Small Modular Reactors Regulators' Forum:

Design and Safety Analysis Working Group

Report on Multi-unit/Multi-module aspects specific to SMRs

INTERIM REPORT

15 December 2019

SMR RF – Design and Safety Analysis Working Group
Report on Multi-unit/multi-module aspects specific to SMRs

TABLE OF CONTENTS

SMR RF – Design and Safety Analysis Working Group
Report on Multi-unit/multi-module aspects specific to SMRs

Executive Summary

The IAEA 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 the previous years. The three topics covered in the second phase are:

- licensing issues
- design and safety analysis
- manufacturing, commissioning and operations

This report concerns design and safety analysis issues specific to multi-unit/multi-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 design and safety analysis working group note 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, 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.

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.

SMR RF – Design and Safety Analysis Working Group
Report on Multi-unit/multi-module aspects specific to SMRs

1 Background

The design and safety analysis working group is composed of volunteer representatives from the following IAEA Member States who are also members of the SMR Regulators' Forum:

- United Kingdom – ONR
- Canada – CNSC
- France – IRSN
- Finland – STUK
- Korea – KINS
- Russian Federation – Rostechnadzor
- Saudi Arabia – NRRC

This working group seeks to develop the work undertaken in the pilot project focusing on SMR related regulatory challenges for which it is considered that value can be added over a 2-3 year timescale. The focus of this working group is on those design and safety analysis issues considered highly relevant and preferably unique to SMRs, such as use of passive and inherent safety features, design extensions conditions and the concept of practical elimination, as well as potential safety challenges relevant for the first of a kind plant or multi-units/multi-modules SMRs.

2 "Multi-unit" vs "Multi-module"

The pilot project report of SMR Regulator's Forum [1] 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 previous report suggested to interpret an SMR "module" as "nuclear installation" or nuclear steam supply system, rather than "plant". From the SMR definition adopted by the working group , 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[1] and USNRC 10 CFR 50 Appendix A and 10 CFR 52.1[2].

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) 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 of "*multiple module's unit*" and "*reactor module*" in the framework of applicability of the IAEA design safety requirements (SSR-2/1(Rev. 1), 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.

[1] In terms of nuclear energy **a unit** is a single reactor at a multi-reactor nuclear power plant
[2] 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.

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. "

WG Common Position

The Design and Safety Analysis WG acknowledge that SMR designers use the term "modular" to denote both "modular design approaches" (consistent with the definition aforementioned) and/or "modular construction approaches" [2], [3], [4]. However, regardless how the modules/units are defined for any particular design, the WG agreed on 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.

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

The previous defense-in-depth (DID) WG [1] 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 [1] noted that although SMR concepts are 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, 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

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 [1] and several relevant papers, presentations and meeting materials.

3.1 Defence in depth

The DID WG [1] 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) 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).

WG Common Position

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.

3.2 Internal and external hazards

SSR2/1 (rev. 1) 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 or SSG-18. 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.

WG Common Position

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 neighboring operating unit or the safety consequences are properly considered. The current requirements usually refers specifically to "units", however the WG considers that its underlying principles are applicable to all SMR designs containing multiple reactor cores, regardless of their nomenclature (i.e. "multiple unit' or "multi module")

3.3 Selection of initiating events

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).

WG Common Position

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.

3.4 Shared SSCs

Typically, the current requirements and guidance limits the sharing of SSCs important to safety between reactors. 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 reactors 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 the Appendix A of this document.

WG Common Position

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

3.5 Risk Assessment for multi-unit/multi-module sites

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 [25]. 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 typically based on an informed judgment taking into consideration a broad range of qualitative and quantitative information. Whole-site PSA is distinguished as a supporting tool and

subset of whole-site risk assessment, and plays a complementary role to other factors in the management of risk. [24].

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 [18] and [25] 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.

WG Common Position

The design and safety analysis working group 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).

3.6 Human factors

The current regulatory guidance addressing specific safety aspects regarding human factors for multi-units is scarce. The IAEA NS-G-2.14 includes expectations dealing with sharing of responsibilities between the shift supervisor and units supervisors: "In multiunit 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 human 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;
3) operating strategies;
4) required interactions among personnel;
5) staffing demands associated to the required tasks; and
6) staffing strategies under all operating conditions including normal operation, anticipated operational occurrences (AOO), design basis accidents (DBA) and emergency conditions

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 unit, under all operating states including normal operations, AOO, DBA and emergency conditions.

3.7 Emergency preparedness

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 (EPZ) 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.

WG Common Position

The design and safety analysis 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.

References

1. *Pilot Project Report*: *Considering the Application of a Graded Approach, Defence-in-Depth and Emergency Planning Zone Size for Small Modular Reactors*, SMR Regulator's Forum, January 2018
2. *Small Modular Reactors: Nuclear Power Fad or Future?*, D.T. Ingersoll, Woodhead Publishing, 2017, ISBN: 978-0—08-100252-0
3. *Handbook of Small Modular Nuclear Reactors*, D. Carelli and D.T. Ingersoll, Woodhead Publishing, 2016, ISBN: 978-0-85709-853-5
4. *Advances in Small Modular Reactor Technology Developments, A Supplement to: IAEA Advanced Reactors Information System (ARIS)*, http://aris.iaea.org, September 2018
5. IAEA SSR-2/1 (Rev. 1), *Safety of Nuclear Power Plants: Design*, Vienna, 2016
6. IAEA-TECDOC-1570, *Proposal for a Technology-Neutral Safety Approach for New Reactor Designs*, Vienna, September 2007
7. IAEA SSG-3, *Development and Application of Level 1 Probabilistic Safety Assessment for Nuclear Power Plants,* Vienna, 2010
8. IAEA SSG-34, *Design of Electrical Power Systems for Nuclear Power Plants,* Vienna, 2016
9. IAEA NS-G-1.4, *Design of Fuel Handling and Storage Systems in Nuclear Power Plants,* Vienna, 2003
10. IAEA NS-G-1.6, *Seismic Design and Qualification for Nuclear Power Plants,* Vienna, 2003
11. IAEA NS-G-1.7 *Protection Against Internal Fires and Explosions in the Design of Nuclear Power Plants*, Vienna, 2004
12. IAEA NS-G-1.9 *Design of the Reactor Coolant System and Associated Systems in Nuclear Power Plants*, Vienna, 2004
13. IAEA NS-G-1.10 *Design of Reactor Containment Systems for Nuclear Power Plants,* Vienna, 2004
14. IAEA NS-G-2.2 *Operational Limits and Conditions and Operating Procedures for Nuclear Power Plants*, Vienna, 2000
15. IAEA NS-G-2.14 *Conduct of Operations at Nuclear Power Plants*, Vienna, 2008
16. IAEA NS-G-2.15 *Severe Accident Management Programmes for Nuclear Power Plants*, Vienna, 2009
17. IAEA-TECDOC-626, *Safety related terms for advanced nuclear plants*, September 1991
18. Summary Report of the International Workshop on Multi-Unit Probabilistic Safety Assessment, CNSC, November 2014
19. Responses on the survey questions – principle of separation/segregation , Finland, January 2019
20. Responses on the survey questions – principle of separation/segregation , South Korea, January 2019
21. Responses on the survey questions – principle of separation/segregation , UK, February 2019
22. Responses on the survey questions – principle of separation/segregation , France, March 2019
23. Update on Whole Site Probabilistic Safety Assessment (PSA) – CMD 17-M64.1, Ottawa, December 14, 2017

24. Whole-Site Risk Considerations for Small Modular Reactors, J. Vecchiarelly, C. Lorencez and G. Archinoff, 1st International Conference on Generation IV and Small Modular Reactors, Ottawa, November 2018
25. Exploring the Need for Standard Approaches to Addressing Risk Associated with Multi-Module Operation in Plants Using Small Modular Reactors, M. A. Caruso, U.S. Nuclear Regulatory Commission

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

An important consideration from [18] 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 Principals (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 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-units 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 [23]. 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 and RD-367).

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-analyze 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: Survey Question

How would member regulators interpret requirements on separation and segregation of systems important to safety in a small footprint, given a lower overall plant risk?

Canada	In the CNSC regulatory framework, separation is recognized as a safety design principle and is invoked in various contexts, such as: - protection against common cause failures and achievement of the necessary reliability for items important to safety. This requirement is outlined in Section 7.6.1 of, REGDOC 2.5.2 Design of Reactor Facilities: Nuclear Power Plants. Section 7.6.1 states that "*The potential for common-cause failures (CCFs) of items important to safety shall be considered in determining where to apply the principles of separation, diversity and independence so as to achieve the necessary reliability. Such failures could be a design deficiency, a manufacturing deficiency, an operating or maintenance error, a natural phenomenon, a human-induced event, or an unintended cascading effect from any other operation or failure within the plant.*" - A means to support demonstration of very low likelihood (i.e. practical elimination) of Design Extension Condition (DEC) scenarios with significant releases. In the guidance of Section 7.3.4 of REGDOC 2.5.2 it is stated: *"The necessary high confidence in low likelihood should, wherever possible, be supported by means such as:* • *multiple layers of protection* • *application of the safety principles of independence, diversity, separation, redundancy* • *use of passive safety features* • *use of multiple independent controls "* - Fire protection, both as physical barriers and spatial separation. Fire separation shall be provided in accordance with the requirements from CSA N293, *Fire protection for nuclear power plants*. In general, it is expected that the layout of SSCs shall be identified, coordinated and applied in the early stage of plant design in order to minimize the impact of fire. Where fire separations are used, the fire resistance rating shall be appropriate for the fire hazards present in a fire compartment and its adjoining fire compartments. Maintenance of these fire separations shall be in accordance with the applicable standards. - Structural layout criteria, including structural separation, expected to follow best engineering practices and lessons learned from past earthquakes. The design shall be such that separation between adjacent building/structures should be large enough to accommodate the maximum structural displacements during an earthquake, in order to avoid any contact.

Specific requirements and guidelines on separation are outlined in Section 7.6.1.1 of REGDOC 2.5.2. As such, physical separation is required between redundant divisions of safety systems, redundant divisions of safety support systems, and between safety support systems and the process systems. Separation shall apply both to equipment and to the routing of items, including electrical cables for power and control of equipment, piping for service water and tubing/piping for compressed air or hydraulic drives for control equipment. The regulatory document also requires that if physical separation by horizontal distance alone is not sufficient for some CCFs (such as flooding), vertical separation or other protection shall be provided.

In section 7.6.1.1 it is acknowledged that the physical separation may not always be possible or practical, thus it allows sharing of space by safety support system equipment, if it is justified. Specific considerations apply:

> *"Where physical separation is not possible, safety support system equipment may share physical space. In such cases, the reasons for the lack of separation and justification for the space sharing arrangement shall be explained in the design documentation.*
>
> *Where space sharing is necessary, services for safety systems and for other process systems important to safety shall be arranged in a manner that incorporates the following considerations:*
>
> 1. *A safety system designed to act as backup shall not be located in the same space as the primary safety system.*
> 2. *If a safety system and a process system must share space, then the associated safety functions shall also be provided by another safety system in order to counter the possibility of failures in the process system."*

It is also required that the design shall provide effective protection against common-cause events where sufficient physical separation among individual services or groups of services does not exist. The design authority shall assess the effectiveness of specified physical separation or protective measures against common-cause events. The physical separation may be achieved by barriers, distance (both horizontal and vertical) or a combination of the two.

Under Section 7.8.1 of RD-367 states that:

> *"The design shall provide sufficient physical separation between redundant divisions of safety systems, safety support systems and process systems.*
>
> *The effectiveness of specified physical separation or protective measures against common-cause events shall be assessed. "*

REGDOC 2.4.1 states that "*A hazards analysis (such as fire hazard assessment or seismic margin assessment) will demonstrate the ability of the design to effectively respond to credible common-cause events. This analysis is meant to confirm that the NPP design incorporates sufficient*

	diversity and physical separation to cope with credible common-cause events". Safety analysis for CCF is required to demonstrate the ability of the design to effectively respond to credible common-cause events (and to confirm that the NPP design incorporates sufficient diversity and physical separation to cope with credible common-cause events). It is noted that although the requirements for separation consider designs with small footprint, allowing not only separation by distance but also by physical barriers or a combination thereof, there are no explicit considerations about a "lower overall plant risk". The plant must be designed in a manner that demonstrates the "sufficiency" and "effectiveness" of separation to the regulator, regardless of the footprint. Such demonstration may include risk-informed considerations, consistent with the application of alternative or graded approaches, allowed by the current regulatory framework. It is also noted that typically SMR designs use inherent and passive safety features to a larger extent than traditional NPP designs.
UK	The UK Office for Nuclear Regulation (ONR) Safety Assessment Principals (SAPs) key principal EDR.2 articulated the high level expectations with respects to redundancy, diversity and separation for high reliability safety systems. It states that *Redundancy, diversity and segregation should be incorporated as appropriate within the designs of structures, systems and components.* Para. 180 of the SAPs provides further detail of the expectation that *The design should incorporate redundancy to avoid the effects of random failure, and diversity and segregation to avoid the effects of common cause failure.* The ONR SAPs incorporate numerous additional principals detailing expectations on segregation in connection with vulnerabilities to internal and external hazards including fire to reduce vulnerability to common cause failures. Although the SAPs do not exclude plants having a small footprint from the expectation, all UK guidance is generally subject to the principal of reducing risk As Low as Reasonably Practicable which is derived from UK legislation. SAPs para. 16 describes this: *The principles are used in helping to judge whether reducing risks to ALARP is achieved and that is why they are written using 'should' or similar language. Priority should be given to achieving an overall balance of safety rather than satisfying each principle, or making an ALARP judgement against each principle. The principles themselves should be met so far as is reasonably practicable. This has not been stated in each case to avoid excessive repetition. ONR's inspectors need to apply judgement on the adequacy of safety in accordance with HSE guidance on ALARP (see HSE website) and ONR's more detailed guidance written specifically for the nuclear context (Ref. 3)* Therefore, in the case of a small SMR footprint, regulatory judgements would need to consider the practicality of separating and segregating systems consistent with the application of the ALARP principal. The prevailing level of plant risk would be considered in this judgement.

Finland	The fundamental principle of Defence in Depth is given in the Nuclear Energy Act but the means of implementation are not stipulated at this level of hierarchy: *The safety of a nuclear facility shall be ensured by means of successive levels of protection independent of each other (safety principle of defence-in-depth). This principle shall extend to the operational and structural safety of the plant*. STUK regulations, which are binding, present high level principles to be applied to achieve the independence of DiD levels, as well as divisional separation/segregation and protection from hazards, e.g. *In order to prevent accidents and mitigate the consequences thereof, a nuclear power plant shall be provided with systems for shutting down the reactor and maintaining it in a sub-critical state, for removing decay heat generated in the reactor, and for retaining radioactive materials within the plant. Design of such systems shall apply redundancy, separation and diversity principles that ensure implementation of a safety function even in the event of a malfunction*. *Common cause failures shall only have minor impacts on nuclear power plant safety*. *The design of a nuclear facility shall take account of any internal hazards that may endanger safety. Systems, structures and components shall be designed, located and protected so that the probability of internal hazards remains low and impacts on nuclear facility safety minor. The operability of systems, structures and components shall be demonstrated in the room specific environmental conditions used as their design bases*. etc. More detailed requirements necessary to fulfill the high level principles are set in YVL guides , e.g. Safety design of a nuclear power plant, Provisions for internal and external hazards at a nuclear facility , Fire protection at a nuclear facility. In general, YVL guides aim to setting targets for plant and system design solutions rather than specifying exact solutions. An alternative solution to that provided for in the guides can be proposed, and if justified, deviations from YVL altogether can be approved in case they are well justified. Hence detailed solutions are always assessed based on the plants safety architecture and safety demonstration. For a small research reactor in Finland, a subset of regulations and guides is applied. It has been recognized lately that even if legislation and binding regulations define only high level principles and YVL guides allow a level of interpretation and flexibility, there may need to define requirements more separately for small facilities (whether meant for power production or research).
Korea	KINS's regulatory framework requires that physical separation or segregation be fundamentally provided for structures, systems and components (SSCs) important to safety, similar to other countries. Regulations on Technical Standards for Nuclear Reactor Facilities, Etc. (hereinafter the Reactor Regulations) provides the relevant provisions as follows. According to Article 44 of the Reactor Regulations, SSCs that are important to safety shall be equipped with redundancy, diversity, independence and physical separation to ensure high reliability, and shall be able to operate in case of loss of offsite or onsite power and single fault assumptions.

Article 44 (Reliability)

Structures, systems, and components that perform safety functions shall meet each of the following requirements to assure and maintain sufficiently high reliability commensurate with the importance of the safety functions.

1. The principles of redundancy, diversity, functional independence, and **physical separation** shall be adopted in the design, considering their structure, operational principles, and safety functions to be performed; and

2. The safety functions shall be accomplished in case of loss of offsite or onsite power-single failure.

The above regulatory requirements are based on nuclear reactors using active safety systems. Therefore, these requirements can be applied to active safety systems. For the all passive safety systems, single failure criteria can be applied. However, the assumption of loss of offsite or onsite power can be exempted for the passive safety systems that do not need the electrical power to operate.

The Reactor Regulations specifically require the following systems to meet physical separation requirements with redundancy, diversity and independence.

- Electric Power System (Article 24)
- Protection System (Article 26)
- Residual Heat Removal System (Article 29)
- Emergency Core Cooling System (Article 30)
- Ultimate Heat Sink (Article 31)

Regarding the physical separation of SSCs, Article 16 of the Reactor Regulation provides the requirements to prohibit the sharing of facilities.

Article 16 (Sharing of Structures, Systems, and Components)

(1) Structures, systems, and components important to safety **shall not be shared among more than two nuclear facilities**.

(2) Notwithstanding the foregoing Paragraph (1), structures, systems, and components important to safety may be shared in cases where such facilities meet all the following requirements:

1. For each nuclear facilities, all the safety requirements for the relevant shared facilities are satisfied; and

2. In the accident conditions of one of the units sharing the structures, systems, and components, an orderly shutdown, cooldown, and residual heat removal of the other units shall be achievable.

In addition, Article 15 of the Reactor Regulations provides that safety-important SSCs shall be designed to prevent damage due to environmental and dynamic effects.
Article 15 (Environnemental Effets Design Bases, etc.)

(1) The structures, systems, and components important to safety **shall be designed to meet** each of the following **requirements** in order **to prevent any damage caused by environmental and dynamic effects:**

1. They shall accommodate the effects of, and be compatible with the **environmental conditions** of normal operation, anticipated operational occurrences and design bases accidents;

2. Aging degradation caused by such environmental conditions as provided in the foregoing Subparagraph 1 shall be considered; and

3. They shall be appropriately protected against **dynamic effects, including the effects of missiles, pipe whipping, discharging fluids, and internal floods,** that may result from equipment failure inside a nuclear power unit. However, in cases where it is demonstrated that the probability of fluid system piping rupture is extremely low under the conditions consistent with the piping design basis, the dynamic effects related with postulated piping rupture may be excluded from the design basis.

(2) The following components shall be installed in such a way that prevents any damage caused by **vibrations** resulting from the circulation, boiling, and etc. of

	primary or secondary coolants: fuel assembly, moderators, reflectors, and associated supports; thermal shields; and vessels, pipes, pumps, and valves that are part of primary coolant system. According to Article 26 of the Reactor Regulations, even if a common mode failure of software occurs, the reactor protection system is required to be designed to perform safety functions. **Article 26** (Protection System) ~ 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**.
Russian Federation	
France	In the French regulatory framework, redundancy, diversity and segregation are addressed in the Order of 7th February 2012 setting the general rules relative to basic nuclear installations. The Article 3.1 of this order states that: *I. — The licensee applies the principle of defence in depth, which consists in deploying successive and sufficiently independent levels of defence aiming, with regard to the licensee, at:* - *preventing incidents;* - *detecting incidents and applying measures that will firstly prevent them from leading to an accident, and secondly restore a situation of normal operation or, failing this, place and maintain the installation in a safe condition;* - *controlling accidents that could not be avoided or, failing this, limit their aggravation by regaining control of the installation in order to return it to and maintain it in a safe condition;* - *managing accident situations that could not be controlled so as to mitigate the consequences, especially for humans and the environment.* *II. — Application of the principle of defence in depth is based chiefly on:* - *the choice of an appropriate site, with particular consideration for the natural or industrial risks weighing on the installation;* - *identifying the functions necessary to demonstrate nuclear safety;* - *a cautious design approach, integrating design margins and* ***wherever necessary introducing adequate redundancy, diversification and physical separation of the elements important for protection that fulfil functions necessary for the demonstration of nuclear safety, to obtain a high level of reliability and guarantee the functions mentioned in the preceding paragraph****;[…]*

These principles of separation and segregation are also addressed with more details in different sections of ASN-IRSN guide n°22 dealing with the design of pressurized water reactors (in the following EIP stands for "structures and components important to safety" and IP systems for "systems important to safety"):

- Section 3.3.2.1.5 (related to the Design objectives and principles associated with the design-basis internal hazards): *In application of II of article 3.1 of the order of 7th February 2012, the risks of common mode failures due to design-basis internal hazards shall be considered and, if necessary,* ***physical or geographical separations*** *shall be provided for between the redundant parts of systems fulfilling a safety function.*
- Section 4.1.1.3(related to the architecture of the safety functions): *In application of the principle of defence in depth set out in II. of article 3.1 of the order of 7th February 2012, the capability of the installation to ensure the safety functions for all the incidents and accidents shall be based on the quality of the specification, design, production and verification of each component IP on* ***the independence as far as necessary*** *between components IP or systems IP, the redundancy and diversity of the components IP or systems IP as far as necessary, and the consideration of the direct and indirect effects of the incidents or accidents for the design of the structures IP in which the EIPs are installed.*
- Section 4.1.2.1 (related to the independance between EIP)*: The architecture of the reactor safety functions shall provide sufficient independence between the levels of defence in depth […]. This requires sufficient independence between the systems IP involved in different levels of the defence in depth.*
- Section 4.1.2.2 (related to the independence between EIP)*: The independence between systems IP involved in distinct levels of defence is materialised by the independence between their constituent EIPs. The independence between EIPs shall be based on adequate implementation of:*
  - *diversification;*
  - ***physical separation or distancing;***
  - *[…]*

  in order to avoid common cause failures and failure propagation between these EIPs.

- Section 4.2.2.1 (related to the reliability of EIPs and IP systems)*: The EIP and systems IP shall be designed such that the safety functions they fulfil are ensured with due reliability in view of their role for nuclear safety. This reliability is obtained through an appropriate combination of:*
  - *design, production, installation, verification and maintenance measures;*
  - ***redundancy, separation and diversification between EIPs in order to reduce the probabilities of common cause failures****;*

Regardless the footprint, regulatory judgements should consider the sufficiency and effectiveness of separation and segregation of the EIP and IP systems. This should be assessed considering deterministic approach completer by PSA (related to hazards).

US	General Design Criterion (GDC) 5 in Appendix A of 10 CFR Part 50 provides guidance on this issue. GDC 5 is titled "Sharing of structures, systems, and components. The text of the criterion reads: "*Structures, systems, and components (SSCs) important to safety shall not be shared among nuclear power units unless it can be shown that such sharing will not significantly impair their ability to perform their safety functions, including, in the event of an accident in one unit, an orderly shutdown and cooldown of the remaining units*." Guidance is provided in the Standard Review Plan (SRP) on the application of this criterion to different SSCs of the nuclear plant, whether it is the containment, reactor system, or turbine building, etc. Even though GDC 5 is for LWRs, the language is exactly the same for the equivalent SFR-DC 5 and mHTGR-DC 5 in NRC's RG 1.232.

APPENDIX D: Representatives of the DSA Working Group

Country	Institution
Canada	Canadian Nuclear Safety Commission (CNSC)
France	Institut de Radioprotection et de Sûreté Nucléaire (IRSN)
Finland	Radiation and Nuclear Safety Authority (STUK)
Korea	Korean Institute of Nuclear Safety (KINS)
Russian Federation	Scientific and Engineering Centre for Nuclear and Radiation Safety (SEC NRS)
Saudi Arabia	King Abdullah City for Atomic and Renewable Energy (KACARE)
United Kingdom	Office for Nuclear Regulation (ONR)