SMR Regulators' Forum

Pilot Project Report:

Report from Working Group on Defence-In-Depth

January 2018

APPENDIX III - REPORT FROM WORKING GROUP ON DEFENCE-IN-DEPTH

Executive Summary

The SMR Regulators' Forum Defence-in-Depth Working Group was established to identify, understand and address key regulatory challenges with respect to defence in depth (DiD) that may emerge in regulatory activities relating to small modular reactors (SMRs). This group's work will help enhance safety and efficiency in licensing, and enable regulators to inform changes to their requirements and regulatory practices.

The DiD WG agreed that, as a fundamental principle for ensuring nuclear safety, the DiD concept is valid for SMRs and should be a fundamental basis of the design and safety demonstration of SMRs. However, since it is recognized that the DiD principles were developed for and applied mainly to large NPPs, the WG discussed their application to SMRs considering the SMR design specifics.

The working group members issued several findings that were divided into three groups: WG common positions, WG recommendations and WG observations. Opportunities to further develop safety guidance to help with the safety assessment of DiD as applied to SMRs were identified and include:

- demonstration of reinforcement of DiD levels 1 and 2
- development of safety criteria and requirements for passive safety systems and inherent safety features
- application of failure criteria for safety functions involving passive systems
- criteria for exclusion of events
- new guidance for procedures may need to be developed for inspections of the manufacturer/producer of the module
- 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-module issues in PSAs
- 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.

It should be noted that the WG members found it difficult to establish a definitive list of common SMR features due to the early stage of their development and limited publicly available detailed design information. Subsequently, the group members identified potential opportunities and challenges related to the features and the application of DiD in a general way.

The International Atomic Energy Agency (IAEA) has seen a significant increase in interest in small modular reactors (SMR) from its Member States. These reactors are being developed to provide flexible power generation for a wider range of users with cogeneration and non-electric applications. The designs include but are not limited to water-cooled reactors, high temperature gas cooled reactors, liquid metal and molten salt cooled reactors. 1

SMR designers purport to have enhanced safety performance through inherent, passive and novel safety design features. There are design options for remote regions with less developed infrastructures, factory-builds, multiple-modules, transportable floating and seabed-based units. Any of these SMR features could challenge traditional licensing processes including legal and regulatory frameworks. Some SMR features have raised questions about how the principles of defence in depth (DiD) are being incorporated into SMR designs.

[1] https://www.iaea.org/NuclearPower/SMR/

As discussed in Section 2, the WG members found it difficult to establish a definitive list of common SMR features due to the early stage of their development and limited publicly available detailed design information. Subsequently, the group members identified potential opportunities and challenges related to the features and the application of DiD in a general way. Their judgment relies on a small set of available SMR documents, and is presented without feedback from SMR designers on how they intend to apply DiD principles to SMRs. For these reasons, the list of SMR features is non-exhaustive and their implications should be considered cautiously.

Purpose

The DiD Working Group (WG) is a sub-group of the IAEA's SMR Regulators' Forum.2 Its purpose is to identify, understand and recommend ways to address key regulatory challenges with respect to DiD that may emerge in future SMR regulatory activities.

Objectives

The group aims to ensure that the integrity of the safety concept of DiD is maintained and, if possible, enhanced for SMRs. It also works to identify efficiencies for licensing, and enable regulators to consider changes, if necessary, to their requirements and regulatory practices by:

- sharing Forum Members' views and regulatory experiences
- capturing best practices and methods, and creating common understandings
- identifying and discussing common safety issues that may challenge regulatory reviews associated with SMRs and, if possible, recommending approaches for resolution

1. Scope of the DiD WG activities

As a basis for its discussions, the DiD WG mainly referred to the IAEA five-level definition of DiD as described in several references. In particular, IAEA SSR-2/1 (Rev. 1), Safety of Nuclear Power Plants: Design [A1], IAEA INSAG-10, Defence in Depth in Nuclear Safety [A2], the Nuclear Energy Agency/Committee on Nuclear Regulatory Activities booklet, Implementation of Defence in Depth in Nuclear Power Plants [A5] and the Western European Nuclear Regulators Association Safety of new NPP designs [A3]. Other basic references for DiD information can be found in Section 8.

The scope of SMR design information was mainly limited to documents available through the IAEA. It also includes member experiences. The SMR design references are included in Section 8.

SMR features have also raised questions about revising traditional requirements in such areas as control room staffing, emergency planning (in light of reduced radioactive inventory) and other site related issues. The implications of SMR design features regarding these areas are not examined in this report.

Within the Forum, it was decided that physical security and safeguards would be considered out of scope.

2. Methodology

2.1. GENERAL APPROACH

To accomplish its objectives, the DiD WG:

- identified the design features typical to SMRs that raise questions about the application of DiD principles
- identified key DiD safety principles and investigated whether each applies to all types of reactors or if some may be adapted to SMRs

[2] The SMR Regulators' Forum emerged from resolutions 9 and 12 adopted at the IAEA 57th General Conference in September 2013. Member states agreed to add language related to improving cooperation and collaboration among SMR regulators.

- surveyed participating Member States about their SMR requirements and experiences

Since DiD is a very general concept that can generate a large set of principles and requirements, the WG selected a number of key safety issues of interest in each of the five levels of DiD. For each issue, and in consideration of the SMR features, the WG made an assessment of its applicability to a broad scope of SMR designs. Given the specific design options of SMRs and the DiD principles, the following questions were proposed to focus the DiD WG discussions:

- Are the definitions of the different levels of DiD for typical large generation III reactors including Fukushima lessons learned and related safety principles fully applicable to SMRs?
- Is there a need to adapt or extend the existing DiD safety principles?

In addition to the above, the WG reviewed the survey responses related to the regulation of SMRs and the expectations for DiD. The results of the survey are summarized in Section 6.

The working group members issued several findings that were divided into three groups: WG common positions, WG recommendations and WG observations. When the WG was not able to reach a consensus, all positions were documented. The results of the WG discussions are presented in Section 5. Section 3 provides background information on DiD and Section 4 discusses SMR-specific features as identified by the WG.

2.2. CONSTRAINTS AND LIMITATIONS

The working group experienced a number of constraints and limitations. It established its scope of work accordingly and implemented other appropriate mitigation measures to address these constraints and limitations. The major constraints and limitations are discussed below.

2.2.1. Limited time available for the WG to work together

The limitation of time available for face-to-face discussion is common among international working groups. This limitation was especially constraining for this WG. Achieving the group's main objective and reaching agreement on complex issues associated with DiD in SMR designs required significant discussion.

The WG limited its review to issues of DiD related to plant design. For example, DiD as it applies to plant operations was not in scope, although some issues associated with SMR deployment, such as remote operation and post-design issues, were considered in Sections 5.4 and 5.6. The WG also limited the extent of its consideration of reduced emergency planning zone size because this topic is the subject of another working group in the SMR Regulators' Forum (i.e., the SMR WG on emergency planning zones). To address communication constraints between in-person meetings, the WG used the IAEA website SharePoint interface, video conferencing, teleconferencing and frequent email communications.

2.2.2. Limited familiarity with SMR designs and availability of design information

The development and deployment of SMRs around the world is at a very early stage in terms of maturity of technologies and varying degrees of activity occurring in WG Member States. Many regulatory bodies of participating countries have exchanged limited information with SMR designers. Consequently, most WG members have limited personal knowledge and experience with SMR designs that could be brought to the Forum at the beginning of the project. Compounding this limitation is the fact that although IAEA has a number of initiatives to collect and disseminate information on SMR designs, most detailed design information is considered proprietary by SMR vendors and not available publicly. For example, limited design information was available on safety systems. Additionally, although one member had a significant amount of information on a design being developed in its country, it was unable to share such information.

To gain familiarity with many SMR designs, WG members identified a number of documents on SMR designs and safety issues. Members also researched their own files for publicly available information on SMR designs they had received from vendors. For studies like this in the future, it may fruitful to pursue interactions with SMR designers and vendors to see if they would be willing to discuss design details with the IAEA.

2.2.3. Limited information about application of existing DiD requirements to SMRs

Perhaps the biggest constraint for the WG was the lack of information from SMR design vendors on the implications of such things as new novel design principles and features (e.g., passive systems) and whether these challenged or complemented DiD principles. For example, to what extent does a multi-module facility design include coupling of modules and sharing of systems? Are designers concluding that provisions for DiD in levels 3 and 4 can be reduced in the presence of simple "inherently safe" design features normally associated with DiD level 1? The WG could address this limitation only by drawing on information available to them from their limited interactions with designers and regulatory bodies.

It could be desirable for future Regulatory Forum activities to organize exchanges on safety information between SMR designers and regulatory bodies with their Technical Support Organizations (TSOs) to better understand and frame future SMR Regulators' Forum activities.

3. Background on defence in depth.

3.1. THE CONCEPT OF DEFENCE IN DEPTH

Defence in depth (DiD) [A1, A2, C1] is the primary means of preventing accidents in a nuclear power plant and mitigating the consequences of accidents if they do occur. DiD is 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 would be compensated for or corrected 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, as shown below, of defence aimed at preventing accidents and to ensure appropriate protection in the event that prevention fails.

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	Offsite emergency response (some onsite response may be included)

3.2. EVOLUTION OF DEFENCE IN DEPTH

DiD is based on an ancient military philosophy of providing multiple barriers of defence. Its application to nuclear power plant design appears to have been first articulated in documents published by the U.S. Atomic Energy Commission in the late 1950s and early 1960s. Indeed, WASH-740, Theoretical Possibilities and Consequences of Major Accidents in Large Nuclear Power Plants, published in 1957, stated that "the principle on which we have based our criteria for licensing nuclear power reactors is that we will require multiple lines of defence against accidents which might release

fission products from the facility." The principle was applied in nuclear power plant design in the decades that followed and the term was better defined following the Chernobyl accident that occurred in 1986.

The definition of DiD in terms of five specific levels was first described in INSAG-3, Basic Safety Principles for Nuclear Power Plants (revised as INSAG-12 [C2]), published by IAEA in 1988. INSAG-10, Defence in Depth in Nuclear Safety [A2] was published in 1996. It presented a very detailed description of DiD including a table with the objective for each level of defence and the essential means of achieving each objective. INSAG-12 [C2] was published by IAEA in 1999. It elaborates on the table of INSAG-10 introducing a link between plant states and levels of DiD. The United States Nuclear Regulatory Commission (USNRC) published Regulatory Guide 1.174, An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis, in 1998. [A20] The guide established a risk-informed regulatory framework for evaluating proposed changes to a plant's licensing basis. This framework included the concept of maintaining adequate DiD as one of its five core principles governing the acceptability of risk-informed changes to the licensing basis. In 2000, the IAEA Safety Standard NS-R-1, Safety of Nuclear Power Plants: Design [A21], adopted the concepts and terminology of INSAG-10, and recognized that DiD is a main pillar for generating safety requirements for the design of nuclear power plants (NPPs), including several requirements that explicitly address DiD. This has continued to be the case as the safety standard has been updated and improved over the years.

Today, an international consensus exists that the DiD concept should be considered as a basis for systematic safety substantiations and safety demonstrations in support of nuclear facility licensing. DiD principles and requirements are addressed in many international documents. Most notable among these is IAEA Safety Standard SSR-2/1 (Rev. 1), Safety of Nuclear Power Plants: Design [A1], which is used primarily for land-based stationary nuclear power plants with water cooled reactors designed for electricity generation or for other heat production applications (such as district heating or desalination). However, as stated in SSR-2/1 (Rev. 1), it may also be applied, with judgment, to other reactor types to determine the requirements that have to be considered in developing the design.

DiD is a key concept of the safety objectives established by the Western European Nuclear Regulators Association (WENRA) for new nuclear power plants. [A3] These safety objectives call for the reinforcement of each level of the DiD concept and the improvement of the independence of the levels of DiD defined as one of the WENRA safety objectives. The objectives also ensure that the DiD capabilities intended in plant design are reflected in the as-built and as-operated plant and are maintained throughout the plant life time.

In particular, WENRA [A3] states that new situations, such as conditions from multiple failures and core melt accidents, should be taken into account in the design of new plants. These situations are identified as design extension conditions in IAEA SSR-2/1 (Rev. 1). This is a major evolution in the range of situations considered in the initial design to prevent and control accidents, and mitigate their consequences.

More recently, the Nuclear Energy Agency (NEA)/Committee on Nuclear Regulatory Activities (CNRA) green booklet on DiD [A5]:

- addresses the main issues related to DiD that were identified by a senior-level task group on DiD through an NEA/CNRA workshop as being of prime interest for further study and clarification in a regulatory context
- discusses how DiD has been further developed in response to lessons derived from the Fukushima Daiichi NPP accident
- provides an overall discussion of the use of DiD post-accident for regulators

Key issues derived from study of the Fukushima Daiichi NPP accident are discussed further below. In addition to the NEA work, the USNRC recently published NUREG/KM-0009, Historical Review and Observations of Defence-in-Depth [A22], which provides an historical review and observations of DiD for reactors, materials, waste, security, international and other United States federal agencies.

3.3. IMPLICATIONS OF THE FUKUSHIMA DAIICHI NPP ACCIDENT ON DEFENCE IN DEPTH

The 2011 accident in Fukushima Daiichi NPP provided unique insight into nuclear safety issues, and raised many questions about the tools used at nuclear power plants, including the effectiveness of the application of DiD. Since the accident occurred there have been extensive studies of the lessons learned by many organizations including the NEA/CNRA, WENRA and IAEA. The efforts of these organizations to improve DiD in light of the Fukushima Daiichi NPP accident are summarized below.

CNRA

The CNRA senior-level task group on DiD found that the use of the DiD concept remains valid despite the Fukushima Daiichi NPP accident. The impact of the accident on the use of DiD has reinforced its fundamental importance in ensuring adequate safety. In its report, the CNRA identifies several key issues related to DiD and provides additional guidance to regulators for addressing these issues.

WENRA

In its 2013 report on the safety of new NPP designs, WENRA discusses how insights gained from studying the Fukushima Daiichi NPP accident have informed the development of positions on the DiD approach, independence of the levels of DiD, and multiple failure events. They point to the Fukushima Daiichi NPP accident as a clear indicator of the importance of properly implementing the DiD principle to ensure the reliability of safety functions and to build provisions into the designs of new NPPs to address multiple failure events and events that involve core melt.

IAEA

The IAEA has studied the Fukushima Daiichi NPP accident extensively and, like other organizations, has gained considerable insight regarding potential improvements in the implementation of the DiD principles in NPP design. Such insights are reflected in a revised version of IAEA Safety Standard No. SSR-2/1 (Rev. 1). [A1] Major revisions being considered with regard to DiD were discussed recently at an IAEA consultancy meeting on the assessment of DiD for NPPs, held December 9–11, 2015 in Vienna, Austria. They include adding new requirements to ensure that provisions necessary for achieving each of the five levels of DiD have been incorporated into the design and that the provisions for each level are as independent from those of the other levels as reasonably achievable.

4. SMR specific features

Several IAEA publications [B1, B2] highlight the variety of SMR technologies and associated features that are being developed around the world. A recent report from the Word Nuclear Association (WNA) titled Facilitating International Licensing of Small Modular Reactors, Cooperation in Reactor Design Evaluation and Licensing (CORDEL) Working Group, Small Modular Reactors Ad-hoc Group [C4] summarizes the intentions of many SMR designers and vendors. The message of the WNA is that to facilitate moving towards international licensing for SMRs, it is necessary to understand the features of an SMR design.

Many SMR features have been developed to assist the reactor designs in fulfilling niche applications (e.g., their use in isolated electrical systems on islands, for mines or remote areas, as district heating units, and for chemical processes such as desalination or oil production). The WNA report [C4] notes that facilitation of changes in international licensing for SMRs will require an understanding of the features of SMR design. It also states that some of the features are not unique in themselves, and it is only when considered collectively that they provide an understanding of the reactor type.

Consistent with IAEA references [B2, B5], the SMR Regulators' Forum members have agreed to define SMRs as reactor facilities that:

- generate less than approximately 300 Megawatt electrical (1000 Megawatt thermal) per reactor

- are designed for commercial use (i.e., for power production, desalination or process heat rather than for research and test purposes)
- are designed to allow the addition of multiple reactors in close proximity to the same infrastructure
- may be light or non-light water cooled

It is important to note that the term modular has also been applied to new large reactors. When applied to these types of reactors, it is used to denote modular construction of the entire power plant – not to the production multiple reactor modules from a design template. The following sections discuss the approach to identifying specific SMR features for inclusion in the report.

4.1. APPROACH TO THE IDENTIFICATION OF SMR SPECIFIC FEATURES

In order to establish a comprehensive list of SMR specific features for comparison against the application of DiD, it was important to have sufficient information on SMR technologies. This includes the intentions of SMR designers and vendors regarding the integration of the DiD concept with design principles such as inherent safety features and with the mitigation of severe accidents.

As a starting point for the features identification, the DiD WG referred to available information on SMR designs as referenced in Section 8. The WG members used their judgment to determine those general design features that were typical to SMRs as compared to traditional large reactor features. Features that were common to several SMRs and not related to one particular design were considered in the selection process. For each of the SMR features identified, and to stimulate discussions, group members tried to specify the design implication and the main opportunities or challenges of the feature on the application of DiD. The results of this task are provided in the detailed table of appendix A. The development of this table is summarized below.

For each feature listed in appendix A, a short description of the implication of the feature on the design was provided in the second column to facilitate a judgment of its potential impact on DiD. The third column lists any opportunity that group members judged to be positive for the application of DiD. Similarly, the fourth column lists potential challenges to the application of DiD.

The last two columns assign the most appropriate DiD level that would be impacted by the implication of the feature. These were identified by comparing the objective of the DiD level and the means of achieving it against the implication of the design feature.

4.2. SMR SPECIFIC FEATURE CATEGORIES

The SMR specific features that were considered by the WG members have been grouped into four categories: facility size, use of novel technologies, modular design and applications. These categories are not mutually exclusive. They simply provide a useful framework for identifying important SMR specific features. The key SMR specific features are listed below and discussed briefly under their general categories. Key safety issues associated with these features are discussed in Section 5.

Facility size

- smaller plant footprint (as compared to a conventional NPP)
- small power of the core
    - reduced decay heat load
    - increased core stability
    - smaller inventory of radionuclides
    - passive safety

Use of novel technologies

- passive cooling mechanisms
    - natural circulation
    - gravity driven injection

- integral design (incorporation of primary system components into single vessel)
- non-traditional or different number of barriers to fission product release
- unique fuel designs (e.g., ceramic materials, molten salt fuel)

Modular design

- compact and simplified designs
    - practical elimination of some severe accidents
    - inherent safety features (e.g., longer grace periods)
    - fewer structures, systems and components (SSCs)
        - elimination of some traditional initiating events
    - introduction of new events
        - internal to single module
        - module to module interactions
        - new construction techniques
- production, assembly and testing in factory
- multi-module facilities
    - control room staffing
    - sharing of SSCs among modules
    - modules dependence/independence
    - multi-module failure in hazards conditions

Application (siting and transportation)

- siting
    - on ground
    - underground
    - on sea
    - under water
    - movable
    - in regions lacking in essential infrastructure (e.g., electrical grid, cooling water)
- module transportation
    - during construction
    - during the operation of other modules
    - for refueling purposes in some designs

As mentioned in Section 2, the WG members found it difficult to establish a definitive list of common SMR features due to the early stage of their development and limited publicly available detailed design information. Their judgment relies on a small set of available SMR documents, and is presented without feedback from SMR designers on how they intend to apply DiD principles to SMRs. For these reasons, the list of SMR features is non-exhaustive and their implications should be considered cautiously.

4.2.1. Facility size

As expected, designers emphasized SMR facility size as a unique and important safety feature. The WG identified lower power output, smaller reactor core size and smaller facility size as the main features. The main implications included smaller fuel load and radionuclide inventory, less decay heat and smaller facility footprint.

The WG noted that the implication of each feature was not straightforward and very design dependent. Opportunities for enhancing DiD were mostly in relation to the smaller facility size, lower radionuclide inventory and lower power load which could potentially be opportunities for DiD at levels 1, 2 and 3. The main challenge for DiD was identified to be designers' desire to lessen

complementary measures, accident management and emergency response measures required at levels 4 and 5.

4.2.2. Novel features and technologies

Novel features and technologies represented the largest category of SMR specific features identified by the WG. These included non-conventional cooling methods (reactor vessel convection cooling with gas), novel vessel and component layout, non-traditional fission product barriers and unique fuel designs. Most of these features appear to be aimed at reducing challenges to DiD at levels 1 and 2. This is proposed to be done through, for example, reducing the number of SSCs available to fail, reduced reliance on active systems, and more failure-resistant fuel materials. One major challenge to DiD in this area is qualification of the novel features and technologies. Although the concept in principle could reduce challenges to DiD, design details and qualification programs were not readily available for discussion.

4.2.3. Modular design

Modular design for SMRs was purported to offer such features as compact and simplified design, improved fabrication, ease of transportability and additive modules for better power output flexibility to meet customer needs. Opportunities for DiD could be mainly related to improved fabrication and installation methods and optimized number of SSCs resulting in reduced potential for failures at levels 1 and 2. A modular design challenge to DiD could be independence between levels due to the proximity and sharing of SSCs, and the potential increase in common cause failures. The use of multiple modules could reduce the source term per module as compared to a larger plant, which could yield benefits at levels 4 and 5.

4.2.4. Facility application

SMRs can be autonomous and can be used to fill remote and isolated application niches for small communities and in industrial sites such as mines. Most challenges here are related to DiD levels 4 and 5, as local infrastructure is not likely to be in place. However, grid independence will force the SMR facility to be more self-reliant and therefore perhaps less prone to traditional initiating events such as loss of class IV power.

5. Consideration of key defence in depth safety issues for SMRs

Selection of key safety issues

Prior to the detailed discussions, WG members 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. However, it was recognized that the DiD principles were developed for, and applied mainly to, large NPPs. Consequently, the design differences and safety claims associated with SMRs as compared to large NPPs raises some questions regarding the application of DiD principles to SMRs. The following discussions consider these principles in the context of SMR features to better understand if they are fully applicable to all types of reactors or if some adaptations may be desirable for SMRs.

As mentioned in Section 2, the WG members found it difficult to establish a definitive list of common SMR features due to the early stage of their development and limited publicly available detailed design information. Subsequently, the group members identified potential opportunities and challenges related to the features and the application of DiD in a general way. Their judgment relies on a small set of available SMR documents, and is presented without feedback from SMR designers on how they intend to apply DiD principles to SMRs. For these reasons, the list of SMR features is non-exhaustive and their implications should be considered cautiously.

WG members looked at the potential implications of SMR features as challenges or opportunities for the application of DiD. This allowed the group to analyze the applicability to SMRs of some DiD principles and requirements. These were selected on the basis of safety requirements, standards and guides published by international organizations (mostly the IAEA, WENRA and the Organization for Economic Co-operation and Development (OECD/NEA)). Since DiD is a very general concept that

can generate a large set of principles and requirements, the WG members selected a number of key safety issues of interest in each of the five levels of DiD. For each selected safety issue and in consideration of the SMR features, the WG made an assessment of its applicability to a broad scope of SMR designs.

Application of defence in depth levels to SMRs

As described in Section 3, the application of the concept of DiD in the design of a nuclear power plant provides for five levels.

WG common position

Since SMRs will produce radioactive materials, it can be logically assumed that, in general, all five levels of DiD, as defined for typical large reactors in IAEA and WENRA documents, can be applied to SMRs.

The descriptions of the five levels in SSR-2/1 (Rev. 1) are very general. The point is to identify the general safety provisions expected for SMRs for each DiD level as compared to large reactors. Below are some key safety issues identified by the WG as particularly important for each DiD level. Some are valid for several DiD levels. These are further discussed in Sections 5.4, 5.5 and 5.6.

Level 1

For the first level of DiD, the objective is to prevent deviations from normal operation and the failure of items important to safety. SSR-2/1 (Rev. 1) states that to meet this objective, the plant must be soundly and conservatively sited, designed, constructed and maintained, and operated in accordance with quality management and appropriate and proven engineering practices.

The WG has identified some key issues for the application of DiD level 1 to SMRs. These include:

- site selection, as discussed in Section 5.4
- design and fabrication quality (see Section 5.5.1 for a discussion on design activities and Section 5.6 for a discussion of the importance of fabrication as it relates to post-design issues)
- the use of novel technologies and new materials as discussed in Section 4.2.2
- the role of inherent safety as discussed in Section 5.5.3
- exclusion of initiating events as discussed in Section 5.5.5
- the potential for hazards as discussed in Section 5.5.6

Note that some of these issues are traditionally discussed under level 1, but are also important for levels 2 to 4. Other cross cutting DiD issues, such as physical barriers, probabilistic safety assessments (PSAs) and multi-module issues are addressed in Sections 5.5.2, 5.5.9 and 5.5.10.

Level 2

For the second level of DiD, the objective is to detect and control deviations (postulated initiating events) from normal operational states in order to prevent anticipated operational occurrences (AOOs) at the plant from escalating to accident conditions. This second level of defence necessitates the provision of specific systems and features in the design, the confirmation of their effectiveness through safety analysis, and the establishment of operating procedures. SMR systems or features for level 2 that use novel technologies could pose a challenge for the safety analysis demonstration, as there could be limited information and qualification experience.

In addition to the issues already mentioned for DiD level 1, the WG has identified some key issues for the application of DiD level 2 to SMRs. In particular, the classification of events as AOOs as discussed in Section 5.5.5.2.

Level 3

In the third level of DiD, it is assumed that an accident could develop. This leads to the requirement that inherent and engineered safety features, safety systems and procedures be provided that are

capable of preventing damage to the reactor core or significant offsite releases and returning the plant to a safe state.

In addition to the issues already mentioned for the previous DiD levels, the WG has identified some key issues for the application of DiD level 3 to SMRs:

- the role of inherent safety, passive and active systems as discussed in Section 5.5.3
- redundancy and diversification of safety systems and engineered safety features as discussed in Section 5.5.4
- design basis accidents (DBA) and design extension conditions (DEC) without core melt as discussed in Sections 5.5.5.3 and 5.5.5.4

Level 4

The main objective of the fourth level of DiD is to mitigate the consequences of severe accidents. The most important aspect for this level is to ensure the confinement function is successful. This ensures that radioactive releases are kept as low as reasonably achievable.

In addition, for level 4, all accidents with core melt which could lead to early or large releases must be practically eliminated.

In addition to the issues already mentioned for the previous DiD levels, the WG has identified some key issues for the application of DiD level 3 to SMRs:

- DEC with core melt as discussed in Section 5.5.5.4
- practical elimination as discussed in Section 5.5.7

Level 5

The final level of DiD, level 5, has to mitigate the radiological consequences of radioactive releases that could potentially result from accident conditions. This requires the provision of an adequately equipped emergency control centre, and emergency plans and procedures for onsite and offsite emergency responses. [A1]

For level 5, SMR designers may seek relaxations due to the claim of smaller source terms as compared to large reactors. Nevertheless, the importance of level 5 has to be determined on the basis of the confinement capabilities of the reactor. Moreover, as mentioned in the NEA green booklet on DiD [A5], the Fukushima Daiichi NPP accident provided several important lessons for the implementation of level 5. It demonstrated that no matter how much we seek to strengthen other levels and practically eliminate event scenarios, effective emergency arrangements and other responses are essential to cover what is not expected.

Independence of the defence in depth levels

In international and national standards and documents, the independence of the DiD levels is considered important for enhancing the effectiveness of DiD. Section 2.13 of SSR-2/1 (Rev. 1) states that the independent effectiveness of the different levels of defence is a necessary element of DiD. It helps to ensure that a single failure or combination of failures at one level does not jeopardize DiD at subsequent levels. The WENRA report, Safety of new NPP designs [A3], states that the levels of DiD shall be "independent as far as is practicable." Lessons learned from the Fukushima Daiichi NPP accident have confirmed and reinforced the need for such a requirement. Therefore it should be applicable to SMRs as well.

Under IAEA SSR-2/1 (Rev. 1) revision 1, requirement 7 for the application of DiD, Section 4.13A states the following:

The levels of defence in depth shall be independent as far as practicable to avoid the failure of one level reducing the effectiveness of other levels. In particular, safety features for design extension conditions (especially features for mitigating the consequences of accidents involving the melting of fuel) shall as far as is practicable be independent of safety systems.

The independent effectiveness of each of the different levels is achieved by incorporating measures to avoid the failure of one level of defence causing the failure of other levels. In particular in DEC, the safety features shall be independent, to the extent practicable, of those used in more frequent accidents such as DBA.

WENRA's Safety of new NPP designs [A3] provides some guidance on the independence principle application that could be used or adapted to SMRs. In particular, the report identifies the stronger independence requirement between features necessary to cope with accidents without core melt and those necessary in case of core melt accidents. "Complementary safety features specifically designed for fulfilling safety functions required in postulated core melt accidents (DiD level 4) should be independent to the extent reasonably practicable from the SSCs of the other levels of DiD."

If the independence of the DiD levels is simple to state, its application is not straightforward and may raise questions about:

- the way to apply the independence concept of two different levels
- the interpretation of "as far as practicable"
- the acceptability of potential non-independent features that may be implemented by the designers

However, these questions are not dedicated to SMRs only. They are also valid for large reactors.

In the case of SMRs, it could be also investigated whether the SMR specific features, in particular the compact design of the modules or some design constraints, may particularly challenge the independence of DiD levels or not.

Concerning the verification of the independence, WENRA indicates "The adequacy of the achieved independence shall be justified by an appropriate combination of deterministic and probabilistic safety analysis and engineering judgment." [A3] Probabilistic safety analyses, for all modes of operation, could also be developed and used for SMRs, in particular for the verification, to the extent practicable, of the independence of DiD levels.

WG common position

The WG believes that these issues are clearly applicable to all SMR designs and should be examined because of their importance in implementing the DiD philosophy.

In the case of SMRs, it could be investigated whether the SMR specific features, in particular the compact design of the modules, the simplicity of the design or some design constraints, may particularly challenge the independence of DiD levels or not.

WG recommendation

PSA is an important tool to assess the sufficiency of independence of the DiD levels and should also be used in SMR design.

PSA aspects are discussed in Section 5.5.10.

Key safety issues related to siting

The purpose of the first level of DiD leads to requirements that the plant be soundly and conservatively sited. It requires proper evaluation and selection of a suitable NPP site. These general issues are a major concern for SMRs, since the performed reviews for SMR development [B1, B2] show the ambitions of the designers and vendors to extend the range of suitable sites for SMR installations, including underground, underwater or floating on water. Siting aspects may have important influence on the SMR safety design and different DiD levels.

The scope and level of detail of the site assessment must be consistent with the possible radiation risks associated with the facility or activity, the type of facility to be operated or activity to be conducted, and the purpose of the assessment (e.g., to determine whether a new site is suitable for a facility or

activity, to evaluate the safety of an existing site or to assess the long term suitability of a site for waste disposal) [A9].

Published IAEA standards and guides, and regulations of individual countries, cover land based stationary NPPs, research reactors and other nuclear facilities [C2]. Therefore, there is an interest in reviewing current international and national requirements and recommendations issued by groups such as the IAEA, WENRA and the USNRC concerning site evaluation and site selection to include designers' and vendors' ambitions for SMR locations and layouts. New site configurations may need to consider the evaluation of additional specific external hazards, environmental phenomena or human activities.

Some recommendations from the sixth International Project on Innovative Nuclear Reactors and Fuel Cycles (INPRO) Dialogue Forum [B5] are important to note.

- There is greater potential for SMR sites to be located where essential infrastructure is insufficient or does not exist. In this regard, site surveys and site characterizations are needed to address safety and security issues and establish plans for ensuring existing infrastructure. Guidance is needed on infrastructure considerations for reactor facilities sited in close proximity to hazardous industrial facilities. As the IAEA's NS-R-3, Site Evaluation for Nuclear Installations [B6] provides only high-level guidance, more details and associated safety guides may be useful to address the issue. Information should consider both policy-based infrastructure such as national emergency plans as well as physical infrastructure.
- Guidance from the IAEA to Member States might be useful to clarify the requirements that should address any difference between a transportable nuclear power plant and a fuel transport package. The IAEA also should facilitate a regulatory discussion to address the issue and whether to integrate shipment routes into site investigations as a basis for site acceptance or rejection. The country of origin of technology shall provide technical support in dealing with this issue.
- The report [B5] identifies "siting" related concepts "that require clarification for public understanding as follows: source term, core damage frequency, practical elimination, essential infrastructure, unacceptable potential effects of the nuclear installation on the regions (NS-R-3 § 2.25), inherently safe, and passive (safety) features. Clarification is also needed on the relationship between emergency planning and the term "inherently safe" – this is an important consideration for both the site survey and the site characterization steps. In this regard, the IAEA should consider adding this information to DS-433 and NS-R-3 to further clarify the guidance."

The question of SMR location in areas with low reliability electrical grids should also be addressed, with verification that this low reliability could be compensated by inherent safety, passive features, and very large autonomy in the design.

For multiple-unit/module plant sites, the design shall take due account of the potential for specific hazards giving rise to simultaneous impacts on several units/modules on the site.

New sites at atypical locations may require the evaluation of specific external hazards, environmental phenomena or human activities that could be important challenges for DiD level 1, (i.e., reinforcement for siting, design and plant operation).

External hazards are also discussed in Section 5.5.6.2.

WG common position

Particular attention should be paid to the characteristics of the selected sites for SMRs and to their impact on the effectiveness of DiD.

WG common position

The WG supports the positions and recommendations of sixth INPRO Dialogue Forum.

WG recommendation

The WG recommends that current international and national requirements and recommendations (such as those issued by the IAEA, WENRA and the USNRC) concerning site evaluation and site selection be reviewed and updated as necessary to include designers' and vendors' ambitions for SMR locations and layouts.

WG recommendation

Because of potential remote location of SMRs and possible different environments, a detailed analysis of possible external hazards and associated risks for SMRs should be performed for each specific SMR application and location.

Key safety issues related to design

Section 2.12 of IAEA SSR-2/1 (Rev. 1) states that the primary means of preventing accidents and mitigating their consequences is the application of defence in depth. This concept is applied to all safety related activities, whether organizational, behavioural or design related, and whether in full power, low power or various shutdown states. Note that the design activities themselves are also considered as an essential part of DiD. [A1]

More specifically for this report, Requirement 7 of IAEA SSR-2/1 (Rev. 1) [A1] clearly states that "The design of a nuclear power plant shall incorporate defence in depth." Accordingly, SMR designs should incorporate and demonstrate the effectiveness and reinforcement of all DiD levels.

Paragraph 4.11 of IAEA SSR-2/1 (Rev. 1) lists a number of design characteristics associated with DiD and design. In the following subsections, some important DiD issues related to design are selected and discussed with respect to their application to SMRs. It is recognized that the SSR-2/1 (Rev. 1) requirements were established mainly for large reactors (or without any consideration of the reactor size and type) but the WG felt that these would also apply to SMRs.

5.1. DESIGN ACTIVITIES

According to the IAEA's Fundamental Safety Principles [C1], "the prime responsibility for safety must rest with the person or organization responsible for facilities and activities that give rise to radiation risk." The licensee's responsibility includes in particular the verification of the appropriate design and of the adequate quality of facilities and activities. Requirements 2 and 3 of SSR-2/1 (Rev. 1) discuss the responsibilities of the plant designer and operating organization. While these requirements will apply to SMRs, the proposed concept of global standardization of SMR designs [C4] could make it more difficult for operating organizations to ensure these requirements are met.

The above is a well-established practice that could be an important challenge for the level and quality of the design considering the large spectra of countries and sites where SMRs may be implemented. There is an initiative by the WNA [C4], which represents most SMR designers and vendors, to optimize the licensing process by making it more international and involving the designer or vendor of the plant in the process. It is based on the application of standard design certification in which the design is assessed and verified by the regulatory body of the country of the designer or vendor with high level of competence.

In the case of a design change of the module after standard design approval (e.g., a change of the design after a large number of modules have been produced), an updated safety assessment may be required because a slight change in the design may have large effects on safety.

WG common position

Global standardization of SMR designs desired by some designers may be challenging for the licensee's responsibility.

5.2. PHYSICAL BARRIERS

Section 2.14 of SSR-2/1 (Rev. 1) states "A relevant aspect of the implementation of defence in depth for a nuclear power plant is the provision in the design of a series of physical barriers… The number of barriers that will be necessary will depend upon the initial source term in terms of the amount and isotopic composition of radionuclides, the effectiveness of the individual barriers, the possible internal and external hazards, and the potential consequences of failures."

DiD shall provide multiple levels for ensuring that each of the fundamental safety functions is performed, thereby ensuring the effectiveness of the barriers.

WG common position

The need for multiple barriers will also be required for SMRs, however, depending on the design and application of the facility, the barriers required and their effectiveness will be a discussion point in the licensing process.

For large reactors, a reactor containment structure is the main barrier for protecting the environment from the radioactive releases in case of accidents in particular severe accidents. In addition to the containment structure, complementary safety features are included in the design of the plant and procedures implemented to mitigate the consequences of core melt accidents.

WG common position

For SMRs, a main barrier for protecting the environment from the radioactive releases is also necessary to ensure the confinement function in case of accidents including severe accidents.

5.3. USE OF INHERENT, PASSIVE AND ACTIVE SAFETY FEATURES

As noted in Section 2.14 of SSR-2/1 (Rev. 1), "A relevant aspect of the implementation of defence in depth for a nuclear power plant is the provision in the design of a series of physical barriers, as well as a combination of active, passive and inherent safety features that contribute to the effectiveness of the physical barriers in confining radioactive material." [A1]

WG common position

DiD implementation requires a well-balanced safety concept that is based on the use of an optimal combination of active, passive and inherent safety features. This principle is also applicable to SMRs

Concerning the importance and role of each of these features, IAEA SSR-2/1 (Rev. 1) states that the expected behaviour of the plant in any postulated initiating event shall be such that the following conditions can be achieved, in order of priority:

(1) A postulated initiating event would produce no safety significant effects or would produce only a change towards safe plant conditions by means of inherent characteristics of the plant.
(2) Following a postulated initiating event, the plant would be rendered safe by means of passive safety features or by the action of systems that are operating continuously in the state necessary to control the postulated initiating event.
(3) Following a postulated initiating event, the plant would be rendered safe by the actuation of safety systems that need to be brought into operation in response to the postulated initiating event.
(4) Following a postulated initiating event, the plant would be rendered safe by following specified procedures.

SMRs that use extensively inherent characteristics and passive features may comply to a large extent with this statement. Indeed, SMRs designers seem to look for more extensive application of inherent and passive safety features and rely less on active safety systems in comparison with existing large reactors.

The impact of the extensive use of inherent characteristics and passive features on the relative importance of the different DiD levels for SMRs in comparison with current practice and requirements could be further investigated. In this regard, it is important to note that large nuclear power plants licensed in the United States that rely on passive safety systems also include back-up

active systems capable of performing safety functions to account for the uncertainty in passive system reliability. The ability of these active systems to perform safety functions is subject to regulatory review during the licensing phase. These active systems are subject to some operational requirements to assure a satisfactory level of reliability and availability.

5.3.1. Inherent safety features

"Inherent safety" refers to the achievement of safety through the elimination or exclusion of inherent hazards through the fundamental conceptual design choice made for the nuclear plant. Potential inherent hazards in a nuclear power plant include radioactive fission products and their associated decay heat, excess reactivity and its associated potential for power excursions, and energy releases due to high temperatures, high pressures and energetic chemical reactions." [B3]

As already mentioned, SMRs designers seem to look for more extensive application of inherent safety and respectively less reliance on safety systems. [B1, B2, C4, C5] Examples of inherent characteristics could be:

- the use of natural circulation in place of reactor coolant pumps to eliminate the hazard of pump seal failure,
- low pressure and temperature of the cooling loops,
- low core power density,
- large coolant inventory providing grace periods,
- reduction in the number, size and location of pipes that penetrate the reactor vessel to reduce the frequency and severity of pipe ruptures and
- negative reactivity coefficients over the whole operating cycle. [B4]

Inherent safety characteristics can contribute to, and reinforce, DiD. Indeed, they can eliminate or limit inherent hazards and minimize the escalation of AOOs into accidents, and thus reinforce DiD levels 1 and 2. In addition, inherent safety characteristics could also minimize the escalation of postulated initiating events into more severe conditions and thus to reinforce DiD level 3 in the prevention of severe accidents.

However, all inherent safety characteristics that are provided by the design and credited in the safety demonstration should be duly substantiated by the designers. The requirements and criteria for this demonstration should be defined beforehand and developed, which may need particular guidance.

Safety assessments of SMR designs with enhanced inherent safety characteristics may require further development of safety requirements and guides for the safety demonstration of inherent features. As many safety requirements are mostly oriented to DiD levels 3 and 4, and as the requirements for these levels have been reinforced in the light of the lessons learned from Fukushima Daiichi NPP accident, it may also be useful to further develop guidance for safety assessment of DiD levels 1 and 2.

After design, inherent safety should be guaranteed during fabrication and construction phases of the nuclear installation. As the modules of the SMRs could be fabricated and assembled in the factory, the role of the manufacturer is essential in this demonstration.

The effectiveness of the passive systems and in some cases inherent safety characteristics will have to be periodically reconfirmed during the operation of the facility. As discussed in appendix II of IAEA NP-T-2.2, Design Features to Achieve Defence in Depth in Small and Medium Sized Reactors [B4], the performance of these features could degrade by some phenomena (e.g., ageing or clogging of passive equipment).

WG common position

The regulatory body needs to seek confidence in the effectiveness, over the life time of the facility, of the inherent safety characteristics of the SMR designs. It should be investigated how the effectiveness of each inherent safety characteristic credited in the safety demonstration is guaranteed over the facility lifetime. In this respect, the requirements for the justifications of this effectiveness expected

from operators at each of the design, construction and operation stages of the SMR need to be discussed.

WG recommendation

All inherent safety characteristics provided by the design and credited in the safety demonstration should be duly substantiated by the designers. The requirements and criteria for this demonstration should be defined beforehand and developed, which may need particular guidance. As many safety requirements are mostly oriented to DiD levels 3 and 4, it is recommended to further develop guidance and requirements for safety assessment of DiD levels 1 and 2.

5.3.2. Passive systems

To achieve their safety function, passive safety systems rely on natural laws, properties of materials and internally stored energy. The concept of passivity as described in IAEA TECDOC-626, Safety related terms for advanced nuclear plants [B3] is considered in terms of four degrees or categories.

The passive safety systems concept assumes some advantages in comparison with so-called active safety systems:

- independence from external AC power supplies and safety function performance ensured in station blackout conditions
- a combination of diversified active and passive safety systems could strengthen DiD levels 3 and 4 or improve the independence of DiD levels
- passive systems are considered as less vulnerable to human error

However, the development and application of passive safety systems induces some challenges for the safety demonstration of levels 3 and 4 DiD principles:

- reliance on new innovative technologies without sufficient operational experience (see Section 5.5.8)
- challenges for the demonstration of passive systems performance and qualification, including:
    - assessment of the sensitivity of the small driving forces to uncertainties
    - methodologies and data for the quantification of the systems reliabilities
    - supporting research programs, performance tests and specific “acceptance criteria” for the qualification
    - assessment of passive system activation
    - assessment of proper function/performance of the Passive feature
- operational aspects such as periodic testing, maintenance and in-service inspections, which must be reconfirmed during facility operation to protect against degradation

WG recommendations

SMR design with enhanced use of passive safety systems requires further development of safety criteria and requirements on the level of IAEA safety standards and safety guides, WENRA recommendations and national regulations.

It should also be investigated how the effectiveness of each passive system credited in the safety demonstration is guaranteed over the facility lifetime. In this respect, the requirements for the justifications of this effectiveness expected from operators at each of the design, construction and operation stages of the SMR could be discussed.

5.3.3. Active systems

Active systems are those whose operation or function depends on an external source of power (e.g., air, electrical and hydraulic). The nuclear industry has a good history of important knowledge, practice and operational experience in the use of active safety systems for the limitation of the consequences of postulated initiating events in DBA conditions.

In nuclear energy development, preference is given to established engineering practices, and confirmation that the design has been proven in equivalent applications or operational experiences.

SMR designers wish to reinforce DiD levels 1 and 2 by design simplification, events exclusion, enhanced inherent safety and safety margins of nuclear installation, or modules. A well-balanced safety approach also requires an optimal use of innovative and proven technologies. This approach may lead to relying less on DiD level 3 and especially the role of active safety systems. However, a combination of diversified active and passive safety systems could strengthen DiD levels 3 and 4 or improve the independence of DiD levels.

WG common position

The well balanced safety approach requires further development and demonstration that postulated initiating events are reliably mitigated at DiD levels 3 and 4. For example, a combination of diversified active and passive safety systems could strengthen DiD levels 3 and 4 or improve the independence of DiD levels.

5.4. REDUNDANCY AND DIVERSIFICATION

According requirement 25 of SSR-2/1 (Rev. 1) "The single failure criterion shall be applied to each safety group incorporated in the plant design", where the term "safety group" is given the definition "the assembly of equipment designated to perform all actions required for a particular postulated initiating event." [A1]

According to the IAEA safety glossary, a postulated initiating event (PIE) is an event that can lead to anticipated operational occurrence or accident condition. Concerning passive components, Section 5.40 of SSR-2/1 (Rev. 1) requires that "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." [A1]

To fulfill these requirements, the single failure criterion must be applied for all safety systems used in DiD level 2 and, in particular, level 3 including passive safety systems. SSR-2/1 (Rev. 1) does not require application of the single failure criterion for level 4, only that the "features (used for DECs) shall have reliability commensurate with the function that they are required to fulfill." The WENRA report Safety of new NPP designs [A3] adds that this may require redundancy of the active parts.

Requirement 24 of SSR-2/1 (Rev. 1) states that "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." [A1]

Safety systems, 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 different levels or sublevels (e.g., 3a and 3b) of DiD. [A8] Regulations in some countries include requirements for diversity. Functional diversity is for instance 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 into a core melt.

SMRs use passive safety systems at level 3 to a much greater extent compared to the current Generation III large reactors. Application of single failure criteria for the passive safety systems should be further developed on the level of the IAEA safety standards and safety guides. This is coupled with the passive system safety demonstration and lack of operating experience. Because of the uncertainties in the reliability and challenges of the safety demonstration of passive systems, it may be preferable to use a combination of passive and active systems to ensure a safety function. This would also provide additional diversification to cope with common cause failures.

Diverse features should be included in the design to prevent a design basis accident with a CCF from developing into a core melt accident.

WG recommendation

Application of single failure criteria for the passive safety systems should be further developed on the level of the IAEA safety standards and safety guides.

Diverse features should be considered in the design to prevent a design basis accident with a CCF to develop into a core melt accident.

5.5. PLANT STATES

Plants states currently covered in IAEA SSR-2/1 (Rev. 1) include:

- normal operation
- AOO
- accidental conditions (i.e., DBA and DEC)

For SMRs, similar categories of plant states are expected, however with specifics in terms of operation modes (e.g., module transportation) and list of postulated initiating events.

The normal operation is defined in IAEA Safety Reports Series No. 48, Development and Review of Plant Specific Emergency Operating Procedures [C7] as a plant operation within specified operational limits and conditions, such as the operation modes of power operation, reactor shutdown, shutdown operation, startup, maintenance, testing and refueling operation. For SMRs, all these operation modes may vary from current practices. In particular, specific refueling practices are expected for SMRs and could induce new risks.

The multi-module nature of some SMRs could affect refueling activities. For example, some designs may use the staggered refueling method in which the shutdown of a single module for refueling does not require shutdown of the other modules. This means that a module can be in refueling state while the other modules in very close proximity are still producing power.

WG recommendation

Due to novel operation and application of SMRs, operation modes should be completely characterized in terms of activities and performance of equipment and humans. During the safety assessment, particular attention should be paid to assuring that all the DiD levels are implemented adequately for all operation modes.

The WG also identified some issues for DBA and DEC that are presented in Sections 5.5.5.3 and 5.5.5.4.

5.5.1. Exclusion of events

SMR design options and features may reinforce the prevention of some incidents and accidents. The tendency of SMR designers seems to be to exclude or limit some initiating events (e.g., some types of loss-of-coolant accidents due to system and equipment design). It could be considered as important reinforcement of the DiD levels 1 and 2. Even if some initiating events are considered to be excluded by the designer, the exclusion should not be used to justify omission of a complete DiD level. This is also discussed in Section 5.5.7.

Requirement 16 of IAEA SSR-2/1 (Rev. 1) for selection of PIEs and Section 5.10 for exclusion of initiating events should also be applied for SMRs:

> IAEA SSR-2/1 (Rev. 1), Requirement 16 says “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.”

> IAEA SSR-2/1 (Rev. 1), Section 5.10 says "A technically supported justification shall be provided for exclusion from the design of any initiating event that is identified in accordance with the comprehensive set of postulated initiating events."

The available information from the SMR designs [B1, B2, B4] does not present systematic selection of PIEs or technically supported justification of exclusion of some initiating events. Description of the plant operational states is limited, and the initiating events that occur in low power or shutdown states have not been presented in literature to date.

Demonstration of the integrity of the SMR module itself should be defined as first priority in this process, because the module is the critical component on which all the SMR safety functions rely. The assessment of the integrity of the primary coolant system should include a systematic approach in order to address/consider all the connections between the module and the safety systems as well as the systems for normal operation, and in the case of pressurized-water reactors (PWRs), the possibilities of steam generator tube ruptures. The publicly available SMR documentation is usually not detailed enough for review of the connections.

WG recommendation

Rules for excluding identified initiating events from the design are not established for SMRs. The IAEA should develop guidance on how to justify the exclusion of initiating events from the design. In particular such guidance should consider applications to SMRs.

5.5.2. Anticipated operational occurrences

The IAEA defines an AOO as an operational process deviating from normal operation which is expected to occur at least once during the operating lifetime of a facility but which, in view of appropriate design provisions, does not cause any significant damage to items important to safety nor lead to accident conditions.

Connections and shared systems between modules could lead to new types of AOOs (e.g., AOOs occurring at several modules at the same time, or an AOO at one module inducing an AOO or even a DBA at another module). The WG evaluation and recommendations regarding multi-modules issues are given in Section 5.5.9.

5.5.3. Design basis accidents

According to the DiD principle for the postulated events that cannot be considered as "excluded", safety features have to be implemented to mitigate their consequences at DiD level 3. PIEs are not described in detail in the available documents from SMR designers. These documents essentially point out the potential for excluding events. In the same way, the safety features that will be implemented to mitigate the postulated events are not described in detail in the available documentation on the module itself.

Despite the efforts on prevention of accidents for SMRs, designers should demonstrate that they have developed safety features to mitigate PIEs and provide justifications of their effectiveness.

Designers wish to create a module that envelopes all classical, well known primary circuits. For this approach, a classical PWR list of PIEs seems no longer applicable in its totality. This design should be verified against new possible internal initiating events inside the module and new types of initiating events in view of the module safety.

It is important that SMR designers demonstrate that they have developed and applied a systematic approach for identifying PIEs that may occur considering the design specifics of their SMRs and taking into account all the plant states. Reviewing the list of PIEs for other designs is necessary but not sufficient, since each SMR design is specific. Some techniques reported for some new designs in the U.S. include use of formal Failure Modes and Effects Analysis and system engineering studies of the failure modes on each system by the system engineer with lead for the system design.

Designers should demonstrate that they have developed safety features to mitigate PIEs and justify their effectiveness.

WG recommendation

Designers should demonstrate that they have developed and applied a systematic approach for identifying PIEs that may occur considering the design specifics of their SMRs and taking into account all the plant states.

Designers should demonstrate that they have developed safety features to mitigate PIE and provide justifications of their effectiveness.

5.5.4. Design extension conditions

DECs were introduced in international requirements in the 2000s and gained more focus after the Fukushima Daiichi NPP accident. [A1, A3] Several types of accidents are grouped as DECs, requiring different kind of measures. IAEA SSR-2/1 (Rev. 1), Rev.1 defines DECs as "Postulated accident conditions that are not considered for design basis accidents, but that are considered in the design process for the facility in accordance with best estimate methodology, and for which releases of radioactive material are kept within acceptable limits. Design extension conditions comprise conditions in events without significant fuel degradation and conditions in events with core melting." [A1]

The definition of DEC is not yet universal. The CNRA green booklet [A5], for example, includes as one type of DECs internal and external events more severe than those considered in the design basis. In the IAEA terminology, a DEC is a postulated plant state that is determined by a postulated sequence of events [A8]. In this report, specific aspects related to internal and external hazards are described in Section 5.5.6.

Events without significant fuel degradation

Sequences involving a postulated initiating event that involves a common cause or common mode failure of and resulting in multiple failures in the safety system designed for coping with the event concerned are particularly important DECs.

The typical method to cope with initiating events that involve a common cause failure is to add diversity to the design. According to IAEA NP-T-2.2, all SMR designs have diverse reactor shutdowns. Most have diverse heat removal systems, some also have diverse heat sinks. Reactor shutdown is the most important safety function, because all safety systems are dimensioned assuming that the reactor shutdown succeeds. Therefore, SMRs must have diverse means for reactor shutdown. Additional diverse features should be considered in the design to prevent a design basis accident (level 3) with a CCF to develop into a core melt accident (see Section 5.5.4).

DECs also include events with combinations of failures selected on the basis of deterministic analysis, probabilistic risk assessment or engineering judgment.

For Generation III reactors, these so-called complex sequences include such initiating events as uncontrolled boron dilution in PWRs, multiple steam generator tube rupture or steam generator tube ruptures induced by main steam line breaks. [A8] These types of sequences should also be identified for SMRs and if significant, appropriate measures should be designed against them. The establishment of these sequences is plant specific and requires a PSA covering all operating states.

A PSA covering all operating states should be developed already in the design stage to identify those areas of the design in which the introduction of safety features for DEC may help to reduce the probability of core melt accidents, and balance the contribution to risk of different accident sequences. [A8]

Events with core melting

These events include severe reactor accidents (i.e., accidents involving core damage or fuel melt) and severe spent fuel storage accidents.

Sections 5.30 and 5.31 of IAEA SSR-2/1 (Rev. 1) state that "the containment and its safety features shall be able to withstand extreme scenarios that include, among other things, melting of the reactor core. These scenarios shall be selected by using engineering judgment and input from probabilistic

safety assessments. The design shall be such that the possibility of conditions arising that could lead to an early radioactive release or a large radioactive release is practically eliminated." [A1] Section 4.13A also states that "In particular, safety features for design extension conditions (especially features for mitigating the consequences of accidents involving the melting of fuel) shall as far as is practicable be independent of safety systems." [A1]

Descriptions of current SMR designs [B1, B2, B4] indicate that designer efforts seem to be oriented towards severe accident prevention based on reinforcement of DiD levels 1, 2 and 3. Despite these efforts, independent features for severe accident mitigation (DiD level 4) should be included in the design of SMRs in order to ensure the successive levels of DiD remain.

WG recommendation

So-called complex DEC sequences should be identified for SMRs and if significant, appropriate measures should be designed against them. For this plant-specific identification, a PSA covering all operating states is necessary.

Despite the efforts to prevent severe accidents, independent features for severe-accident mitigation (level 4) should be included in the design of SMRs in order to ensure the successive levels of DiD.

5.5.6. Internal and external hazards

Internal and external hazards are important challenges for the DiD levels and for the independence of the levels. They can cause common mode failures that could impact the safety features involved at one DiD level and even simultaneously affect several DiD levels.

According to IAEA SSR-2/1 (Rev. 1), all foreseeable internal hazards and external hazards, including the potential for human induced events that could directly or indirectly affect the safety of the nuclear power plant shall be identified and their effects shall be evaluated. Hazards shall be considered for the determination of the postulated initiating events and of generated loadings for use in the design of relevant items important to safety for the plant. [A1]

The most recent revision of IAEA SSR-2/1 (Rev. 1) incorporates the lessons learned after the Fukushima Daiichi NPP accident especially in terms of reinforcement of safety in internal hazards and external hazards conditions.

The accident in Fukushima Daiichi NPP demonstrated that it is vital to consider the impact of common cause and common mode failures when implementing the concept of DiD, particularly from external hazards, as they can lead to a loss of several levels of DiD safety provisions or significantly reduce independent effectiveness. [A5]

WG common position

IAEA, OECD, NEA and WENRA experiences and lessons learned after the Fukushima Daiichi NPP accident with regard to the reinforcement of safety in view of internal and external hazards should be applied to SMR design.

5.5.6.1. Internal hazards

An NPP should be designed with adequate physical separation (e.g., by barriers, by distance or both) to protect the safety features implemented at each of the DiD levels against all potential internal hazards (such as fires, explosions and floods).

Internationally available documentation on SMRs [B1, B2, B4] does not present in detail the list of postulated internal hazards, how they are considered in the design and the provisions foreseen to protect the safety functions against such hazards.

WG recommendation

The list of internal hazards taken into account in the safety demonstration should be justified by SMR designers, considering all SMR design specifics. All potential internal hazards that may occur within the module or in areas common to multiple modules should be considered.

Provisions should then be defined to protect the safety functions against such hazards and avoid common cause failures (e.g., physical or geographical separation). As constraints may be induced for SMRs due to their small sizes and compact modular designs, particular attention should be paid to these provisions from the early stage of SMRs design.

Particular attention should be paid in SMR design to potential common mode failures due to internal hazards (such as fires, explosions, internal flooding and load drops) and to their influence on DiD levels effectiveness and independence, taking into account the SMR design specifics (e.g., modularity, compact design and multi-units).

As stated in IAEA SSR-2/1 (Rev. 1), for multiple unit 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. [A1] This statement is particularly applicable to multi modules/units SMRs.

WG recommendation

The multi modules/units aspect of SMRs should be considered in the internal hazard safety assessment, particularly in terms of:

- propagation of internal hazards from one module to another (e.g., fire propagation)
- the impact of operating activities of one module on the risk of internal hazard of other modules (e.g., the risk of load drop due to the refueling of one module)

These aspects are also addressed in Section 5.5.9.

5.5.6.2. External hazards

Like typical large reactors, SMRs could be threatened by their environments. Therefore, the risks of external hazards – natural or man-induced – should be taken into account in the safety assessment of SMRs, considering their specific location and environment.

WG recommendation

Because SMRs may be located remotely or in many different environments, a detailed analysis of possible external hazards and associated risks for SMRs should be performed for each specific application.

As stated in IAEA SSR-2/1 (Rev. 1), for multiple unit 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. [A1] Concerning the simultaneous impacts of external hazards on several units, WENRA states that "On multi-unit sites, the plant should be considered as a whole in safety assessments and interactions between different units need to be analyzed. Hazards that may affect several units need to be identified and included in the analysis." [A3]

These statements are particularly applicable to multi modules/units SMRs in case of external hazards. These aspects are also addressed in Section 5.5.9.

WG recommendation

The multi modules/units aspect should be considered in the external hazard safety assessment.

Taking into account the lessons learned from the Fukushima Daiichi NPP accident, IAEA [A1], OECD [A5] and WENRA [A3, A13] documents emphasize the reinforcement of DiD principles and in particular the need to address severe external hazards. IAEA SSR-2/1 (Rev. 1) requires that "The design of the plant shall also provide for an adequate margin to protect items ultimately necessary to prevent an early radioactive release or a large radioactive release in the event of levels of natural hazards exceeding those considered for design, derived from the hazard evaluation for the site." [A1]

WG common position

Considering the lessons learned from Fukushima, SMRs should include in their design adequate margins against external hazards as derived from the site evaluation to guard against uncertainties and to avoid cliff edge effects.

5.5.7. "Practical elimination" concept

WENRA's Safety of new NPP design [A3] includes that accidents with core melt which would lead to early or large releases have to be practically eliminated. Here "early release" means situations that would require offsite emergency measures, but with insufficient time to implement them. "Large release" situations would require protective measures for the public that could not be limited in area or time. The objective includes also nuclear fuel at fuel pools and storage locations and severe degradation mechanisms other than melting, (e.g., severe reactivity increase accidents). IAEA SSR-2/1 (Rev. 1) [A1] requires that the design shall be such that design extension conditions that could lead to significant radioactive releases are 'practically eliminated'. The OECD/NEA/CNRA Implementation of Defence in depth in Nuclear Power Plants following the Fukushima Daiichi NPP accident [A5] states that practical elimination of significant radioactive releases should be addressed in the design of new plants and can be applied to both prevention and mitigation safety measures. IAEA TECDOC-1791, Considerations on the Application of the IAEA Safety Requirements for the Design of Nuclear Power Plants [A8] has a chapter on the concept of practical elimination.

WG common position

SMRs, as well as other types of new reactors, must meet the IAEA SSR-2/1 (Rev. 1) requirement of practical elimination of accidents which would lead to significant releases.

According to IAEA SSR-2/1 (Rev. 1) [A1], the possibility of certain conditions arising may be considered to have been 'practically eliminated' if:

- it 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

Practical elimination of an accident scenario or more than one scenario should not be claimed solely based on compliance with a probabilistic cut-off value. Practical elimination should be primarily justified by design provisions, in some cases also strengthened by operational provisions (e.g., adequately frequent inspections). The safety measures supporting practical elimination must be available throughout the life of the plant and for all fault sequences or circumstances that may affect them. This may be difficult where the form of the additional safety measure does not lend itself to inspection, testing or maintenance. To apply the concept, the phenomena must be well understood and the actions proposed must be adequately supported by experiments, testing, theory and analysis. Similarly, the development of the design must be adequately based on criteria such as appropriate design codes and choices of materials. [A5]

Accident sequences that are practically eliminated have a specific position in the DiD approach because mitigation of their consequences does not need to be included in the design. The IAEA TECDOC-1791 [A8] groups the events that should be practically eliminated into five categories:

1. events that could lead to prompt reactor core damage and consequent early containment failure
2. severe accident phenomena that could lead to early containment failure
3. severe accident phenomena that could lead to late containment failure
4. severe accident with containment bypass
5. significant fuel degradation in a storage pool

The practical elimination concept should not be used to justify omission of a complete DiD level. For example, the concept should not be used to justify absence of severe accident management arrangements and capabilities that are expected at DiD level 4 or absence of offsite emergency response at level 5.

The practical elimination requirements and criteria are widely discussed in nuclear safety regulations. They should be deeply assessed using deterministic and probabilistic approaches. Expert judgment is indispensable as well. Technical guidelines for the design and construction of nuclear power plants with pressurized water reactors [A10] emphasizes that if events cannot be considered as physically impossible, design provisions have to be taken to design them out. The above guidelines are applicable to SMRs as well as large reactors.

WG common position

The practical elimination concept should not be used to justify omission of a complete DiD level. For example, it should not be used to justify the absence of severe accident management arrangements and capabilities that are expected at DiD level 4 or the absence of offsite emergency response at level 5.

5.5.8. Proven technologies

The safety case will dictate requirements necessary for Systems, Structures and Components, and therefore, point to those SSCs that require robust and proven design, versus those that are not so important [A9].

Items important to nuclear safety shall preferably be of a design that has previously been proven in equivalent applications, and if not, these items shall be of high quality and be derived from a technology that has been qualified and tested. [A1] The preference is given to the established engineering practice, which uses the design that has previously been proven in the equivalent applications or the so-called operational experience.

SMR designs are considered to be innovative technologies, since they feature many safety aspects that are not yet supported by established engineering practices and operational experiences.

Requirement 9 of IAEA SSR-2/1 (Rev. 1) states that 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 programs, performance tests with specific acceptance criteria or the examination of operating experiences 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 behavior of the plant is as expected.

As most of the proposed SMR concepts are new innovative technologies without sufficient operational experience, these requirements are very important for SMRs. Special attention should be paid to how the technologies will be qualified and tested.

Where innovative improvements beyond current practices have been incorporated into the design, it has to be determined in the safety assessment whether compliance with the safety requirements has been demonstrated by an appropriate program of research, analysis and testing complemented by a subsequent program of monitoring during operation. [A9]

WG common position

Regulatory bodies should focus attention on the proposed innovative technologies that are without operational experiences. The new features and practices shall be adequately tested before being brought into service to the extent practicable to demonstrate their qualification, and shall be monitored in service to verify that the behaviour of the plant is as expected.

WG recommendation

Requirements and guidance be established for qualification programs of new materials and features applicable to SMR designs including the extent and scale of the testing, verification and validation of models, and fabrication processes.

5.5.9. Multi-module issues

The concept of multi-modules is specific to SMRs, and thus should be considered as an important safety issue to be investigated, particularly in comparison with current practices on nuclear safety for large reactors.

5.5.9.1. Application of defence in depth for multi-unit nuclear power plants

Historically, the safety assessment and safety demonstration for large reactors are based on a single-unit safety concept. This safety assessment approach does not assume any interaction between units and only single-unit impact for consequences. For the majority of participating countries in this project, according to the survey questions, a license is given for a single unit without specific regulatory requirements for multi-units issues. However, in the United States and Canada, there are requirements related to the sharing of structures, systems or 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 issue of shared SSCs may be a challenge for the regulation of SMRs, as the smaller designs and the use additive reactor modules may lead to sharing that introduces risk significant vulnerabilities into the design.

There have been important evolutions over the last years in the expectations regarding safety assessment of multi-units, especially after the Fukushima Daiichi NPP accident. Safety considerations for sites with more than one unit are provided in several international documents. [A1, A3, A5]

Safety concerns about multi-units include the:

- impact of shared systems between several units on the site (such as for important, supporting or not important safety systems)
- simultaneous impacts of external hazards on several units on the site

Regarding the first point, in the current safety practice, each unit is fully autonomous. It features its own safety systems, safety support systems (e.g., heat sink and AC power) and control systems. IAEA SSR-2/1 (Rev. 1) Rev. 1 stipulates that "Each unit of a multiple unit nuclear power plant shall have its own safety systems and shall have its own safety features for design extension conditions." [A1]

Interconnections among the units of a multi-unit NPP are encouraged when they enhance safety. "To further enhance safety, means allowing interconnections between units of a multiple unit nuclear power plant shall be considered in the design". [A1] Further "For sites with multiple units, appropriate independence of them shall be ensured. The possibility of one unit supporting another could be considered as far as this is not detrimental for safety." [A13]

Concerning the simultaneous impacts of external hazards on several units, IAEA SSR-2/1 (Rev. 1) requires "For multiple unit 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." [A1] Additionally, WENRA states "On multi-unit sites, the plant should be considered as a whole in safety assessments and interactions between different units need to be analyzed. Hazards that may affect several units need to be identified and included in the analysis." [A3]

Multi-unit safety issues are also addressed with some interpretation in the recent NEA booklet on Implementation of Defence in depth in Nuclear Power Plants following the Fukushima Daiichi NPP accident. [A5]

5.5.9.2. "Multi-units" versus "multi-modules"

According to the limited publically available information on SMR designs, the WG observed that "multi-modules" could not be considered as equivalent to "multi-units", as with large reactors. Further, such concepts were not well defined for SMRs. For instance the "module" may or may not be autonomous and does not include individual safety systems and safety support systems such as separate heat sinks or AC power. It was observed in some designs that the control room, reactor building and ultimate heat sink, as examples, can be common to several modules. In addition, some SMRs may use a single confinement common to several modules. Therefore, the definition of SMR

"module" may be better interpreted as "nuclear installation" or nuclear steam supply system (safety classified part of the primary and secondary circuit for PWR) than as "plant".

The safety issues that should be investigated for multi-module facilities include:

- requirements for shared systems or interconnections between several modules
- impact of multi-module configurations on the risk of propagation of an AOO, a DBA or a DEC or an internal hazard from one module to other modules
- simultaneous impact of external hazards on several modules of the facility
- confinement function
- common spent fuel pool
- human and organizational aspects
- a single control room common to several modules

At this stage, the list of potential safety issues for multi-modules facilities remains open and cannot be completed until more detailed SMR design information is available.

WG observation

As the concept of SMR "module" is not equivalent to the "unit" or "plant" concept for large reactors, the safety principles developed for the "multi-units" issue cannot be transposed to "multi-modules" in SMR facilities. Therefore, the principles and requirements for the safety assessment of a "multi-module" SMR must be developed.

WG recommendation

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.

Even though the SMR concept is based on module design with small unique power, on multi module/unit sites, the SMR design should take due account of the potential consequences on several or even all units on the site simultaneously caused by specific external hazards. It may affect the methodology for EPZ assessment.

WG common position

A "multi-module safety assessment" could contribute to verifying that all common features and dependencies do not induce unacceptable effects. As discussed in Section 4.6.8, PSA methods will need to be developed in order to model the simultaneous occurrence of accident sequences leading to severe accidents involving multiple modules.

In the absence of PSA methods, the USNRC has recently established high-level guidance and qualitative criteria [B7] that applicants with small, modular integral pressurized water reactor designs may use to show that the risk from multi-module accidents is acceptably low. This guidance does not assume the availability of a PSA that can model multi-module accidents nor provide numerical acceptance criteria. Rather, it directs applicants to conduct systematic assessments to identify accident sequences that could lead to multi-module core damage and large release events. Such assessments can then be used to demonstrate that a facility has been designed so that any such accident sequences are not significant contributors to risk (e.g., practically eliminated).

5.5.10. Role of probabilistic approach

Even if the design relies firstly on deterministic bases, probabilistic safety assessments could bring about many insights about the safety of SMRs, as they have for large reactors. Experience gained from the use of PSAs has revealed that, even when carried out from the very early design stage of a reactor, PSAs are very beneficial to evaluate the application of DiD, to check that the DiD principles have been properly applied and to identify potential weak points in the design not revealed by deterministic analyses.

Indeed, relying on a systematic investigation and assessment of a large set of initiating events and sequences, PSA results help identify the dominant contributors to the risk and thus to point out key safety issues. In particular, PSA results reflect the reliability of the features implemented at each of the DiD levels and the independence of the DiD levels. They are also useful to check the sufficiency of the redundant and diversified features implemented and to verify that the risks of common cause failures are limited. PSAs could also contribute to the identification of the postulated initiating events and of the set of design extension conditions to be considered in the design.

For all these reasons, the WG position is that for SMRs, PSAs should be used to complement the deterministic approach on which the design first relies – just as they are for large reactors.

Another specific issue to be considered for SMRs is the multi-modules configuration. As mentioned in Section 5.5.9, a "multi-module safety assessment" could be needed to assess the impact on safety of the connections and shared systems among modules. The role of the probabilistic approach in this safety assessment and the methods that could be applied to carry out a site risk assessment could be investigated.

WG recommendation

For SMRs, PSAs should be used to complement the deterministic approach on which the design first relies – just as they are for large reactors.

WG observation

The methods to deal with passive features and with multi-module issues in the PSA could be enhanced (or investigated) in the context of PSA developments for SMRs.

5.6. POST-DESIGN ISSUES – IMPORTANCE OF FABRICATION

After the design phase, safety should be guaranteed during fabrication, construction, transportation, commissioning, operation and decommissioning of the installation.

The WG focused the discussions on DiD application in siting and design activities. Post-design activities were not discussed in detail. The WG has identified fabrication and transportation as specific features of many SMRs. High-quality fabrication is an important element in the success of DiD. It is noteworthy that INSAG-12 states: "A primary safety requirement is that a nuclear power plant be manufactured and constructed according to the design intent. The plant manufacturers and constructors discharge their responsibilities for the provision of equipment and construction of high quality by using well proven and established techniques and procedures supported by quality assurance practices." [C2]

For SMRs, a lot of the work is expected to be done at the factory (i.e., the fabrication of the whole module) and less on site. Therefore, there is an increasing role of the manufacturer/producer of the main equipment of the module in the factory conditions. In this context, inspections performed in the factory are particularly important and new procedures for such inspections may need to be developed.

According to international conventions and IAEA safety standards, regulating safety is a national responsibility and the prime responsibility for safety rests with the person or organization responsible for facilities. This well-established practice could be an important challenge for the level and quality of the design taking into account the large spectra of countries and sites where SMRs may be implemented.

During commissioning, it is necessary to demonstrate that the completed plant is satisfactory for service before it is made operational. This may pose specific challenges in the case of factory fueled SMRs. A well planned and properly documented site acceptance testing and commissioning program should be prepared and carried out.

WG common position

Since there is an increasing role of the manufacturer/producer of the main equipment of the module in the factory conditions, inspections performed in the factory are particularly important and new guidance for procedures for such inspections may need to be developed. A well planned and properly documented site acceptance testing and commissioning program should be prepared and carried out.

6. Sharing regulatory experiences with defence in depth among Forum Members

6.1. SURVEY OBJECTIVE

The DiD WG Member State regulators are either engaging or preparing to engage with proponents who are preparing safety cases for SMR deployment. These SMRs are anticipated to contain unique safety claims due to the inclusion of novel approaches and technologies. Some of these claims are expected to propose alternate interpretations of existing regulatory requirements as compared to large nuclear power plants. It is also possible that the proposals will contain new safety approaches where regulatory requirements may not yet exist.

This survey attempted to understand how, in each Member State, DiD requirements can be applied to alternative approaches being developed by SMR designers such that the safety principles of DiD are maintained. Alternative approaches being employed by SMR developers (for example passive and inherent features) can be similar to those being employed for larger nuclear power plants (generations III, III+ and IV). However, the use of these approaches is expected to be more intense for SMR designs with a goal by developers being to drive improvements both in efficiency of maintenance and operation and in overall safety. Of particular interest to the DiD WG is finding out where similarities and differences in practices exist in application to alternative approaches.

The results of this survey are presented to highlight similarities, differences and challenges in the application of DiD in each Member State, and to illustrate what this might mean for future SMR projects. The survey questions and Member State responses are summarized in appendix C.

6.2. RELATIONSHIP TO CNRA GREEN BOOK SURVEY

The OECD/NEA CNRA green booklet [A5] described survey results on the use of DiD among the regulatory bodies represented at CNRA. These results cover the main regulatory activities applicable to existing reactors and new large reactors, such as regulations, codes of practice and guidance, assessments of design/safety case/events/etc., inspections, enforcement/regulatory decisions and training of regulatory staff.

The DiD WG survey was concerned with regulatory framework and the industry's application of requirements focused on the SMR application. It was not clear if all countries have incorporated the lessons learned of Fukushima Daiichi NPP accident in their regulations related to DiD. The industry's application of the requirement is covered in the design management/control assessment in the green booklet survey, however, most WG Member States have not responded to the survey yet.

6.3. SURVEY RESULTS

The survey shows that all Member States apply the DiD concept to some extent in the regulations but the level of detail varies. Some use the five levels in the way specified by IAEA; others use the DiD concept as a general legislative framework.

All Member States require that NPPs are designed against external events. IAEA SSR-2/1 (Rev. 1) [A1] also requires that the design of the plant shall provide for an adequate margin to protect items ultimately necessary to prevent an early radioactive release or a large radioactive release in the event of levels of natural hazards exceeding those considered for design, derived from the hazard evaluation for the site (hazards exceeding the design basis).

None of the Member States is currently developing DiD requirements specific to SMR applications. A need is recognized to develop requirements concerning specific questions, such as passive safety features. Currently, there is no difference of design requirements between the research reactors and the commercial NPPs.

Very few responses were given to questions concerning application of DiD to specific SMR designs. This may reflect the fact that the DiD concept has not been the focus of discussion between the regulators and the designers in countries with active SMR projects. The DiD WG encourages the regulators to review the SMRs in the future by application of the DiD concept.

7. Findings, conclusions and recommendations

The DiD WG agreed that, as a fundamental principle for ensuring nuclear safety, the DiD concept is valid for SMRs and should be a fundamental basis of the design and safety demonstration of SMRs.

However, it was recognized that the DiD principles were developed for and applied mainly to large NPPs. Consequently, the design specifics and safety claims associated with SMRs as compared to large NPPs raise some questions for discussion regarding the application of DiD principles to SMRs. These SMR design specifics notably include facility size, modular design, the use of novel technologies, and SMRs applications.

It is not possible to express detailed requirements at this stage because the spectrum of SMRs is very large and because of the lack of information about SMR designs and designer intentions.

At this stage, the DiD WG identified some important issues for consideration in the evaluation of DiD for SMRs. The conclusions of the WG about the application of these issues to SMRs are presented in Section 7.1.

Among these issues, the DiD WG identified safety areas for which the opportunity to further develop safety guidance to help the safety assessment of DiD applied to SMRs may be investigated. This is presented in Section 7.2.

It could 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 as mentioned in Section 7.2.

7.1. CONCLUSIONS ABOUT THE APPLICATION OF DEFENCE IN DEPTH TO SMRs

Application of defence in depth levels

In general, all five DiD levels as defined for typical large Generation III NPPs and taking into account lessons learned from the Fukushima Daiichi NPP accident are also applicable to SMRs. Appropriate features should be included in the SMRs design at each level.

In order to ensure the successive levels of DiD, and despite the efforts of SMR designers on DiD levels 1 and 2 reinforcement, it is important to get a clear demonstration of the effectiveness of the design safety features to mitigate PIE (level 3) and of the features to mitigate severe accidents (level 4) for all operating modes.

For DiD level 5, the DiD WG is in agreement with the NEA statement that, no matter how much other levels may be strengthened, effective emergency arrangements and other responses are essential to cover the unexpected.

Independence of the DiD levels

The independence among DiD levels, as far as practicable, is considered to be an important requirement to enhance the effectiveness of defence in depth in international and national standards and documents. The Fukushima Daiichi NPP accident has confirmed and reinforced this requirement. Therefore it should apply to SMRs as well. In the case of SMRs, it could be investigated whether the SMR specific features, in particular the compact design of the modules and the multi modules design, may particularly challenge the independence of DiD levels.

Some questions raised by the application of the independence concept in SMR design could be discussed. These include in particular the interpretation of "as far as practicable" and the acceptability of potential non-independent features that may be implemented by the designers.

Siting issues

Taking into account SMR specific features, selected site characteristics could be an important challenge for DiD reinforcement.

The design shall take due account of site-specific conditions to determine the maximum delay time by which offsite services need to be available.

Siting aspects may have important influence on SMR safety design and different DiD levels due to applicable range of suitable site for SMR installations, including underground, underwater or floating on water.

New site configurations may require the evaluation of additional specific external hazards and environmental phenomena. For multi-unit/module plant sites, designs shall take due account of the potential for specific hazards giving rise to simultaneous impacts on several units/modules on the site.

Design issues

Design activities

The DiD WG identified that the tendency of global standardization and certification of SMR designs desired by some designers and proposed by WNA may be challenging for current licensees and regulators. It may require significant changes in the national licensing process.

Inherent safety and passive systems

An important challenge for DiD in SMR design is to achieve a well-balanced safety concept based on the use of optimal combination of active, passive and inherent safety features.

All inherent safety characteristics that are provided by the design and credited in the safety demonstration should be duly substantiated by SMR designers. The requirements and criteria for this demonstration should be defined beforehand and developed, which may need particular guidance. As many safety requirements are mostly oriented to DiD levels 3 and 4, it could be useful to further develop guidance and requirements for safety assessment of DiD levels 1 and 2. (See Section 7.2.)

SMR design with enhanced use of passive systems is required to develop safety criteria and requirements on the level of IAEA safety standards and safety guides, WENRA recommendations and national regulations. (See Section 7.2.)

The use of passive systems may induce new challenges: new innovative technologies without sufficient operational experiences, uncertainties related to qualification and reliability assessments, operational aspects as periodic testing, maintenance and in-service inspections. Particular attention should be paid to these issues at each of the design, construction and operation stages of SMRs. Further development of safety criteria and requirements may be necessary. This includes the application of failure criteria for safety functions involving passive systems. (See Section 7.2.)

In case of uncertainties in passive features reliability or common cause failure mechanisms in active systems, a combination of active and passive safety systems may be desirable. Such a combination could even strengthen safety function performances at DiD levels 3 and 4 and improve the independence between those two levels.

Excluded events versus postulated initiating events

The designers should demonstrate that they have developed and applied a systematic approach for identifying postulated initiating events that may occur considering the design specifics of their SMRs and taking into account all plant states.

If some initiating events are considered to be "excluded" by SMR designers, without any safety features to mitigate their consequences, sufficient provisions (e.g., design, fabrication and operation) shall be implemented and duly justified.

Criteria for exclusion of events should be established. (See Section 7.2.)

Internal and external hazards

Common mode events due to internal hazards and their influence on DiD levels independence should be considered, taking into account SMR design specifics (e.g., modules, compact design and multi units/modules aspects).

Regarding the external hazards, because SMRs may be located remotely or in many different environments, a detailed analysis of all possible hazards and associated risks for SMRs should be performed for each specific SMR application. The IAEA, OECD NEA and WENRA international experiences and the lessons learned after the Fukushima Daiichi NPP accident should also be extensively used in the design of SMRs regarding the risks of external hazards.

Moreover, multi modules/units aspect should be considered in the safety assessment of internal and external hazards.

Practical elimination

The practical elimination concept should not be used to justify omission of a complete DiD level. For example, it should not be used to justify absence of severe accident management arrangements and capabilities that are expected at DiD level 4 or in the absence of offsite emergency response at level 5.

Multi-modules issues

As the concept of SMR "module" is not equivalent to the "unit" or "plant" concept for large reactors, the safety principles developed for the "multi-units" issue cannot be transposed to "multi-modules" in SMR facilities. Therefore, principles and requirements for the safety assessment of a "multi-module" SMR should be developed. (See Section 7.2.)

It is necessary to demonstrate that for "multi-modules" facilities, connections, shared features and dependencies among modules are not detrimental to DiD. A "multi-modules safety assessment" could contribute to verifying that all common features and dependencies don't induce unacceptable effects.

Even if the SMR concept is based on modular design with small unique power on multi modules/units sites, the SMR design shall take due account of the potential consequences of several – or even all – units failing simultaneously due to external hazards. It may affect the methodology for EPZ assessment.

Role of PSAs

As for large reactors, PSAs should be used for SMRs to complement the deterministic approach on which the design relies first.

PSAs could be used to check that DiD principles have been properly applied. PSA results could reflect the reliability of the features implemented at each DiD level and the sufficient independence of the levels. PSAs could also be used for the identification of so-called complex DEC sequences and for the assessment of the risks induced by multi-modules.

Methods to deal with passive features and with multi-module issues in PSAs should be investigated or enhanced. (See Section 7.2.)

Post-design issues

After the design phase, safety should be guaranteed during fabrication, construction, transportation, commissioning, operation and decommissioning of the installation.

The DiD WG focused the discussions on DiD application in siting and design activities. Post-design activities were not discussed in detail. However, the DiD WG has identified fabrication and transportation as specific aspects to focus on for many SMRs.

Since there is an increasing role of the manufacturer/producer of the main equipment of the module in the factory conditions, inspections performed in the factory are particularly important and new guidance for procedures for such inspections may need to be developed. (See Section 7.2.) A well

planned and properly documented site acceptance testing and commissioning program should be prepared and carried out.

Novel technologies

Detailed assessments should be applied to innovative technologies of SMR designs that are without operational experiences. The new features and practices shall be adequately qualified through verifications, validations and testing before being brought into service to the extent practicable, and shall be monitored in service to verify that the behavior of the plant is as expected. Requirements and guidance are necessary for qualification programs of new materials and features applicable to SMR designs including the extent and scale of the testing, verification and validation of models, and fabrication processes. (See Section 7.2.)

7.2. RECOMMENDATIONS FOR THE IAEA

The DiD WG identified safety areas for which the opportunity to further develop safety guidance to help the safety assessment of DiD applied to SMRs may be investigated. These include:

- demonstration of reinforcement of DiD levels 1 and 2
- development of safety criteria and requirements for passive safety systems and inherent safety features
- application of single failure criteria for safety functions involving passive systems
- criteria for exclusion of identified initiating events from the design
- new guidance for procedures may need to be developed for inspections of the manufacturer/producer of the module
- 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-module issues in PSAs
- 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.

The following activities could be desirable for the next SMR Regulators' Forum:

- organize exchanges on safety information among designers, regulators and their TSOs to better understand and frame the SMR characteristics
- exchange information and share common positions on DiD with Member States in an effort to enhance harmonization on national and international levels of the licensing process

Such a report could be published by the IAEA.

References

A. Basic references

1. IAEA SSR-2/1 (Rev. 1), *Safety of Nuclear Power Plants: Design*, Vienna, 2016
2. IAEA INSAG-10, *Defence in Depth in Nuclear Safety*, Vienna, 1996
3. WENRA study by RHWG, *Safety of new NPP designs*, March 2013
4. IAEA-TECDOC-1570, *Proposal for a Technology-Neutral Safety Approach for New Reactor Designs*, Vienna, September 2007
5. OECD/NEA green booklet No. 7248, *Implementation of Defence in depth in Nuclear Power Plants*, 2015
6. IAEA SSG-12, *Licensing process for Nuclear Installations*, Vienna, 2010
7. IAEA INSAG-25, *A Framework for an Integrated Risk Informed Decision Making Process*, Vienna, 2011
8. IAEA-TECDOC-1791, *Considerations on the Application of the IAEA Safety Requirements for Design of Nuclear Power Plants*, May 2016
9. IAEA GSR Part 4, *Safety Assessment for Facilities and Activities*, Vienna, 2009
10. *Technical guidelines for the design and construction of the next generation of nuclear power plants with pressurized water reactors*, IRSN/GRS, France, 2000
11. IAEA SRS No. 46, *Assessment of Defence in Depth for Nuclear Plants*, February 2005
12. INL/EXT-09-17139, *Next Generation Nuclear Plant Defence-in-Depth Approach*, NRC Project #0748
13. WENRA *Safety Reference Levels for Existing Reactors*, WENRA RHWG report, September 2014
14. Responses on defence in depth survey questions, USA, September 2015
15. Responses on defence in depth survey questions, Finland, September 2015
16. Responses on defence in depth survey questions, Korea, September 2015
17. Responses on defence in depth survey questions, Russia, September 2015
18. Responses on defence in depth survey questions, Canada, September 2015
19. Responses on defence in depth survey questions, France, September 2015
20. USNRC Regulatory Guide 1.174, *An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis*, revision 2, May 2011
21. IAEA Safety Standard NS-R-1, *Safety of Nuclear Power Plants: Design*, September 2000
22. U.S. Nuclear Regulatory Commission, *Historical Review and Observations of Defence-in-Depth*, NUREG/KM-0009, April 2016

B. Basic SMR references

1. *Status of Small and Medium Sized Reactor Designs, A Supplement to the IAEA Advanced Reactors Information System (ARIS)*, http://aris.iaea.org, September 2012
2. *Advances in Small Modular Reactor Technology Developments, A Supplement to: IAEA Advanced Reactors Information System (ARIS)*, http://aris.iaea.org, September 2014
3. IAEA-TECDOC-626, *Safety related terms for advanced nuclear plants*, September 1991
4. IAEA Nuclear Energy Series No. NP-T-2.2, *Design Features to Achieve Defence in Depth in Small and Medium Sized Reactors*, Vienna, 2009
5. Proceeding of the 6th INPRO Dialogue Forum, *Licensing and Safety Issues for Small Modular Reactors*, Vienna, 2013
6. IAEA NS-R-3, *Site Evaluation for Nuclear Installations*, November 2003
7. U.S. Nuclear Regulatory Commission, *Probabilistic Risk Assessment and Severe Accident Evaluation for New Reactors*, NUREG-0800, Section 19.0, Revision 3, December 2015
8. U.S. Nuclear Regulatory Commission, *An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis*, Regulatory Guide 1.174, Rev. 2, May 2011
9. IAEA Safety Standard NS-R-1, *Safety of Nuclear Power Plants: Design*, 2000

C. Additional references

1. IAEA SF-1, *Fundamental Safety Principles*, Vienna, 2006
2. IAEA INSAG-12, *Basic Safety Principles for Nuclear Power Plants*, 75-INSAG-3 Rev. 1, Vienna, 1999
3. IAEA Safety Requirements No. NS-R-3, *Site Evaluation for Nuclear Installations*, November 2003
4. *Facilitating International Licensing of Small Modular Reactors, Cooperation in Reactor Design Evaluation and Licensing (CORDEL) Working Group*, Small Modular Reactors Ad-hoc Group, WNA Report No. 2015/004, August 2015
5. Mario D. Carelli et all, *The design and safety features of the IRIS reactor*, Nuclear Engineering and Design 230 (2004) 151–167
6. IAEA-TECDOC-1624, *Passive Safety Systems and Natural Circulation in Water Cooled Nuclear Power Plants*, Vienna 2009
7. IAEA Safety Reports Series No. 48, *Development and Review of Plant Specific Emergency Operating Procedures*

Appendix A: Defence-in-Depth Working Group Members

V. Abdulkadyrov	Russian Federation
M. Caruso	USA
S. Cook	Canada
B. Dimitrov	France
P. Dupuy	France
A. Lahkola	Finland
J. Park	Korea
V. Poldiaev	Russian Federation
R. Sairanen	Finland

Appendix B: Typical SMR specific features

Facility size			
SMR feature	Implications of the feature	Opportunities for DiD application	Challenge for DiD application
Low thermal power output	Smaller fuel load required to sustain the output	Impact of this characteristic has to be assessed considering the features below	Levels 4 and 5 – Vendor desire for reduced barriers (e.g., confinement or containment requirements)
	Proportionally lower decay heat power	Level 1 – Equilibrium power can be removed to environment without fuel damage Levels 2 and 3 – Lower decay heat can lead to longer grace periods; less heat sink capacity required Level 4 – Reduced risk of fuel damage and consequential release of fission products	Levels 2 and 3 – Vendor desire to reduce heat sink capability; demonstration of decay removal capability still required
	Smaller radionuclide inventory	Levels 4 and 5 – Reduction in the dominant radiation hazard as the radiation hazard is roughly proportional to power level	Levels 4 and 5 – Vendor desire for reduced barriers (e.g., confinement or containment requirements)
	Smaller core power density	Levels 1 and 2 – Better safety margins and inherent safety Level 3 – better safety	Depends on the ratio between thermal power and core volume

		margins and inherent safety	
Small reactor core size	Smaller core volume	Level 1 – possibly better control stability; depending on design, the core could be less sensitive to minor perturbations due to lower quantities of fissile material	Level 1 – Control may be more sensitive depending on the percent enrichment of fissile material; small volume could lead to high core power density
	Larger coolant-to-fuel thermal power ratio	Levels 2 and 3 – Greater inventory of water per unit of power allows increase in thermal inertia due to heat capacity of water; slower temperature rise on loss of flow	See comments for modular section
	Better neutronic spatial control	Levels 1 and 2 – A smaller spatial design of the core would result in less control challenges from flux tilts	
	Larger surface to volume ratio	Level 3 – Facilitates easier decay heat removal with single phase coolant	
Small reactor facility size	Smaller plant footprint		
	Less space in facility	Level 1 – reduced complexity; reduced number of structures, systems and components	Level 1 – More common cause possibilities; reduced space for maintenance activities Levels 3 and 4 – Fewer possibilities for physical separation from internal and external hazards

			Level 3 – Reduced redundancy
Novel features and technologies			
Non-conventional cooling methods	Reliance on natural circulation	Levels 1 and 2 – Main pump failures and therefore associated loss-of-cooling initiating events are eliminated; reactor can be started without class IV power	Levels 1, 2, 3 and 4 – Uncertainties in natural circulation (cooling) performance in certain conditions; increased aspect ratio required; possibility of power oscillations Levels 2 and 3 – Main circuit depressurization may be required before sufficient thermosyphoning can be established
	Reliance on air cooling as a final heat sink	Levels 3 and 4 – Air is readily available	Levels 3 and 4 – Heat loads must be adequately understood in accident conditions
	Reliance on other non-water cooling media	Level 1 – May allow operation just above atmospheric pressure so no pressure vessel required therefore fewer design implications for the coolant pressure boundary piping	Levels 3 and 4 – Less operating experience available for non-water cooling media Level 1 – New novel designs have not been proven
		Level 2 – Higher boiling point of coolant allows more margin to overheat the fuel	
		Level 1 – Less operating	

		experience (e.g., chemistry, aging effects)	
Novel vessel and component layout	Incorporation of primary system components into a single vessel	Level 1 – Design simplification feature Level 1 – Reduces size and number of vessel penetrations Level 3 – Eliminates large break loss of cooling	Levels 1 and 2 – Limited volume within the vessel for mechanical equipment; loss of inherent safety, safety margins and grace periods; uncertainty in models used for design and assessment; applicability of current codes and standards Level 1 – New novel designs have not been proven
Emphasis on passive safety features	Reduced reliance on electrical power	Level 1 – De-emphasizes systems requiring large amounts of electricity and therefore eliminates failure possibilities Redundancy requirements for passive safety systems involved in DiD Level 3.	Levels 3 and 4 – Functional failure is possible without mechanical failure (e.g., small driving forces, higher level of uncertainties, etc.); no rules for safety assessments, no reliability data, no statistics Level 1 – Problems for periodical testing, inspections and maintenance; unclear how to guarantee the capability during the lifetime of the plant

	Purported to have higher reliability	Levels 2, 3 and 4 – Can remove heat in all operating plant states and accident conditions; stored energy is not required	Level 1 – Harder to test, model and operate manually Levels 3 and 4 – Less operating experience with passive safety systems; passive system may need active component initiation
	Use of natural forces such as gravity	Level 1 – Natural forces are readily available	Levels 3 and 4 – Weak driving force may lead to lower reliability under harsher environmental conditions; passive system needs to be activated; activation is important for system reliability
	Reduction in complex logic	Level 1 – Fewer failure possibilities; lower event frequency	
	Failure modes are more subtle		Level 1 – Active components have more obvious failure modes; passive systems maybe a challenge to test and qualify
	Less reliance on operator	Level 2 – Rapid response is not required from the operator for initial shutdown, reach control state and long term safe shut down	Levels 3 and 4 – Information for the operator for safety function performance
Non-traditional or different number of barriers to fission product release	New types of barriers to release of radioactivity (e.g., ceramic	Levels 3 and 4 – Barrier performance may be enhanced (e.g., lead-bismuth – lead will solidify when released so	Levels 1 and 2 – Uncertainty in safety margins; applicability of current codes and

	materials, molten salt fuel)	fission products are contained in lead) Enhanced safety margin resilience	standards Level 1 – New novel designs have not been proven
	Higher temperature fuel sheath integrity	Levels 3 and 4 – No fuel melt and therefore a reduction in accident scenarios rated as potentially severe	Levels 3 and 4 – How will the qualification be done?
	Designer claims containment not required		
Unique fuel design	Good neutron economy	Level 1 – Smaller amounts of fissile material are required	
	Higher melting temperature	Level 3 – Greater margin to prevent fuel failure	
	More efficient heat transfer	Level 3 – Design allows long-term passive decay heat removal	
	Higher heat capacity	Levels 2 and 3 – Slower progression of transients	Levels 3 and 4 – A high temperature gas-cooled reactor unit capacity below ~600 MWt is a necessary condition to ensure long-term passive decay heat removal from the core
		Level 1 – Achievement of a large temperature margin between the operation limit and the safe operation limit	

	Higher critical heat flux	Level 3 – Allows fuel to withstand higher temperatures	
	New materials for better barrier to fission product release	Levels 3 and 4 – Allows inherent fission product confinement properties at high temperatures and fuel burnups; enhanced safety margins	Level 1 - Qualification demonstration is a challenge
Modular design			
Compact/simplified design	Fewer structures, systems and components (SSCs)	Level 3 – Reduction in accident frequency (e.g., loss-of-coolant accident, steam line break or boron dilution)	Level 3: New initiating event for module; reduction of redundancy and diversity?
		Level 1 – Less piping, fewer penetrations, less maintenance burden; elimination of some Initiating events	Levels 1, 2 and 3 – May increase susceptibility to common cause multi-module events (e.g., internal fire, flood)
Module fabrication	Standardization (modular)	Level 1 – Predictability of product; simplified construction and installation	Level 1, 2,3 Slight design changes may progressively evolve the design; introduces a new possibility for common cause failure between modules
	Factory produced		Level 1 – Multiple construction interfaces between module constructors could lead to weaknesses; common codes and standards between countries may not exist
	Multiple organizations		Level 1 – Configuration control

	involved		issues
Transportability			Level 1 – Potential damage to module during transport; size limitation for transport
Module dependence and independence	Sharing of SSCs among modules	Levels 1,2,3 - Shared SSCs can be designed with additional DiD to enhance DiD for overall facility	Levels 1, 2, 3 and 4 – Increase common cause failures
Number of modules	Staffing		Level 1 – Multiple modules operated by single operator
			Levels 2, 3 and 4 – Control room staffing; operator may need to perform emergency response simultaneously on multiple modules
			Level 2 - Lack of operational data
	Radionuclide inventory	Levels 3 and 4 – Reduction in potential source term for single unit accident sequences	Level 3,4 and 5 Accumulative radionuclide inventory
	Accident analysis		Levels 3 and 4 – Increased complexity in accident sequences and responses
	Fuel storage requirements		Level 5 – Additional source term requires fuel cooling
Application			
Siting closer to populations			Level 5 – Emergency planning zone
Grid independence	Operation in island mode, site	Level 2 – Improved resistance to loss-of-grid	Level 4 – Less external response

	autonomy	events	capability
Novel locations (e.g., shipyard, mines, northern communities)	Lack of local infrastructure		Level 4
	Remote operation		Level 4
	External hazards change with environment		
Floating reactor assembly	Subject to the pitch and roll of the medium		Level 1 – More potential stressors leading to failure modes
Submerged reactor	Access to facility is restricted		All levels – Facility is not easily accessible

Appendix C: Survey results summary

A. Regulatory framework responses

Question 4.1

(a) Please describe how the use of DiD is articulated in your regulations, supplementary regulatory requirements (if applicable) and guidance.

Country	Regulations/guidance	Remarks
Canada	RD/GD-369, *Licence to Construct a Nuclear Power Plant* and REGDOC-1.1.3, *Licence Application Guide: Licence to Operate a Nuclear Power Plant*	
Finland	Nuclear energy act, Sec.7b, Radiation and Nuclear Safety Authority Regulation on the Safety of a Nuclear Power Plant, 1/Y/2016, Sec. 9 and 10	
France	DiD is addressed in the Technical Guidelines for Generation III reactors. These TG don't explicitly mention the size of reactors under scope, but assume large NPP. DiD is addressed in some Basic Safety Rules, in particular BSR I.3.a related to the SFC. DiD is interpreted in some ASN Guides, as draft ASN Guide 22 "Safety requirements and recommendations for the conception of PWR".	
Korea	Regulations on technical standards for nuclear reactor facilities, etc. Article 26	
Russia	OPB-88/97, par. 1.2.3	
United States	No explicit DiD requirements in regulation. To implement DiD level, the following rules are illustrated; Level 1: 10CFR 50, App. A and B Level 2: 10CFR 50, App. A, 10CFR 50.36, 10CFR 50.49, 10CFR 50.65 Level 3: 10CFR 50.44, 10CFR 50.46, 10CFR 50.48 Level 4: 10CFR 50.62, 10CFR 50.63, 10CFR 50.54(h)(h)(2), 10CFR 50.150, 10CFR 52.47(a)(27), 10CFR 52.47(a)(23) Level 5: 10CFR 100, 10CFR 50.47, 10CFR 50, App. E, 10CFR 50.54(h)(h)(2)	

Question 4.1

(b) When comparing research reactor design requirements to NPPs, how do the above requirements differ (if at all) and why are they different? (Note: SMRs occupy a spectrum of core inventories and power outputs in between research reactors and NPPs.)

Country	Regulations/guidance	Remarks
Canada	No difference in requirements, but application to SMR may differ	
Finland	Requirements for NPPs are applicable to research reactors on a case-by-case basis. No difference in requirements or guidance for reactors intended for production of heat or electricity.	
France	No difference in requirements or guidance	
Korea	No difference in requirements	

Russia	No difference in requirements	
United States	Due to the large difference of thermal power generated, the implementation of DiD for non-power reactors differ from commercial nuclear reactors – such as emergency planning zones	

Question 4.2

Does your country have any specific requirements related to the independence of the DiD levels?

Country	Regulations/guidance	Remarks
Canada	REGDOC-2.5.2, *Design of Reactor Facilities: Nuclear Power Plants*, sections 4.3.1 and 6.1	
Finland	Radiation and Nuclear Safety Authority Regulation on the Safety of a Nuclear Power Plant, 1/Y/2016, Sec 9,Guide YVL B.1 Safety design of a nuclear power plant, section 4	
France	The draft ASN Guide 22 "Safety requirements and recommendations for the conception of PWR" focus on safety requirements related to the independence of the DiD levels. It refers to WENRA Reference Levels for existing NPPs (September 2014) and the WENRA Report "Safety of new NPP designs" (March 2013) including insights from Fukushima Daiichi NPP accident. It is in good agreement with IAEA SSR 1/2 (Rev. 1) as well.	
Korea	No specific requirements, but Article 2, Article 27 of Regulations on Technical Standards for Nuclear Reactor Facilities, etc. applies	
Russia	OPB-88/97	
United States	10CFR 50, App. A (GDC), Reg. Guide 1.174 and 1.177	

Question 4.3

In your regulation, supplementary regulatory requirements and guidance for new reactor (any size and output), please describe any specific requirements for the design of features for each of the following:

(a) Level 1 normal operation.
(b) Level 2 anticipated operational occurrences.
(c) Level 3 design basis accidents (e.g. single failure criteria).
(d) Level 3 multiple failure accidents or for other design extension conditions.
(e) Level 4 severe (core melt) accidents.
(f) A "practical elimination" approach.
(g) Extreme hazards.

Country	Regulations/guidance	Remarks
Canada	REGDOC-2.5.2 (INSAG-10, SRS #46) Levels 1 to 4: REGDOC-2.5.2, sections 6.1 and 7.3.2 "Practical elimination" approach: RECDOC-2.5.2, section 7.3.4 Extreme hazard: RECDOC-2.5.2, section 7.4.2	
Finland	Guide YVL B.1 Level 1: Comply with high standards of quality and reliability with adequate safety margin Level 2: Provisions for deviations from normal operation	

	Level 3 (DBA): N+2 failure criterion, Remove the decay heat within 72 hours Level 3 (DEC): Comply with diversity principle with N+1 criterion and remove the decay heat within 72 hours Level 4: Independent systems from other levels Practical elimination: Deterministic analysis with PRA and expert assessments Extreme hazard: Decay heat removal within 72 hours and control of reactivity without relying on power supply at least eight hours	
France	Technical Guidelines for Generation III reactors, some examples: Level 1: Quality must be obtained and demonstrated notably by an adequate set of requirements for design, manufacturing, construction, commissioning and operation, as well as by quality assurance. Level 2: The inherent reactor behavior is stable (e.g. negative moderator feedback). To reduce the number of significant incidents and accidents by improvements of the equipment and systems used in normal operation Level 3 : DBA: Physical and spatial separation, SFC. Minimize the possibility of common cause failure. DEC: Assess the multiple failures condition deterministically, independence and diversification requirements. Level 4: Substantial improvement of the containment function. No containment venting. Maximum conceivable releases would necessitate only very limited protective measures in area and in time for the public. Practical elimination: Accident with large early release frequency is a matter of judgment. Practical elimination cannot be demonstrated by the compliance with a general "cut-off" probability. Hazard: Possible links between internal and external hazards and single initiating events have also to be considered. The improvements in the "defence-in-depth" should lead to the achievement of a global frequency of core melt less that 10-5 per plant operating year, uncertainties and all types of failures and hazards being taken into account.	
Korea	Levels 1 to 4 and extreme hazard: Regulations on Technical Standards for Nuclear Reactors Facilities, etc. No description on "practical elimination"	
Russia	Levels 1 to 4: None Practical elimination: Not implemented Extreme hazard: not less than 0.1g of gravity and 1.5 hours in the standard fire, spatial and physical separation of safety systems	
United States	Levels 1 to 3 (DBA): Same requirements Levels 3 (DEC) and 4: 10CFR 52.79, 10CFR 50.44, 10CFR 50.71 Practical elimination: Extreme hazard: Order EA-12-049	

B. Industry's application of requirements – responses

Question 4.4

Have any difficulties been identified (in particular by the designers and utilities) in applying DiD principles defined for large reactors to SMRs? If so, please describe them.

(a) For DiD level 1?
(b) For DiD level 2?
(c) For DiD level 3?
(d) For DiD level 4?
(e) For DiD level 5?

Country	Regulations/guidance	Remarks
Canada	Information is not publicly available at this time	
Finland	Comparison to Finnish regulations and guidance is ongoing. Results are not yet available.	
France	No experience	
Korea	Awaiting Input	
Russia	Level 1: Siting and size of protection zone Levels 2 to 4: No difficulty Level 5: EPZ in remote districts	
United States	No specific difficulties but some of DiD level may be different from that of large NPPs	

Question 4.5

(a) Have designers requested up-front 'relief' from some DiD principles for SMRs? If so, which one and for what reasons? For example:

- e.g., Specific systems for mitigation for a an anticipated transient without scram accident are not required because unique design features make the probability of such an accident negligibly small; or
- reduction in emergency preparedness requirements based on the "smallness" of the reactor?

(b) Have compensatory measures or justifications been provided?

Country	Regulations/Guidance	Remarks
Canada	Information is not publicly available at this time	
Finland	There is no application for licensing submitted. Comparison to regulations and guidance is ongoing and possible challenges have not yet been identified.	
France	No experience	
Korea	Awaiting Input	
Russia	Not identified	
United States	(a) Functional containment performance, emergency planning. (b) Regulatory gap analysis	

Question 4.6

What types of events or situations generally addressed in the safety cases of typical large GEN III or GEN IV reactors are considered as eliminated or excluded by SMR designers and for what reasons? (ex.: some break sizes excluded because of limited pipe diameters, some events excluded thanks to inherent safety characteristics).

Country	Regulations/Guidance	Remarks
Canada	Information is not publicly available at this time	
Finland	There is no application for licensing submitted. Comparison to regulations and guidance is ongoing and possible challenges have not yet been identified.	
France	No experience	
Korea	Awaiting Input	
Russia	Large brakes in primary circuit piping	
United States	Large breaks in primary circuit piping of light water reactors; gross melting of fuel in high temperature gas reactors	

Question 4.7

What types of requirements do the SMRs designers use in terms of:

a) Redundancy for active or passive safety systems (for accident prevention / for core damage prevention / for core damage mitigation)?
b) Diversification between systems involved in different levels of DiD?
c) Geographical or physical separation regarding CCF and internal hazards?
d) Potential for an accident in one module affecting other modules in a multi-module plant?

Other significant issues you would like to point out?

Country	Regulations/Guidance	Remarks
Canada	Information is not publicly available at this time	
Finland	There is no application for licensing submitted. Comparison to regulations and guidance is ongoing and possible challenges have not yet been identified.	
France	No experience	
Korea	Awaiting Input	
Russia	Requirements for redundancy, diversity and physical separation for safety system	
United States	Passive and active systems performing safety functions include redundancy in design in a graded fashion based on their safety classification and level of risk significance; SMR applicants address multi-module risk in accordance with guidance in NRC Standard Review Plan 19.0, Revision 3. One SMR designer has developed a simplified approach for estimating the frequency of core damage events in multiple modules occurring within a short time of one another.	