Small Modular Reactors Regulators' Forum

Working Group on

Design and Safety Analysis

Phase 2 REPORT

June 2021

Table of Contents

EXECUTIVE SUMMARY

There is a sustained global interest in small modular reactors (SMRs), which have the potential to play an important role in globally sustainable energy development as part of an optimal energy mix. Such reactors have the potential to enhance energy availability and security of supply in both countries expanding their nuclear energy programs and those embarking on a nuclear energy program for the first time.

The SMR Regulators' Forum was formed in 2014 to identify, improve understanding of and address key regulatory challenges that may emerge in future SMR regulatory discussions. This will help enhance safety, improve efficiency in SMR regulation, including licensing, and enable regulators to make informed changes, if necessary, to their requirements and regulatory practices.

The Forum entered its second phase in 2017, following up on the work carried out in previous years. This document is the Phase 2 final report of the Working Group on Design and Safety Assessment (DSA-WG). Appendix G shows the list of the contributors to the report

The following three topics were covered in the second phase which was completed at the end of 2020:

- Multi-unit, multi-module aspects of SMRs
- Considerations in the use of passive and inherent safety features in SMR designs
- Aspects of Beyond Design Basis Analysis relevant to SMRs

This report was developed based on information, insights, and experience gained from the regulatory activities of the SMR Regulators' Forum members. It is considered to be generally consistent with existing IAEA documents but may deviate in some cases. This report is intended to provide useful information to regulators and industry in the development, deployment and oversight of SMRs.

Introduction

This report is divided into a high-level description of the main common positions of the authors of the report and three main technical chapters:

Content of the report

Chapter 1: Multi-unit, multi-module aspects of SMRs

This chapter presents common positions on the design and safety analysis aspects specific to multi-unit/multi-module SMR facilities.

Chapter 2: Considerations in the use of passive and inherent safety features in SMR designs

This chapter presents common regulatory positions on the regulatory assessment of passive and inherent safety features for SMRs. Although the inclusion of passive and inherent safety features within designs is not exclusive to SMRs, the subject is of particular importance for SMRs because of the extent to which such features are deployed in SMR design proposals.

Chapter 3: Aspects of beyond design basis analysis relevant to SMRs

This chapter presents common positions on the consideration of safety features at Level 4 defence-in-depth (design extension conditions, severe accidents, and the concept of 'practical elimination' as introduced in SSR-2/1 (Rev 0, 2012)) for SMRs.

Positions generated by the Working Group are provided for each chapter in turn below:

Common Positions

Common Positions for Chapter 1: Multi-unit, multi-module aspects of SMRs

Terminology and definitions

- The DSA-WG acknowledge that SMR designers use the term "modular" to denote both "modular design approaches" and/or "modular construction approaches" [1], [2], [3]. However, irrespective of how the modules/units are defined for any particular design, the WG agreed a common position that it is most important to:

    - Clearly define terminology in each instance that terms are used
    - Understand safety and regulatory implications of sharing the structures, systems, and components and/or infrastructure. In these cases, it is important to ensure that the safety of the nuclear power plant is not negatively impacted by the adoption of a modular reactor deployment.
    - Recognize that multi-unit/multi-module SMR designs may have certain potential operational and safety benefits, such as interconnections between units/modules to

strengthen the availability and reliability of support services (electric power, compressed air, water) or qualified personnel.

Defence-in-Depth

- The WG agreed a common position that it will be important to consider the impact of multi-unit/module issues at all levels of DiD (level 1 to level 5). Specific positions relating to relevant issues are given below:

Internal and external hazards

- For sequential deployment or maintenance of units, consideration should be given to ensuring that a hazard in units/modules under construction, in maintenance or in operation would not have any safety consequences for neighbouring operating units or the safety consequences are properly considered. The current requirements usually refer specifically to "units"; however the working group considers that its underlying principles are applicable to all SMR designs containing multiple reactor cores, regardless of the nomenclature adopted (i.e. "multiple unit' or "multi module")

Selection of initiating events

- The working group acknowledges that multi-unit/module SMRs may use shared systems to a greater extent than multi-unit NPPs because of their compact configuration and close proximity, therefore the selection of initiating events should consider these aspects of a design.

Shared SSCs

- For SMR designs which shared SSCs the safety assessment should consider all relevant safety implications, in recognition that sharing may introduce risk significant vulnerabilities in the design.

Risk Assessment for multi-unit/multi-module sites

- The DSA-WG members consider that it would be beneficial for both designers and regulators to think beyond the single unit mindset. This might involve extending their considerations to whole site risk including developing methods of aggregating risk from differing on site sources (e.g. new and old reactors, spent fuel pools). Furthermore, the proper balance between deterministic and probabilistic safety approaches should be achieved.

Emergency preparedness

- The DSA-WG considers that the presence of multiple modules/units at the site could exacerbate challenges that the plant personnel would face during an accident. The events and consequences of an accident at one unit may affect the accident progression or hamper accident management activities at the neighbouring unit; available resources (personnel, equipment, and consumable resources) would need to be shared among

several units. These challenges should be identified and the available resources and mitigation strategies shown to be adequate.

Common Positions for Chapter 2: Considerations in the use of passive and inherent safety features in SMR designs

Identifying and Addressing Uncertainties in Performance claims for First of a Kind Facilities

- A facility safety case, in particular for a First of a Kind (FOAK) facility, is expected to systematically identify, account for and address uncertainties in performance claims for passive and inherent features through a strategy that considers aspects such as:
    - results from substantiation activities (e.g. use of sufficiently validated computer models, experimental prototypical systems, integrated test facilities)
    - compensatory design enhancements (if required),
    - control provisions expected to be implemented by the operator; and,
    - any additional activities necessary to demonstrate and/or support functional performance claims and gather experience data.

- The greater the combination of interfacing inherent and passive design features the more complex the performance uncertainties become. In such cases, design substantiation should pay particular attention to the need for integrated testing activities both during the design process and in the commissioning program for the First of a Kind facility.

Assessment of Reliability for Passive Systems in the Presence of Weak Driving Forces

- Designers should establish clear criteria for characterising the strength of driving forces in features that support safety functions with a particular emphasis on understanding conditions that may weaken those forces to the point where their effectiveness or predictability is significantly impacted. This information should be used to identify and understand failure modes that could, in principle, impact the delivery of a safety function with sufficient reliability. Designers should ensure that all parameters potentially affecting the delivery of a safety function are taken into account within the safety demonstration.

Optimization of the Use of Passive and Active Features in the Design Process

- Subject to a prioritisation which favours first inherent characteristics and then passive features or continuously operating systems over systems that need to be brought into service (Safety of Nuclear Power Plants: Design, SSR-2/1 Rev1SSR-2/1 [4] Requirement 16), any combination of active and passive safety systems can be acceptable provided defence in depth and safety design principles are met. The designer should document the approach for establishing optimization in the use of passive and active features in

consideration of the availability of supporting information to substantiate safety claims and to support the conduct of safety classification.

Applicability of the Single Failure Criterion to Provisions that Include Passive Features and Inherent Characteristics

- Designers should apply the single failure criteria in safety evaluations of passive safety systems deployed within SMRs. Dis-applications of the single failure criteria may be considered for passive systems if it is not reasonably practicable to achieve compliance, for instance via the incorporation of redundancy into a design, however this should be accompanied by a demonstration that adequate reliability can otherwise be achieved. Particularly in circumstances where driving forces are weak, analyses should account for all potential system failure modes and consider how these may evolve in time in order that the worst-case single failure mode is captured.

Requirements for Diversity and the Treatment of Common Cause Failure

- Designs should incorporate redundancy, diversity and, where practicable, physical separation for safety systems to mitigate common cause failures. Particular attention should be paid to functional diversity where exclusively passive safety systems are deployed in SMR designs. There may be some benefit in using combinations of passive and active systems to ensure a safety function is delivered as this may provide additional diversification to improve resilience to common cause failures.

Recommendations from Chapter 2

The difference between Passive and Inherent Safety Features

- In view of the wide variety of passive systems that may be deployed in a single SMR, the benefits of providing guidance within a framework that recognises that a spectrum of passivity is possible should be explored. This could include the development of requirements in a more granular way, based on the categorisation proposed in TECDOC-626 [5] and separately addressing expectations for substantiation with respect to inherent system characteristics, passive system features and any active elements that may be involved in system actuation.

Assessment of Reliability for Passive Systems in the Presence of Weak Driving Forces

- Current regulatory guidance from member states set quantitative expectations for the reliability of passive safety systems despite there being no accepted general methodology for conducting such an assessment. Continued research in this area is of particular importance for SMRs which may incorporate exclusively passive safety features. The work of the IAEA in this area is acknowledged (e.g. TECDOC-1752 [6]), and we recommended continued work on the development of assessment methodologies to support the deployment of SMRs.

Applicability of the Single Failure Criterion to Provisions that Include Passive Features and Inherent Characteristics

- Where a passive flow is evolving, the parameters most affecting the flow could change radically such that single failures relevant to each stage of a transient might not be easily determined. In such situations iterative evaluation of transient scenarios may be necessary to identify worst case failures. Further work in this area may be of benefit since it does not appear that this issue has received significant attention.

Common Positions for Chapter 3: Aspects of Beyond Design Basis Analysis relevant to SMRs

Challenges with Characterising Severe Accidents for Novel SMR Concepts

- For novel design characteristics of SMRs, there is a need to identify criteria against which some event sequences and accidents scenarios are judged to be severe, taking account of the potential for barrier failure with radioactive release or fuel relocation. Both designers and regulators will have a role in defining such criteria. This is particularly important for SMR designs in which the concept of "core melt" is claimed not to apply. The potential for severe consequences to arise from actions required to clean-up following an accident, including the case of multi-module units and/or in co-located facilities[1] should also be considered.

The Role of DiD in Preventing and Mitigating Severe Accidents

- SMR designers need to identify, from the outset, how defence-in-depth principles, based on the provision of multiple independent barriers to accident progression, are applied within the safety provisions and information substantiating those provisions. The progression of faults/accidents should be analysed assuming failure or degradation of the primary barriers (levels 1-3 DiD) to fission product release in order to establish a facility's vulnerability to severe accidents. All areas of a facility having the potential for severe accidents have to be assessed.

- SMR designers need to systematically identify credible severe accident scenarios for their designs including very low frequency events. Severe accident scenarios are expected to consider the consequences of accidents that result from credible failures of the level 1-3 of defence in depth. Where claims are being made that severe accidents will be precluded by design provisions, such conclusions need to document how accidents based on unmitigated consequences associated with a fault have been characterised and analysed. Any assumptions with respect to the maintenance of barrier integrity should be robustly justified.

Design Extension Conditions

- Safety features at level 4 DiD are necessary to assure fundamental safety functions, particularly confinement/containment of radionuclides, in all credible severe accident

[1] For example, some molten salt designs incorporate co-located fuel processing facilities which should be assessed for their severe accident potential

scenarios so far as is reasonably practicable. The inclusion of additional features for accidents scenarios involving multiple failures needs to be considered to improve resilience to common cause failure.

Practical Elimination of Event Sequences and Accident Scenarios that Could Lead to a Large or Early Release

- A systematic and defensible demonstration that event sequences that could lead to a large or early release have been practically eliminated ([4], Sections 2.11 and 2.13) needs to involve a complementary and iterative use of deterministic and probabilistic analyses coupled with use of experiential information[2]. For the First-of-a-Kind facility the demonstration of practical elimination will need to take account of the absence of OPEX.

Recommendation from Chapter 3:

Challenges with Characterising Severe Accidents for Novel SMR Concepts

- A definition of a severe accident based on the unmitigated[3] consequence associated with a fault, such as is applied in the United Kingdom, has the benefit of being technology neutral and more readily adaptable to the assessment of SMRs for which LWR concepts such as core melt does not apply. It is recommended that the IAEA considers this consequence-based definition as an acceptable alternative definition and explores the benefit of adopting such a definition for SMRs.

[2] Information derived from OPEX, R&D activities, computer modelling etc.
[3] The unmitigated consequence is the radiological consequence obtained when no severe accident safety measures are provided

Chapter 1: Design and safety analysis issues specific to multi-unit/module SMR facilities

A relatively large number of SMR designs envision deployment of their reactors on multiple units/multiple modules configurations in order to better respond to the evolving energy demands and enhance operational flexibility.

The current operational experience with multi-unit nuclear power plants indicates that they may require specific considerations for nuclear safety, emphasized by the lessons learned from the multi-unit Fukushima Daiichi nuclear accident. In this context, the design and safety analysis working group considers that the specific safety considerations for safety of multi-unit/multi module SMRs are important and relevant for the scope of the SMR Regulators' Forum.

It is also consistent with the approach outlined in the pilot project report of SMR Regulator's Forum which \identified the concept of "multi-module" specific to SMRs. The DSA-WG note that multi-unit/module SMRs may use shared systems to a greater extent than multi-unit NPPs because of their compact configuration and close proximity, and this may impact among others, the selection of initiating events, internal and external hazards, the approach to shared systems, defence in depth, human factors engineering and risk assessment.

1.1 Scope of the Working Group Discussions

The DID WG [7] concluded that *"It is necessary to demonstrate that for "multi-module" facilities, all connections, shared features and dependencies between modules/units are not detrimental to DiD. The safety issues to be included in the safety demonstration for "multi-module" facilities should be investigated and completed as further SMR design information becomes available. The impact of the common features and dependencies between modules on each of the DiD levels and on the independence of them should be investigated."*

The DID WG noted that although SMR concept is typically based on modules/units with small power and radioactive inventory, the SMR design should consider the potential consequences on several or even all units on the site simultaneously caused by specific external hazards or internal hazards, throughout a "*multi-module safety assessment*".

Specific safety aspects relevant for multi-units/multi-modules identified by various working groups and reports typically include the following:

- potential for interactions among the modules
- potential for sharing safety systems and features.
- multi-module failure in hazards conditions
- modules dependence/independence
- human factors engineering, including aspects related to

- main control room;
- supplementary control and other emergency response facilities and locations;
- maintenance of the multiple modules;
- potential remote control of the main control room;
- minimum shift complement;
- training

- emergency preparedness and response
- capacity for the addition of future modules

1.2 Specific nuclear safety aspects relevant to multi-units/modules SMRs

The above-mentioned safety aspects may require additional considerations for design and safety assessment of multi-unit/multi-module stations. A review of selected IAEA design safety standards and guides and regulatory requirements and guidance from several Member States reviewed as a part of this study with regard to safety of multi-unit stations highlighted a number of safety aspects which are presented in the following paragraphs. They are complemented by the views expressed in the pilot project report of SMR Regulators' Forum [7] and several relevant papers, presentations and meeting materials.

1.2.1 Terminology and definitions

Common Position #1.1: The DSA-WG acknowledge that SMR designers use the term "modular" to denote both "modular design approaches" and/or "modular construction approaches" [1], [2], [3]. However, irrespective of how the modules/units are defined for any particular design, the WG agreed a common position that it is most important to:

- Clearly define terminology in each instance that terms are used
- Understand safety and regulatory implications of sharing the structures, systems and components and/or infrastructure. In these cases, it is important to ensure that the safety of the nuclear power plant is not negatively impacted by the adoption of a modular reactor deployment.
- Recognize that multi-unit/multi-module SMR designs may have certain potential operational and safety benefits, such as interconnections between units/modules to strengthen the availability and reliability support services (electric power, compressed air, water) or qualified personnel.

The pilot project report of SMR Regulator's Forum [7] identified the concept of "multi-module" specific to SMRs, and acknowledged that *"the list of potential safety issues for multi-modules facilities remains open and cannot be completed until more detailed SMR design information is available"*. The report noted the difference between "multi-unit" and "multi-module", especially given that, typically, IAEA and the Member States regulatory requirements are addressing nuclear facilities consisting of "multiple-units", rather than "multi-

modules". The WG members stated that, based on the limited available information on SMR designs at the time when the report was issued, "multi-modules" could not be considered as equivalent to "multi-units", as with large reactors. The report also acknowledged that such concepts were not well defined for SMRs. An SMR "module" may or may not be completely autonomous and may not always include individual safety systems and safety support systems such as separate heat sinks or AC power. As such, for some SMR designs the control room, reactor building and ultimate heat sink, as examples, can be common to several modules. Moreover, some SMRs may use a single confinement common to several modules. Therefore, the DID WG suggested to interpret an SMR "module" as "nuclear installation" or nuclear steam supply system, rather than "plant"[4]. From the SMR definition adopted by the WG, modular reactors are "*designed to allow addition of multiple reactors in close proximity to the same infrastructure*", thus the term "modular" refers to the capability to allow additional power units on the same site. This interpretation seems consistent with the definitions from the IAEA Glossary [8][5] and 10 CFR [9] Part 50 Appendix A and 10 CFR [9] Part 52.1[6]. It should be noted that some SMR designers use the term "modular" to refer to "modular construction" denoting a simple assemble of components fabricated in factory without welding. These two concepts may co-exist, and they need to be clearly defined and understood for each case they are invoked. For the current report, the most relevant aspects are those related to the existence of multiple reactors in close proximity to the same infrastructure, rather than modular construction. More details about this are provided in the following paragraphs.

Recent discussions on the interpretation of "multiple modules' unit" were held in the framework of a study organized by the IAEA on the current views of a team of international experts regarding the applicability of SSR-2/1 (Rev. 1) [4] to SMR technologies intended for near-term deployment , i.e. light water-cooled SMRs (LWc-SMRs) and high temperature gas-cooled SMRs (HTGc-SMRs). The team of international experts (i.e. the working group) included representatives from regulatory bodies but also from designer and operating organizations of SMRs. The group noted that both LWc-and HTGc SMRs can be deployed in units that consist of multiple reactor modules (referred to as "multiple modules' units"). In some of the designs available, multiple reactor modules share some safety systems, safety features for design extension conditions, or supporting services. The potential for design approaches using multiple modules introduces new safety considerations in areas such as common-cause failures, internal hazards and human factors (e.g. shared control room design). Therefore, although the existing multi-unit requirements were deemed in general appropriate and applicable to SMRs, it was felt they need to be complemented by specific considerations for units consisting of multiple reactors (reactor modules) which may share space or safety systems/features to a greater extent than large reactors. The definitions and the main features

[4] Note that some designs could share steam generators between different reactors (e.g. HTRPM)
[5] In terms of nuclear energy **a unit** is a single reactor at a multi-reactor nuclear power plant
[6] 10 CFR 50 Appendix A: **Nuclear power unit**. A nuclear power unit means a nuclear power reactor and associated equipment necessary for electric power generation and includes those structures, systems, and components required to provide reasonable assurance the facility can be operated without undue risk to the health and safety of the public. 10 CFR 52.1 **Modular design** means a nuclear power station that consists of two or more essentially identical nuclear reactors (modules) and each module is a separate nuclear reactor capable of being operated independent of the state of completion or operating condition of any other module co-located on the same site, even though the nuclear power station may have some shared or common systems.

of "*multiple module's unit*" and "*reactor module*" in the framework of applicability of the IAEA design safety requirements (SSR-2/1(Rev. 1 [4]), proposed by the working group is reproduced below: "The term *multiple modules' unit* refers to units that include more than one nuclear reactor.

(i) A *multiple modules' unit* might include only one reactor module in the first stage of its planned development

(ii) Essential features of the *multiple modules' unit* approach typically include the following:
   a. Allow the addition of several modules in close proximity to the same infrastructure;
   b. The modules may be deployed in compact configurations and share structures, systems and components to a larger extent than in units using a single reactor design approach;
   c. Each module can be operated mostly independently of the state of completion or operating condition of any other module of the multiple modules' unit;
   d. The different modules are essentially identical.

The term *reactor module* (or *module*) refers to *multiple modules' units* and is understood as a nuclear reactor and its associated structures, systems, and components. "

1.2.2 Defence in depth

Common Position #1.2: The WG agreed a common position that it will be important to consider the impact of multi-unit/module issues at *all* levels of DiD (1-5). Specific aspects of the relevant issues are discussed in the sub-sections below.

The DID WG [7] agreed that, as a fundamental principle for ensuring nuclear safety, the DID concept is valid for SMRs, and should form an integral part of the design and safety demonstration. With regard to the application of defence in depth for multi-unit nuclear power plants, the WG acknowledged that, historically, the safety assessment and safety demonstration for large reactors are typically based on single-unit safety concept. For the majority of participating countries in the WG, a license is given for a single unit without specific regulatory requirements for multi-unit issues. However, in many countries (e.g. US, Canada, UK,) there are requirements related to the sharing of structures, systems and components important to safety among nuclear units – unless it can be demonstrated that such sharing will not significantly impair each unit's ability to perform its safety functions. The report also mentioned that shared SSCs may be a challenge for the regulators because it may introduce risk significant vulnerabilities into the design. A similar conclusion was reached by the WG who assessed the applicability of SSR-2/1 (Rev.1) [4] to near deployment SMRs, who stated that the general safety requirements of SSR-2/1 (Rev.1) are mainly technology neutral and can be applied without modifications or interpretations to different types of SMR reactor designs. Such general design safety requirements include: those related to management of safety in

design, some of the principal technical requirements (e.g. those regarding fundamental safety functions, radiation protection in design, application of defence in depth and proven engineering practices) and some of the general requirements on plant design (e.g. engineering design rules and single failure criterion). The report [7] concluded that " *The number of safety requirements having suggestions for changes and interpretation is the following:*
• *Eight (8) of the existing safety requirements for LW-SMRs (Appendix I);*
• *Thirty (30) of the existing safety requirements for HTG-SMRs (Appendix II).*
All the other safety requirements (i.e. 74 for the LW-SMRs and 52 for the HTG-SMRs) were considered fully applicable as they are without needing any change or interpretation. Regarding multi-module units, considerations about aspects having potential for establishing additional safety requirements are provided at the end of Section 6 in each of the two appendices, Appendix 1 and Appendix 2.
The considerations confirmed that the main features of the set of safety requirements established for nuclear power plants in SSR-2/1 (Rev. 1), including the guiding principles, formulation (in general terms) and relevance to contribute to defence in depth and to fulfilment of the fundamental safety functions, remain valid when applied to the two SMR technologies evaluated in this publication."

1.2.3 Internal and external hazards

Common Position #1.3: For sequential deployment or maintenance of units, consideration should be given ensure that a hazard in units/module under construction, in or maintenance or in operation would not have any safety consequences for neighbouring operating unit or the safety consequences are properly considered. The current requirements usually refer specifically to "units", however the WG considers that its underlying principles are applicable to all SMR designs containing multiple reactor cores, regardless their nomenclature (i.e. "multiple unit' or "multi module")

SSR-2/1 (rev. 1) [4] requires that "For multiple plant sites, the design shall take due account of the potential for specific hazards to give rise to impacts on several or even all units on the site simultaneously". Specific hazards (e.g. meteorological, fire, explosions) are addressed in other IAEA guides, such as NS-G-1.7 [10] or SSG-18 [11]. In general, these requirements stipulate that the plant design should consider spreading of a hazard from one unit to adjacent units. Also, the potential for common cause effects and damage across the site should be an important consideration for a design, especially if SSCs are shared between units.

1.2.4 Selection of initiating events

Common Position #1.4: The working group acknowledges that multi-unit/module SMRs may use shared systems to a greater extent that multi-unit NPPs because of their compact configuration and close proximity, therefore the selection of initiating events should consider these aspects of a design.

Selection of initiating events is impacted by the set of internal and external hazards identified for the design. It is expected that, for sites with more than one unit, initiating events should include these which can affect simultaneously more than one unit (e.g. loss of off-site power) or events that can arise in one unit and lead to an initiating event in another unit (e.g. a strike from a missile generated by disintegration of a turbine in an adjacent unit). Selection of initiating events should also consider faults originating in SSCs used by more than one reactor, such as fuel handling equipment. Most SMR designs claim the use of inherent and passive safety features, which may reduce their vulnerabilities to some postulated initiating events and external hazards which impact the whole site. However, given that a significant number of SMR designs envision multiple modules or units on the site, they may use shared SSCs, thus it is expected that the importance of some internal initiating and external events for safety may increase and they may need to be adequately addressed in the design (e.g., support system faults).

1.2.5 Shared SSCs

Common Position #1.5: For SMR designs which shared SSCs the safety assessment should consider all relevant safety implications, in recognition that sharing may introduce risk significant vulnerabilities in the design.

Typically, the current requirements and guidance limits the sharing of SSCs important to safety between units. In exceptional cases sharing of SSCs important to safety is permitted if it can be demonstrated that it is not detrimental to nuclear safety. As such, if sharing of SSCs between units/modules is arranged, safety requirements shall be met for each reactor for all operating and accident states. Also, in the event of an accident involving one of the reactors, orderly shutdown, cool down and removal of residual heat should be achievable for the other reactors. An important number of novel SMR designs include the use of common infrastructures and SSCs for several reactors, in normal operation and accident conditions. Typical examples include the reactor building/containment, ultimate heat sink, main control room, electric grid and the fuelling equipment. In this context, the specific safety considerations and experience of Member States who licensed multiple units (such as Canada) are very important. Additional details are provided in Appendix A of this document.

1.2.6 Risk Assessment for multi-unit/module sites

Common Position #1.6: The DSA-WG members consider that it would be beneficial for both designers and regulators to think beyond the single unit mindset. This might involve extending their considerations to whole site risk including developing methods of aggregating risk from differing on site sources (e.g. new and old reactors, spent fuel pools). Furthermore, the proper balance between deterministic and probabilistic safety approaches should be achieved.

The Fukushima Daiichi accident demonstrated the possibility of accidents involving nearly concurrent core damage at multiple reactor units and spent fuel pools. It was recognized that

the accident progression was influenced by complex interactions involving operator actions to protect each facility, as well as interactions and dependencies among the facilities.

In this context, there is a need for the evaluation of site risk in an integrated way, which includes consideration of the potential for accidents involving multiple installations concurrently [12, 13, 14]. This may require integration of the various risk contributions from different sources, hazard groups and plant operating states. It is important to note that the whole-site risk assessment is not expressed by a single number and it is rather based on an informed judgment taking into consideration a broad range of qualitative and quantitative information. Whole-site PSA is considered as a supporting tool and subset of whole-site risk assessment and can play a complementary role to other factors in the management of risk. [12]. Appropriate tools need to be used for SMR integrated site risk evaluation.

Traditionally, PSAs have continued to work with single unit risk metrics such as Core Damage Frequency (CDF) and Large Release Frequency (LRF). Nuclear regulators are actively developing site-based safety goals to support Risk Informed Decision Making (RIDM) and addressing risk communication to the public. In a multi-unit PSA (MUPSA), it is necessary to consider multi-unit accidents either of a causal nature, in which a single-reactor accident may propagate to affect other units, or as a result of a common cause event that affects multiple units or radiological sources concurrently. Some MUPSA technical issues and challenges applicable to multi-unit or multi module facilities identified in [14] and [15] and the main themes as follows:

1) Selection of initiating events
2) Accident sequence modelling
3) Accident sequence quantification and site-based risk metrics
4) Accident progression and source term characterization
5) Evaluation of radiological consequences
6) Site-based safety goals, risk integration and interpretation

Additional details are included in Appendix B.

During recent years, the IAEA has made significant progress in the work related to the development of internationally recognized methodologies for multi-unit risk assessment including risk-informed decision making and risk management in a multi-unit context. Relevant work has been made under the project on Multi-unit (MU) Probabilistic Safety Assessment implemented by IAEA Division of Nuclear Installation Safety.

1.2.7 Human factors

The current regulatory guidance addressing specific safety aspects regarding human factors for multi-units is scarce. The IAEA NS-G-2.14 [16] includes expectations dealing with sharing of responsibilities between the shift supervisor and units supervisors: "In multi-unit power plants, where one shift supervisor may be responsible for all units, other persons, designated

as unit supervisors, should be made responsible to the shift supervisor for the operation of each unit." Also, for multiple unit plants, arrangements should be put in place to prevent operator error resulting in the isolation of equipment in the wrong unit or that major changes to work in progress in one unit do not affect the safe operation of other units. Designers of multi-module SMR plants are considering novel operational approaches, such as single operator monitoring several modules or controlling remotely the reactors. Typically, the design of human factor engineering should include a systematic analysis to determine the basis of the minimum staff complement while considering:

1) the most resource-intensive initiating events and credible failures considered in the Safety Analysis and the PSA;
2) required actions with clearly pre-defined and thorough action manuals;
3) operating strategies;
4) required interactions among personnel;
5) staffing demands associated to the required tasks offering necessary trainings and simulation drills; and
6) staffing strategies under all operating conditions including normal operation, AOO, DBA and emergency conditions. A specific consideration may be the exceptional societal situations such as COVID-19 epidemic that may impact staffing (e.g. max number of operators in the control room/at site and protective measures to be implemented)

Proper consideration should be given to validation of human factors engineering that demonstrates the safe operation and response to the most resource-intensive conditions, including events that affect more than one unit, under all operating states including normal operations, AOO, DBA and emergency conditions.

1.2.8 Emergency preparedness

Common Position #1.7: The DSA-WG considers that the presence of multiple modules/units at the site could exacerbate challenges that the plant personnel would face during an accident. The events and consequences of an accident at one unit may affect the accident progression or hamper accident management activities at the neighbouring unit; available resources (personnel, equipment and consumable resources) would need to be shared among several units. These challenges should be identified, and the available resources and mitigation strategies shown to be adequate.

The existing requirements and guidance for multiple units emphasize the use of available means and/or support from other units, provided that their safe operation is not compromised. Proper consideration should be given to the operating state (e.g. operation/shutdown/maintenance) of all unaffected units on the site and the limitations of non-standard equipment (e.g. cross-ties of electric or heat removal systems) that might be shared between the units. The size of the emergency planning zone may be impacted by the number of reactor modules/units postulated to be built at the site, in a simultaneous or sequential

deployment, therefore these aspects should be adequately addressed at design stage . Most SMR technology developers claim that their passive and inherent safety features, simpler operation and smaller source terms, require very limited emergency management and render the size of EPZ significantly smaller than that of large NPPs.

Chapter 2: Considerations in the use of passive and inherent safety features in SMR designs

2.1 Introduction

The DSA-WG has sought to develop aspects of the work undertaken in the Pilot Project (first phase) of the SMR Regulators' Forum [7] and, in particular, the work of the Defence-in-Depth (DiD) WG of the Pilot Project. The subject of passive and inherent safety features for SMRs was one of a number of topics taken forward by the DSA-WG for in-depth discussion. The decision to consider this topic arose primarily from recommendations for further work made by the DiD-WG, whilst also noting the particular importance of the topic for SMRs because of the extent to which SMR designers incorporate passive and inherent safety features in their designs. Ref. [3] provides an up to date summary of proposed SMR designs.

2.1.1 The difference between Passive and Inherent Safety Features

A recent WENRA report [17] on regulatory aspects of passive systems notes that international standards do not establish a clear definition of *passive safety* and the term is not defined in the IAEA safety glossary [8], although the glossary does define a *passive component*.

As the term *passive safety* is sometimes used interchangeably with *inherent safety*, the group members considered that it would be useful to agree on more precise definitions to avoid possible confusion. For the purposes of group discussions, the definitions provided in IAEA TECDOC-626 [5] were adopted:

> *"a passive safety system is defined as either a system which is composed entirely of passive components and structures or a system which uses active components in a very limited way to initiate subsequent passive operation whereas an inherent safety characteristic is defined as a safety (characteristic) achieved by the elimination of a specified hazard by means of choice of material and design concept."*

TECDOC-626 makes a clear distinction between "inherent safety" and "passive safety". In this regard, the document discourages the unqualified use of term "inherent safety" recognizing that elimination of all inherent hazards (such as radioactive fission products and their associated decay heat or excess reactivity and its associated potential for power excursions) is required to make a nuclear power plant "inherently safe" and that for practical power reactor sizes this appears to be impossible. However, a reactor design in which one of the inherent hazards is eliminated is inherently safe with respect to the eliminated hazard. In this context, TECDOC-626 [5] alternatively defines an *inherent safety (characteristic)* as *a fundamental property of a design concept that results from the basic choices in the materials used or in other aspects of the design, which assures that a particular potential hazard cannot become a safety concern in any way*. The key distinction between the *passive* and *inherent* descriptors is that engineered

safety systems, structures and components (SSCs), either active or passive, remain in principle subject to failure (albeit with low probability), whereas *inherent safety characteristics* cannot fail so that the associated hazards are therefore eliminated.

In the context of this paper, the term *system* (or SSC) is intended to be read as encompassing all items contributing to the delivery a specified function, following the definition given in the IAEA glossary [8]). A passive safety system is then composed of items which deliver a safety function by passive means. Consistent with SSR-2/1 Rev 1 [4]: Requirement 22, classification of safety systems is expected based on the assessed importance to safety of the function delivered. Engineering requirements (e.g. failure frequency, manufacturing standard) should then follow from the assigned classification. The need to demonstrate that engineering requirements are met applies to all safety systems, regardless of whether they are passive or active, in order to provide confidence that the associated safety functions are delivered with a reliability commensurate with their importance to safety.

Inherent characteristics may also contribute to the delivery of a safety functions but the reliability which this contribution is delivered should not, at least in principle, be in dispute. However, significant regulatory challenges may still arise where claims are made with respect to an inherent safety characteristic that is either complex or novel. Boron free operation serves as an example of an inherent safety feature which contributes to the delivery of the reactivity control safety function with respect to the elimination of the hazard associated with boron dilution. It is worth noting that passive safety systems will often depend on inherent characteristics which are assumed not to fail. This should not be taken to imply that the safety systems themselves cannot fail. For example, a natural circulation heat exchanger will depend on buoyancy forces to drive a flow. Buoyancy forces cannot fail to act in the presence of a temperature difference, however it is still possible for the heat exchanger system to fail to deliver the heat removal safety function for a wide range of reasons including flow instability, gas locking phenomena and structural failures.

TECDOC-626 [5] proposes a categorisation scheme (A-D) to describe the range of "passiveness" of systems which takes into account whether a system has signal inputs of "intelligence", external power sources or forces, moving mechanical parts or moving working fluids:

Cat	moving mechanical parts	moving working fluid	self- contained external DC power sources or signal inputs for automatic initiation only	Examples
A	no	no	no	fuel clad
B	no	yes	no	Natural circulation inside an integral RPV
C	yes	yes or no	no	ECCS accumulator with check valve
D	yes	yes	yes	ECCS accumulator with fail safe trip logic

Particularly with respect to SMR designs, which may incorporate many differing types of passive systems of varying degrees of importance to safety, it could be beneficial to develop regulatory guidance within a framework that recognises that a spectrum of passivity is possible in order to ensure that all aspects of each passive system are addressed. This could include the development of requirements in a more granular way, based on the above categorisation and separately addressing expectations for substantiation with respect to inherent system characteristics, passive system features and also any active elements that may be involved in system actuation.

***Recommendation* #1:** In view of the wide variety of passive systems that may be deployed in a single SMR, the benefits of providing guidance within a framework that recognises that a spectrum of passivity is possible should be explored. This could include the development of requirements in a more granular way, based on the categorisation proposed in TECDOC-626 [5] and separately addressing expectations for substantiation with respect to inherent system characteristics, passive system features and any active elements that may be involved in system actuation.

2.1.2 The Increased use of Passive and Inherent Systems in SMR Concepts

Many SMR designers are seeking to incorporate a greater range of inherent and passive safety features, characteristics and SSCs, that work in an integrated fashion to support safety functions and improve overall plant safety. Although, the use of passive and inherent safety features are not exclusive to SMRs, SMRs can be distinguished by the greater extent to which such systems are deployed. Technology developers are proposing concepts that include features and operating characteristics such as:

- accident tolerant fuel designs that resist degradation and failure during events,
- core arrangements that promote inherent physics behaviours in a safe direction under operating and accident conditions,
- core power densities that provide greater margins-to-fuel-failure,
- increased core surface to volume ratios which can further protect the fuel from temperature transients by enabling more efficient emergency heat removal from the reactor vessel.

In all of the above instances, provisions are being used to support fundamental functions of control, cool and contain while making transient characteristics predictable in a safe direction while affording significant grace time to respond to events.

SMR safety features at level 1 DiD are claimed to eliminate or reduce vulnerabilities to a large spectrum of well-known postulating initiating events (PIEs). Inherent characteristics, such as predictable 'safe direction' physics behaviours in temperature transients are being leveraged to contribute to the ease of operational control and increase operator grace times to respond to plants events. The design intent is to enhance safety at levels 1 and 2 of DiD. For any remaining

PIEs, passive features are being proposed at DiD levels 3 and 4 based on claimed advantages such as:

- Simplicity of the systems used to achieve the functions,
- "always-on" demonstrated high reliability,
- greater independence from external actuation and related energy supplies,
- reduced vulnerability to operator error and
- reduced maintenance requirements.

SMR designers have sought to balance enhancements to safety at levels 1-4 DiD associated with use of passive and inherent features with an expectation for less onerous arrangements at level 5 DiD. Such expectations include the possibility of more flexible siting, reduced emergency planning zones and potentially eliminating the need for detailed emergency planning.

2.1.3 Scope of the Working Group Discussions

During the first phase of the SMR's Regulator's Forum, the DiD WG considered a wide range of issues concerning the application of DiD to SMR technologies, and as part of their output they identified a range of opportunities for further work. This included a general recommendation to undertake further work on passive safety and also the identification of a number of specific opportunities for further development of guidance on the following topics:

- The demonstration of reinforcement of DiD levels 1 and 2 for SMRs,
- The development of safety criteria and requirements for passive safety systems and inherent safety features,
- The application of single failure criteria for safety functions involving passive systems,
- The development of criteria for the exclusion of identified initiating events from an SMR design,
- Investigation or enhancement of methods to deal with passive features and with multi-module issues in PSAs, and
- Requirements and guidance for qualifying new materials and features applicable to SMRs designs, including the extent and scale of the testing, verification and validation of models, and fabrication processes.

These recommendations formed the basis for the discussions of the DSA-WG. In our discussions we have sought to develop common positions informed by consideration of the national guidance of our member states and of the existing international guidance and research outputs from the IAEA and other bodies such as WENRA. The work undertaken in the Forum's pilot project was subject to constraints associated with both the limited availability of SMR related design information and limited interactions that were possible with SMR designers at the time. Whilst the current Forum activities are still subject to constraints, these are now less now restrictive than was the case for the pilot project as many designs have achieved a more advanced stage of development and a number of vendors are actively pursuing

design certification/pre-licensing reviews with Forum members. Therefore, to address limitations of previous work, we took a decision to perform a limited survey of SMR vendors in order that our discussions could be directly informed by vendor perspectives. We compiled a survey questionnaire covering a number of SMR related topics and solicited vendor responses via the CORDEL[7] organisation. We agreed that vendor responses would not be directly disclosed to maintain commercial confidentiality. The vendor questionnaire is given in Appendix C and addresses a range of topics including passive safety. Responses were obtained from eight (8) SMR vendors which were mainly, but not exclusively, for developing PWR designs. The responses are not disclosed but are summarised and at a high-level to support the discussion of issues in the proceeding sections of this paper. The WG also considered regulatory guidance from each of its member states relevant to the vendor survey questions. The regulatory positions are given in Appendix D and are also referenced and discussed within the main text of this paper.

2.2 Common Positions for Consideration in Design and Deployment of SMR Facilities

This section summarises the outputs of WG discussions concerning inherent and passive safety features of SMR designs. WG outputs are presented under the following topic headings which address varying aspects of uncertainty and reliability assessments and align with our survey questions:

2.1 Identifying and Addressing Uncertainties in Performance Claims for FOAK Facilities
2.2 Assessment of Reliability in the Presence of Weak Driving Forces
2.3 Optimization of the Use of Passive and Active Features in the Design Process
2.4 The Applicability of the Single Failure Criterion to Passive Features
2.5 Requirements for Redundancy, Diversity and Treatment of Common Cause failure

Each sub-section is structured as statements of WG common positions followed by a summary of the key points of the WG discussions supporting the common position including insights obtained from our surveys and recommendations.

2.2.1 Identifying and Addressing Uncertainties in Performance claims for First of a Kind Facilities

Common Position #2.1*:* A facility safety case, in particular for a First of a Kind (FOAK) facility, is expected to systematically identify, account for and address uncertainties in

[7] The World Nuclear Association's Cooperation in Reactor Design Evaluation and Licensing (CORDEL) working group was established in 2007 as the counterpart to the Multilateral Design Evaluation Programme of the OECD Nuclear Energy Agency (NEA). CORDEL focuses on promoting the international standardization of nuclear reactor

performance claims for passive and inherent features through a strategy that considers aspects such as:

- results from substantiation activities (e.g. use of sufficiently validated computer models, experimental prototypical systems, integrated test facilities)
- compensatory design enhancements (if required),
- control measures expected to be implemented by the operator; and,
- any additional activities necessary to demonstrate and/or support functional performance claims and gather experience data.

Common Position #2.2*:* The greater the combination of interfacing inherent and passive design features the more complex the performance uncertainties become. In such cases, design substantiation should pay particular attention to the need for integrated testing activities both during the design process and in the commissioning program for the First of a Kind facility.

Discussion

Requirement 9 of the IAEA Safety Standard SSR-2/1 [4] articulates a general expectation for design to be in accordance with relevant codes and standards and a preference for the use of items that have been previously proven in application. Where this is not the case, the standard articulates an expectation for appropriate research, testing and monitoring to support safety (paragraph 4.16):

> *" Where an unproven design or feature is introduced or where there is a departure from an established engineering practice, safety shall be demonstrated by means of appropriate supporting research programmes, performance tests with specific acceptance criteria or the examination of operating experience from other relevant applications. The new design or feature or new practice shall also be adequately tested to the extent practicable before being brought into service and shall be monitored in service to verify that the behaviour of the plant is as expected."*

Particularly for unproven design features in SMRs, the characterisation of sources of uncertainty will be a key element in designing programmes to support an overall demonstration of safety. Requirement 42 of SSR-2/1 [4] (paragraph 5.73) articulates a general expectation with regards to the consideration of uncertainties:

> *"The safety analysis shall provide assurance that uncertainties have been given adequate consideration in the design of the plant and in particular that adequate margins are available to avoid cliff edge effects and early radioactive releases or large radioactive releases"*

Despite their purported advantages, passive safety features may be subject to complex conditions and modes of instability and weak driving forces such that the safety performance can be sensitive to uncertainties in plant operating and environmental conditions. In general, methods to account for such uncertainties are not well established. This makes the assessment

of performance claims for passive features a significant regulatory challenge, particularly where novel SMR plant arrangements are proposed. It is to be expected that the greater the combination of interfacing inherent and passive features within a design, the more complex the performance uncertainties may become.

The definition we have adopted for an inherent safety features precludes failure with respect an associated hazard so that, in principle, it can be assumed that no measures will be needed to mitigate that hazard. In many circumstances, the exclusion of hazards arises from design choices and is not controversial. For example, the use of submerged CRDMs to eliminate rod ejection faults. However, regulatory judgements can be more difficult, and regulators may need to consider the consequences of failure, in circumstances where designers advance complex claims reliant on an inherent safety characteristic. This is a particularly significant issue for FOAK plant because of the uncertainties associated with a lack OPEX and because of the potential to circumvent defence in depth principles if claims are not valid.

In both the above cases, design substantiation should pay particular attention to the need for integrated testing activities both during the design process and in the commissioning program for the FOAK. Unless the technology developer can address uncertainties with specific substantiation activities and/or compensatory design enhancements, confidence in the predicted performance of structures, systems and components supporting the safety functions is reduced until sufficient operating experience exists.

Survey Insights

Our vendor survey included two questions (Appendix C: Questions 1.1-2) on approaches to mitigating uncertainty for FOAK plant with novel features: the first question sought information on vendor research and validation programmes for novel features and the second question queried intentions to include additional safety measures to mitigate uncertainty for FOAK plant. The majority of survey respondents were proposing PWR based designs and considered their proposals to be of essentially *proven* performance based on adherence to standards applied to large NPPs. As such, they did not consider that additional systems to mitigate uncertainty for FOAK facilities would be needed. This was generally true even where a variety of passive safety systems and inherent features were incorporated into designs in combinations that appeared to be quite novel. However, a few respondents proposing non-PWR based designs did indicate that they were considering additional measures for FOAK plant to mitigate uncertainty. These included increased safety margins, additional commissioning tests and leak-tight containments for plants operating at low pressure (with an intent to consider relaxing these measures for subsequent plant once confidence was increased). All respondents recognised the potential need for suitable research programmes and separate effects and integral testing to support the design development, code validation and the safety demonstration for novel features. Indeed, some respondents were able to cite programs that had been conducted over decades in support of their designs.

In our survey of regulatory guidance (Appendix D), no regulators reported any explicit references to FOAK plant in their current guidance. All regulators report references to situations for which an *unproven design or feature* is introduced or where there is a *departure from an established engineering practice*. The associated guidance for these situations is generally aligned with SSR-2/1 [4] Requirements 9 and 42 without constraining the manner in which the objectives are met. This regulatory position would seem to reflect a view in which the safety objectives for FOAK plant are not regarded as different from subsequent plants whilst recognising that greater effort that may be required to demonstrate that safety objectives are met in the absence of prior OPEX.

2.2.2 Assessment of Reliability for Passive Systems in the Presence of Weak Driving Forces

Common Position #2.3*:* Designers should establish clear criteria for characterising the strength of driving forces in features that support safety functions with a particular emphasis on understanding conditions that may weaken those forces to the point where their effectiveness or predictability is significantly impacted. This information should be used to identify and understand failure modes that could, in principle, impact the delivery of a safety function with sufficient reliability. Designers should ensure that all parameters potentially affecting the delivery of a safety function are taken into account within the safety demonstration.

Discussion

Requirement 23 of SSR-2/1 [4] articulates a general requirement on the reliability of items important to safety which should be *operated and maintained to be capable of withstanding, with sufficient reliability and effectiveness, all conditions specified in the design basis for the items*. This requirement is equally applicable to passive and active systems. Some regulatory regimes set quantitative targets for failure frequencies, however experience indicates that issues can arise in assessing reliabilities for passive systems if the driving forces are weak [6, 18]. This will occur most often in the context of buoyancy driven natural circulation (categories B, C, D) where the pattern of flow may be sensitive to deviations in environmental conditions, internal conditions or plant geometry which may not be well characterised for a particular transient. This leads to a potential for uncertain failure modes that could, in principle, impact the delivery of a safety function. Examples would be a small leak of cold fluid or dissolution of condensable gas disrupting a weakly buoyant circulation. Methods have been proposed to assess reliability in these circumstances however there is no general consensus on how this should be done [21]. The key point is to ensure that all parameters potentially affecting the delivery of a safety function are taken into account within the safety demonstration.

Survey Insights

Questions 3.3 (Appendix C) of our vendor survey queried approaches to dealing with uncertainty for passive safety systems in the presence of weak driving forces occur. In general, responses did indicate an awareness of the need to qualify passive systems over a full range of operating conditions and the potential for uncertainty associated with weak driving heads. Vendors cited a range of techniques for assessing the reliability of passive safety systems in their designs including the use of validated thermal hydraulic codes, PRA analysis and experimental testing. However, it was not clear whether systematic methods had been used by all vendors to ensure that *all* relevant parameters that might impact performance had been identified.

A common feature of regulatory guidance from the member states surveyed (see Appendix D) with respect to the assessment of reliability for safety systems/features is that it does not, for the most part, differentiate between active and passive principles of operation. Regulators typically sets quantitative expectations for reliability based on the importance to safety of the functions systems are designed to deliver. For example, in Canada safety systems (having the greatest importance to safety) and their support systems shall be designed to ensure that the probability of a safety system failure on demand from all causes is lower than 10^{-3}/yr. In the UK, the design principles place additional specific requirements for redundant or diverse methods to maintain control of fundamental safety functions, although it is recognized that passive systems may be exempted if an adequate demonstration of safety based on the inherent features of such systems can be provided. In Finland, the reliability analysis/PRA failures and events potentially affecting the boundary conditions for system operation shall be considered and described in the analysis (e.g. natural circulation may be impaired by non-condensable gases, blockage, wrong valve positions, impurities, corrosion, algae in tanks, maintenance errors). Although currently aligned with the approach described above, Korea is in the process of developing specific regulatory guidance for the design and performance of passive safety systems (including passive systems for SMRs) within the context of their more prescriptive regulatory regime. The scope of such guidance will address relevant design aspects that can affect the overall assessment of reliability such as definition of passive SSCs, application of single failure criterion, defence in depth, leakage monitoring and isolation, testability and inspectability, along with guidelines for performance of passive systems.

The development of methods to assess the reliability of passive safety systems is subject to ongoing international research, with the IAEA hosting a number of coordinated research projects on this subject (e.g. TECDOC-1752 [6]). We note that current regulatory guidance from member states set quantitative expectations for the reliability for passive safety systems despite there being no general methodology for conducting such an assessment. Thus, the WG considers that continued research in this area is of particular importance for SMRs which may have exclusively passive safety systems.

Recommendation #2: Current regulatory guidance from member states set quantitative expectations for the reliability for passive safety systems despite there being no accepted

general methodology for conducting such an assessment. Continued research in this area is of particular importance for SMRs which may incorporate exclusively passive safety features. The work of the IAEA in this area is acknowledged (e.g. TECDOC-1752 [6]), and we recommended continued work on the development of assessment methodologies to support the deployment of SMRs.

2.2.3 Optimization of the Use of Passive and Active Features in the Design Process

Common Position #2.4*:* Subject to a prioritisation which favours first inherent characteristics and then passive features or continuously operating systems over systems that need to be brought into service (SSR-2/1 [4]: Requirement 16), any combination of active and passive safety systems can be acceptable provided defence in depth and safety design principles are met. The designer should document the approach for establishing optimization in the use of passive and active features in consideration of the availability of supporting information to substantiate safety claims and to support the conduct of safety classification.

Discussion

Requirement 16 of SSR-2/1 [4] Paragraph 5.8) expresses a priority for the expected behaviour of a plant in any postulated initiating event. This priority favours first inherent characteristics and then passive features or continuously operating systems over systems that need to be brought into service in response to the initiating event. For systems that need to be brought into service as a response to a postulated initiating event international guidance does not strongly favour either passive or active approaches, although account should generally be taken of the advantages that passive safety systems have in reducing vulnerabilities to external failures. At the same time, some recognition must be given to the potential complexity of validating a novel passive system where weak driving heads are involved since, as is explained above, there may be a degree of uncertainty in the assessment.

Having maximised possible use of the inherent and passive safety features provided by the design, remaining accident sequences should be dealt with using dedicated active or passive safety systems. A case can be made for selection of an optimum combination of active and passive safety systems depending on the extent of prior validation and testing for the design and the extent of the existing OPEX. SMR designs have been proposed using either exclusively passive or a combination of active and passive safety systems. For the latter circumstance active systems are sometimes specified as "non-safety grade" or classified as a lower safety category. The approach may have some merit in introducing an element of diversity in the line of protection which could off-set potential uncertainties associated with safety measure based on a weak naturally driven flow.

Survey Insights

Many survey respondents proposed designs that relied exclusively on passive safety systems and inherent safety features (Appendix C: Question 3.2). The primary design objective was to reduce reliance on support functions and particularly the need for operator intervention. A few respondents did propose the use of combinations of passive and active systems citing diversity as a key consideration.

The regulatory guidance reviewed for forum member states on the use of active vs passive systems is broadly consistent with SSR-2/1 [4] Requirement 16 (see Appendix D). Concerning the use of combinations of active and passive safety systems/features it appears that all regulatory jurisdictions Appendix D) allow implicitly or explicitly such combinations, as long it can be demonstrated that no adverse effects and interferences detrimental to safety occur. Some jurisdictions (e.g. UK, Canada) either explicitly or implicitly express a preference for inherent and/or passive safety measures followed by the automatic action of engineered control and safety systems.

2.2.4 Applicability of the Single Failure Criterion to Provisions that Include Passive Features and Inherent Characteristics

Common Position #2.5*:* Designers should apply the single failure criteria in safety evaluations of passive safety systems deployed within SMRs. Dis-applications of the single failure criteria may be considered for passive systems if it is not reasonably practicable to achieve compliance, for instance via the incorporation of redundancy into a design, however this should be accompanied by a demonstration that adequate reliability can otherwise be achieved. Particularly in circumstances where driving forces are weak, analyses should account for all potential system failure modes and consider how these may evolve in time in order that the worst-case single failure mode is captured.

Discussion

The single failure criterion (SFC) is applied to safety systems as a means of ensuring high reliability. In simple terms, it requires that a safety system should be capable of delivering its safety function if any single component within the system fails. An analysis of compliance with the single failure criterion should demonstrate a system's ability to deliver its safety function in the presence of the worst-case single failure (and usually consequential failures arising from this). This will often necessitate the incorporation of redundancy and physical separation into a system's design.

Where the response of a passive system depends on a wide range of factors, some care needs to be exercised is evaluating the worst-case single failure ensuring that all possible failure modes are accounted for. Even where redundancy is included in a design, it may still be possible for both systems to be defeated by the same single failure. For instance, it may be possible for a single failure to introduce gas into a system that gas locks both redundant trains of a heat exchanger.

Requirement 25 of SSR-2/1 (Rev 1) [4] articulates general requirements on the application of the single failure criterion for NPPs: t*he single failure criterion shall be applied to each safety group incorporated in the plant design*. For passive systems, the requirement is qualified under section 5.40 as *the design shall take due account of the failure of a passive component, unless it has been justified in the single failure analysis with a high level of confidence that a failure of that component is very unlikely and that its function would remain unaffected by the postulated initiating event*.

Passive safety systems are generally adopted for SMRs because of their perceived high reliability and, particularly where this is assured by inherent system characteristics, it seems reasonable to allow for possible dis-applications of the single failure criterion. However, at noted above, the performance characteristics of passive systems can be subject to high levels of uncertainty where driving forces are weak. Any proposed dis-applications of the single failure criterion will need to fully account for such uncertainties. In some instances, the single failure criterion may only be applied to actuating components required to initiate passive safety systems (Categories C and D) and care should be exercised in distinguishing parts of a system for which high reliabilities are being claimed and ensuring that an appropriate demonstration of performance is provided for them.

Discussions within the WG have also highlighted potential problems with the application of the single failure criterion in so far as identifying the worst-case single failures is concerned. Where a passive flow is evolving, the parameters most affecting the flow could change radically such that single failures relevant to each stage of a transient might not be easily determined. In such situations iterative evaluation of transient scenarios may be necessary to identify worst case failures, however it does not appear that this issue has received significant attention.

Recommendation #3: Where a passive flow is evolving, the parameters most affecting the flow could change radically such that single failures relevant to each stage of a transient might not be easily determined. In such situations iterative evaluation of transient scenarios may be necessary to identify worst case failures. Further work in this area may be of benefit since it does not appear that this issue has received significant attention.

Survey Insights

In our review of regulatory guidance (Appendix D), all regimes require that designers consider single failures in systems delivering safety functions (including the impact of consequential failures resulting from the assumed single failure). Some regimes provide additional guidance depending on the nature of the systems involved. For example, in Finland, for engineered safety systems the application of the SFC requires the assumption of a single failure and maintenance/repair (that is, an N+2 criterion). However, for systems with passive components that have very low probability of failure an N+1 criterion may be applied (only the maintenance /repair is assumed). In France, a distinction may be made between active and passive single failures (see Appendix D) whereby, in certain circumstances, short term failures (< 24hrs) need

only be considered for active components. In Canada, single failures should also include unintended actions and failure of passive components. However, passive components may be exempt from SFC provided that adequate justification is provided either by analysis, testing or a combination of analysis and testing. It is particularly interesting that, although China currently requires adherence to the SFC, future adoption of a risk-informed methodology is being considered.

Questions 3.3 (Appendix C) of our vendor survey queried approaches to application of the single failure criterion. Most survey respondents reported an intention to apply the single failure criterion to safety systems in their design whereby the designs incorporated multiple redundant trains to comply with single failure and maintenance criteria.

2.2.5 Requirements for Diversity and the Treatment of Common Cause Failure

Common Position #2.6*:* Designs should incorporate redundancy, diversity and, where practicable, physical separation for safety systems to mitigate common cause failures. Particular attention should be paid to functional diversity where exclusively passive safety systems are deployed in SMR designs. There may be some benefit in using combinations of passive and active systems to ensure a safety function is delivered as this may provide additional diversification to improve resilience to common cause failures.

Discussion

Safety systems will, in general, rely upon redundancy, functional independence, robust design and physical separation to ensure high reliability. Diversity is usually a measure applied to reduce the likelihood of common cause failures (CCFs) between independent safety systems which may be at either the same or different levels of defence in depth. Requirement 24 of SSR-2/1 (Rev 1) [4] articulates general requirements with respects to common cause failure:

> *The design of equipment shall take due account of the potential for common cause failures of items important to safety, to determine how the concepts of diversity, redundancy, physical separation and functional independence have to be applied to achieve the necessary reliability.*

Functional diversity may be required in the generation of signals of the reactor protection system. A plant deviation can escalate into a DEC due to multiple failures of safety systems. CCFs are probably the most important group for these types of failures. Diversification of safety features for DECs is a powerful tool to prevent the accident escalation to unacceptable consequences. Because of the potential uncertainties in reliability and challenges of the safety demonstration of passive systems, there may be some benefit in using combinations of passive and active systems to ensure a safety function as this can provide additional diversification to improve resilience to common cause failures..

Survey Insights

From our review of guidance (Appendix D), we note that regulatory requirements for CCF do not appear to differentiate between active and passive principles of operation. The expectation is that CCF should be addressed via the use of redundant and/or diverse components, actions or measurements, to minimize the likelihood of failures induced by common causes. In Finland, it is expected that CCF is accounted for by adequate diversity in the safety system design. In Canada, the existing CCF requirements are applicable to all items important to safety, regardless of their principle of operation (active and/or passive) whilst in the UK there is an expectation that CCF claims should be substantiated. Further UK guidance is provided for the extent of quantitative claims: Safety Assessment Principles For Nuclear Facilities [28], SAP Paragraph 185, states that w*here required reliabilities cannot be achieved due to CCF considerations, the safety function should be achieved taking account of the concepts of diversity and segregation, and by providing at least two independent safety measures.*

Questions 3.3 (Appendix C) of our vendor survey also queried approaches to dealing with common cause failure. Respondents generally reported an intention to use diverse safety systems in their design to mitigate CCF and to apply PRA to assess the vulnerability of designs to CCF phenomena. The approaches were generally consistent with expectations for large NPPs.

Chapter 3: Aspects of Beyond Design Basis Analysis relevant to SMRs

3.1 Introduction

The provision of safety features at Level 4 DiD (design extension conditions, severe accidents, practical elimination) was one of a number of topics considered in the first phase of the Forum that the DSA-WG has taken forward for further in-depth discussion.

3.1.1 Challenges Associated with the Application of Defence in Depth Principles at Level 4 to Take into Account Novel Safety Approaches

DiD is the primary means of preventing accidents in a nuclear power plant and mitigating the consequences of accidents if they do occur (IAEA Fundamental Safety Principles [19]). The principles are applied to all organizational, behavioural and design-related safety and security activities to ensure that they are subject to layers of provisions, so that if a failure should occur it will be compensated for without causing harm to individuals or the public. This concept is applied throughout the design and operation of a reactor facility to provide a series of levels of defence aimed at preventing accidents and to ensure appropriate protection in the event that prevention fails. The IAEA Specific Safety Requirements (SSR-2/1 Rev. 1 [4], Section 2) defines five levels of DiD (levels 1-5), that are described in Table 1 below:

Table 1: Levels of Defence in Depth

Level	Objective	Means for achieving the objective
1	Prevention of abnormal operation and failures	Conservative design and high quality in construction and operation
2	Control of abnormal operation and detection of failures	Control, limiting and protection systems and other surveillance features
3	Control of accidents within the design basis	Engineered safety features and accident procedures
4	Control of severe plant conditions including prevention of accident progression and mitigation of the consequences of severe accidents	Complementary measures and accident management
5	Mitigation of radiological consequences of significant releases of radioactive materials	Onsite emergency response measures (site specific) and Offsite emergency response

An essential feature of the DiD approach is that measures should be included at each level and that measures at any particular level should, in so far as is reasonably practicable, remain independent of those at all other levels (c.f. SSR-2/1 Rev 1 [4] Requirement 7). Regulatory

expectations with respect to DiD for large scale NPPs with standard fuel assemblies are well established and at Level 4 DiD will commonly include (c.f. SSR-2/1 Rev 1 Requirement 20):

- additional engineering measures to prevent accident progression for beyond design basis scenarios in which the fuel cladding maintains containment even though safety criteria are exceeded (so called Design Extension Condition (DEC A), and
- engineering measures to mitigate the consequences of severe accidents in which the fuel cladding fails and material is released (DEC B).

For large scale NPPs engineering measures can include additional systems for removing decay heat for DEC A scenarios if multiple failures are assumed and safety features such as hydrogen recombiners and core catchers for DEC B scenarios in which there is a release of fission products into the reactor containment. Broadly the same considerations are expected to apply to water cooled SMRs with standard fuel assemblies. However, many SMR designs are now being proposed (see [8]) which include reactors operating at low pressure (e.g. molten salt reactors, sodium cooled reactors) and reactors using specifically designed accident tolerant fuels (e.g. molten salt reactors, high temperature gas reactors). Some of the novel features being introduced by these non-water-cooled concepts are introducing different approaches to the application of DiD that require careful interpretation of these principles to ensure they are still being met in an effective manner. For example, many design concepts implement inherent characteristics and safety features at levels 1-3 DiD that are claimed to limit the potential for escalation of serious accident sequences to level 4. What this means is that designers are seeking to balance enhancements in safety features at levels 1-3 DiD with less onerous engineering measures at level 4 DiD. A case in point is the use of encapsulated TRISO fuel in HTGRs. Designers are introducing claims and supporting R&D evidence that gross fuel failures are simply not possible and therefore, even for the worst case BDBA, a leak-tight reactor containment structures is not necessary for safety. In this case, the emphasis on design of such civil structures is claimed to be less influenced by internal events and more so by impacts of external events that could impair systems important to safety.

Safety requirements for HTGRs have recently been considered by the IAEA in a review of the applicability of SSR-2/1 Rev 1 [4] to these designs. The review involved both designers and regulators and the outcomes are particularly notable because of the inability of the two stakeholder groups to achieve consensus in certain areas. The regulatory judgement of the extent to which such "balancing" is justified presents a significant challenge for SMRs and was a key driver in the groups decision to address the subject of beyond design basis analysis.

3.1.2 Scope of the Working Group Discussions

During the first phase of the SMR's Regulator's Forum, the DiD WG considered a wide range of issues concerning the application of DiD to SMR technologies, and as part of their outputs developed common regulatory positions on a range of significant issues. They also identified

a number of specific recommendations for future development of guidance for SMRs in the following areas:

- The demonstration of reinforcement of DiD levels 1 and 2 for SMRs,
- safety criteria and requirements for passive safety systems and inherent safety features,
- The application of single failure criteria for safety functions involving passive systems,
- The development of criteria for the exclusion of identified initiating events from an SMR design[8],
- Investigation or enhancement of methods to deal with passive features and with multi-module issues in PSAs, and
- Requirements and guidance for qualifying new materials and features applicable to SMRs designs, including the extent and scale of the testing, verification and validation of models, and fabrication processes.

In our discussions we have sought to further consider the common positions proposed by the DiD WG informed by consideration of the national guidance of our member states and of the existing international guidance and research outputs from the IAEA. The work undertaken in the Forum's pilot project was subject to constraints associated with both the limited availability of SMR related design information and limited interactions that were possible with SMR designers at the time. Whilst the current Forum activities are still subject to constraints, these are now less now restrictive than was the case for the pilot project. Many designs have achieved a more advanced stage of development and a number of vendors are actively pursuing more detailed pre-licensing[9] reviews with Forum members. Therefore, to address limitations of previous work, we took a decision to perform a limited survey of SMR vendors in order that our discussions could be directly informed by vendor perspectives. We compiled a survey questionnaire covering a number of SMR related topics and solicited vendor responses via the CORDEL organisation. We agreed that vendor responses would not be directly disclosed to maintain commercial confidentiality. The vendor questionnaire is given in Appendix C and addresses a range of topics including beyond design basis analysis (Section 5). Responses were obtained from 8 SMR vendors which were mainly, but not exclusively, for developing PWR designs. The responses are not disclosed but are summarised and at a high-level to support of the discussion of issues in the proceeding sections of this paper. The DSA-WG also considered regulatory guidance from each of its member states relevant to the vendor survey questions. The regulatory positions are given in Appendix E and are also referenced and discussed within the main text of this paper.

3.2 Common Positions for Consideration in Design and Deployment of SMR Facilities

[8] Or in other words, considerations important to developing a credible list of postulated initiating events from first principles for a novel design.
[9] Includes design certification processes where adopted by some member states.

This section summarises the outputs of DSA-WG discussions concerning beyond design basis analysis for SMR designs. WG outputs are presented under the following four topic headings which address varying aspects of beyond design basis analysis:

3.2.1 Challenges with Characterising Severe Accidents for Novel SMR Concepts
3.2.2 The Role of DiD in Preventing and Mitigating Severe Accidents
3.2.3 Design Extension Conditions
3.2.4 Practical Elimination of Event Sequences and Accident Scenarios that Could Lead to a Large or Early Release

Each sub-section is structured as statement of WG common positions followed by a summary of the key points of the WG discussions supporting the common position including insights obtained from our surveys and where applicable recommendations.

3.2.1 Challenges with Characterising Severe Accidents for Novel SMR Concepts

Common position #3.1*:* For novel SMRs, there is a need to identify criteria against which accidents are judged to be severe taking account of the potential for barrier failure and fuel relocation. Both designers and regulators will have a role in defining such criteria. This is particularly important for designs in which the concept of "core melt" does not apply. The potential for severe consequences to arise from actions required to clean-up an accident or in co-located facilities[10] should also be considered.

The term *severe accident* for nuclear power plants is mainly interpreted with reference to water cooled technologies. The IAEA safety glossary [8] provides basis information to support existing definitions. The glossary defines an *accident* as:

> *any unintended event, including operating errors, equipment failures and other mishaps, the consequences or potential consequences of which are not negligible from the point of view of protection and safety,*

and a *severe accident* as:

> *an accident more severe than a design basis accident and involving significant core degradation*

This definition implies that the term *significant core degradation* should be interpreted (on a case by case basis) as a degradation of whatever primary barriers are provided to the release of radioactive material, within the context of the designer's particular application of DiD. For water cooled reactors, decades of research and lessons learned from events have led to the global industry and regulators coming to a consensus on specific plant and fuel conditions that

[10] For example, some molten salt designs incorporate co-located fuel processing facilities which should be assessed for their severe accident potential

signify the onset and progression of a severe accident. However, SMRs are introducing design features that either:

- increase the plant's resilience to severe accidents (claimed reduction of event probability by one or more orders of magnitude; or,
- claim that traditional fuel system failures have been precluded.

It should be noted, however, that some novel design approaches may shift the flow of energy or fission products inventory to other plant systems that may fail and cause radioactive releases to the environment.

For example, molten salt SMRs are based on design concepts that are very different from those encountered in water cooled NPPs. For some designs, the fuel is dissolved in a liquified molten salt coolant and is supplied continuously to the reactor as burn-up proceeds [3]. The nature of the salt (i.e. extremely high boiling point, chemistry stability, and high retention of fission products) mean that concerns associated with fuel clad failure, or core melt will not apply. However, the structural integrity of the reactor vessel tank itself is still necessary to ensure confinement of radionuclides and therefore needs to be protected from failures. This means, DiD principles are still expected to apply to the design and designers should identify the multiple independent barriers provided to fission product release (or reveal deficiencies with respect to the provision barriers). Recent studies undertaken within the European Framework programme have demonstrated how this might be done for MSRs [20]. Once the barriers are identified, the potential for severe accidents can be analysed based on the assumptions of failure or degradation of the identified barriers.

For SMRs in general, where DiD principles are expected to be applied to a design, in accordance with regulatory expectations, the severe accidents definition given in the glossary can be interpreted as including:

- accidents involving the failure/degradation of measures proposed at levels 1-3 DiD (design basis measures) for which consequences or potential consequences may be severe, and
- accident with severe consequences or potentially severe consequences that are not considered within the plant design basis (e.g. due to the low frequency of occurrence of the initiating event or involving additional failures).

For an accident to be considered severe does not necessarily require that the consequences are actually severe but only that they potentially could be. This means that technology designers are expected to provide analyses that consider potential consequences rather than ruling them out from the outset based on safety claims of plant SSCs. Hence the proposed definition of a severe accident for a specific technology should include situations in which there is significant unintended relocation of radioactive material even though that material remains contained. The potential for severe consequences to arise from actions required to clean-up an accident should also be considered. Although the IAEA glossary references *significant core degradation*, the

expectation for DiD considerations to apply spent fuel management (e.g. handling systems and spent fuel storage systems) is now well established (Post Fukushima) so the potential for severe accidents in spent fuel pools or other co-located facilities[11] should also be included.

Regulatory Definitions for Severe Accidents

We have surveyed the definition adopted for a severe accident in the member states represented in the forum. The definitions are summarised in Appendix F from which it is evident that, for most member states, the definitions are aligned with the IAEA glossary definition. Hence, in most cases the definitions are likely to require some interpretation for novel SMR configurations.

The UK provides an alternative approach to other member states to defining a severe accident. In the UK, severe accidents are defined as those fault sequences that have unmitigated consequences that exceed a defined threshold value (currently set at 100mSv) when conservatively assessed or for which there is a substantial unintended relocation of material which places a demand on the integrity of remaining physical barriers. The UK approach has the benefit of being technology neutral and more readily adaptable to the assessment of SMRs for which LWR concepts such as core melt does not apply. However, if proposed as a possible approach to the IAEA, it will introduce the need to establish a threshold value that fits within each regulator's legal framework for safety (i.e. societal tolerance for risk).

Recommendation #1: A definition of a *severe accident* based on the unmitigated consequence associated with a fault, such as is applied in the United Kingdom, has the benefit of being technology neutral and more readily adaptable to the assessment of SMRs for which LWR concepts such as core melt does not apply. It is recommended that the IAEA considers this consequence-based definition as an acceptable alternative definition and explores the benefit of adopted such a definition for SMRs.

3.2.2 The Role of DiD in Preventing and Mitigating Severe Accidents

Common position #3.2*:* SMR designers need to identify, from the outset, how defence-in-depth principles, based on the provision of multiple independent barriers to accident progression, are applied within the safety provisions and information substantiating those provisions. The progression of faults/accidents should be analysed assuming failure or degradation of the primary barriers to fission product release in order to establish a facility's vulnerability to severe accidents. All areas of a facility having the potential for severe accidents should be assessed.

Common position #3.3*:* SMR designers need to systematically identify credible severe accident scenarios for their designs including very low frequency events. Severe accident scenarios are expected to consider the consequences of accidents that result from credible

[11] For example, some molten salt designs incorporate co-located fuel processing facilities which should be assessed for their severe accident potential

failures of the level 1-3 of defence in depth. Where claims are being made that severe accidents will be precluded by design measures, such conclusions need to document how accidents based on unmitigated consequences associated with a fault have been characterised and analysed. Any assumptions with respect to the maintenance of barrier integrity should be robustly justified.

The IAEA safety standards (SSR-2/1 (Rev 1) [4] Paragraph 2.13) identifies the purpose of the fourth level of DiD as being *to mitigate the consequences of accidents that result from failure of the third level of defence in depth* which is *achieved by preventing the progression of such accidents and mitigating the consequences of a severe accident*.

Although this expectation seems quite straightforward, the judgement of the extent to which failures at level 1-3 DiD should be considered in the assessment of accident progression can be challenging in particular consideration of:

- Novelty of specific design provisions and
- Lack of integrated plant operating experience for the design configurations being proposed

SMR designers are seeking to enhance safety at level 1-3 DiD through the incorporation of inherent characteristics and passive safety features. Where designs incorporate passive, permanently available safety features with large claimed margins to failure, complete failure of such provisions during an internal accident scenario becomes less likely. However, the safety case will still need to consider potential impacts of external and human induced events that could impair those provisions. On the other hand, an assumption that the integrity of a primary barrier is substantially maintained when identifying requirements for level 4 features appears to conflict with the identified purpose of level 4 DiD. The resolution of these conflicting positions in difficult and needs to be considered on a case-by-case basis; a very robust justification for whatever assumptions that are made should be provided. It is important that designers assess the potential impacts of their assumptions on DiD for the overall design to ensure that safety is not too dependent on the integrity of any single barrier.

As a result, the identification of severe accident scenarios should consider a full range of initiating events for which accident progression should be assessed based on justified assumptions concerning the credible degree of barrier degradation. Technology specific PIE lists (e.g. IAEA SR-54 [21]) can be cross checked for completeness of the range of events considered. Probabilistic assessment can also be used in a complementary manner as part of overall safety analysis and design activities to assess the potential for initiating events to develop into severe accidents where scenarios are complex, however it should not be used to screen low frequency events since, clearly, measures at level 4 are intended to address such events.

Survey Insights

In our vendor survey we queried approaches to the design of severe accident measures (Appendix C: Question 5.4). The majority of vendor responses were for LWR designs and they reported that they had used similar approaches to severe accident mitigation as used for large LWR NPPs. Some vendors reported that severe accident mitigation could be more easily incorporated into their smaller designs than for larger NPPs (e.g. increased margins). Only a few responses were received from non-LWR vendors noting that postulated worst cases scenarios had been considered (not related to specific accident sequences) in order to "stress tests" designs in extreme conditions.

3.2.3 Design Extension Conditions

Common position #3.4*:* Safety features at level 4 DiD are necessary to assure fundamental safety functions, particularly confinement of radionuclides and containment of releases, in all credible severe accident scenarios so far as is reasonably practicable. The inclusion of additional features for accidents scenarios involving multiple failures needs to be considered to improve resilience to common cause failure.

Safety is expected to be assured by the provision of multiple independent barriers so that accidents cannot progress due to the failure of any one barrier. With respects to Level 4 DiD, SMR designs are expected to include independent safety features to mitigate the consequences of severe accidents if they are not precluded by the design. Work conducted post-Fukushima has led to the introduction of further requirements intended improve resilience to beyond design basis events, particularly those involving multiple failures. SSR-2/1 Rev 1 [4] Requirement 20 concerning design extension conditions provides a general framework for consideration of these enhanced beyond design basis measures:

> *A set of design extension conditions shall be derived on the basis of engineering judgement, deterministic assessments and probabilistic assessments for the purpose of further improving the safety of the nuclear power plant by enhancing the plant's capabilities to withstand, without unacceptable radiological consequences, accidents that are either more severe than design basis accidents or that involve additional failures. These design extension conditions shall be used to identify the additional accident scenarios to be addressed in the design and to plan practicable provisions for the prevention of such accidents or mitigation of their consequences.*

The important characteristics of DECs (SSR-2/1 Rev 1 [4] para. 5.29) are that the associated features:

- should be independent, to the extent practicable, of those used in more frequent accidents,
- should be capable of performing in the environmental conditions pertaining to these design extension conditions, including design extension conditions in severe accidents, where appropriate,

- should have reliability commensurate with the function that they are required to fulfil.

For water cooled reactors, IAEA safety standards and WENRA have divided DECs into two groups for events not involving core melt, DEC A, and for events involving core melt, DEC B. Not all Forum member states have chosen to follow this classification approach however consideration of non-degraded and degraded states for the primary barrier(s) is useful. The key point is that any analysis should address accidents that are both *more severe than design basis accidents or that involve additional failures* as articulated in SSR-2/1 Rev 1 [4] Requirement 20.

The expectation to conduct beyond design basis analysis for sequences *that involve additional failures* arises from the response to a Fukushima in order to strengthen DiD (as discussed in [22]), and, as such, should be addressed in an appropriate manner for any SMR design concept.

The set of DECs should be derived on the basis of deterministic and probabilistic assessments, engineering judgement and operational experience. Safety features associated with the design extension conditions are expected to be called upon less frequently than those protecting design basis faults. Thus, DECs will usually be assessed on a best-estimate basis and the associated safety features assigned a lower classification than equivalent design basis safety measures.

Survey Insights

To inform group discussions, we surveyed the regulatory expectations with respect to DECs for the member states represented in the forum (see Appendix E). Most regulatory requirements are aligned with Requirement 20, although terminology may vary. For example, UK ONR does not use the term DECs but requires that "*fault states, scenarios and sequences beyond the design basis that have the potential to lead to a severe accident should be analysed*". Some jurisdictions (e.g. Finland) explicitly require the set of DECs to include common cause failures combined with the so-called class 1 postulated accidents, "complex sequences" and rare external events. UK ONR requires that that "*SAA should, through a systematic approach, analyse beyond design basis states and scenarios".* In Canada the regulator requires that the "*choice of the DECs to be analysed should be explained and justified, indicating whether it has been made on the basis of a PSA or other analysis that identifies potential vulnerabilities of the plant*". The principles for DEC derivation can be considered technologically neutral, however some challenges specific can be expected for SMRs. In particular, the current DECs derivation principles are high level and dependent on the maturity and status of deterministic and probabilistic safety analysis. Furthermore, for a number of novel designs the available OPEX may be limited or non-existent. For multi-module configurations, the accident complexity is increased by additional inter-module interactions. The general approach to DEC analysis is that it is acceptable to use a best-estimate approach, with realistic boundary and initial conditions, system configurations and operator response. UK ONR requires that if "*a*

realistic analysis cannot be performed with confidence, a conservative or bounding case approach should be adopted to avoid optimistic conclusions being drawn"

Our vendor survey (Appendix C) included six questions querying different aspects of the vendor approach to design extension conditions. LWR vendor responses, the majority, indicated that the approach essentially follows that applied for large NPPs:

- Analysis conducted on a best-estimate basis using established modelling tools
- Additional consideration of measures for events involving multiple failures (DEC A)
- Provision of established LWR features (e.g. core catchers, hydrogen recombiners, filtered venting, leak-tight containments) designed to withstand challenges associated with credible accident scenarios

Responses from non-LWR vendors queried the utility of DEC A-B categorisations to their designs. It was also noted that analysis tools would likely need further development for a full evaluation of beyond design basis events.

3.2.4 Practical Elimination of Event Sequences and Accident Scenarios that Could Lead to a Large or Early Release

Common position #3.5*:* A systematic and defensible demonstration that event sequences that could lead to a large or early release have been practically eliminated ([4] Section 2.11 and 2.13) needs to involve a complementary and iterative use of deterministic and probabilistic analyses coupled with use of experiential information[12]. For the First-of-a-Kind facility the demonstration of practical elimination will need to take account of the absence of OPEX and may be initially supplemented with additional safety and control provisions.

The concept of *practical elimination* sets a higher standard for any new reactor technology with respect to safety for those accidents that could lead to either large or early releases.

From IAEA SSR-2/1 (Rev. 1) [4], the possibility of certain conditions arising may be considered to have been 'practically eliminated' if:

- would be physically impossible for the conditions to arise, or
- these conditions could be considered with a high level of confidence to be extremely unlikely to arise

The IAEA safety standards reinforce that practical elimination should not be claimed solely based on compliance with a probabilistic cut-off value but should primarily be justified by design provisions, and in some cases also strengthened by operational provisions (e.g. maintenance, reliability evaluation and in-service inspections). The demonstration should include consideration of cliff edge effects (SSR-2/1 (Rev 1) [4] para. 4.11(b)). In fact, the working group members agreed that a systematic and defensible demonstration that event

[12] Information derived from OPEX, R&D activities, computer modelling etc.

sequences that could lead to a large or early release have been practically eliminated ([4] Section 2.11 and 2.13) needs to involve a complementary and iterative use of deterministic and probabilistic analyses coupled with use of experiential information[13]. For the First-of-a-Kind facility the demonstration of practical elimination will need to take account of the absence of OPEX and may be initially supplemented with safety and control provisions such as an extended commissioning and test program, operating limits and conditions, and instrumentation to gather performance data. As the design evolves and is optimized with experience gained, analyses should reflect ongoing lessons-learned in order to increase confidence that the event sequences have, in fact, been practically eliminated.

Survey Insights

We have surveyed the regulatory expectations with respect to practical elimination for the member states represented in the forum (see Appendix E). All jurisdictions require a demonstration of practical elimination for sequences potentially leading to either large or early releases. Most also require a demonstration that is not solely based on probabilistic arguments, although, notably, Korea (KINs) does appear to allow demonstrations based solely based on probabilistic arguments.

Vendor survey responses (Appendix E) for LWRs SMRs designs again mirror approaches for expected larger NPPs. Responses from non-LWR vendors indicated that their approaches are likely to be based on a demonstration of physical impossibility.

[13] Information derived from OPEX, R&D activities, computer modelling etc.

REFERENCES

[1] Small Modular Reactors: Nuclear Power Fad or Future?, D.T. Ingersoll, Woodhead Publishing, 2017, ISBN: 978-0—08-100252-0

[2] Handbook of Small Modular Nuclear Reactors, D. Carelli and D.T. Ingersoll, Woodhead Publishing, 2016, ISBN: 978-0-85709-853-5

[3] INTERNATIONAL ATOMIC ENERGY AGENCY, Advances in Small Modular Reactor Technology Developments, A Supplement to: IAEA Advanced Reactors Information System (ARIS), http://aris.iaea.org, IAEA, Vienna (2020)

[4] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Nuclear Power Plants: Design, SSR-2/1 Rev 1, IAEA, Vienna (2016)

[5] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety related terms for advanced nuclear plants, TECDOC 626, IAEA, Vienna (1991)

[6] INTERNATIONAL ATOMIC ENERGY AGENCY, Progress in Methodologies for the Assessment of Passive Safety System Reliability in Advanced Reactors, TECDOC 1752, IAEA, Vienna (2014)

[7] SMALL MODULAR REACTORS REGULATORS' FORUM, Pilot Project Report: Considering the Application of a Graded Approach, Defence-in-Depth and Emergency Planning Zone Size for Small Modular Reactors, SMRRF, Vienna (2018)

[8] INTERNATIONAL ATOMIC ENERGY AGENCY, IAEA Safety Glossary: 2018 Edition, STI/PUB/1830, Vienna (2018)

[9] UNITED STATES CODE OF FEDERAL REGULATIONS, Title 10 "Energy",

[10] INTERNATIONAL ATOMIC ENERGY AGENCY, Protection Against Internal Fires and Explosions in the Design of Nuclear Power Plants, NS-G-1.7, IAEA, Vienna (2004)

[11] INTERNATIONAL ATOMIC ENERGY AGENCY, Meteorological and Hydrological Hazards in Site Evaluation for Nuclear Installations, SSG-18, IAEA, Vienna (2011)

[12] INTERNATIONAL ATOMIC ENERGY AGENCY, Technical Approach to Probabilistic Safety Assessment for Multiple Reactor Units, Safety Report Series To Be Published, IAEA, Vienna (2019)

[13] 1ST INTERNATIONAL CONFERENCE ON GENERATION IV AND SMALL MODULAR REACTORS, Whole-Site Risk Considerations for Small Modular Reactors, J. Vecchiarelly, C. Lorencez and G. Archinoff, Ottawa (2018)

[14] U.S. NUCLEAR REGULATORY COMMISSION, Exploring the Need for Standard Approaches to Addressing Risk Associated with Multi-Module Operation in Plants Using Small Modular Reactors, M. A. Caruso, US NRC, Washington DC

[15] CANADIAN NUCLEAR SAFETY COMMISSION, Summary Report of the International Workshop on Multi-Unit Probabilistic Safety Assessment, CNSC, Ottawa (2014)

[16] INTERNATIONAL ATOMIC ENERGY AGENCY, Conduct of Operations at Nuclear Power Plants, NS-G-2.14, IAEA, Vienna (2008)

[17] WESTERN EUROPEAN NUCLEAR REGULATORS ASSOCIATION, Regulatory Aspects of Passive Systems, WENRA (2018)

[18] INTERNATIONAL ATOMIC ENERGY AGENCY, Passive Safety Systems and Natural Circulation in Water Cooled Nuclear Power Plants, TECDOC-1624, IAEA, Vienna (2009)

[19] INTERNATIONAL ATOMIC ENERGY AGENCY, Fundamental Safety Principles, Safety Fundamentals, SF1, Vienna (2006)

[20] Stéphane Beils, Delphine Gérardin, Anna Chiara Uggenti, Andrea Carpignano, Sandra Dulla, Elsa Merle, Daniel Heuer, Michel Allibert, Application of the lines of defence method to the molten salt fast reactor in the framework of the SAMOFAR project, EPJ Nuclear Sci. Technol. 5, 18 (2019)

[21] INTERNATIONAL ATOMIC ENERGY AGENCY, Accident Analysis for Nuclear Power Plants with Modular High Temperature Gas Cooled Reactors, Safety Report No. 54, IAEA, Vienna (2008)

[22] Nuclear Energy Agency, Implementation of Defence in depth in Nuclear Power Plants, Green booklet No. 7248, OECD/NEA, Paris (2015)

[23] CANADIAN NUCLEAR SAFETY COMMISSION, Design of Reactor Facilities: Nuclear Power Plants, REGDOC-2.5.2, CNSC, Ottawa (2014)

[24] CANADIAN NUCLEAR SAFETY COMMISSION, Design of Small Reactor Facilities, RD-367, CNSC, Ottawa (2014)

[25] INTERNATIONAL ATOMIC ENERGY AGENCY, Terms for describing new, advanced nuclear power plants, TECDOC-936, IAEA, Vienna (1997)

[26] INTERNATIONAL ATOMIC ENERGY AGENCY, Deterministic Safety Analysis for Nuclear Power Plants, Specific Safety Guide No. SSG-2 Rev. 1, IAEA, Vienna (2019)

[27] NUCLEAR SAFETY AUTHORITY, Design of Pressurized Water Reactors, Guide n°22, ASN, Montrouge (2017)

[28] OFFICE FOR NUCLEAR REGULATION, Safety Assessment Principles for Nuclear Facilities, 2014 Edition Rev 1, ONR, Bootle (2020)

[29] OFFICE FOR NUCLEAR REGULATION, New nuclear reactors: Generic Design Assessment Guidance to Requesting Parties for the UK HPR1000, ONR-GDA-GD-001. Rev 4, ONR, Bootle (2019)

[30] RADIATION AND NUCLEAR SAFETY AUTHORITY REGULATION (STUK), Regulation on the Safety of a Nuclear Power Plant, Y/1/2018, STUK, Helsinki (2018)

[31] RADIATION AND NUCLEAR SAFETY AUTHORITY REGULATION (STUK), Safety design of a nuclear power plant, YVL B.1, STUK, Helsinki (2019)

[32] RADIATION AND NUCLEAR SAFETY AUTHORITY REGULATION (STUK), Probabilistic risk assessment and risk management of a nuclear power plant, YVL A.7, STUK, Helsinki (2019)

[33] FEDERAL ENVIRONMENTAL, INDUSTRIAL AND NUCLEAR SUPERVISION SERVICE, General Provisions for Ensuring the Safety of Nuclear Power Plants, NP-001-15, Moscow

[34] NATIONAL NUCLEAR SAFETY ADMINISTRATION, Nuclear Power Plant Design Safety Regulations, Standard Document, HAF102, NNSA, Beijing (2016)

Appendix A: Examples of relevant regulatory experience from licensing of multi-unit sites

An important consideration from [7] was "*that the single-reactor mindset in nuclear safety evaluations needs to be replaced by a site-based perspective.*"

The UK is one regime that does currently include expectations on the maximum level of site wide risk posed by multi-facility sites. The Safety Assessment Principles For Nuclear Facilities [28] (SAPs) include qualitative high-level guidance which can, in principle, be used to support judgements on multi-unit interactions as part of the regulatory assessment of MT SMR designs. The UK regime specifies numerical targets for both on-site (Targets 5 and 6) and off-site risk (Targets 7 and 8). Targets 5 and 7 are expressed as per site risk. In relation to Numerical Target 7, paragraph 748 of the UK SAPs [28] states that: "*the individual risk from a site that contains multiple facilities should be determined from an appropriate combination of the individual contributions. UK safety cases sometimes adopt a risk quota approach, facility by facility".* This simple approach clearly has limitations.

Canada has been licensing stations with multiple units for decades. The CNSC issues a one-site licence for stations consisting on multiple units. A licence is issued for all activities concerned with a facility. If differences exist between units, they are reflected in the licensee's licensing basis documents. The mandatory compliance verification criteria are grouped per safety and control areas (SCAs). For CANDU stations, shared systems were designed to supplement unit-specific defence-in-depth, following a station-wide approach to safety. Current practice for the existing fleet of multiple unit nuclear power facilities in Canada has shown that a single licence enveloping all activities for the facilities on the site can be done efficiently and in consideration of:

- technical / configuration differences between units
- units of different vintage (age differences)
- units in a station that are in various lifecycle stages, for example, units operating, units in refurbishment and units in safe storage state awaiting decommissioning.

Currently in Canada there is one certified nuclear operator (plus other staff) operating each reactor. An operations concept where a single certified operator would be operating multiple reactors needs in-depth scrutiny and demonstration of safe operation. Operating experience with single licences for multiple-unit facilities has shown that licensees needs to consider how they will manage the differences between units as described above, in all of their programs for operating and maintaining the facility as a whole. Therefore, it will be a challenge for one certified nuclear operator to operate multiple-module/multiple-unit facilities. This would include, for example, an aging management program for "common services" features that are

shared between modules – including civil structures, common electrical systems, and compressed air systems.

For a proposal for a multiple- module license to construct or operate a facility, it is important for the applicant to consider the facility's ultimate total capacity over its life and the timelines for deploying the modules. This will affect, for example the environmental assessment (study of potential adverse impacts to the environment) as well as the safety analyses that will support the facility's safety case. In the license application, the CNSC expects the applicant's programs and processes to describe how multiple-unit activities will be managed under all safety and control areas. For example:

- configuration management – addressing differences between units
- human performance – personnel training and preventing errors such as performing maintenance on the wrong unit
- concept of operations – an operator overseeing multiple reactors

If an applicant proposes to construct and operate a facility, all of the activities associated with the proposal will be considered in the license application, including construction and operation of multiple modules (or units) on a single site. The Nuclear Control and Safety Act (NSCA) permits the Commission the flexibility to encompass all activities either under one single license, or multiple licenses depending on the nature and timelines of the proposed activities. This requires the applicant to demonstrate they meet the requirements applicable to the activities proposed to be licensed.

During the 2013 Pickering relicensing hearings, the topic of "whole-site" risk was raised given that PSA results have been expressed on a "per (reactor) unit" basis for each hazard type. OPG committed to provide a whole-site PSA for Pickering by end of 2017 and in support of 2018 Pickering licence renewal. The work was performed in collaboration with industry. Scope included the assessment of risk for:

- multiple reactor units
- internal and external hazards
- different reactor operating modes
- other on-site sources of radioactivity (e.g. spent fuel bays and used fuel dry storage)

The whole-site risk is not expressed as a single number but rather as an informed judgement based on a broad range of qualitative and quantitative information. The NPP utilities ensure that the site risk is reasonably low by means of rigorous programs that are in place for all aspects of operations, comply with applicable regulatory requirements and collectively assure NPP safety. Quantitative information may be provided by whole-site PSA, which is distinguished as a supporting tool and subset of whole-site risk assessment. In the whole-site risk assessment PSA plays an important complementary role to other factors in the management of risk. Risk quantification via PSA provides an indication of the level of plant risk, not an

absolute measure of safety. Numerical aggregation of reactor PSA results indicated that the total whole-site LRF is bellow than per-unit LRF safety goal, which confirmed that Pickering whole-site risk is low. It is expected that, in principle, same overall approach (as used for Pickering) could be applied for SMR sites [24]. Like for NPPs, evaluation of whole-site risk is based on many qualitative and quantitative factors, including programmatic, deterministic, and defence-in-depth aspects. Key attributes of whole-site PSA for current operating multi-unit NPPs may also apply to multi-unit/multi-module SMR sites (e.g. any shared systems among units, internal events in one unit/module affecting adjacent units/modules). The results should be revisited if more SMR will be subsequently added. Similar considerations may apply for mixed sites, that is, when SMRs are added near pre-existing operating NPPs. However, it should be noted that PSA methodologies and metrics may need some development for application to SMRs, due to novel designs. Also, a common risk metric should be considered for the SMR and NPP PSA results (e.g. LRF). While NPP and SMR LRF definitions may differ, LRF values may be aggregated if the underlying basis of per-unit LRF safety goal definitions is the same for NPPs and SMRs (e.g., limiting the likelihood of long-term relocation, per CNSC REGDOC-2.5.2 [23] and RD-367 [24]). In some SMRs, modules may share many of safety systems and each module's operation status or module's failure has a great influence on other module unlike currently operating large NPPs. Special care and considerations should be taken to apply key attributes of whole-site PSA to multi-module SMRs.

Although the current regulatory experience is relevant and applicable to multi-unit/multi-module SMR facilities, the novelty of most SMR designs including their deployment strategy (e.g. replaceable reactor modules, different reactor designs on the same site, multiple reactors operated by one operator), substantiation of passive and inherent safety features, quality management system and the supply chain control for multiple design developer may pose additional challenge for future regulatory reviews and licensing.

Appendix B: Summary of technical issues and challenges for Multi-unit site PSA

Technical area	Issues and challenges
MUPSA infrastructure	• Lack of experience and guidance for performing MUPSA; small body of existing case studies in MUPSA. • Lack of existing deterministic safety analyses of multi-unit accidents to support MUPSA. • Need to revisit and re-analyse the international operating experience for lessons to be learned from significant events and accidents for MUPSA insights; many examples of such events discussed at workshop.
Selection of initiating events	• Many single-unit PSA-initiating events (e.g., loss of off-site power, loss of heat sink, external events) challenge multiple units. • Need to delineate single unit/facility and multi-unit/facility events. • Most external events involve multi-unit challenges. • Extent of shared systems increases the importance of some internal initiating events (e.g., support system faults).
Accident sequence modelling	• Need to delineate single and multi-unit accident sequences. • Need to account for multi-unit common cause and causal dependencies, including functional, human and spatial dependencies; MUPSA models more than just a set of single-reactor PSA models. • Need to consider adverse impacts of single reactor/facility accident on other units, thus creating additional multi-unit accident scenarios. • Need to consider how operator actions may be adversely affected by multi-unit interactions. • Need to consider the timing of releases from different units. • Need to consider how radiological contamination of the site may inhibit operator actions and accident management measures. • Need to consider new end states involving multi-unit accidents and interactions, including the effects of combined and correlated hazards. • Problem of proliferation of multi-unit combinations for sites with three or more reactor units. • Limitations of static PSA modelling approaches may require a re-evaluation of dynamic PSA approaches.
Accident sequence quantification and site-based risk metrics	• Need for additional risk metrics beyond CDF and LERF to fully express the risk profile of a multi-unit site. • Need to change frequency basis from events per reactor year to events per site year to capture risks from non-reactor sources and multi-unit accidents. • Lack of surrogate frequency-based risk metrics for spent fuel accidents; temporal variations in the radiological hazard in spent fuel storage. • Need to delineate CCF models and supporting data analysis to address interunit and intra-unit CCFs. • Need to improve human reliability models and analyses to address performance-shaping factors unique to multi-unit accidents.

	• Need to rethink the selection of mission times and consider extending beyond 24 hours. • Need to address variations in site response to the same earthquake and correlation among component fragilities in the MUPSA context. • Current issues in single-reactor PSA with proliferation of scenarios, impact of conservatisms and difficulties in achieving realistic fire PSA results will be compounded in the multi-unit PSA context. • Current issues in single-reactor Level 2 PSA with treatment of human actions during implementation of Severe Accident Management Guidelines (SAMGs) and prioritization of emergency response measures will be even more difficult in the MUPSA context.
Accident progression and source term characterization	• Existing severe accident models that are limited to single-reactor accidents will have to be enhanced to treat multi-unit and fuel storage accidents • Need to define new release categories that adequately describe the releases from multi-unit accidents; this includes release magnitudes, energies, and timing from reactor units, spent fuel storage and other radiological sources
Evaluation of radiological consequences	• Consequence models need to consider how to model releases from multi-unit and multi-facility accidents; this includes consideration of different points of release from the plant, possible differences in time of release and release energies for plume rise considerations. • Method of decoupling consequence models from inventories needs revision for spent fuel accidents.
Site-based safety goals, risk integration and interpretation	• Method of aggregating risk contributions across different reactor units and facilities, single- and multi-unit and facility accidents, hazard groups and operating states with due regard to differences in level of realism/conservatism, level of detail in modelling, and uncertainty treatment. • Methods for comparing calculated risks against existing and new site-based safety goals. • Question of whether safety goals should be quantitative or qualitative, supported by quantitative safety design objectives. • Lack of multi-unit site-based acceptance criteria for evaluating the integrated risks from a multi-unit site PSA. • Need for more international consensus on approach to safety goals and use of such goals to interpret PSA results.

Appendix C: Vendor Survey Questionnaire

IAEA Small Modular Reactors Regulators Forum
Design and Safety Analysis Working Group Vendor Question Set

1. Introduction

This short paper details a set of vendor questions that has been developed to further understanding of the challenges associated with the future regulation of small modular reactors (SMRs). It is intended that these questions will be addressed to a range of SMR vendors and the responses used to inform the discussions and ultimately the recommendations of the DSA-WG of the IAEA SMR Regulator's forum.

2. Background

This activity is intended to build on the work of the Defence-in-Depth (DiD) Working Group (WG) of the IAEA Regulator's Forum Pilot Project [7] which sought to identify, understand and explore ways to address key regulatory challenges related to the application of the defence-in-depth concept to SMRs with novel design features. In Ref. 1, the DiD WG identified topics that might usefully be further investigated to help the future safety assessment of SMRs, including:

- demonstration of reinforcement of DiD levels 1 and 2
- development of safety criteria and requirements for passive safety systems and inherent s afety features
- application of single failure criteria for safety functions involving passive systems
- criteria for exclusion of identified initiating events from the design
- development of principles and requirements for the safety assessment of "multi-module" SMRs
- investigation or enhancement of methods to deal with passive features and with multi-mo dule issues in PSAs

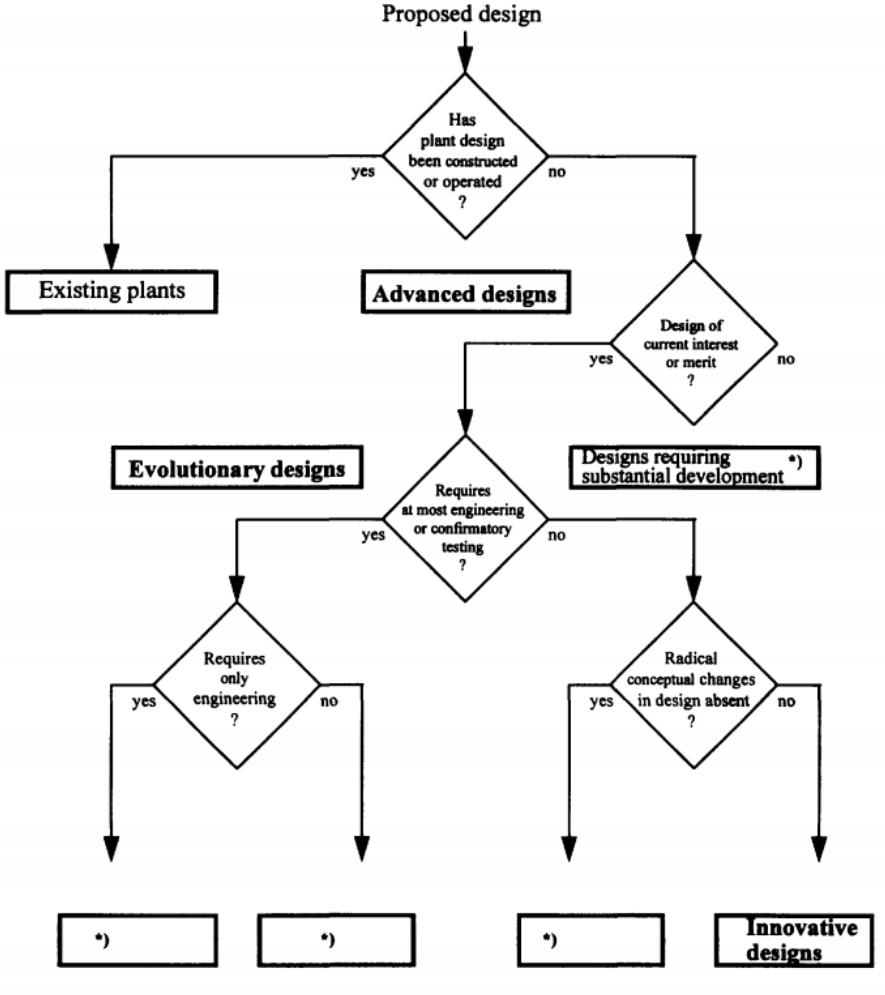
The DiD-WG also acknowledged that its recommendations were based on limited available information on the existing SMR designs and that it would *be desirable for future SMR Regulators' Forum activities to organize exchanges on safety information among SMR designers, regulatory bodies and their TSOs to better understand and frame SMR characteristics*.
Based on this recommendation, the current safety analysis WG has developed a question set to be addressed to SMR designers/vendors on issues of significance to SMR design. The current Safety Analysis WG includes regulators representing Canada, the United Kingdom, Finland, France, South Korea, Russia and Saudi Arabia. Following initial discussions, the WG identified the following scope for the next phase of the work on which further information will be requested from vendors:

- First of a Kind (FOAK) issues
- Multi-unit/multi-module issues
- Passive Safety
- Exclusion of Faults from Safety Analysis
- Severe Accidents and Design Extension Conditions

3. Discussion of Issues

3.1. FOAK Considerations

Modern SMRs designs, as summarized in [3], can incorporate innovative technology types and configurations which cannot be considered to be operationally proven; the extent to which this is true for any particular design being dependent on the degree of innovation. IAEA TECDOC-936 [25] provides a useful discussion of definitions for Advanced, Evolutionary and Innovative designs which can be applied to distinguish proposed SMR designs. Figure 1 from TECDOC 936 [25] summarises schematically this distinction:



*) *No consensus could be found on suitable existing terms for these categories.*

FIG. 1. Relationship between design related terms.

Irrespective of the SMR design type, SSR-2/1 Rev 1 [4] Requirement 9, Paragraph 4.16, relating to unproven design features would still be expected to apply:

Requirement 9: Proven engineering practices:

4.16. Where an unproven design or feature is introduced or where there is a departure from an established engineering practice, safety shall be demonstrated by means of appropriate supporting research programmes, performance tests with specific acceptance criteria or the examination of operating experience from other relevant applications. The new design or feature or new practice shall also be adequately tested to the extent practicable before being brought into service, and shall be monitored in service to verify that the behaviour of the plant is as expected

However, the scale of the development activity needed is expected to vary dependent on the degree of novelty incorporated into a design. Figure 2 from TECDOC 936 [25] illustrates this expectation schematically:

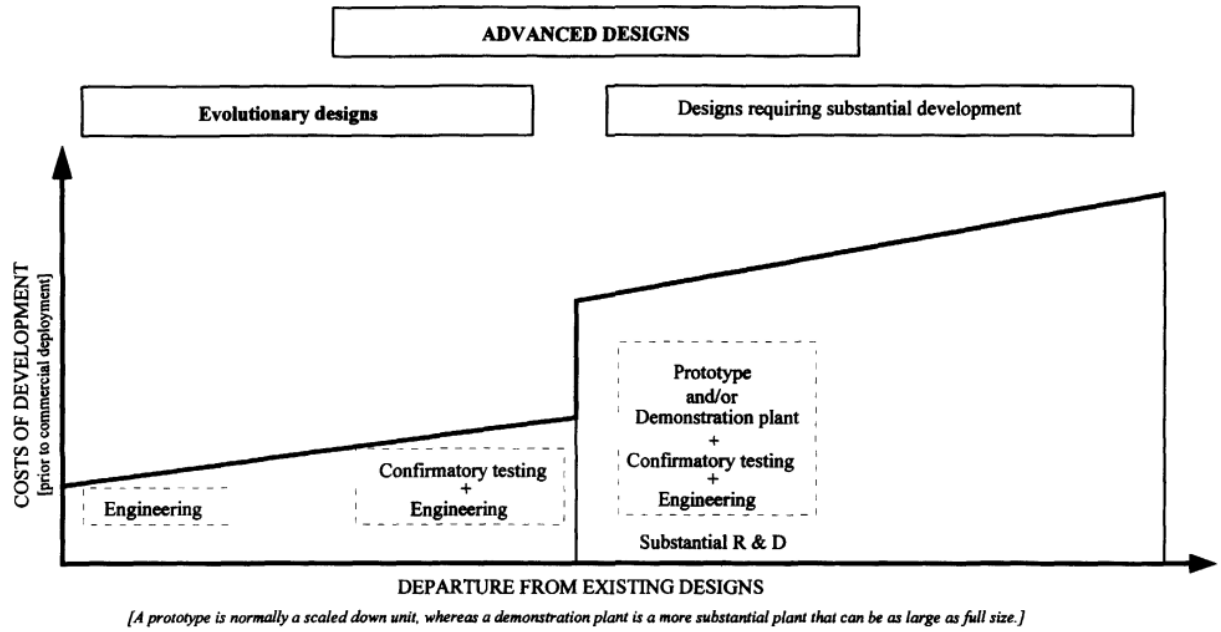


FIG 2. Efforts and costs of development for advanced designs versus departure from existing designs

Even given supporting R&D, residual risk may still exist for FOAK plant because of the absence of operational experience and regulators may wish to retain the option to impose additional requirements, for example with respects to safety margins or siting, to mitigate potentially unknown uncertainties (i.e. USNRC Regulatory Guide 1.68).

Through dialogue with SMR vendors, the Safety Analysis sub-group will seek to explore the degree to which SMR designs have been developed in accordance with SSR-2/1 [4] Requirement 9, the extent of any gaps in the necessary R&D and whether vendors have given consideration to measures to mitigate potentially unknown uncertainties for FOAK plant.

3.2. Multi-unit/modules

A significant number of small modular reactor designs incorporate the flexibility of deployment in various configurations, which may include multiple reactor units either adjacent to one another on a site or even, in some cases, within a single building on a site. The utilization of multiple small units instead of one large one enables long term planning on the site to add capacity as demand grows. In addition, such an approach can enable sequential deployment of units to match regional load demand and levelize the capital spending over a prescribed time horizon.

Nevertheless, the Fukushima Daiichi accident demonstrated the possibility of accidents involving nearly concurrent core damage at multiple reactor units and spent fuel pools. It was recognized that the accident progression was influenced by complex interactions involving operator actions to protect each facility, as well as interactions and dependencies among the facilities. In this context, it is acknowledged that there is a need for the evaluation of site risk in an integrated way, which includes consideration of the potential for accidents involving multiple installations concurrently. This may involve integration of the various risk contributions from different sources, hazard groups and plant operating states. Specific aspects may include:

- Identification of suitable risk-metrics for multi-unit sites
- The role of the multi-unit and site-based safety goals in the licensing process
- Consideration of sequential deployment of individual units
- Development of requirements for shared systems or interconnections between several units
- Challenges for conducting safety analysis (e.g. deterministic, probabilistic and hazard analysis) for multi-unit facilities, such as:
    - Identification of multi-unit accident scenarios, recognizing that connections and shared systems between modules can lead to new types of postulated initiating events
    - Understanding the impact of multi-unit configurations on the risk of propagation of an AOO, a DBA or a DEC or an internal hazard from one unit to other units
    - Assessment of simultaneous impact of external hazards on multiple/all units of the facility
    - Assessment of source term
    - A single control room common to several units
    - Common versus separate but connected spent fuel pool
- Consideration of human and organizational aspects (e.g. minimum staff complement, human factor engineering)

- Extent of emergency planning zone, severe accident management and emergency mitigation equipment

The international nuclear community is making significant efforts in collating best practice while developing and reaching consensus on how the safety aspects of multi-unit configurations should be assessed and on how multi-unit safety should be defined and evaluated.

Through dialogue with SMR vendors, the Safety Analysis sub-group will seek to understand how SMR designs consider multi-unit aspects of their design within the safety analysis developed for their designs.

3.3. Passive Safety

Passive safety systems have been used for the important engineering safety features of many SMRs because they are considered to be highly reliable, inherently safe and less vulnerable to operator error. Although the trend towards the use of passive safety systems is not exclusive to SMRs, SMRs are distinguished by the degree to which passive systems may be adopted; indeed, some SMR designs employ exclusively passive systems for at power and decay heat removal and for LOCA protection. Thus, passive safety is regarded as a particularly significant issue for SMRs. Despite the benefits, passive systems generate some regulatory challenges particularly with regards to:

- the assessment of reliability
- the application of the single failure criterion
- the provision of redundant, diverse and separated safety systems
- and the level of substantiation evidence needed

Again, the international nuclear community is making significant efforts in collecting best practice while developing and reaching consensus on how the safety aspects of passive systems should be evaluated.

Through dialogue with SMR vendors, the Safety Analysis sub-group will seek to explore vendor philosophies for the incorporation of passive safety systems into their designs and to understand how the principles of redundancy, diversity and separation are applied.

3.4. Exclusion of Faults

SMR vendors claim that some faults applicable to traditional large NPP designs do not apply to their SMRs designs. For LWR based SMR designs, this list will typically include:

- LBLOCA for integral designs
- Rod ejection faults for designs incorporating submerged CRDMs
- Complete Loss of Flow faults where natural circulation is used for DHR

In some cases, for example the rod ejection fault, the exclusion may be uncontroversial. In other cases, for example the Complete Loss of Flow faults, more complex arguments may be needed to demonstrate that all possible scenarios have been considered.

SSR-2/1 Rev 1 [4] Requirement 16 articulates a general expectation on the development of PIEs that would be expected to apply to SMRs:

> *The design for the nuclear power plant shall apply a systematic approach to identifying a comprehensive set of postulated initiating events such that all foreseeable events with the potential for serious consequences and all foreseeable events with a significant frequency of occurrence are anticipated and are considered in the design.*

Through dialogue with SMR vendors, the Safety Analysis sub-group will seek to understand the approach SMR vendors have taken to systematically identify PIEs and the criteria applied for the exclusion of events.

3.5. Design Extension Conditions and Severe Accidents

SSR-2/1 Rev 1 [4] Requirement 20 articulates a general expectation on the provision of protections for beyond design basis events that would be expected to apply to SMRs:

> *A set of design extension conditions shall be derived on the basis of engineering judgement, deterministic assessments and probabilistic assessments for the purpose of further improving the safety of the nuclear power plant by enhancing the plant's capabilities to withstand, without unacceptable radiological consequences, accidents that are either more severe than design basis accidents or that involve additional failures. These design extension conditions shall be used to identify the additional accident scenarios to be addressed in the design and to plan practicable provisions for the prevention of such accidents or mitigation of their consequences.*

Key considerations for measures are:

- independence from of those used in more frequent accidents
- ability to withstand extreme scenarios (e.g. melting of the reactor core)
- 'practical elimination' of early release
- consideration of operation actions

Through dialogue with SMR vendors, the Safety Analysis sub-group will seek to understand the approach SMR vendors have taken to Identifying and demonstrating resilience to Design Extension Conditions for their proposed designs.

4. Vendor Questions

WG participants from each member state have contributed proposals for questions on each issue which were reviewed by the working group as a whole. These were then rationalised into

the set of questions presented in Table 1 below. It has been agreed that the use of vendor responses will be subject to the following restrictions:

- There will be no judgement or assessment of acceptability of vendor responses
- The development of overall WG positions will be technology neutral
- Vendors should remain anonymous in any WG outputs

The WG intends to use responses in a number of ways as outlined below:

- To Identify common themes
- To Identify differences in approaches to achieving similar safety goals
- To inform WG common positions
- To inform WG recommendations for future IAEA work
- To identify SMR specific areas where additional regulatory guidance may be advantageo us
- To enhance WG member's understanding of vendor safety philosophies
- To enhance understanding of latest developments in SMR technologies

In addition, the working group:

- recognizes that vendors may not wish to answer all questions, for commercial or other rea sons, and welcomes answers to a limited sub-set of questions
- views the exercise as an opportunity for vendors to present their views on themes of inter est to the WG because the WG recognizes that vendors views may be informed by a more in depth understanding of specific SMR technology
- encourages vendors to include any information they view as relevant to the theme, even w here not directly addressing a specific question
- encourages vendors to respond to questions in any way (length and depth) they consider a ppropriate

Table 1. Design and Safety Analysis Vendor Question Set (Version 0.3)

#	Question
1.0 First of a Kind (FOAK) Plant (Ref. IAEA SSR-2/1 Rev. 1 [4], Requirement 9)	
1.1	Please provide an outline description of the supporting research and validation programmes that have either been undertaken or are planned to justify novel features of your proposed SMR design (i.e. those features that might be considered a departure from an established engineering practice)
1.2	Do you plan to implement any additional safety measures or increased safety margins to mitigate uncertainties associated with FOAK plant, which might in principle be removed for subsequent plant?
2.0 Multi-Unit/Modules	

2.1	Please explain your approach to the application of single unit safety goals to multi-unit SMRs.
2.2	Please explain your approach to the use of shared systems in your proposed SMR design (e.g. containment, control room, support systems).
2.3	If applicable, what criteria do you use to evaluate the safety performance of shared systems? Please provide relevant examples if possible.
2.4	Does your design documentation (e.g. design guides) include specific requirements related to multi-unit aspects of the design? Please provide relevant examples if possible.
3.0 Passive Safety	
3.1	Please outline your approach to the assessment of reliability for passive safety systems in your proposed SMR design.
3.2	Please explain your approach to the use of combinations of passive and active systems in your design.
3.3	Passive safety systems are generally considered to be inherently safe and reliable due to the use of natural forces (e.g. buoyancy and gravity). However, the driving force is often weaker than for the equivalent active system and may be subject to a greater degree of uncertainty. For example, uncertainties may arise due to the follow factors: - Effects of aging (corrosion, geometric change due to creep, pipe scaling, etc.) - Uncertainties on initial conditions (initial temperature distribution in a tube, etc.) and boundary conditions (changes in wall temperature close to other systems or containment pressure after accidents, etc.) - Effect of construction tolerance (small inclination in horizontal pipes, small leakage of valves, etc.) - Changes in driving forces over the time. - Effects of non-condensable gas, thermal stratification, and flow instability Please explain how such uncertainty is considered in your design.
3.4	Please explain whether and how a) the single failure criterion has been applied and b) common cause failure has been considered for any passive safety systems in your design.
3.5	In connection with the role of the operator and the provision of coping measures in unlikely accident scenarios, please describe the extent of the possibility for operator intervention for scenarios protected by passive safety systems. Do you provide a means for operator intervention in the event a passive safety system departs from the expected behaviour?
4.0 Exclusion of Faults from Safety Analysis (Ref. IAEA SSR-2/1 Rev. 1 [4], Requirement 16)	
4.1	Describe your approach to identifying the postulated initiating events that are considered in the design basis of your proposed SMR design.
4.2	Please identify any postulated initiating events applicable to large NPP that are excluded from the design basis of your proposed SMR design and outline the basis for this exclusion.
5.0 Severe Accidents, Design Extension Conditions and Practical Elimination (Ref. IAEA SSR-2/1 (Rev. 1) [4], Requirement 20)	
Design extension conditions A (appropriate interpretation e.g. without core melt for LWR):	
5.1	Please describe any design extension conditions (CCFs, failure combinations, internal and external hazards) and cliff edge phenomena that have been considered for your proposed SMR design. If applicable, how have you selected the cases considered?

5.2	What challenges have you identified in connection with protection for design extension conditions on your proposed SMR design compared to design of a large NPP?
5.3	What type of analysis methods (e.g. best estimate) you have used, *or do you propose to use* for analysing design extension conditions without core melt? Have modifications to modelling methodology or to analyses tools been necessary in order to apply them to SMR analyses? Have you identified any challenges in performing the analyses?
Design extension conditions B (appropriate interpretation e.g. with core melt for LWR):	
5.4	What approach have you used in designing SA mitigation measures (e.g. have you chosen certain scenarios that must be managed, or have you designed mitigation measures without reference to specific scenarios?
5.5	In comparison with a large NPP, are some phenomena approached or managed in a different way? Are some phenomena more / less challenging in SMRs?
5.6	What type of analysis methods (e.g. best estimate) you have used for analysing design extension conditions with core melt? Have modifications to modelling methodology or to analyses tools been necessary in order to apply them to SMR analyses? Have you identified some challenges in performing the analyses?
Practical Elimination	
5.7	Please explain your approach to demonstrating practical elimination of large early releases
6. Defence In Depth - Fault Tolerance	
6.1	Please explain your approach to the application of redundancy, diversity and separation in the development of your SMR design

Appendix D: Regulatory Positions on Vendor Survey Topics - Chapter 2 Topics

United Kingdom (ONR)	
#	Question
	1.0 First of a Kind (FOAK) Plant (Ref. IAEA SSR-2/1 Rev. 1 [4], Requirement 9)
1.1	**Please summarise your regulatory expectations for research and validation programmes to justify novel features with reference to FOAK SMR designs (i.e. those features that might be considered a departure from an established engineering practice)**
	There are no explicit references to FOAK plant in UK regulatory guidance, however there is guidance provided on the assessment of novelty in design that is relevant. The key expectation is articulated in the ONR SAPs [28] para. 281: *Novel approaches and features may be acceptable provided they are supported by appropriate research and development, are tested before coming into service to demonstrate the delivery of safety functions and are then monitored during service* The Generic Design Assessment (GDA) guidance document ONR-GDA-GD-001 [29] also provides the following relevant regulatory guidance: *ONR's expectation is that adequate research and technical studies will have already been completed before the start of GDA. These should be made available to ONR by the RP where necessary, including research findings relevant to ONR's assessment for which the RP does not hold the intellectual property rights.* *Factors affecting research requirements include:* • departure from proven technology; • uncertainties in performance; and • degree of defence-in-depth.
1.2	**Is there an expectation that vendors will implement additional measures or increase safety margins to mitigate uncertainties associated with FOAK plant, which might in principle be removed for subsequent plant?**
	SAPs [28] Engineering Safety Systems Principle ESS.10 gives relevant guidance on safety systems and states that *the capability of a safety system, and of each of its constituent sub-systems and components, should be defined and substantiated.* Para 406 further states that: *The capability should exceed that necessary for the effective delivery of the safety functions in the prevailing operating environment (e.g. in fault or accident conditions) by a clear margin (see also Principle EQU.1). The selected margins should make do allowance not only for uncertainties in plant characteristics, but also for the effects of foreseeable degradation mechanisms (see Principle EAD.2).*

	Hence it may be inferred that the application of greater margins might be one acceptable route to demonstrating capability in the presence of uncertainty within the UK regulatory regime.
	3.0 Passive Safety
3.1	**Please summarise regulatory expectations with respects to the assessment of reliability for passive safety systems with reference to SMR designs.**
	SAPs [28] EDR.1 to EDR.4 present ONR's expectations for the demonstration of reliability of engineered systems, structures and components and so provide confidence in the robustness of the overall design. When applied to current reactor designs these principles place onerous requirements for redundant or diverse methods to maintain control of the fundamental safety functions (such as the provision of two independent safety measures for frequent faults). However, the UK SAPs [28] Paragraph 396 do recognise that *in the case of passive safety systems, not all of the principles may apply, or their application may be more restricted because of the inherent features of such systems.*
3.2	**Please summarise regulatory expectations with respects to the use of combinations of passive and active systems with reference to SMR designs.**
	Within the UK regulatory regime there is a preference for the use of passive safety systems. SAPs para 155 states that: *Safety should be secured by characteristics as near as possible to the top of the list below:* *(a) Passive safety measures that do not rely on control systems, active safety systems or human intervention.* *(b) Automatically initiated active engineered safety measures.* *(c) Active engineered safety measures that need to be manually brought into service in response to a fault or accident.* *(d) Administrative safety measures (see paragraph 446 ff.).* *(e) Mitigation safety measures (e.g. filtration or scrubbing).* Combinations of active and passive systems might in principle contribute to diversity but are not otherwise preferred within the UK regulatory regime.
3.3	**Please summarise regulatory expectations with respects to the application of a) the single failure criterion and b) common cause failure for passive safety systems with reference to SMR designs.**
	(a) Single Failure Criterion SAP ER.4 addresses the application of the Single failure criterion and states that *during any normally permissible state of plant availability, no single random failure, assumed to occur anywhere within the systems provided to secure a safety function, should prevent the performance of that safety function.* Further detail is given is SAP [28] Paragraph 188: *Consequential failures resulting from the assumed single failure should be considered as an integral part of the single failure. Further discussion of the single failure criterion is given in IAEA Safety Standard SSG-2 [26]. A system that is the principle means of fulfilling a Category A safety function (principle means of achieving nuclear safety) should, other than in exceptional circumstances, always be designed to meet the single failure criterion. However, other systems which make a contribution to fulfilling the same safety function, but are independent of the principal system, do not necessarily need to meet the single failure criterion.*

	(b) Common Cause Failure SAP [28] ER.4 addresses expectations on CCF and states that *Common cause failure (CCF) should be addressed explicitly where a structure, system or component employs redundant or diverse components, measurements, or actions to provide high reliability.* There is an expectation that CCF claims should be substantiated (SAPs ER.1 para 185). SAP para 185 limits the extent of quantitative claims: *In general, claims for CCF should not be better than one failure per 100 000 demands. The figure of one failure per 100 000 demands represents a judgement by ONR of the best limit that could reasonably be supported for a simple system by currently available data and methods of analysis. A worse figure may need to be used (say 1 per 10 000 or 1 per 1000) according to the complexity and novelty of the system, the nature of threat and the capability of the equipment. Nevertheless, it is conceivable that the continuing accumulation of good data and advances in its analysis could lead, in exceptional circumstances, to a situation where a strong case could be made by the duty holder for better figures. Such a case would not then be ruled out of consideration. Where required reliabilities cannot be achieved due to CCF considerations, the safety function should be achieved taking account of the concepts of diversity and segregation, and by providing at least two independent safety measures.*

Finland (STUK)	
1.0 First of a Kind (FOAK) Plant (Ref. IAEA SSR-2/1 Rev. 1 [4], Requirement 9)	
1.1	**Please summarise your regulatory expectations for research and validation programmes to justify novel features with reference to FOAK SMR designs (i.e. those features that might be considered a departure from an established engineering practice)**
	There is no explicit definition for a FOAK plant in the Finnish regulations and guidance. However, it is explicitly stated that "*If new[novel] solutions are proposed, they shall be validated through tests and experiments*." (This is necessary but not sufficient alone.) In addition, in the regulatory guides it is required that features that have "considerable safety significance" shall be assessed by an "independent third-party organisation". Third-party organisation refers to expert and research organisations other than the safety authority. In the current renewal of regulatory guides, the "considerable safety significance" is being changed into a definition referring to FOAK type of solutions.
1.2	**Is there an expectation that vendors will implement additional measures or increase safety margins to mitigate uncertainties associated with reference to FOAK plant, which might in principle be removed for subsequent plant?**
	There are multiple requirements addressing uncertainties in general, e.g. (STUK Y/1/2018 [30]) :"Any uncertainty in the results shall be considered when assessing the meeting of the safety requirements." None of them concern FOAK specifically. Rather than requiring

	increased margins for the first plant, experience from commissioning and operation etc. could possibly be used as justification for e.g. smaller margins in the subsequent plants.
3.0 Passive Safety	
3.1	**Please summarise regulatory expectations with respects to the assessment of reliability for passive safety systems with reference to SMR designs.**
	For the most part there are no dedicated requirements for assessment of reliability of passive systems; general requirements apply:" *The nuclear facility's safety and the technical solutions of its safety systems shall be assessed and substantiated analytically and, if necessary, experimentally*." In case of passive systems this implies extensive experimental programs for safety demonstration. As to reliability analysis/PRA, failures and events potentially affecting the boundary conditions for system operation shall be considered and described in the analysis. For example, natural circulation may be impaired or prevented by non-condensable gases, blockage, wrong valve positions, impurities, corrosion, algae in tanks, maintenance errors, foreign objects in process etc. All potential scenarios shall be considered, and relevant scenarios shall be modelled and quantified in the PSA.
3.2	**Please summarise regulatory expectations with respects to the use of combinations of passive and active systems with reference to SMR designs**.
	Irrespective of type of the combination of systems, it is required that there shall be no interference or adverse effects between systems that function on the different defence-of-depth levels. Combinations of active and passive systems are not specifically addressed in the regulations.
3.3	**Please summarise regulatory expectations with respects to the application of a) the single failure criterion and b) common cause failure for passive safety systems in SMR designs.**
	The failure criterion for engineered safety systems intended for mitigation of postulated accidents is "N+2" i.e. single failure and maintenance/repair. However, "*if the decay heat removal systems or their auxiliary systems have passive components that have a very low probability of failure in connection with the anticipated operational occurrence or postulated accident, the (N+1) failure criterion may be applied to those components instead of the (N+2) failure criterion.".* Common cause failure is expected to be accounted for by diversity in the safety system design; requirements do not specifically address passive safety systems. What type of diversity is required in case of passive safety systems has not been explicitly addressed in the current regulations and guidance. (It has been recognised defence in depth related requirements will likely require further discussion in relation to SMRs.)

France (IRSN)	
#	Question
1.0 First of a Kind (FOAK) Plant (IAEA SSR-2/1 Rev. 1 [4], Requirement 9)	

1.1	**Please summarise your regulatory expectations for research and validation programmes to justify novel features with reference to FOAK SMR designs (i.e. those features that might be considered a departure from an established engineering practice)**
	There are no references to FOAK in French regulatory guidance.
1.2	**Is there an expectation that vendors will implement additional measures or increase safety margins to mitigate uncertainties associated with reference to FOAK plant, which might in principle be removed for subsequent plant?**
3.0 Passive Safety	
3.1	**Please summarise regulatory expectations with respects to the assessment of reliability for passive safety systems with reference to SMR designs.**
	There are no explicit references to multi-units in the French regulatory guidance, but French expectations can be found in the WENRA RHWG report of June 2018 dealing with regulatory aspects of passive systems.
3.2	**Please summarise regulatory expectations with respects to the use of combinations of passive and active systems with reference to SMR designs.**
	There are no explicit references to a combination of passive and active systems in the French regulatory guidance. The ASN-IRSN guide n°22 [27] addresses the use of passive systems in its section 4.1.1.4 that :"*The use of passive systems, without it being necessary to favour this as a matter of course, can have advantages in certain cases when it is possible to justify the relevance and the effectiveness*."
3.3	**Please summarise regulatory expectations with respects to the application of a) the single failure criterion and b) common cause failure for passive safety systems in SMR designs.**
	The ASN-IRSN guide n°22 addresses [27] the application of the Single failure criterion in its paragraph IV.2.3 "***Section 4.2.3.1*** *The systems IP necessary for the control of the design-basis condition categories 2 to 4 (DBC-2 to 4) shall be designed in compliance with the single failure criterion.* ***Section 4.2.3.2*** *The active single failure of an EIP shall be postulated when it is called upon, in the short or long term.* ***Section 4.2.3.3*** *The passive single failure of an EIP[14] shall be postulated for the long term as from 24 hours after the event necessitating operation of the IP system. The possible leaks in the short term shall be considered for the headers.* *Furthermore, it shall be verified through sensitivity analyses that a passive single failure postulated before 24 hours have elapsed or leading to a higher leakage rate than the conventionally defined value (up to the break of a connected pipe of 50 mm inside diameter), would not lead to more severe consequences than those resulting from an active single failure or would not lead to a cliff-edge effect in terms of system IP effectiveness, or in terms of radiological consequences.* ***Section 4.2.3.4*** *Measures to prevent and limit the consequences of passive failures shall be implemented, particularly with regard to detection, isolation and leak collection.*

[14] The concept of passive single failure does not apply to the main primary system or the main secondary system.

	Section 4.2.3.5 *Some single failures could be excluded, notably those relative to the opening of certain check valves subjected to high pressure differentials or to the operation of certain equipment items that are not subject to significant load variations, on the basis of appropriate justifications taking into account in particular:* - *the design and operating measures implemented;* - *an analysis of operating experience feedback;* - *if necessary; for active single failures, an analysis of the consequences of the failure conducted with less-conservative rules, methods or assumptions than those adopted for the analysis of the design-basis conditions."* Definition of active and passive failure can also be found: *"An active single failure is characterised by:* - *an error in the position of a mechanical or electrical equipment item;* - *the failure of a mechanical or electrical equipment item to respond when a mechanical movement is necessary to fulfil the required function;* - *the failure of an I&C hardware component leading to non-fulfilment of the required function.* *Spurious functioning of equipment due to I&C failures is addressed in chapter VII.4."* "*A passive single failure is applicable to an item of equipment which does not need to change position to fulfil its required safety function. A passive failure can be, for example:* - *a leak in the pressurised envelope of a fluid system, with a conventional leakage value[15] until it is isolated. If such a leak affects a pipe and is not detected and isolated, it is assumed to increase until it reaches the flow rate corresponding to a total break;* *a mechanical failure preventing the normal flow of a fluid."*

KOREA (KINS)	
#	Question
1.0 First of a Kind (FOAK) Plant (IAEA SSR-2/1 Rev. 1 [4], Requirement 9)	
1.1	Please summarise your regulatory expectations for research and validation programmes to justify novel features with reference to FOAK SMR designs (i.e. those features that might be considered a departure from an established engineering practice)
	There are no separate Korean guidelines for FOAK power plants and SMR design, however guidance and main expectations regarding the evaluation of the relevant design are given in each chapter in the Safety Review Guideline (SRG) for pressurized water reactor plants. For example, *[SRG Chapter 1.0 Introduction and Interfaces]* *I. Areas of Review* *5. Performance of <u>New Safety Features</u>* *The review addresses information or references to the location of information that demonstrates the performance of new safety features for nuclear power plants that are significantly different from the previously licensed design of light-water nuclear power*

[15] The basic safety rule RFS 1.3.a, "*Utilisation of the single failure criterion in the safety analysis*", sets this conventional leak at 200 L/min.

	plants or that employ simplified(integral), inherent, passive or other innovative methods to accomplish their safety functions. *II. Acceptance Criteria* *For performance of new safety features, the information is sufficient to provide reasonable assurance that (1) these new safety features will perform as predicted in the applicant's SAR, (2) the effects of system interactions are acceptable, and (3) the applicant provides sufficient data to validate analytical codes. The design qualification testing requirements may be met with either separate effects or integral system tests; prototype tests; or a combination of tests, analyses, and operating experience.* *[SRG Chapter 4.4 Thermal and Hydraulic Design]* *I. Areas of Review* *… The review of new prototype plants, new critical heat flux (CHF) or correlations, and new analysis methods require additional independent audit analyses in the following forms:* • *Independent computer calculations to substantiate reactor vendor analyses.* • *Reduction and correlations of experimental data to verify processes or phenomena which are applied to reactor design.* • *Independent comparisons and correlations of data from experimental programs. Th ese reviews also include analyses of experimental techniques, test repeatability, an d data reduction methods.*
1.2	Is there an expectation that vendors will implement additional measures or increase safety margins to mitigate uncertainties associated with reference to FOAK plant, which might in principle be removed for subsequent plant?
	It is expected that safety margin will be increased further if there are areas that are not clearly assessed.
3.0 Passive Safety	
3.1	Please summarise regulatory expectations with respects to the assessment of reliability for passive safety systems with reference to SMR designs.
	Basically, the passive safety systems shall satisfy as much safety as the active systems that have the same safety functions required. Currently, a corresponding regulatory guideline for design and performance of passive safety systems, including passive systems for SMR design, is being developed, and the draft guidance will include the following. • *Definition of passive component and passive systems* • *Guidelines for design of passive systems* *1) Single failure criteria* *2) Defence in depth* *3) Leakage monitoring and isolation* *4) Testability and inspectability* • *Guidelines for performance of passive systems* *1) Operability* *2) Ultimate heat sink* 3) *Make up system for secondary side* The regulatory expectations for the assessment of reliability for passive safety systems, for example, are shown in detail at the relevant design chapter as follows:

	[SRG Chapter 15.6.5 Loss-of-coolant accidents resulting from spectrum of postulated piping breaks within the reactor coolant pressure boundary] *III Review Procedures* *In the case of new reactor designs that use passive rather than active systems to provide ECCS to the reactor vessel, pressure drop test results should be reviewed to determine that the passive ECCS flow rate is consistent with that in the analyses of the system performance.*
3.2	Please summarise regulatory expectations with respects to the use of combinations of passive and active systems with reference to SMR designs.
	Regulatory guideline under development for passive safety systems (draft) states that the operability in combination with active devices or systems should be ensured if active devices or systems are installed to assist the operation of the passive systems.
3.3	Please summarise regulatory expectations with respects to the application of a) the single failure criterion and b) common cause failure for passive safety systems in SMR designs.
	a) Regulatory guideline under development for passive safety systems (draft) states that the safety systems should be designed for performing the inherent safety functions even in the single failure, regardless of active or passive type. b) Current regulation requires the diversity protection system for ATWS situations that might be resulted from CCF of safety systems. This is basically applied also to passive safety systems in SMR designs. Similarly, the reactor protection system that adopts software-based digital equipment, to be designed to maintain its original function, even under a common mode failure of software. *Regulation on Technical Standards for Nuclear Reactor Facilities, Etc.* *Article 27 (Diversity Protection System)* *(1) An additional independent protection system (hereinafter referred to as "diversity protection system") which has the functions of reactor shutdown, actuation of emergency auxiliary feedwater system, and turbine trip shall be installed to prepare for anticipated transients without scram.* *(2) The diverse protection system shall be separated from the protection system, ranging from the part of producing output signal of the equipment to monitor the operating condition to the driving mechanism of final actuator.* *Article 26 (Reactor Protection System)* *(2) The protection system shall be designed in accordance with each of the following requirements in order to assure the performance of its safety functions:* *8. In the case of adoption of software-based digital equipment, the design concepts of defence-in-depth and diversity including manual functions shall be applied to the design of the protection system in order to assure the implementation of protection functions required at a common mode failure of software.*

Canada (CNSC)	
#	Question
1.0 First of a Kind (FOAK) Plant (IAEA SSR-2/1 Rev. 1 [4], Requirement 9)	

1.1	**Please summarise your regulatory expectations for research and validation programmes to justify novel features with reference to FOAK SMR designs (i.e. those features that might be considered a departure from an established engineering practice)**
	REGDOC 2.5.2. [23] Section 5.4 *Proven engineering practices* requires that the design authority evaluate codes and standards used in the design "*for applicability, adequacy, and sufficiency to the design of SSCs important to safety*". It is also expected that that SSCs important to safety shall be of proven design. However, if a new SSC design, feature or engineering practice is introduced, "adequate *safety shall be demonstrated by a combination of supporting research and development programs and by examination of relevant experience from similar applications. An adequate qualification program shall be established to verify that the new design meets all applicable safety requirements. New designs shall be tested before being brought into service and shall be monitored while in service so as to verify that the expected behaviour is achieved."* Similar requirements are articulated in section 6.4 of RD-367 [24] "*Design of Small Reactor Facilities*". ***Proven Design*** *A design of a component(s) can be proven either by showing compliance with accepted engineering standards, by a history of experience, by test, or by some combination of these. New component(s) are 'proven' by performing a number of acceptance and demonstration tests that show the component(s) meets pre-defined criteria. (as per Definitions from REGDOC 2.5.2 [23])*
1.2	**Is there an expectation that vendors will implement additional measures or increase safety margins to mitigate uncertainties associated with reference to FOAK plant, which might in principle be removed for subsequent plant?**
	Section 5.4 of REGDOC 2.5.2 [23] stipulates that "*where needed, codes and standards shall be supplemented to ensure that the final quality of the design is commensurate with the necessary safety functions*." However, there are no specific requirements on how a reactor designer should address the uncertainties associated with reference to FOAK. CNSC expect the designers/vendors to identify their additional features and design approaches. Mitigation of the uncertainties associated with the new technologies/FOAK may include incorporating of additional safety margins in the FOAK, installing supplementary safety system, applying a conservative safety classification methodology, providing adequate monitoring capabilities/parameters along to maintaining situational awareness of system states under all operating conditions, such that the relevant regulatory requirements are met and an adequate level of safety is demonstrated. Also, a FOAK plant may need additional commissioning tests than the subsequent plants to demonstrate its safety.
3.0 Passive Safety	
3.1	**Please summarise regulatory expectations with respects to the assessment of reliability for passive safety systems with reference to SMR designs.**
	There are no specific regulatory expectations with regard to reliability assessment of passive safety systems. Reliability requirements for safety systems are independent of their principles of operation (active or passive). As per REGDOC 2.5.2 [23], the safety systems and their support systems shall be designed to ensure that the probability of a safety system failure on demand from all causes is lower than 10^{-3}.

3.2	**Please summarise regulatory expectations with respects to the use of combinations of passive and active systems with reference to SMR designs.**
	It is expected that postulated initiating events include failure of passive systems, such as breaks in the reactor's pressure-retaining boundaries, including pipes and rupture discs. The CNSC encourages the use of passive SSCs, but it is not a requirement. As per REGDOC 2.5.2, [23] section 6.3, following a PIE, the plant is rendered safe by: 1. inherent safety features 2. passive safety features 3. specified procedural actions 4. action of control systems 5. action of safety systems 6. action of complementary design features In the guidance section on the Emergency Heat Removal System it is mentioned that passive or non-passive (e.g. natural circulation or pumped) heat removal may be used. However, natural circulations systems are expected to demonstrate their capability over the full range of applicable operating conditions. According to REGDOC 2.5.2 [23] a **passive component** is defined as "*A component whose functioning does not depend on an external input such as actuation, mechanical movement or supply of power*."
3.3	**Please summarise regulatory expectations with respects to the application of a) the single failure criterion and b) common cause failure for passive safety systems in SMR designs.**
	Per REGDOC 2.5.2 [23], in the considerations about the single failure criterion, unintended actions and failure of passive components shall be considered as two of the modes of failure of a safety group. The single failure shall be assumed to occur prior to the PIE, or at any time during the mission time for which the safety group is required to function following the PIE. Passive components, however, may be exempt from this requirement. The exemptions of SFC requirements for passive components may be applied only to those components that are designed and manufactured to high standards of quality, that are adequately inspected and maintained in service, and that remain unaffected by the PIE. Design documentation shall include justification of such exemptions, by analysis, testing or a combination of analysis and testing. The justification of exemption shall take loads and environmental conditions into account, as well as the total period of time after the PIE for which the functioning of the component is necessary. In order to exempt passive components from the SFC, the following should be addressed as part of demonstrating a high degree of performance: adequate testing during the manufacturing stage sample testing from those components received from the manufacturer adequate testing during construction and commissioning stages necessary testing to verify their reliability after the components have been removed from service during the operation stage There are no specific requirements for common cause failures for passive safety systems. The existing common cause failures requirements are applicable to all items important to safety, regardless their principle of operation (active and/or passive).

China (CAEA)	
#	Question
1.0 First of a Kind (FOAK) Plant (IAEA SSR-2/1 Rev. 1 [4], Requirement 9)	
1.1	**Please summarise your regulatory expectations for research and validation programmes to justify novel features with reference to FOAK SMR designs (i.e. those features that might be considered a departure from an established engineering practice)**
	There are no specific exemptions for FOAK in CHINA regulatory guidance. For novel design features of a nuclear reactor, the basic regulatory principles we follow include: 1. the first choice is engineering verification through test facilities; 2. some features could be tested in the commissioning stage of the demonstration project; 3 extrapolation could be done based on conservative assumptions for some features that are similar to those proven design features.
1.2	**Is there an expectation that vendors will implement additional measures or increase safety margins to mitigate uncertainties associated with reference to FOAK plant, which might in principle be removed for subsequent plant?**
	For innovative reactors, uncertainties shall be analyzed based on bounded and conservative assumptions. If it's difficult to evaluate the uncertainties, vendors shall implement additional measures or increase safety margins.
3.0 Passive Safety	
3.1	**Please summarise regulatory expectations with respects to the assessment of reliability for passive safety systems with reference to SMR designs.、**
	At first functional experiments shall be conducted for the verification of passive systems. And then factors influencing the reliability shall be analyzed and evaluated. Regarding these two aspects, there is no difference with those in the reliability assessment of passive systems of large-scale nuclear power plants.
3.2	**Please summarise regulatory expectations with respects to the use of combinations of passive and active systems with reference to SMR designs.**
	The designer could choose passive systems or active systems. What the regulator concerns is the adequate analyses, evaluations and function verifications for the selected systems.
3.3	**Please summarise regulatory expectations with respects to the application of a) the single failure criterion and b) common cause failure for passive safety systems in SMR designs.**
	The methodology of deterministic safety analysis (DSA) is still the main method used in SMR designs and safety review, so the single failure criterion is still applicable. However, in the future some necessary adjustments based on the risk-informed methodology could be expected. Necessary evaluations shall be made for the common cause failure of passive systems, which shall be avoided in the design.

Appendix E: Regulatory Positions on Vendor Survey Topics – Chapter 3 topics

United Kingdom (ONR)	
#	Question
5.0 Severe Accidents, Design Extension Conditions and Practical Elimination (IAEA SSR-2/1 Rev. 1 [4], Requirement 20)	
5.1	**Please summarise regulatory expectations with respects to the identification of design extension conditions and practical elimination for SMR designs.**
	SAP [28] principle FA.15 considers the scope of severe accident analysis (SAA) and states that Fault states, scenarios and sequences beyond the design basis that have the potential to lead to a severe accident should be analysed. SAPs [28] para 6111 considers practical elimination: *In line with wider international guidance, the SAA should form part of a demonstration that potential severe accident states have been 'practically eliminated'. To demonstrate practical elimination, the safety case should show either that it is physically impossible for the accident state to occur or that design provisions mean that the state can be considered to be extremely unlikely with a high degree of confidence. Each instance where practical elimination is claimed should be assessed separately, taking into account relevant uncertainties, particularly those due to limited knowledge of extreme physical phenomena (eg the behaviour of molten reactor cores). Moreover, an accident state should not be considered to have been practically eliminated simply on the basis of meeting probabilistic criteria. Instead, any claims made on SSCs in relation to practical elimination need to be substantiated appropriately.* SAPs [28] para 665-669 provide further relevant guidance: *The SAA should, through a systematic approach, analyse beyond design basis states and scenarios arising from the circumstances listed in paragraph 609. In line with the principle of practical elimination (see paragraph 611), states and scenarios should not be dismissed from the analysis on frequency grounds alone. Indeed, SAA is not normally concerned with the sequences leading to the severe accident (these being the province of DBA and PSA), but instead should be focused on how the accident state or scenario will be controlled and/or mitigated.* *For each state or scenario, the SAA should:* *(a) determine the magnitude and characteristics of the predicted source term and its potential radiological consequences, including societal effects; and* *(b) demonstrate that there is no sudden escalation of consequences just beyond the design basis (see Principle EHA.7 – cliff edge effects).*

	The analysis should include consideration of failures that could occur in the physical barriers containing radioactive material, or in the shielding against direct radiation. *A best estimate approach should normally be followed. However, where uncertainties are such that a realistic analysis cannot be performed with confidence, a conservative or bounding case approach should be adopted to avoid optimistic conclusions being drawn. Where a best estimate approach is not followed, the extent to which the analysis could nevertheless be used to inform emergency response activities (eg in regard to the expected timings of escalations in the accident sequence) should be considered..*

Finland (STUK)	
#	Question
5.0 Severe Accidents, Design Extension Conditions and Practical Elimination (IAEA SSR-2/1 Rev. 1 [4], Requirement 20)	
5.1	**Please summarise regulatory expectations with respects to the identification of design extension conditions and practical elimination for SMR designs.**
	The current regulations require that common cause failures combined with the so-called class 1 postulated accidents, "complex sequences" and rare external events are accounted for as "design extension condition". In general identification is expected to be performed and justified by the designer (and/or license applicant/holder) but there are some rare cases that are prescribed. Severe reactor accidents are explicitly required to be provided for by dedicated and independent means in the current, binding regulations. (It has been recognised defence in depth related requirements will likely require further discussion in relation to SMRs.) Regarding practical elimination, there are both deterministic and probabilistic requirements e.g. YVL B.1 [31]: "*Events that may result in a release requiring measures to protect the population in the early stages of the accident shall be practically eliminated*." "*Events to be practically eliminated shall be identified and analysed using methods based on deterministic analyses complemented by probabilistic risk assessments and expert assessments. Practical elimination cannot be based solely on compliance with a cut-off probabilistic value. Even if the probabilistic analysis suggests that the probability of an event is extremely low, all practicable measures shall be taken to reduce the risk. As an example, events to be practically eliminated include:* *There are some practical examples listed:* YVL A.7 [32]: "*the accident sequences, in which the containment function fails or is lost in the early phase of a severe accident, have only a small contribution to the reactor core damage frequency. Release assessments shall take into account all of the nuclear fuel located at the plant unit. A spent nuclear fuel storage external to the plant unit is considered a separate nuclear facility for whose analysis the aforementioned criteria apply*."

France (IRSN)	
#	Question
5.0 Severe Accidents, Design Extension Conditions and Practical Elimination (IAEA SSR-2/1 Rev. 1 [4], Requirement 20)	
5.1	**Please summarise regulatory expectations with respects to the identification of design extension conditions and practical elimination for SMR designs.**

	Regarding identification of design extension conditions, the ASN-IRSN guide n°22 [27] states: Section 3.1.1*:" In order to determine the events to analyse in the demonstration of nuclear safety (see III.2), all the events that can affect the nuclear safety of the installation during normal operation (including reactor outage states) shall be identified on the basis of:*
	- *postulated initiating events (PIE) comprising:*
	  o *the single initiating events (SIE);*
	  o *the internal hazards that can lead directly or indirectly to damage of the EIPs necessary to fulfil the safety functions;*
	  o *the external hazards of natural origin or associated with human activities in the environment of the installation, which can lead directly or indirectly to damage of the EIPs necessary to fulfil the safety functions;*
	- *plausible combinations of initiating events or one initiating event with failure of the measures implemented to cope with it."*
	
	Section 3.4.1.1: "*The list of events to consider in the design extension envelope shall be based on deterministic and probabilistic considerations, consolidated by expert judgment if necessary.*
	The events in the design extension envelope shall consider:
	- *conditions termed "DEC-A" for which fuel meltdown shall be prevented. They consider, in principle, with respect to the fuel meltdown frequency objective:*
	  o *combinations of a DBC condition and a common cause failure affecting the redundant parts of a system IP necessary for the control of this DBC condition;*
	  o *common cause failures on the systems IP used in normal operation.*
	- *The probabilistic analyses enable the list of DEC-A conditions (see article 6.3.1) to be confirmed and supplemented if necessary;*
	- *conditions termed "DEC-B" in which fuel meltdown is postulated despite the measures taken to prevent this. The situations mentioned in article 3.2.6* [those that must be practically eliminated] *are not included in the design extension envelope;*
	- *natural external hazards of greater severity than those considered in the design reference envelope (see chapter III.4.6 for the corresponding particularities)*."
	
	Regarding practical elimination, section 3.2.6 states that *" accident situations with core meltdown which could lead to significant radioactive releases that develop too rapidly to allow timely deployment of the necessary population protection measures shall be rendered physically impossible or, failing this, measures shall be implemented to render them extremely improbable with a high level of confidence. The justifications for these measures shall be based on a deterministic analysis, consolidated where relevant by probabilistic evaluations, taking account of uncertainties due to the limited knowledge of certain physical phenomena*."

Korea (KINS)

#	Question
5.0 Severe Accidents, Design Extension Conditions and Practical Elimination (Ref. IAEA SSR-2/1 (Rev. 1) [4], Requirement 20)	
5.1	**Please summarise regulatory expectations with respects to the identification of design extension conditions and practical elimination for SMR designs.**
	The Nuclear Safety Act revised in 2015 with new requirement for the submission of Accident Management Program (AMP) for operating license applications for new NPPs. In the rulemaking process, the accident management basically designed to adopt the DiD concept from IAEA INSAG-10 and the philosophy of Vienna Declaration on Nuclear Safety, in the light of the Fukushima Daiichi accidents. The applicants or licensees have to show the capability of prevention and mitigation of each level of DiD. The term 'practical elimination' can be differently understood in its level of depth. Applicants or licensees can show how the plant can achieve the practical elimination through deterministic or probabilistic methods. The regulations regarding the design extension conditions and practical elimination are shown in Articles below: *Regulation on Technical Standards for Nuclear Reactor Facilities, Etc.* *Article 85-19 (Scope of accident management)* *(1) The scope of accidents subject to accident management shall be as follows:* *1. Accidents related to design standards;* *2. Accidents attributable to multiple failures;* *3. Natural and artificial disasters exceeding the external causes when considering the design standards provided under Article 13: and* *4. Accidents in which the reactor core is seriously damaged beyond the scope of the design standards.* *(2) The Nuclear Safety and Security Commission shall determine and announce the details of the selection of accidents falling under paragraph 1 Items 2 to 4.* *Article 85-22 (Assessment of accident management capabilities)* *(1) The accident management plan shall be developed and implemented with the objective of achieving the below-listed by assessing accident management capabilities, including the equipment related to accident management, accident management strategies, and performance systems:* *1. The accident management plan shall prevent the discharge of large quantities of radioactive materials that may threaten the health of residents in the surrounding areas or cause long-term contamination outside the site in the event that an accident takes place.* *2. It shall minimize the increased rate of risk that the operation of nuclear reactor and related facilities is likely to have on the health and the environment of the residents in the surrounding areas.* *(2) The attainment of the objectives provided under the items of paragraph 1 shall be assessed using deterministic and probabilistic methods. The Nuclear Safety and Security Commission shall determine and announce the specifics of such assessment.*

Canada (CNSC)	
#	Question
5.0 Severe Accidents, Design Extension Conditions and Practical Elimination (IAEA SSR-2/1 Rev. 1 [4], Requirement 20)	
5.1	**Please summarise regulatory expectations with respects to the identification of design extension conditions and practical elimination for SMR designs.**
	Regulatory requirements with regard to Design Extension Conditions are included in section 7.3.4 of REGDOC 2.5.2. [23] Design extension conditions (DECs) are a subset of beyond-design-basis accidents that are considered in the design process of the facility in accordance with best-estimate methodology to keep releases of radioactive material within acceptable limits. Design extension conditions could include severe accidents. Accidents in this category are, typically, sequences involving more than one failure (unless these are taken into account in the DBAs at the design stage). Such sequences may include DBAs with degraded performance of a safety system, and sequences that could lead to containment bypass. The design authority shall identify the set of design-extension conditions (DECs) based on deterministic and probabilistic methods, operational experience, engineering judgment and the results of research and analysis. It is expected that "*design shall be such that plant states that could lead to significant radioactive releases are practically eliminated. For plant states that are not practically eliminated, only protective measures that are of limited scope in terms of area and time shall be necessary for protection of the public, and sufficient time shall be made available to implement these measures.*" The choice of the DECs to be analysed should be explained and justified, indicating whether it has been made on the basis of a PSA or other analysis that identifies potential vulnerabilities of the plant. It is acceptable to use the best estimate analysis methodology (models and assumptions), take credit for realistic system performance and operator actions. In the guidance section, REGDOC-2.5.2 [23] states that: *"The design should identify the features that are designed for use in, or that are capable of preventing or mitigating events considered in DECs. These features include complementary design features and other SSCs that may be credited for DECs. These features should:* *1. be independent, to the extent practicable, of those used in more frequent accidents* *2. have a reliability commensurate with the function that they are required to fulfil* *The choice of the DECs to be analysed should be explained and justified, indicating whether it has been made on the basis of a PSA or other analysis that identifies potential vulnerabilities of the plant.* *Accident conditions with a significant release are considered to have been practically eliminated:* • *if it is physically impossible for the condition to occur, or* • *if the condition can be considered with a high degree of confidence to be extremely unlikely to arise*

	Physical impossibility can be demonstrated by a design feature that would preclude initiation or further progress of an accident scenario. Care should be taken when assumptions are used to support the demonstration. Such assumptions should be adequately acknowledged and addressed."

	China (CAEN)
5.1	**Please summarise regulatory expectations with respects to the identification of design extension conditions and practical elimination with reference to SMR designs.**
	The requirements on DECs and practical elimination of SMRs (at least for PWR SMR) are the same as those of large-scale NPPs.

Appendix F: Severe Accident Definitions

1. **Canada (CNSC)**

   Severe Accident (REGSOC 2.5.2 [23]):

   An accident more severe than a design-basis accident and involving severe fuel degradation in the reactor core or spent fuel pool.

2. **Finland (STUK)**

   STUK definition can be found here:

   https://www.stuklex.fi/en/maarays/stuk-y-1-2018 [30]

   1. For the purposes of this regulation….

      20) *severe accident* shall refer to an accident in which a considerable part of the fuel in a reactor or of the spent fuel in a spent fuel pool or storage loses its original structure,

      21) *severe reactor accident* shall refer to an accident in which a considerable part of the fuel in a reactor loses its original structure.

3. **Russia (SEC NRC)**

   According to Federal Rules and Regulations NP-001-15 [33]: Severe accident is a beyond design basis accident with fuel elements damage above the maximum design limit.

   By the way also in NP-001-15 [33] there is another definition: Harbinger of a severe accident is a deviation of the NPP from design characteristics detected during operation or an event that occurred during operation that did not lead to a severe accident, but indicates the presence of a serious flaw in the systems important to safety design, NPP design or NPP operation, or there is a significant part of the emergency sequence could lead to a serious accident.

4. **UK (ONR)**

   Safety Assessment Principles (Para. 664):

   Undertaking *SAA is not proportionate for all types of facilities, as not all present hazards of sufficient magnitude to warrant this. However, SAA is beneficial for facilities presenting the highest hazards, such as operating reactors, spent fuel storage facilities and facilities storing significant quantities of nuclear matter. In these principles, severe accidents are defined as those fault sequences that could lead either to consequences exceeding the highest off-site radiological doses given in the BSLs of Numerical Target 4 (i.e. 100 mSv, conservatively assessed) or to an unintended relocation of a substantial quantity of radioactive material within the facility which places a demand on the integrity of the remaining physical barriers. A substantial quantity of radioactive material is one which if released could result in the consequences specified in the societal risk Target 9.*

Total risk of 100 or more fatalities	Target 9
The targets for the total risk of 100 or more fatalities, either immediate or eventual, from accidents at the site resulting in exposure to ionising radiation, are: BSL: 1×10^{-5} pa BSO: 1×10^{-7} pa	

5. **France (IRSN)**

In the ASN Guide n°22 [27] on PWR design, DEC (A and B) situations are defined as situations with initiating events that are more complex or more severe than those considered in the design reference envelope.

Regarding DEC-B, the guide refers to fuel meltdown.

6. **Korea** (KINS)

Nuclear Safety Act
Article 2 (Definitions)

25. "Accident management" shall mean the actions taken to recover a nuclear reactor to a safe condition in the event of an accident at a reactor facility by mitigating the impact of an accident while preventing its proliferation. It also includes the management of an accident (hereinafter referred to as the "severe accident") that causes remarkable damage to the reactor core in excess of the design basis defined by the Korea Nuclear Safety and Security Commission.

7. Japan

"Severe Accident" refers to the serious events designated in the Ordinance of Nuclear Regulatory Authority, such as serious damage of the reactor core of the power generating nuclear reactor.

8. **China**

In the Appendix of '***Safety regulations for design of nuclear power plant'(HAF102-2016 [34])***, the definition of accident management and severe accident as follows:

accident management. The taking of a set of actions during the evolution of a *beyond design basis accident*:

(a) To prevent the escalation of the *event* into a *severe accident*;

Appendix G: Contributors to the Report

The DSA-WG was established to develop common position statements and areas of enhanced cooperation where practicable to inform near term SMR projects being undertaken by member states. This working group is composed of volunteer representatives from the following IAEA member states who are also members of the SMR Regulators' Forum:

Contributor	Country	Institution
Jerry Ismael (Chair)	UK	Office for Nuclear Regulation (ONR)
Aurelian Tanase (Co-chair)	Canada	Canadian Nuclear Safety Commission (CNSC)
Sebastien Israel	France	Institut de Radioprotection et de Sûreté Nucléaire (IRSN)
Nina Lahtinen	Finland	Radiation and Nuclear Safety Authority (STUK)
Sergey Sinegribov	Russian Federation	Federal Environmental, Industrial and Nuclear Supervision Service of Russia (Rostechnadzor)
Majid Shah Wali	Saudi Arabia	King Abdullah City for Atomic & Renewable Energy (KACARE)
Seung Hun Yoo	Republic of Korea	Korea Institute of Nuclear Safety (KINS)
Jinkun Wu	China	National Nuclear Safety Administration (NNSA)
Marcel de Vos	Canada	Canadian Nuclear Safety Commission (CNSC)
Diego Lisbona	UK	Office for Nuclear Regulation (ONR)
Palmiro Villalibre Ares	IAEA	International Atomic Energy Agency (IAEA)

Appendix H: Abbreviations used in this report

AOO:	Anticipated Operational Occurrence
BDBA:	Beyond Design Basis Accident
CCF:	Common Cause Failures
CDF:	Core Damage Frequency
CFR:	United States Code of Federal Regulations
CNSC:	Canadian Nuclear Safety Commission
CORDEL:	Cooperation in Reactor Design Evaluation and Licensing
CRDM:	Control Rod Drive Mechanism
DBA:	Design Basis Accident
DEC:	Design Extension Conditions
DID:	Defence in Depth
DSA-WG:	Design and Safety Analysis Working Group
EPZ:	Emergency Planning Zone
FOAK:	First of a Kind
LRF:	Large Release Frequency
LWR:	Light Water Reactor
HTGR:	High Temperature Gas-Cooled Reactor
IAEA:	International Atomic Energy Agency
I&C:	Instrumentation and control (also commonly known as C&I)
IRSN:	Institut de Radioprotection et de Sûreté Nucléaire (Technical Support Organization to the nuclear regulator for France)
MUPSA:	Multi-unit Probabilistic Safety Assessment
MWe:	Mega-Watt, electrical
NOAK:	Nth of a Kind (where N is any number above 1)
NPP:	Nuclear Power Plant
ONR:	Office for Nuclear Regulation (The nuclear regulator for the United Kingdom)
OPEX:	Operating experience (from events)
PSA:	Probabilistic Safety Assessment
R&D:	Research and Development
RIDM:	Risk-Informed Decision Making

SFC: Single Failure Criterion

SMR: Small Modular Reactor.

SSC: Structures, systems and components

STUK: Säteilyturvakeskus -The Radiation and Nuclear Safety Authority (The nuclear regulator for Finland)

US NRC: United States Nuclear Regulatory Commission

WENRA: Western European Nuclear Regulator's Association