Western European
WENRA RHWG
Nuclear Regulators Association

Report
Applicability of the Safety Objectives to SMRs

12 January 2021

Table of Content

Applicability of the Safety Objectives to SMRs

01	Introduction		3
02	SMR Features		5
03	Applicability of the Safety Objectives		8
	03.1	O1. Normal operation, abnormal events and prevention	8
	03.2	O2. Accidents without core melt	9
	03.3	O3. Accidents with core melt	9
	03.4	O4. Independence between all levels of defence-in-depth	10
	03.5	O5. Safety and security interfaces	10
	03.6	O6. Radiation protection and waste management	11
	03.7	O7. Leadership and management for safety	12
04	Conclusions		14
	References		15
	Appendix 1: Preliminary considerations about “new evolutionary LWR” designs and DiD		16

01
Introduction

During the past years, global interest in Small Modular Reactors (SMRs) has developed. As the interest in SMRs has increased, there has also been discussion about the applicability of the present-day safety requirements, licensing processes and regulatory approaches to SMRs.

SMRs are nuclear reactors and the fundamental principles of protecting the people and environment from the harmful effects of radiation apply. However, the existing safety requirements have often been drafted with the mindset of regulating larger, water-cooled reactors intended for electricity production. Thus, it is worthwhile to consider the existing requirements to determine whether they are technology neutral, enabling their application to the different designs, or whether some adaptation would be necessary.

In particular, the WENRA Safety Objectives for new NPPs [1] are upper level principles that should be applicable to all types of reactors. It was expected that the safety objectives would be applicable to SMRs, too. However, it was considered beneficial to study them from the point of view of SMRs to confirm the applicability and to identify potential questions that would benefit from further study or guidance.

WENRA RHWG established in May 2019 a subgroup dedicated to SMRs. The task given to the group was to evaluate the impacts of different safety features of SMRs on the Safety Objectives for new NPPs as presented in [1].

Considering the wide variety of SMR designs currently being developed, it is not easy to identify safety features that would be common to all designs. Instead, the group considered generic design features and features of different deployment schemes[1] of the new concepts that may affect the applicability of the Safety Objectives. This report presents the results of this task.

There is no universally agreed definition for the term SMR, but a commonly used definition is that SMRs are considered to be nuclear reactors that have several of the following features:

- a power < 300 MWe or < 1000 MWt;
- designed for commercial use i.e., electricity production, desalination, district heating, process heat (as opposed to research and test reactors);
- designed to allow addition of multiple units / modules in close proximity to the same infrastructure;
- could be built and assembled in factories to a greater extent than traditional reactors and shipped to utilities for installation as demand arises;

In addition, some SMRs use novel designs that have not been widely analysed or licensed by regulators.

[1] Deployment scheme takes into consideration the factors related to the utilisation of the reactor that affect the characteristics of the plant. Such factors are for example number of modules to be installed, interactions and dependencies between the modules, location (e.g. in remote area or in close vicinity to population), dynamics of the linked process and refuelling, maintenance and operating concepts. An example of different deployment schemes for Fluoride-Salt-Cooled, High-Temperature Reactor (FHR) technology is given under chapter 2.

As will be discussed in the following chapters, especially in chapter 2, the term SMR covers a wide range of different designs, technologies and deployment schemes. Due to that, it is not recommended to lay down principles to be applied to SMRs in general. The label “SMR” in itself does not justify changes in safety requirements. Each design and application needs to be considered individually, taking into account the case specific characteristics. This report elaborates in general the characteristics associated with SMRs and different deployment schemes that may have an impact on the application of the Safety Objectives. The effect of these features on the practical application of the Safety Objectives is elaborated where considered useful. Many of the features considered are not characteristic only to SMRs, but to new designs regardless of the power or modularity of the concept.

SMR related work is currently going on in many different fora. For example, the SMR Regulators’ Forum (supported by IAEA) discusses regulatory knowledge and experience and tries to identify and resolve common safety issues that may challenge regulatory reviews associated with SMRs. IAEA has many activities related to SMRs, see https://www.iaea.org/topics/small-modular-reactors .

02
SMR features

There are numerous SMR concepts under development around the world, in varying development stages and utilising different technologies (water-cooled reactors, gas-cooled reactors, liquid metal-cooled reactors, molten salt reactors) and neutron spectra. The sizes range from very small (< 10 MWe) to relatively large (300 MWe[2]).

Due to the large variety of different designs, SMRs are sometimes further classified either by intended use, by size or by technology. One example of classification by size uses the following categories:

- Large-scale SMR (300 MWe /~1000 MWt)
- Medium-scale SMR (50 MWe /~150 MWt)
- Small-scale SMR (10 MWe /~30 MWt)

Example of classification as per intended use:

- Centralized medium to large-scale units intended as an alternative to current NPPs with a large local infrastructure base.
- Local small to medium-scale units intended for local use in populated areas, such as larger cities or large fabrication facilities with medium-sized localized infrastructure.
- Remote small-scale units intended for remote deployment with minimum infrastructure and personnel.

An example for the classification as per technology is:

- Thermal, light water reactors
- Fast reactors
    - SFR - Sodium-Cooled Fast Reactor
    - LFR - Lead-Cooled Fast Reactor
    - GFR - Gas-Cooled Fast Reactor
    - MSFR - Molten Salt Fast Reactors
- Thermal reactors
    - MSR - Molten Salt Reactor
    - FHR - Fluoride-Salt-Cooled, High-Temperature Reactor
    - HTGR - High Temperature Gas-cooled Reactor
    - SCWR – Supercritical Water Reactor

[2] According to the SMR definition the maximum electrical output of an SMR is 300 MWe. However, the term SMR is used flexibly. In the concepts included in IAEA's SMR book [2], the largest reactor has an electrical output of 443 MWe.

However, the size or the technology or the intended use alone do not define the characteristics of the facility, but the deployment scheme has an effect, too[3]. The combination of intended use and designated technology will result in a specific design.

Below are listed some features of SMRs that are different from the traditional large reactors. As little detailed design information is available about many of the innovative designs that are being considered or proposed, it is difficult to examine the level of support for the claims of enhanced safety. However, the purpose of this report is not to evaluate the proposed concepts or the validity of the safety claims but to evaluate the applicability of the WENRA Safety Objectives to SMRs.

Claimed features and potential challenges of SMR concepts:

- low power resulting in reduced decay heat and smaller activity inventory per reactor module;
- novel measures to enhance safety, such as "inherently safe" fuel, coolant material with enhanced safety features, natural circulation as a main means of heat removal, wide use of passive safety systems and practical elimination of situations that can lead to early or large releases;
- partially different initiating events (e.g. absence of some events like LB-LOCA in integrated designs, but also new potential events like module to module interactions);
- long grace periods for operator actions;
- challenges for periodic inspections of components in integrated designs where all the main primary component are incorporated inside one single vessel;
- unconventional number of physical barriers between fission products and environment;
- use of novel fuels (e.g. molten salt, ceramic);
- operating concept – high degree of automation and reduced role of operators, remote control, unmanned units, several reactors operated by one operator team;
- use of common SSCs between several reactor cores;
- unconventional siting: underground, sea-bed based, remote locations lacking basic infrastructure, off-grid locations;
- factory-fuelled reactor cores;
- focus of initial testing shifted from site to factory; and
- emergence of new companies both as developers and as utilities.

Many of the features are not unambiguously beneficial or detrimental to safety but can have both aspects. For example, the multi-unit installations with the potential for systems to be shared between modules offers both, potential benefits (such as the ability of one unit to support another) and new challenges

[3] For example, consider FHR technology (Fluoride-Salt-Cooled, High-Temperature Reactor); a low pressure / high temperature system using solid fuel. For a large-scale deployment, such a design would require refueling on site, significant localized onsite nuclear infrastructure similar to that of a "conventional" large nuclear power reactor, e.g., a large power output would require a comparable refueling frequency. However, the same technology in a small-scale deployment could be designed for a minimum refueling frequency, and the low power would enable the plant size to be significantly reduced, and remove the necessity for some components (for low power designs, FHR reactors are typically claimed to rely on natural convection to circulate coolant and thus not to require primary coolant pumps). Refueling would not occur on site, but rather in a form of battery-like procedure, exchanging whole modules (primary system) instead of only fuel.

(such as hazards that affect multiple units, common cause failures, the need for multi-unit risk assessment techniques and considerations of shared control rooms). Use of passive systems could *„bring promising safety benefits" but some "attributes of passive systems […] are worthwhile to be considered with regards to safety in view of current regulatory practices"* and some potential specific issue to be dealt have been highlighted in WENRA/RHWG Report "Regulatory Aspects of Passive Systems", 01 June 2018 [3].

Some of the technology being considered or proposed is unproven, with little or no operational experience. If examples of the designs exist, they may be prototypes or experimental-level. Analyses, simulations and/or testing will be needed to fill the gaps in knowledge.

Modularity and multi-module aspects

Modularity has not been defined explicitly and it can have different meanings. Sometimes it is used to refer to serial production of reactor modules, other times it refers to the facility consisting of several reactors.

Serial production may have some benefits for safety, like ensuring controlled settings for manufacture and assembly, and having a large base for collecting feedback and experiences. On the other hand, serial production may pose a challenge for the oversight, as the module may have been designed, manufactured and tested before the involvement of the licensee (or regulator) in question (this is discussed further under O7).

On site, the modularity can have different degrees. A multi-module facility can be similar to current multi-unit sites, each reactor being independent from the others and having its own systems. The other extreme is a facility where reactor cores share several structures, systems, and components, including those important to safety, the reactors are dynamically linked by feeding the same process and are operated by a single operating team from a shared control room.

With SMRs, the consideration of the multi-unit/multi-module aspects is becoming more important, because in many concepts there are more interactions and dependencies between the units (modules) than typical for current multi-unit sites. The current Safety Objectives, especially O2 and O3, describe the traditional approach to safety demonstration, based on analysis of a single reactor. Therefore, the safety demonstration may have to be expanded to the site level, so that the impacts of all facilities on the site are studied.

03
Applicability of the Safety Objectives to SMRs

In this chapter, the applicability of each WENRA Safety Objective is discussed. Some features that differ from the present-day reactors are given as examples, even if they do not impact the applicability of the objective.

03.1 O1. Normal operation, abnormal events and prevention of accidents

- *reducing the frequencies of abnormal events by enhancing plant capability to stay within normal operation.*
- *reducing the potential for escalation to accident situations by enhancing plant capability to control abnormal events.*

This objective is applicable.

Some designs features of some of the new concepts may be beneficial for O1. For example, the number of active systems may be reduced (resulting in reduced number of component failures) and materials less prone to failures might be utilised. Some concepts require very little operator invention which helps to reduce the probability of human errors.

On the other hand, novel and innovative solutions may induce unexpected disturbances in the early phase before operating experience is accumulated and the reactor design and mode of operation evolves accordingly. Different operational aspects may, at least in the first projects, pose a challenge. New aspects may be, for example:

- higher degree of automation in the plant control and reduced number of operating staff;
- the role of the operating staff may differ from what is traditional in large NPPs;
- one operating team may operate several reactors (potentially from a remote location);
- use of new technologies in plant control and monitoring as well as in condition monitoring (artificial intelligence, diagnostics, robotics...);
- interactions between several coupled reactor modules;
- potential feedback of co-generation/process heat industrial application.

High quality in design, manufacturing and construction are important elements in meeting Safety Objective O1. This remains valid also for a manufacturing process of “modules” involving more activities off-site.

03.2 O2. Accidents without core melt

- *ensuring that accidents without core melt induce no off-site radiological impact or only minor radiological impact (in particular, no necessity of iodine prophylaxis, sheltering nor evacuation).*
- *reducing, as far as reasonably achievable,*
    - *the core damage frequency taking into account all types of credible hazards and failures and credible combinations of events;*
    - *the releases of radioactive material from all sources.*
- *providing due consideration to siting and design to reduce the impact of external hazards and malevolent acts.*

The objective is applicable.

However, for those SMR concepts where molten is the normal state of the fuel, the term ”core melt” is not meaningful but for example a fuel leakage or failure of the heat removal pathways could still cause a release. The idea of the Safety Objective is valid, but the terminology “core melt” needs to be refined depending on the SMR concept.

03.3 O3. Accidents with core melt

- *reducing potential radioactive releases to the environment from accidents with core melt, also in the long term, by following the qualitative criteria below:*
    - *accidents with core melt which would lead to early or large releases have to be practically eliminated;*
    - *for accidents with core melt that have not been practically eliminated, design provisions have to be taken so that only limited protective measures in area and time are needed for the public (no permanent relocation, no need for emergency evacuation outside the immediate vicinity of the plant, limited sheltering, no long term restrictions in food consumption) and that sufficient time is available to implement these measures*

The objective is applicable.

As for O2, the term “core melt” is not fitting for all SMR concepts. However, the Safety Objective should be interpreted to mean ”accidents which would lead to large or early releases”. Therefore, O3 addresses also possible other scenarios that may lead to large or early release than core melt (e.g. leakage of liquid fuel from a molten salt reactor).

According to footnote 15 in [1], the safety demonstration has to cover all risks induced by the nuclear fuel, even when stored in the fuel pool. For some concepts, especially for molten salt or pebble-bed reactors, other means of fuel storage can be used. The safety demonstration has to cover situations where the fuel or part of it is outside of the reactor, no matter what kind of solution is used to store the fuel.

Nevertheless, if SMRs are deployed in areas with relatively high density of population since several designers claim that no EPZ is needed for their SMR concept, more stringent acceptance criteria than those for O3[4], such as those for O2[5], could be required by the national Safety Authorities.

[4] "no permanent relocation, no need for emergency evacuation outside the immediate vicinity of the plant, limited sheltering, no long term restrictions in food consumption" [1]
[5] "no off-site radiological impact or only minor radiological impact (in particular, no necessity of iodine prophylaxis, sheltering nor evacuation)" [1]

03.4 O4. Independence between all levels of defence-in-depth

- *enhancing the effectiveness of the independence between all levels of defence-in-depth, in particular through diversity provisions (in addition to the strengthening of each of these levels separately as addressed in the previous three objectives), to provide as far as reasonably achievable an overall reinforcement of defence-in-depth.*

This objective is applicable.

The independence between levels of defence-in-depth, to the extent reasonably practicable, is a key element of ensuring the effectiveness of the defence-in-depth concept and that is applicable independent of the technology used.

As noticed in the introduction of this report, the term SMR covers a wide range of designs and there is no universally agreed definition for this term. Considering the wide variety of SMR designs currently being developed [2], it is not easy to identify safety features that are common to all designs. Therefore, discussions on the application of defence-in-depth (DiD), and in particular of the concept of independence between all levels of DiD (Safety Objective O4) to SMRs should be based on particular SMR designs or at least design types.

In Appendix 1, as an example for such a discussion, the application of DiD and of O4 to "new evolutionary LWR" designs is considered. These designs are characterised by a stepwise introduction of new safety features based on existing LWR technology. However, for some non-LWR concepts, possible postulated initiating events and the application of the defence-in-depth concept may be different from the concepts applying LWR technology.

03.5 O5. Safety and security interfaces

- *ensuring that safety measures and security measures are designed and implemented in an integrated manner. Synergies between safety and security enhancements should be sought.*

This objective is applicable.

Several SMRs have features enhancing security (e.g. compact integrated design with smaller number of systems needing physical protection and with fewer access points, difficult access due to e.g. underground location, long grace periods and less need for operator actions to reduce the likelihood of the main control room being targeted). On the other hand, some aspects may bring new challenges (e.g. remote operation, having unmanned stations possibly in remote locations or, on the other hand, close to densely populated areas, transportation of modules with loaded core). However, the new features do not affect the applicability of the Safety Objective, they rather confirm the importance of considering both safety and security aspects in an integrated manner.

However, the objective could be expanded to cover also safeguards; for instance via safeguards by design. For some concepts, the traditional safeguards methods are not applicable. Some molten salt reactors are expected to be particularly challenging from the point of view of safeguards. Although the means by which

safeguards is assured on the current generation of new NPPs is well understood, the novel elements of many SMR designs pose significant challenges, as does the unfamiliarity of many new vendors with the safeguards concept.[6]

03.6 O6. Radiation protection and waste management

- *reducing as far as reasonably achievable by design provisions, for all operating states, decommissioning and dismantling activities:*
  - *individual and collective doses for workers;*
  - *radioactive discharges to the environment;*
  - *quantity and activity of radioactive waste.*

The objective is applicable.

SMRs may have features that differ from the present-day reactors, but they do not affect the applicability of the Safety Objective.

Many SMR concepts feature a compact design with small footprint and minimized building volume. This may result in lesser available space for radiation shielding and may require access routes and working areas closer to radiation sources than in present-day reactors. In addition, certain generation IV technologies (e.g. SFR and LFR) utilise coolants which can become highly radioactive in a fast neutron flux. Neutron activation of such coolants (or impurities therein), may therefore result in increased maintenance doses to operational staff, and increased radiological consequences from accidental releases of primary coolant if adequate protection is not provided. Some coolants (or their reaction products) also present a significant chemotoxic hazard. The secondary waste streams associated with normal operations (e.g. cold traps, filters, etc.) may also be challenging to handle. Graphite moderated reactors may generate significant quantities of radioactive graphite dust (particularly pebble bed designs), which may also present similar challenges.

On the other hand, the need to access the nuclear island during operation might be minimized, there might be a reduced number of components needing maintenance and there might be less activation (of structural materials) by design. SMRs thus have both beneficial and detrimental features regarding radiation protection of workers.

Waste generated by evolutionary LWR SMR concepts will probably be rather similar as the waste from the current LWRs and it can be treated and disposed of by similar technical solutions that are already in use or planned. However, some concepts propose the use of high assay low enriched uranium, for which the burn-up and decay heat may be higher. On the other hand, non-LWR concepts may generate unique waste streams that are very different from LWRs, and for which no disposal routes are currently available.

Nevertheless, whilst some aspects of this objective may prove to be challenging to implement on SMR designs, it remains fully appropriate and applicable to new reactor technologies, including both evolutionary LWR (Gen III+) and Gen IV designs.

[6] Including safeguards in the scope of O5. would be in line with IAEA SSR 2/1 Requirement 8: *Safety measures, nuclear security measures and arrangements for the State system of accounting for, and control of, nuclear material for a nuclear power plant shall be designed and implemented in an integrated manner so that they do not compromise one another.*

03.7 O7. Leadership and management for safety

- *ensuring effective management for safety from the design stage. This implies that the licensee:*
  - *establishes effective leadership and management for safety over the entire new plant project and has sufficient in house technical and financial resources to fulfil its prime responsibility in safety;*
  - *ensures that all other organizations involved in siting, design, construction, commissioning, operation and decommissioning of new plants demonstrate awareness among the staff of the nuclear safety issues associated with their work and their role in ensuring safety.*

The objective is applicable.

Many SMRs are intended to support other purposes in addition to electricity production. The reactors may be utilised for example for district heating, for small scale electricity production, to produce process heat for industry or for desalination. As a consequence, the companies interested in SMRs may be very different from the traditional users of nuclear energy, which typically have been power companies with electricity production as a core business. The new companies may have very little experience on use of nuclear energy and a wish to outsource as many tasks as possible. The organisational arrangements for construction, operation and decommissioning may also differ from the current NPPs. For example:

- Vendors may have a role also in the operation and/or decommissioning. For example, the vendor may lease the loaded core module to the operator and recover it at the end of the core's operating cycle.
- The role of manufacturer may be more significant, if a large part of construction takes place at the factory (e.g. assembly of the primary circuit, pre-operational commissioning testing, even fuel loading in some concepts).

Whatever the organisational arrangements are, the Safety Objective is valid. However, in application of requirements, a graded approach should be used. As discussed in chapter 2, there is a wide variety of different reactor concepts and deployment schemes. The risk caused by the facility and the commensurate requirements should be considered case by case. In addition to the radiological hazard potential of the facility, factors affecting the risk can be:

- complexity of the organisation and operation;
- complexity, uniqueness and novelty of the product or function and the resulting lack of experience.

The licensee

For SMRs, some proponents have been presenting having different licensees e.g. for construction and operation (for factory-fuelled SMRs this may be inevitable). Whatever the licensing system or organisational arrangements are, there must at all times be a licensee, who has the prime responsibility of safety.

As some licensees may wish to outsource different tasks, it is necessary to consider the minimum preconditions for bearing the responsibility of safety. Mere acceptance of the responsibility on paper, in other words commitment to take the financial or juridical consequences in case of an accident, is not

adequate. The licensee must have a genuine possibility and authority to influence safety related matters and decision-making and it must be able to justify safety related decisions. To accomplish this, the licensee must

- have understanding of nuclear safety and of the special features of using nuclear energy;
- understand the licensing basis and operation of the facility;
- be able to instruct and evaluate safety related work carried out by contractors.

The licensee may rely strongly on the vendor's support. For the new designs, the design lifetime is typically 60 years. It may be that vendor support is not available throughout the whole lifetime. The licensee must ensure proper consideration of operating experience, research results and results of e.g. periodic safety reviews also in case the vendor is not anymore developing the design. This is valid for all kind of facilities, not only SMRs, but it may be that some licensees of SMRs are less experienced and less prepared for such activities than the traditional operators.

Other involved organisations

The Safety Objective obliges the licensee to ensure that all organisations demonstrate awareness of safety issues associated with their work. This too is valid for the licensees of all kind of facilities, but is further highlighted with SMRs, as the role of other organisations in addition to the licensee may be more significant than is currently customary.

The role of manufacturer becomes more important, if some features are impossible to inspect or test after the module leaves the factory. The leadership and management for safety in the manufacturing company is emphasized and the licensee must ensure their effectiveness. This is not different from what is expected of the licensees of current reactors, but it may be more challenging for the licensee to influence the performance of a serial production company than in case of a customized project. The importance of the manufacturer's performance is essential if, as explained above, there is no possibility later to verify product conformity.

If SMRs gain ground and a serial production of reactor modules is established, the licensee may purchase a module that has been designed, manufactured and tested before the involvement of the licensee (or regulator) in question. Regulatory frameworks in different states may have varying expectations for the regulatory control and licensee's involvement during manufacturing of the components most important to safety. If the regulatory framework allows utilising components whose manufacture has not been controlled by the regulator or the licensee, the licensee must then find the adequate evidence for ensuring the proper performance of the manufacturing company and the quality of the end product. Observing the performance of the manufacturer at the time of the assessment and utilising inspection and oversight results of other customers or regulators could potentially be utilised to support the safety assessment.

04
Conclusions

WENRA RHWG established in May 2019 a subgroup dedicated to SMRs. The task given to the group was to evaluate the impacts of different safety features of SMRs on the Safety Objectives for new NPPs. However, when considering the wide variety of SMR designs currently under development, it is not easy to identify safety features that would be common to all the designs. Instead, the group considered generic design features and features of different deployment schemes of the new concepts that may affect the applicability of the Safety Objectives.

The conclusion is that the Safety Objectives are applicable to SMR designs, including evolutionary LWR (Gen III+) and Gen IV technologies. Widening the scope of Safety Objective O5 to also cover safeguards would be beneficial. O5 obliges to design and implement safety and security measures in an integrated manner.

References

[1] WENRA/RHWG Report “Safety of new NPP designs, Study by Reactor Harmonization Working Group RHWG”, March 2013

[2] Advances in Small Modular Reactor Technology Developments. A Supplement to: IAEA Advanced Reactors Information System (ARIS). 2020 Edition. https://aris.iaea.org/Publications/SMR_Book_2020.pdf

[3] WENRA/RHWG Report “Regulatory Aspects of Passive Systems”, 01 June 2018

Appendix 1: Preliminary considerations about "new evolutionary LWR" designs and DiD

DiD background

One of the objectives of the defence in depth (DiD) concept for reactor safety is to prevent or limit off-site radiological impacts such that solely limited off-site emergency protective measures in area and time will be necessary[7].

The means, by which DiD aims to fulfil this objective, are (see e.g. IAEA Safety Glossary, 2018 Edition): *a hierarchical deployment of different levels of diverse equipment and procedures*

- *to prevent the escalation of anticipated operational occurrences and*
- *to maintain the effectiveness of physical barriers placed between a radiation source or radioactive material and workers, members of the public or the environment, in operational states and, for some barriers, in accident conditions.*

For "traditional" LWR designs, the following DiD levels are defined

- Level 1: Prevention of abnormal operation and system failures
- Level 2: Control of abnormal operation and failures and avoid the occurrence of accidents
- Level 3: Control of design basis accidents to limit radiological releases and prevent escalation to severe accidents
- Level 4: Control of severe accidents, including prevention of accidents progression and mitigation of the consequences of severe accidents
- Level 5: Mitigation of radiological consequences of significant releases of radioactive material

and the following physical barriers[8]:

- Barrier 1: Fuel pin cladding
- Barrier 2: Pressure-retaining boundary
- Barrier 3: Containment

[7] See Council of the European Union, Council Directive 2014/87/Euratom of 8 July 2014, amending Directive 2009/71/Euratom establishing a Community framework for the nuclear safety of nuclear installations

[8] Sometimes, the fuel pellet matrix or retention functions (such as maintaining negative pressure gradients) are also considered as barriers.

A main characteristic of DiD is to have independence between all DiD levels, as far as reasonably achievable (see Safety Objective O4 in [1][9]). According to the IAEA Safety Glossary, 2018 Edition, *independent equipment possesses both of the following characteristics: a) The ability to perform its required function is unaffected by the operation or failure of other equipment. b) The ability to perform its required function is unaffected by the occurrence of the effects resulting from the initiating event for which it is required to function*.

In the following, thoughts about the applicability of the above mentioned characteristics of the DiD concept, i.e.

- the number of hierarchical DiD levels,
- the degree of independence between all DiD levels and
- the existence of barriers

with regard to new reactor designs are presented.

Considerations about "new evolutionary LWR" designs and DiD

The following considerations look at those new reactor designs that may be called "evolutionary LWR" designs, because they can be characterised as developments based on stepwise introduction of new safety features based on existing LWR technology. The "evolutionary" developments essentially are achieved by further implementation of passive safety features that are sometimes claimed not to require operator intervention and/or power sources. In addition, for some of these designs, "in-vessel retention" capabilities in case of core damage are claimed. These characteristics will be reflected in the following considerations.

In general, the main characteristics of DiD will have to be applied to any reactor concept. However, depending on the reactor design characteristics, the manner of execution of DiD may be changed, as discussed subsequently.

With regard to the number of hierarchical DiD levels, the following considerations are proposed:

- *Level 1:* *Prevention of abnormal operation and system failures*:

  This level and the related equipment and procedures will always exist, independent from the reactor design.

- *Level 2:* *Control of abnormal operation and failures and avoid the occurrence of accidents:*

  It seems reasonable to assume that deviations from normal operation or level 1 equipment failures can't be excluded by design, and therefore, this level and the related equipment and procedures will also exist, independent from the reactor design.

[9] O4: *enhancing the effectiveness of the independence between all levels of defence-in-depth, in particular through diversity provisions (in addition to the strengthening of each of these levels separately as addressed in the previous three objectives), to provide as far as reasonably achievable an overall reinforcement of defence-in-depth.*

- *Level 3: Control of design basis accidents and prevent escalation to severe accidents:*

  It is possible that basic design features could be relied upon to screen out certain initiating events and potentially consequential, challenging phenomena on the basis of their physical impossibility. This may potentially impact the scope of safety measures provided at level 3 of DiD, according to the list of single initial and multiple failure events postulated for the specific reactor design.

  Thus, the thoroughly based definition of a reactor design specific list of postulated initiating events (PIEs) for single initial and multiple failure events is considered as an essential task for establishing the scope of implementation of the 3rd DiD level for new reactors designs.

- *Level 4: Control of severe accidents, including prevention of accidents progression and mitigation of the consequences of severe accidents:*

  For existing LWR types, severe accident management measures have been derived for the prevention of severe accident progression and the mitigation of the consequences of such accidents. If, for new reactor designs, certain severe accident conditions can be considered as practically eliminated, it can potentially be argued that some of these measures are not required.

  For "new evolutionary LWR" designs, it is considered not to be feasible to practically eliminate severe accident conditions, unless core melt can be demonstrated to be physically impossible. In case, "in-vessel retention" features of the design are put forward, severe fuel degradation is postulated and the retention capabilities would be assigned to DiD level 4.

With regard to the degree of independence between all DiD levels (as far as reasonably achievable), the following considerations are proposed:

According to the DiD definition from the IAEA Safety Glossary, 2018 Edition, see above, the different DiD levels deploy diverse equipment and procedures. With regard to DiD level 3, additionally inherent safety features are mentioned (see also IAEA Safety Glossary). Therefore, in the following, independence between DiD levels is discussed with regard to the independence of

- procedures,
- inherent features, and
- equipment (i.e., systems, structures and components, SSCs).

Procedures[10]:

Procedures that are necessary on different DiD levels have to be written and applicable specifically for the respective level. Otherwise the concept of independence is not relevant regarding procedures. Procedures have to be applied by the plant staff and there is no requirement on independence of staff. This will also be true for "new evolutionary LWR" designs.

Inherent features[11] :

In general, the non-functioning of an inherent feature that is based on empirical evidences or laws of nature could potentially be considered as physically impossible and could be excluded on this basis. If this is the case, such features can be credited on different DiD levels and there is no requirement for an independent measure.

However, certain boundary conditions that may be necessary for functioning of an inherent feature may not be available adequately in time or place[12]. Therefore, if the non-functioning of an inherent feature can't be shown to be excluded, this features should not be credited on different DiD levels, but independent measures should be available, in particular because the independence between the DiD levels shall be strengthened in new reactor designs (see Objective O4 in [1]). This will also be true for "new evolutionary LWR" designs.

Equipment (systems, structures and components, SSCs[13]):

For existing LWR types, there are SSCs that are credited on different DiD levels (e.g. the reactor core control rods, the pressure retaining boundary). According to Objective O4 in [1], independence between the DiD levels shall be strengthened in future designs, and therefore, the extent of SSCs that are credited on different DiD levels be reduced. However, this may lead to unreasonable technical solutions, e.g. when looking at the containment. Therefore, for new reactor designs, non-independent SSCs should be listed and well-founded. This is also true for so called passive systems, as long as the non-functioning of these systems can't be excluded. Again, this also should be the case for "new evolutionary LWR" designs.

With regard to the number of barriers, the following considerations are proposed:

The three physical barriers mentioned above have been developed because of the reactor operation design characteristics of most LWR plants, not purely or systematically due to safety considerations. Thus, in our understanding, the existence of these barriers, is design dependent and may be different in future designs (e.g. molten fuel reactor types).

However, as long as there are significant radioactive inventories in a plant, a multi-barrier approach is considered as necessary. The number and kind of barriers will depend on the design characteristics of new reactor designs and definition of what is considered as minimum will need detailed analyses. For "new evolutionary LWR" designs, this is not relevant since the three physical barriers are still present.

[10] *A series of specified actions conducted in a certain order or manner* (Definition from IAEA Safety Glossary, Edition 2018).

[11] There is no definition of this term in the IAEA Safety Glossary. In the following text, inherent features are understood as properties of e.g. a material (such as heat capacity, neutron cross sections), that are quantified by empirical evidences, physical laws etc.

[12] With regard to the availability of passive systems, see e.g. WENRA/RHWG Report "Regulatory Aspects of Passive Systems", 01 June 2018.

[13] SSCs: A general term encompassing all of the elements (items) of a facility or activity that contribute to protection and safety, except human factors (Definition from IAEA Safety Glossary, Edition 2018).