Ensuring conservatism in the analysis and the various sources of uncertainties (e.g. assumptions, design information or analytical model)?
			
			Similar principles are expected to be adhered to as mentioned in the response to the same question in the section above on high energy pressure failure.
			
			The use of probabilistic analysis?
			
			Similar principles are expected to be adhered to as mentioned in the response to the same question in the section above on high energy pressure failure.
				What are the regulatory expectations for: the methodologies used in the deterministic analysis by vendors?
				
				ARN does not prescribe a specific methodology, however should be carried out on a conservative basis.
				
				It is expected that for each identified hazard combination sequence, the analysis should also take into consideration any deterioration or damage to SSCs important to safety and hazard barriers after being subjected to each of the various hazards.
				
				The process for identification, screening and quantification of credible bounding events (including credible combined hazards) within the DBA?
				ARN expects a performance-based approach be implemented. This approach should be comprehensive and systematic.
				
				In principle, three types of hazard combinations could be considered:
				(1) Consequential (subsequent) events: An initial event results in another consequential event, e.g. an internal hazard.
				(2) Correlated events: Two or more events, at least one of them representing an internal hazard, which occur as a result of a common cause. The common cause can be any anticipated event including an external hazard, or may be from an unanticipated dependency.
				(3) Unrelated (independent) events: An initial event occurs independently from (but simultaneously with) an internal hazard without any common cause.
				Screening criteria should be developed to ensure that the list represents a credible and reasonable set of plant challenges. The screening criteria can be deterministic or probabilistic. Screening criteria may include the following:
				(a) The event combination is not credible;
				(b) The event combination, even if credible, would not lead to conditions beyond what has already been assumed in the design.

Hazard	NNSA Response	ONR Response	NNR Response	ARN Response
	The **design basis** should **take account** for a **combination** of **extreme weather condition**s that **can reasonably** be **assumed** to occur **simultaneously** **External flooding**: The **surrounding environment** of the nuclear power plant should be **evaluated** to determine the **likelihood** of **external flooding** that would **compromise** the **safety** of the nuclear power plant. External flooding should **include flooding** due to **high rainfall**, **high tides**, **river overflow**, **dam collapse**, and **possible combinations**. **Nuclear safety related structures** and **components should** be **designed** to **withstand all associated loads** caused by **operational conditions** and **design basis accidents**, including internal and external hazards. HPR1000 **Some of the combined hazards are identified and calculated** according to detailed system and layout design. The consequence of some combined hazards has been evaluated. For **example**, the **internal flooding induced** by **internal fire** and **earthquake** has been identified and evaluated. **Combining correlated, consequential and independent hazards (i.e. on a frequency basis, and positively and negatively related external hazards)?** Regulatory expectations for types of combined hazards can refer to the previous description. The design details are as follows : Independent hazards combinations are considered in the design of structures and buildings in HPR1000 to protect against the external hazards. Independent internal hazards are not considered to occur at the same time. **The process for identification and quantification of hazard combinations for beyond design basis?** The design details are as follows: **Internal hazards** Conservative design and high-quality construction must be adopted to ensure that nuclear power plant failures and deviations from normal operation are minimised, to ensure accident prevention as far as practicable, and to ensure that there is no cliff edge effect in NPPS. (HAF102-2016)	caused by a weather-related loss of heat sink event. • A deterministic analysis of all credible hazard combination should be undertaken, demonstrating that the severity of hazard consequences as a result of unmitigated consequence under the worst-case operational states have been used to define the appropriate design and engineering provisions for the HIC component and demonstration of HIC withstand under these hazard conditions. • The analysis should be carried out on a conservative basis and the unmitigated consequences should be evaluated. o Detailed knowledge of the site layout and the plant is required: o Location of plant equipment; o Location of items important to safety; o Redundancy, diversity and reliability requirements of the items important to safety. • The analysis should not only focus on the number of most combined events present, in a given plant area, but also on their severity. • Appropriate modelling of all combined hazards should be undertaken and the impact loads, duration and sequence should be determined. • The sequence and timeline of individual events (e.g. fire causing pipe whip, missile, steam or flood) is important in determining whether simultaneous loads may occur, and the barrier response to the combined hazard loading. • A robust demonstration of physical defence-in-depth in the plant design. Demonstration of optimisation of plant layout and identification of safety systems to eliminate, mitigate the hazard loads on the HIC component. • Demonstration of additional measures beyond normal practice defined in codes and standards that will underpin highest reliability claims for SSCs. • Demonstration of conservative assumptions in the hazard analysis. • Sensitivity analysis and assessment of cliff edge effects. • Demonstration of HIC qualification • Application of appropriate standards, codes and analysis tools. **The process for identification, screening and quantification of credible bounding events (including credible combined hazards) within the DBA?** See HEPF section description of ONR expectation on deterministic screening and probabilistic screening. Key considerations in addition to the above:		Following screening, some hazard combinations could be determined to be credible but need to be assessed against specific acceptance criteria. **Combining correlated, consequential and independent hazards (i.e. on a frequency basis, and positively and negatively related external hazards)?** See previous answer. **The process for identification and quantification of hazard combinations for beyond design basis?** For ARN, it is not feasible to identify a priori a set of hazard combinations that should be required for beyond design basis. A set of DECs should be derived and justified as representative, based on a combination of deterministic and probabilistic assessments as well as engineering judgement. **Ensuring conservatism in the analysis and the various sources of uncertainties (e.g. assumptions, design information or analytical model)?** Conservative analysis using either an appropriate and verified computer model or a simplified approximation on the basis of experimental data, or other appropriate and justified conservative assumptions **The use of probabilistic analysis?** ARN expects deterministic and probabilistic assessments as well as engineering judgement.

Hazard	NNSA Response	ONR Response	NNR Response	ARN Response
	External hazards a. Considering lessons learnt from Fukushima accident, DBF combined with precipitation of 1000 year occurrence is applied to evaluate the external flooding. **Ensuring conservatism in the analysis and the various sources of uncertainties (e.g. assumptions, design information or analytical model)?** For the combined hazards considered as the design basis event, the conservative method is considered, as well as the uncertainties, such as the definition of the design basis flood. For the combined hazards considered as the beyond design basis event, the realistic method is adopted for the analysis. **The use of probabilistic analysis?** Engineering judgement, deterministic safety assessments and probabilistic safety assessments are considered for the combined protection design.	• The duration of the hazards when considering the possibility of other hazards during this period. • The duration of consequential effects on plant. • The time it would take to introduce alternative equipment to take over the long-term provision of safety functions. The mission times - the time that the safety systems will need to operate should be specified based on the consequences of the event and not just the duration of the hazards themselves **Combining correlated, consequential and independent hazards (i.e. on a frequency basis, and positively and negatively related external hazards)?** See comments in Drop load section above. **The process for identification and quantification of hazard combinations for beyond design basis?** See Comments in HEPF section. **Ensuring conservatism in the analysis and the various sources of uncertainties (e.g. assumptions, design information or analytical model)?** See comments in Drop load section above. **The use of probabilistic analysis?** See comments in Drop load section above.		
Multi-hazard barriers	**What are the regulatory expectations in the assessment and substantiation of multi-hazards barriers (internal and external) and penetrations?** Relevant safety classified structures and components **should** be **designed** to **withstand all relevant loading** resulting from operational states and **design basis accidents** including those resulting from internal and external hazards. (NS-G-1.2) The design details are as follows : **HPR1000** For HPR1000, as some general design principles, the design of safety classified structures and components considered the internal and external effects. For example, the containment of Reactor Building and safety classified	**What are the regulatory expectations in the assessment and substantiation of multi-hazards barriers (internal and external) and penetrations?** Civil barriers are a key claim in internal hazards safety cases. ONR expectations required that the Civil barrier is adequately designed to protect against a number of credible internal hazards individually and in combination (combined hazards). Substantiation of barriers provides the requisite evidence for the claim made on barriers, in general: • All barriers should be identified and listed in the hazard schedule. • All loads should be characterised. • All design codes and analytical methods should be made explicit. • All acceptance criteria and margins of safety should be stated.	**What are the regulatory expectations in the assessment and substantiation of multi-hazards barriers (internal and external) and penetrations?** For each identified hazard combination sequence, the analysis should consider any deterioration or damage to SSCs important to safety (including hazard barriers) after being subjected to each of the various hazards. For example, for a pipe failure that leads to a missile and a subsequent flood, the analysis of the capability of a hazard barrier to withstand the hydrostatic loads from flooding will need to take account of any damage caused by successive or simultaneous hazards (e.g. the failure of pressurised parts, which could lead to pipe whip, jets, and steam pressure effects on barriers or other SSCs important to safety). See also responses in the section on "Expectations on layout" below.	

Hazard	NNSA Response	ONR Response	NNR Response	ARN Response
	valves used in DBC can understand the pressure and temperature induced by steam release. **What are the regulatory expectations on layout design against internal hazards, including for those areas of the design where full segregation of systems, structures and components is not feasible?** The reply can refer to topic #8.	• The assessment of multi-hazard barriers is a multi-discipline effort between internal hazards and civil engineering. Substantiation of Multi-Hazards Barriers – Combined Hazards should consider: • The sequencing, duration and timing of individual loads can be critical to the combined effects and may play a part in the engineering substantiation of multi-hazard barriers. • Assumptions on timing and duration should be based on robust consequence assessment, the layout of the plant in question, and the qualification and proven performance of the SSCs under the conditions of the hazard. • Should take into consideration any deterioration or damage to safety related SSCs after being subjected to each of the various consequences to determine its overall performance. • Alternatively and conservatively an assumption can be made that all loads apply at the same time, but this may lead to over design. • All penetrations on divisional barriers should be identified and minimised where possible. Their location should also be optimised. • Penetration design guidelines and rules should be made available. o Ventilation dampers on divisional barriers should be generally avoided. If included, dampers on either side of divisional barriers should be included in line with UK regulatory expectations. o Single doors on divisional barriers should be generally avoided. If included, the single doors are required to withstand all relevant internal hazard loadings equivalent to those of the Class 1 barriers. An appropriate monitoring system, of appropriate classification, should be also included. Lobby configurations (doors in series for defence-in-depth) are likely to be reasonably practicable. **What are the regulatory expectations on layout design against internal hazards, including for those areas of the design where full segregation of systems, structures and components is not feasible?** The design and layout of the site, its facilities (including enclosed plant), support facilities and services should be such that the effects of faults and accidents are eliminated or minimised. The design layout should: • minimise the direct effects of initiating events, particularly from internal and external hazards, on structures, systems or components;	**What are the regulatory expectations on layout design against internal hazards, including for those areas of the design where full segregation of systems, structures and components is not feasible?** See responses in the section on "Expectations on layout" below.	

Hazard	NNSA Response	ONR Response	NNR Response	ARN Response
		• not compromise the safety of the site, or its facilities, structures, systems and components; • minimise any interactions between a failed structure, system or component and other structures, systems or components; • ensure that site personnel are physically protected from direct and indirect effects of faults; and • facilitate access for necessary recovery actions and re-supply of essential stocks, materials, equipment and personnel following an accident. Essential services and support facilities important to the safe operation and/or safe shutdown of the facility should be designed and routed so that, in the event of a fault or accident, sufficient capability to perform their safety functions will remain. Support facilities and services include access roads, water supplies, fire mains, flood defences and drainage, essential services and site communications. Also See guidance in layout section Below.		
Expectations on layout	**What are the regulatory expectations in the assessment and substantiation of multi-hazards barriers (internal and external) and penetrations?** The reply can refer to topic #7. **What are the regulatory expectations on layout design against internal hazards, including for those areas of the design where full segregation of systems, structures and components is not feasible?** **Regulatory expectations for combined hazards**： **HPR1000** **Redundant trains** should be **separated** by **barriers** or **distance** in order to ensure that an internal hazard cannot lead to the loss of more than one train. （NS-G-1.2) **The design details are as follows**： **HPR1000** HPR1000 adopted the same general requirements. Internal hazards have been taken into account in the general arrangement so as to ensure the delivery of safety functions in the event of internal Hazards. Priority should be given to passive barriers, such as the safeguard building and the SEC pumping station, which are segregation areas to protect the effects of internal hazards from impacting	**What are the regulatory expectations in the assessment and substantiation of multi-hazards barriers (internal and external) and penetrations?** See relevant section above. **What are the regulatory expectations on layout design against internal hazards, including for those areas of the design where full segregation of systems, structures and components is not feasible?** In addition to the relevant sections above: ONR requires demonstration of the adoption of inherently safe design and hazard / fault tolerant options from concept design stages, so far as is reasonably practicable. This can lead to: • A simpler and more robust set of "hazard informed" layout decisions, • Increased "hazard robustness" – in particular the adoption of simple solutions such as "massive and passive" barriers with a reduced number of penetrations though primary hazard barriers, • Avoidance of more complex and potentially less robust safety cases. ONR expects Nuclear plants to show hazard resilience e.g. layout optimisation and segregation of redundant and diverse safety systems by robust passive barriers to withstand the maximum credible loadings.	**What are the regulatory expectations in the assessment and substantiation of multi-hazards barriers (internal and external) and penetrations?** The design shall be such as to ensure that items important to nuclear safety are capable of withstanding the effects of internal and external events considered in the design, and if not, other features such as passive barriers shall be provided to protect the facility and to ensure that the required safety function will be performed. For the currently operating plant, US NRC regulations concerning containment isolation and penetrations are the following: • General Design Criteria 10 CFR 50 Appendix A • No. 54: Piping systems penetrating containment, • No. 55: Reactor coolant pressure boundary penetrating, • Containment, • No. 56: Primary containment isolation, • No. 57: Closed system isolation valves, (Justified exceptions to compliance with these GDCs are penetrations of the containment hydrogen monitoring system, penetrations for containment radioactivity measurement, low head safety injection and containment spray system recirculation line penetrations, etc.),	**What are the regulatory expectations in the assessment and substantiation of multi-hazards barriers (internal and external) and penetrations?** ARN expectation includes the separation and protection of safety divisions as well as for penetrations and openings in the boundaries of safety divisions. Some of these expectations are the following: • In rooms where safety divisions cannot be constructed as separate compartments, they shall be separated by partly separating structures or by distance. The methods of separation to be used in these cases shall take into account the defence-in-depth concept of fire protection and they shall be justified by analyses. Examples of such cases include the containment as well as the control room and the cable spaces below it. • The functional need for doors, hatches and penetrations in structures between safety divisions shall be justified, and they shall be designed to fulfil the leak-tightness, pressure resistance, fire resistance and other environmental requirements set for structures between safety divisions. • The number of doors, hatches and penetrations shall be kept to a minimum between a safety division and any other compartment containing heavy fire loads or substantial flood sources. The functional need

Hazard	NNSA Response	ONR Response	NNR Response	ARN Response
	the delivery of safety function. The structure considers the combination of loads from different kinds of external hazards. The general plant layout also preferentially adopts geographic separation, physical separation or a combination thereof between safety related or non-safety related systems to preclude adverse interaction between safety related and non-safety related systems. The consideration for Reactor Building: The **three primary loops** are arranged within the **internal containment** and **enclosed** by the **secondary** shielding walls. **Inside** the secondary shielding walls, **each loop** is **separated** from the others **by massive walls**. **Between** the **internal containment** and the **secondary shielding** walls is annular space for personnel access. **Different safety trains are generally arranged in it by spatial separation.** But it still have some exception to segregation areas in Reactor Building, which hazards safety assessments are carried out to demonstrate that hazard effects will not lead to unacceptable consequences	Approaches based entirely on separation by distance or on SSCs qualification may be challenging to substantiate in the absence of suitable segregation. ONR expects that **all areas where exception to segregation exists should be identified and assessed and an ALARP demonstration provided.** A safety case should provide analysis to demonstrate the risks have been reduced to ALARP for the perspectives of: • Normal operation, • Potential faults and accidents, • Engineering design. ALARP requires the demonstration of: • Everything 'reasonably practicable' has been done to reduce risks - [i.e. all credible hazards and combinations of have either been prevented or the severity of the hazard loading and associated nuclear Consequences are sufficiently limited]. • An adequate balance is maintained between the level of risk and the measures required to control the risk in terms of money, time or trouble. • Where action is not taken the safety case need to demonstrate that those measures would be grossly disproportionate to the level of risk averted.	• Regulatory Guide No. 1-11: Instrumentation pipe penetrations. Piping penetrating the containment walls shall be provided with either permanent leak tight closure devices, or remote-controlled closing devices. Penetrations for these pipes and penetrations provided in the containment to allow the passage of cables, wiring, equipment, and personnel, and more generally, any discontinuity in containment leak-tightness devices, shall, as far as necessary, be designed so that their leak-tightness may be examined independently from the containment leak-tightness tests; the appropriate leak-tightness test shall be performed at containment design pressure. Containment leak-tightness between the outside and inside atmosphere is provided by: • Welds of sleeves to the containment liner, • Outside surfaces of the sleeves inside the containment and the welds between the adapters, sleeves and pipes, • Surfaces of the sleeves outside the containment in the case of main steam and feedwater lines, • Surfaces of the sleeves outside and inside the containment, in the case of containment sweeping ventilation system (for which the sleeves form part of the process pipes) penetrations. The sleeves and adapters are designed to support the loads resulting from a pipe break. For the currently operating plant, all supports for piping crossing through the containment wall are designed to absorb loads resulting from pipe failures without inducing large scale stresses on the penetration. Moreover, piping supports are designed in such a way that no additional penetration loads are induced, even in the event of LOCA or earthquake. On the other hand, penetrations are designed to withstand the loads induced by piping (in the event of a LOCA), should the pipe supports be unable to support such loads. **What are the regulatory expectations on layout design against internal hazards, including for those areas of the design where full segregation of systems, structures and components is not feasible?** One example of a practice is as follows: When it is impossible to install a concrete barrier to protect safety	for these doors, hatches and penetrations shall be justified. In a broader approach ARN expects that the applicant demonstrates the adoption of an inherent safe design. **What are the regulatory expectations on layout design against internal hazards, including for those areas of the design where full segregation of systems, structures and components is not feasible?** The aim of considering internal hazards in the design of nuclear power plants is to ensure that the fundamental safety functions are fulfilled in any plant state and that the plant can be brought to and maintained in a safe shutdown state after any internal hazard occurrence. This implies that: (a) The redundancies of the systems are segregated to the extent possible or adequately separated, and protected as necessary to prevent the loss of the safety function performed by the systems; (b) The design of individual structures, systems and components (SSCs) is such that design basis accidents or design extension conditions induced by internal hazards are avoided to the extent practicable; (c) The implemented segregation, separation and protection are adequate to ensure that the modelling of the system response described in the analysis of PIEs is not compromised by the effects of the internal hazard; (d) The design is such that an internal hazard does not lead to a common cause failure between safety systems designed to control design basis accidents, and safety features required in the event of accidents with core melting; (e) An internal hazard occurring elsewhere in the plant does not affect the habitability of the main control room. In case the latter is not habitable, access to the supplementary control room is to be ensured. In addition and when necessary, access by plant personnel to equipment in order to perform local actions is also to be possible. The layout design should be such that the fulfilment of the above mentioned objectives can be achieved.

Hazard	NNSA Response	ONR Response	NNR Response	ARN Response
			important SSCs against pipe break impact, anti-whip devices are employed. More generally, based on p.57 of IAEA -TECDOC-1791: Physical separation of redundant trains and components is efficient against CCFs and other dependent failures originated by harsh environmental conditions and the effects of several hazards, as well as the direct impact of mechanical or electrical failures of one train on the redundant train. Earthquakes, fires and floods among other hazards have the potential to fail or degrade the condition of many plant SSCs at once. Moreover some of these hazards can induce other hazards as it happened in the Fukushima accident. Physical separation, adequate plant layout and design robustness are at the core of the defensive measures to reduce the impact of hazards, in addition to adequate safety margins and protective measures as well as good operational practices. Of particular importance is the adequate separation of cable routings of different electrical and instrumentation divisions. A full physical separation of trains might not be feasible in all plant areas. Physical separation can be accomplished either by full separations of trains through qualified barriers, the installation of protections on one train's relevant equipment and the separation by sufficient distance. The first option gives in general the highest protection.	The expected measures include physical separation that can be accomplished either by full separations of trains through qualified barriers, the installation of protections on one train's relevant equipment and the separation by sufficient distance. The first option gives in general the highest protection. When full separation is not feasible, justification and assessment of a "robust" alternative solution must be done.
Fire modelling (including validation & verification)	**What are the regulatory expectations for analytical modelling code validation?** **Empirical curve method** is widely used in fire hazard analysis of nuclear power plants in China. Some applicants are exploring the application of numerical simulation method. If the fire analysis **software is used** in the project, the **applicability of the software in engineering should be evaluated**.	**What are the regulatory expectations for analytical modelling code validation?** It is ONRs expectation that a modern standards safety case should demonstrate that analysis undertaken in the design base assessment of nuclear safety is relevant, conservative, complete and tolerant to uncertainty. Hazard analysis should be conducted on a deterministic basis, ensuring that all credible hazards (including combination of hazards) are identified, their severity determined and affects to nuclear safety related structures, systems and components assessed. For all safety case hazard analysis, the safety case should present a clear auditable trial of documentation to underpin the conclusions drawn from the modelling analysis. This should include (but not limited to):	**What are the regulatory expectations for analytical modelling code validation?** According to Section 8.7 of NNR RG-0019 "Interim Guidance on Safety Assessments of Nuclear Facilities", the applicant should demonstrate that there is reasonable assurance that the applicant designed a facility that provides for "adequate protection against fires and explosions" and is based on defense-in-depth practices. This should also establish that the radiological consequence from fires is considered in determining how the facility will meet the fundamental safety requirements. Amongst others, Section 8.7 lists fire protection features and systems that should be used. As such, they [as well as elements from the latest guidance from IAEA SSG-64 "Protection against Internal Hazards in the Design of	**What are the regulatory expectations for analytical modelling code validation?** The fire hazard analysis should be developed on a deterministic basis, with the following assumptions: (a) A fire is postulated wherever fixed or transient combustible material could be present; (b) Only one fire is postulated to occur at any one time; consequential fire spread should be considered as part of this single event, if necessary; (c) The fire is postulated whatever the normal operating status of the plant, whether at power or during shutdown. The fire hazard analysis should take into account any credible combinations of fire and other events. Fire hazard analysis should be complemented by fire probabilistic safety analysis (Fire PSA). PSA is

Hazard	NNSA Response	ONR Response	NNR Response	ARN Response
	Are analytical modelling codes formally approved by the Regulator? China's Regulator have not yet carried out the certification and evaluation of fire analysis software **Does the Regulator maintain and use an independent set of analytical modelling codes?**	• Justification that the analysis is representative of the scenario to be applied. • Both global and local effects should be evaluated. • Justification of the modelling methods used and demonstration that the analysis is within the models valid ranges. • Justification that the data used is valid for its application and verified. • Description of all the uncertainties of the model and data. • User guidelines, relevant good practice and input description. • Sensitivity studies to determine the sensitivity of the analysis (and the conclusions drawn from it) to the assumptions made, the data used and the methods of calculation. The safety case should demonstrate that all analytical models are adequately validated (i.e. the correct analytical model is used for the scenario being assessed) for each application within the safety analysis. The validation should be of the model as a whole and for those individual dominant phenomena (as identified for example by the phenomena identification and ranking table (PIRT) method), where this is not practicable, a modular approach can be adopted (if multiple analytical models are being used). Validation of the models should be against experiments that replicate as closely as possible the expected plant condition. Where more complex analysis is required, computer models such as computational fluid dynamics (CFD) are often used. These computer models allow the solving of multiple analytical models and thus are far more complex. As a result it is essential that the analyst understands the valid range of the computer model and they have assurances that the model itself has been through a robust verification and validation regime in line with relevant good practice and is adequately documented. **Are analytical modelling codes formally approved by the Regulator?** ONR doesn't prescribe, maintain or frequently use analytical fire models. **Does the Regulator maintain and use an independent set of analytical modelling codes?**	Nuclear Power Plants" on Internal fires (4.1–4.59)] might be expected to feature in fire modelling. Item 2) d) of Section 8.7 states: "The Fire Hazards Analysis consists of a systematic analysis of the fire hazards, an identification of specific areas and systems important to plant fire safety, the development of design basis fire scenarios, an evaluation of anticipated consequences, and a determination of the adequacy of plant fire safety." The validation aspects of analytical fire modelling code are governed by the following general guidance on safety analysis validation: From Section 7.3 of NNR RG-0019 "Interim Guidance on Safety Assessments of Nuclear Facilities": '7.3.8 Safety Analysis Methodology and Validation 1) The safety analysis methodology relevant to the safety analyses for each licensing stage should be described in detail along with those of the calculation codes and models used and their validation thereof. 2) It is important that the methodology to be used for any computational analyses should be specified and justified in terms of the overall approach to be adopted, computer codes used, benchmarking, development of models, and standards. As the review of these aspects may be time-consuming, it is preferable that these be addressed in the preconstruction SAR. 3) In the case of safety analyses previously performed in another country in accordance with the nuclear regulatory requirements of that country, the relevant regulatory approval letter(s), along with confirmation of the present regulatory status, provide strong supporting evidence for local acceptability. 4) Where this is not available, or the analysis differs significantly from that approved elsewhere, additional information may be required. For example, an independent in-depth review, including computational analysis, by the licensee or a third party, may be required. 5) Any calculation methods and computer codes used in the safety analysis have to undergo verification and validation of sufficient pedigree.	used to support decision making in the deterministic design of plant layout and fire protection systems. ARN understand that validation entails a comparison of the software model results to actual test or physical data through scientific assessment and benchmarking against other models. Benchmarking involves comparing the output of one software code with the output of similar code, or the results of a hand calculation or spreadsheet that serves as a baseline. This type of comparison does not necessarily constitute validation, but has merit as part of a validation procedure to the extent the baseline model is generally accepted as a reasonably accurate predictor for the phenomena of interest. Benchmarking can also provide insight into model limits of applicability, computing expense, input requirements, and important sensitivities or uncertainties. Ideally, computer code results should be compared against experimental results that were obtained in environments that mimic those to which the model will be applied. However, this type of data is generally very limited. It is an applicant responsibility to justify how the used code was validated and the adequacy of the model. **Are analytical modelling codes formally approved by the Regulator?** ARN does not approve the modelling codes, instead review and assess the submission. **Does the Regulator maintain and use an independent set of analytical modelling codes?** ARN maintain and use an independent set of "limited" modelling codes. However, it is not the case for fire. **Are there any other ways of assessing analytical modelling codes (for example, by involving services of independent technical organisations)?** ARN has the practice to use TSOs. Some of the TSOs are: GRS from Germany, US NRC, some US National Labs (like Sandia NL).

Hazard	NNSA Response	ONR Response	NNR Response	ARN Response
	If the fire simulation analysis code is used in the project, Regulator will select some typical scenarios and used independent software to verify the analysis results. **Are there any other ways of assessing analytical modelling codes (for example, by involving services of independent technical organisations)?** Consideration may be given to assess the analytical modelling codes based on fire test cases that have been carried out by other organisation.	See comments in response above **Are there any other ways of assessing analytical modelling codes (for example, by involving services of independent technical organisations)?** • Access to commercially available models could be obtained should there is a need to use analytical models. • ONR could use technical support contractor to assess models. • Various models can be used of various degree of complexity (e.g. empirical models, zone models and CFD Models) in the quantification of fire consequences.	6) Detailed guidance is provided in NNR RG-0016, "Guidance on the Verification and Validation of Evaluation and Calculation Models used in Safety and Design Analysis".' **Are analytical modelling codes formally approved by the Regulator?** The NNR doesn't prescribe nor formally approve analytical fire modelling codes but evaluate them for acceptance as part of the review of the Safety Case. **Does the Regulator maintain and use an independent set of analytical modelling codes?** The NNR is acquiring (mostly from the US NRC environment) and developing an independent set of analytical modelling codes (but not on fire modelling) through its recently established TSO, the Centre of Nuclear Safety and Security. **Are there any other ways of assessing analytical modelling codes (for example, by involving services of independent technical organisations)?** In the case of the Pebble Bed Modular Reactor Project (a high temperature gas cooled reactor), the NNR contracted services of independent technical organisations in the UK and Germany.	
Beyond design basis events	**What are the regulatory expectations for the approach to beyond design basis hazards (i.e. definition and consideration in analysis)? cf. DEC / DEE / BDB approaches.** **Combinations of events and failures (HAF102-2016)** 5.1.5.7. The design of the plant shall provide for an **adequate margin to protect items important to safety** against levels of external hazards to be considered for design, derived from the hazard evaluation for the site, and to avoid cliff edge effects. 5.1.5.8. The design of the plant shall also provide for an **adequate margin** to protect items ultimately necessary to **prevent an early radioactive release or a large radioactive** release in the event of levels of natural hazards exceeding those considered for design, derived from the hazard evaluation for the site.	**What are the regulatory expectations for the approach to beyond design basis hazards (i.e. definition and consideration in analysis)? cf. DEC / DEE / BDB approaches.** Fault sequences initiated by internal and external hazards beyond the design basis should be analysed applying an appropriate combination of engineering, deterministic and probabilistic assessments. It is generally accepted that two levels of BDB events are relevant to non-discrete hazards, one of which is primarily concerned with the potential for cliff edge plant failures for events marginally above the design basis. The second concerns more extreme events that could severely challenge plant safety functions across the site. Consequently, beyond design basis analysis has two purposes: • To demonstrate that the plant design is robust to uncertainties in the definition of external hazards design bases and the plant design that flows from them. In other words, confirm the absence of 'cliff	**What are the regulatory expectations for the approach to beyond design basis hazards (i.e. definition and consideration in analysis)? cf. DEC / DEE / BDB approaches.** From Section 7.1.1 of NNR RG-0019: '6) For DBECs, best estimate analyses plus uncertainty or sensitivity analyses, may be justified.' The NNR expects operators (i.e. according to Section 8.2 of NNR Position Paper PP-0014 Considerations of External Events for New Nuclear Installations) to make provisions for events with hazard levels that has a potential to exceed levels considered for design and to prevent the potential for small deviations in plant parameters from giving rise to severely abnormal plant behaviour (cliff edge effects). To achieve this an additional safety goal (called beyond design basis safety goal) is defined which requires an applicant to meet the design basis safety goal limit with a sufficient safety margin. The NNR	**What are the regulatory expectations for the approach to beyond design basis hazards (i.e. definition and consideration in analysis)? cf. DEC / DEE / BDB approaches.** For design extension condition, the regulatory expectation is that the analysis be done following a best estimate approach together with an evaluation of the uncertainties to compare the results of calculations with acceptance criteria (BEPU). A best estimate approach provides more realistic information about the physical behaviour of the reactor, identifies the most relevant safety issues and provides information about the existing margins between the results of calculations and the acceptance criteria. An uncertainty analysis should be performed to address the uncertainties in the code models, in the plant model and in plant data, including uncertainties in measurements and uncertainties in calibration, for the analysis of each

Hazard	NNSA Response	ONR Response	NNR Response	ARN Response
	The conservative definition of design basis external hazards and suitable margin given in the design by following the nuclear industry guidance are considered to avoid cliff edge effect. • Considering lessons learnt from Fukushima accident, DBF combined with precipitation of 1000 year occurrence is applied to evaluate the external flooding. • Detail SMA is performed to evaluate seismic margin for NPP. • Large commercial aircraft impact is considered in the NPP design.	edge' effects just beyond the design basis. This is a success based analysis, where the intent is to show that plant failure does not occur • To demonstrate that for external hazard events significantly beyond the design basis, the Licensee has an understanding of how nuclear safety significant plant (Structures, Systems and Components) respond, what failure modes can occur and how the ability of plant and Systems, Structures and Components, and operators to deliver safety functions is degraded Beyond design basis Analysis for hazards should: • Identify plant / SSC vulnerabilities and potential measures to improve robustness. • Demonstrate sufficient margin to avoid cliff edge effects just beyond the design basis. • For non-discrete hazards identify the hazard level at which safety functions could be lost (i.e. determine the beyond design basis margin). • Provide an input to probabilistic safety analysis of whether risks targets are met. • Ensure that safety is balanced so that no single type of hazard makes a disproportionate contribution to overall risk. • Ensure that small changes to the design basis fault or event assumptions do not lead to a disproportionate increase in radiological risk. • Provide an input to severe accident analysis (non-discrete hazards only). ONR's expectations for Beyond design basis Analysis are given in the Safety Assessment Principles, specifically EHA.7 'Cliff edge' effects and 18 'Beyond design basis events'. Additional guidance is provided in NS-TAST-GD-013. <u>Cliff edge effects</u> EHA.7 introduces the need to demonstrate that there will not be a disproportionate increase in radiological consequences from an appropriate range of events that are more severe than the design basis event. The analysis should seek to provide confidence that the plant design and its operation are robust in the face of uncertainties to design basis definition (i.e. uncertainties in the data and analysis) and the plant design process, and those safety functional requirements if degraded, does so in a predictable and gradual manner. ONR considers events relating to cliff edge effects just beyond the design basis are broadly consistent with a WENRA DEC "A" event. ONR expects Licensees to:	considers this approach similar to the IAEA approach used for the definition of design extension conditions, and consequently the IAEA approach is applicable. [13] NNR Position Paper PP-0014 Considerations of External Events for New Nuclear Installations	individual event. The overall uncertainty in the results of a calculation should be obtained by combining the uncertainties associated with each individual input. Studies to quantify the scaling effect between an experimental arrangement and the actual plant size should also be considered. In addition, the uncertainty in parameters associated with the results of a computer code may be determined with the assistance of a phenomena identification and ranking table (PIRT) for each event that is analysed. The ranking should identify the most important phenomena for which the suitability of the code has to be assured and should be based to the extent possible on available data.

Hazard	NNSA Response	ONR Response	NNR Response	ARN Response
		• accurately identify critical failure modes and their nature (e.g. ductile or non-ductile) as this is helpful to aid the identification of the actual threshold of failure • establish that the hazard varies gradually around the design basis frequency, and that the plant response does not suddenly change in this region, say due to the failure mechanism • demonstrate margin between the design basis and the loss of the design basis safety function that reflects the known uncertainties in both hazard analysis and plant response analysis • demonstrate that loss of safety function should not, where practicable, lead to another fault condition, ie equipment should be designed, where practicable, to fail safe following an external hazard Note: the design basis hazard value may well be very much greater than the site-specific hazard analysis value, implying a large in-built margin to the design basis hazard definition. Beyond design basis Analysis EHA.18 introduces the need to analyse fault sequences initiated by internal and external hazards beyond the design basis should through an appropriate combination of engineering, deterministic and probabilistic assessments to understand the hazard level at which safety functions could be lost. The use of good engineering practice applied to protect and mitigate conservatively defined non-discrete faults initiated down to the 10-4/yr. exceedance frequency value, is likely to provide a level of risk control that will satisfy the SAP risk targets. However, because non-discrete EHs are described by hazard curves covering a wide range of frequencies, parts of which extend well below 10-4/yr. the BDB component may contribute significantly to facility risk. For non-discrete hazards therefore, BDBA is important and can help to define the hazard severity at which plant / SSC failure or loss of safety function occurs. Where a design basis is established for a discrete EH and a hazard curve is not defined, the possibility of an event more severe than the design basis may also need consideration. This applies if the event initiation frequency is difficult to determine or if the IEF is less than the design basis criterion. A possible approach to demonstrate sufficient margin to loss of safety function for the former is to select one or more hazard-specific loading values that are higher than the design basis event loads and demonstrate that the safety functions are not endangered by these loads. The severity of the loading		

Hazard	NNSA Response	ONR Response	NNR Response	ARN Response
		values may be chosen to correspond to a safety margin that is considered adequate. The use of a MCE for such analyses may also be useful, but caution should be exercised if the selected MCE is very severe, since this might lead to the conclusion that for such an event reasonably practicable plant improvements do not exist. Selecting a more reasonable choice of BDB event may provide opportunities for reasonably practicable plant improvements. For the latter, where the hazard occurrence frequency is estimated to be below the design basis criterion but above the EH screening criterion the fault analysis guidance given in SAPs paragraph 609-610 is applicable. In this case it is expected that assessment of the likely accident progression and potential consequences should take place to allow consideration of reasonably practicable means of protection or mitigation of the consequences such that the risks are ALARP. It has previously been accepted that one satisfactory approach to the demonstration of absence of a disproportionate increase in consequences is via an EHs PSA. This has the merit of exploring the response of the plant to a wide range of hazard levels and is accepted internationally as a reasonable approach for EHs.		
Maximum credible events	**What are the regulatory expectations for differentiating between the approach for man-made and natural external hazards from a MCE perspective including:** NO.SSG-18 Meteorological and Hydrological Hazards in Site Evaluation for Nuclear Installations. 2.23. In some cases in which a physical limit exists (e.g. the amount of water vapour required to reach saturation in a volume of air), deterministic methods may provide rational limits to the statistical extrapolation by means of the concept of the 'physical limit': an upper limit on the variable of interest, such as flooding level or wind velocity, irrespective of the frequency of occurrence.	**What are the regulatory expectations for differentiating between the approach for man-made and natural external hazards from a MCE perspective including:** It is ONR's expectation that the safety case should list all initiating faults that are included within the design basis analysis of the facility. For external hazards, the design basis event should be derived conservatively to take account of data and model uncertainties. The thresholds set for design basis events are 1 in 10,000 years for external hazards and 1 in 100,000 years for internal hazards. Initiating fault frequencies should be determined on a best estimate basis with the exception of natural hazards where a conservative approach should be adopted to account for data and model uncertainties. For some discrete hazards, usually man-made hazards, it may be possible to characterise a worst-case event, called a Maximum Credible Event (MCE), that can be used as a surrogate for the hazard as a whole. For example, the release of a toxic gas from a nearby off-site tank farm will likely be limited by the maximum storage	**What are the regulatory expectations for differentiating between the approach for man-made and natural external hazards from a MCE perspective including:** • Identification of physical limits for natural hazards (e.g. atmospheric energy constraint on precipitation). • Identification of physical limits for correlated and unrelated/independent natural hazards (e.g. air temp and contemporaneous enthalpy cf. air temp and wind speed). The NNR philosophy is to distinguish between non-discrete hazards (i.e. some if not most natural hazards fall under this category) and discrete hazards (i.e. some if not most man-made hazards fall under this category). NNR expectation is that non-discrete hazards will be determined probabilistically, as a conservative estimate of hazard severity at the 10-4/yr. frequency of exceedance point on the hazard curve. Beyond design basis hazards are determined at a frequency that is less than this. This frequency needs to be justified by the operator/applicant. However, the	**What are the regulatory expectations for differentiating between the approach for man-made and natural external hazards from a MCE perspective including:** AR 10.10.1 regulation for sitting a NPP deals with both, discrete hazards and non-discrete hazards. For discrete hazards, typically man –made, the approach is to follow a Maximum Credible Event compatible with the site characteristic when possible, for example, regarding toxic from ships due to traffic river, the distance from the plant location to the river has to be consider. For external hazards, the regulatory expectation with respect to design basis is to determine the hazard severity through a probabilistic approach. According to the current experience, the practice is to set external events at the 10-4/yr. frequency of exceedance point on the hazard curve.

Hazard	NNSA Response	ONR Response	NNR Response	ARN Response
		capacity of the tanks. The MCE concept is useful for quickly estimating worst-case scenarios and is generally applied to hazards whose nuclear safety implications are minor. Quite often, the Licensee is able to demonstrate in a straightforward way that, even at the MCE level, the nuclear safety implications are negligible and therefore the hazard can be screened out from further consideration. The MCE can also be useful in helping to define a design basis event when probabilistic methods for the hazard in question carry large uncertainties, and also provides a useful insight for BDBA Some hazards may not be amenable to the derivation of a design basis event based on frequency. In principle, it may also be possible to develop a MCE for a non-discrete hazard. In such cases a surrogate Maximum Credible Event, supported by scientific evidence, may be defined. For example, if the hazard curve is asymptotic to some upper value of severity, or if a relevant physical limit can be defined that limits hazard severity. Where hazards are not amenable to the derivation of a design basis event based on frequency, a surrogate MCE, supported by scientific evidence, may be defined. The severity of the surrogate MCE should be chosen and justified to reach an equivalent level of safety (that is, it should be compatible with the principles of SAP FA.5).	NNR recognises that nuclear facilities are quite broad and such a definition is more reasonable if it is applied to power reactor facilities as they demand a higher level of safety. Therefore, the NNR follows a graded approach when applying these criteria.	