Towards European Licensing of Small Modular Reactors

Development of requirement management approach for safety analysis methodology

WP 2: Development of safety analysis methodology for LW-SMRs

Authors:

A. Rantakaulio, O. Suurnäkki, A. Helminen

Confidentiality:

Public

Revision 0

This project has received funding from the Euratom research and training programme 2014-2018 under Grant Agreement No. 847553.

Report's title	
Development of requirement management approach for safety analysis methodology	
Author(s) Antti Rantakaulio (Fortum), Olli Suurnäkki (Fortum), Atte Helminen (VTT)	**Pages** 20
Keywords SMR, safety systems, passive safety features, safety assessment, safety requirements, requirement management	**Report identification code**

Summary

For the licensing of small modular reactors (SMR), it is important to find consensus on the reliability assessment methods of passive safety systems. This is required to ensure the benefits of serial production and standard design. In ELSMOR Task 2.3 the aim is to develop an approach to elaborate high-level safety goals to more concrete lower level requirements in a systematic and hierarchical manner. The approach aims to provide a framework for defining requirements of different levels of detail and creating tangible and traceable linking between the elaborated safety requirements and the safety assessment results.

The report focuses on safety assessment of passive safety features and the new ideas how to ensure passive safety. The report presents three different hierarchical levels to handle this issue: plant, system and phenomena. Practical demonstration on the approach is given using the conceptual design and passive safety systems of NUWARD™ as an example reference design.

Confidentiality	Public

Espoo, 30.11.2020

Written by	Reviewed by	Accepted by
Antti Rantakaulio	Nathalie Playez	Ville Tulkki
Task 2.3 Leader	Work package 2 leader	ELSMOR project coordinator

Contents

1. Introduction

Small modular reactors (SMR) promise a lot of new innovative solutions to the nuclear power business. Some of them are related to project and construction management such as faster and cheaper projects (schedule and budget), common and standardized design, serial production etc. Some of them are more technical such as inherent safety, increased autonomy and extensive usage of passive safety features.

Some of these technical aspects are not new to nuclear power business. Similarly to large power reactors, the safety of SMR relies on the Defence-in-Depth (DiD) principle and therefore fulfilment of DiD requirements will be essential for the licensing of SMR. However, unlike in the case of mainstream large power reactors, the passive safety features are incorporated extensively in SMR. Safety systems applying passive features are seen as a sustainable solution for two contradicting basic requirements: adequate safety vs. economical design. The passive safety systems help to ensure adequate DiD, and on the other hand, due to their simplicity they help to ensure economically viable design solutions. However, there is no common international methodology to license and assess the safety of passive safety features. For the licensing of SMR, it is important to find consensus on the reliability assessment methods of passive safety systems. This is required to ensure the benefits of serial production and standard design.

In ELSMOR Task 2.3 the aim is to develop an approach to elaborate high-level safety goals to more concrete lower level requirements in a systematic and hierarchical manner. The approach aims to provide a framework for defining requirements of different levels of detail and creating tangible and traceable linking between the elaborated safety requirements and the safety assessment results.

2. Safety requirement management and assessment approach

The Defence-in-Depth (DiD) requirements and their assessment create the foundation of the requirement management approach presented later in the report. The approach is originally generated for large power reactors. However, the approach is based on generic safety principles, and therefore, applicable for the safety design of SMR as well.

2.1 Defence-in-Depth principle

Defence-in-Depth is the most commonly applied principle in the safety design of nuclear power plants. IAEA defines DiD as the primary means of preventing and mitigating the consequences of accidents. DiD is implemented primarily through the combination of a number of consecutive and independent levels of protection that would have to fail before harmful effects could be caused to people or to the environment. If one level of protection or barrier were to fail, the subsequent level or barrier would be available. When properly implemented, DiD ensures that no single technical, human or organizational failure could lead to harmful effects, and that the combinations of failures that could give rise to significant harmful effects are of very low probability. The independent effectiveness of the different levels of defence is a necessary element of DiD. /5/

Defence-in-Depth is generally structured in five levels as follows /6/:

Level 1: Prevention of abnormal operation and failures.

Level 2: Control of abnormal operation and detection of failures.

Level 3: Control of accidents within the design basis.

Level 4: Control of severe plant conditions, including prevention of accident progression and mitigation of the consequences of severe accidents

Level 5: Mitigation of radiological consequences of significant releases of radioactive material.

For new reactors designs there is need to consider complex situations, such as multiple failure events, as part of the 3rd level of DiD, but with a clear distinction between means and conditions. This has led to division of the 3rd level of DiD to sub-levels 3.a and 3.b in /8/.

2.2 Safety functions and plant states

Safety design based on DiD principle includes both functional and physical solutions and covers both technical and organisational means to ensure plant safety. For the functional solutions, the requirements are to be fulfilled in all plant states for the fundamental safety functions: (i) control of reactivity; (ii) removal of heat from the reactor and from the fuel store; and (iii) confinement of radioactive material, shielding against radiation, as well as limitation of accidental radioactive releases.

The plant design has to ensure that plant states that could lead to high radiation doses or to a large radioactive release are extremely unlikely to arise, and that there is no, or only minor, potential radiological consequences for plant states with a significant likelihood of occurrence. Plant states are identified and grouped into a limited number of categories primarily on the basis of their frequency of occurrence. The different plant states have been defined in /7/ as follows:

(a) Normal operation;

(b) Anticipated operational occurrences, which are expected to occur over the operating lifetime of the plant;

(c) Design basis accidents;

(d) Design extension conditions, including accidents with core melting.

Plant states are called “plant condition categories” by /8/. Mapping of plant condition categories with DiD levels and the categories presented in Appendix 1 (explained later in the report) is shown in Table 1.

Table 1. Mapping of DID levels, plant condition categories and categories of Appendix 1

DiD level	Objective	Plant condition category	Categories of Appendix 1
1	Prevention of abnormal operation and failures	Normal operation	DBC1
2	Control of abnormal operation and failures	Anticipated operational occurrences	DBC2
3a	Control of accident to limit radiological releases and prevent escalation to core melt conditions	Postulated single initiating events	DBC3 DBC4
3b		Design extension cases	DEC A
4	Control of accidents with core melt to limit off-site releases	Postulated core melt accidents (short and long term)	DEC B
5	Mitigation of radiological consequences of significant releases of radioactive material		

2.3 Defence-in-Depth requirements and their assessment

Defence-in-Depth requirements and associated safety assessments have the primary role in safety management of nuclear power plants. In /9/, DiD requirements have been grouped into four categories: 1) deterministic plant condition category related requirements; 2) probabilistic plant condition category related requirements; 3) independence requirements between DiD levels; and 4) individual DID level strength requirements.

DiD related requirements form the basis of requirements for design of NPP, but there are of course large number of important safety function and system specific requirements. Many of those requirements are however covered by the above DiD concept originated requirements.

A summary of DiD requirements and their assessment is given below. The summary is based on descriptions given in /9/.

2.3.1 Deterministic plant condition category related requirements

Deterministic plant condition category related requirements refer to the traditional way of performing deterministic safety assessment (DSA). The content of DSA can be encapsulated into the following tasks:

1. Generation of scenarios (postulated initiating events and failure criteria)

2. Assessment of scenarios.

In order to effectively manage the multitude of scenarios, it is necessary to define certain topology of scenarios so that scenarios which are close to each other can be grouped together after which only the enveloping scenario needs to be assessed.

Scenarios shall be classified according to the plant condition categories since these determine the applied failure criteria and acceptance criteria. Plant condition categories are associated with frequency criteria but these are not the only rules how events are actually classified. In reality, the classification of events often follows pre-determined categorisations e.g. included in the regulatory guides, previously done classifications for similar designs. Application of the frequency criterion is more relevant when new types of postulated initiating events need to be considered in DSA.

2.3.2 Probabilistic plant condition category related requirements

Probabilistic end state based requirements are assessed by probabilistic risk assessment (PRA). Equivalently PRA verifies Defence-in-Depth as follows:

- Level 1 PRA and core damage frequency (CDF) verifies DiD levels 1–3
- Level 2 PRA and large release frequency (LRF) verifies DiD levels 1–4
- Level 3 PRA and societal risk metric verifies DiD levels 1–5.

Assessment against numerical risk criteria is not the only usage of PRA. One important impact of using PRA is the design simplification and optimization and removal of excess conservativism from the safety design.

2.3.3 Independence requirements between DiD levels

/4/ defines independence as the following characteristics for an equipment:

- The ability to perform its required function is unaffected by the operation or failure of other equipment;
- The ability to perform its function is unaffected by the occurrence of the effects resulting from the postulated initiating event for which it is required to function.

In order to assess independence at least the following features should be addressed:

- No shared parts
- No common support systems
- No functional dependences
- Physical separation
- No failure propagation.

To large extent these assessments will be covered when the plant condition category based assessments (DSA, PRA) are made. These assessments usually include analyses of different initiating events and failure postulations. With this approach DiD levels and systems in different levels are challenged from different angles. Information collected and analysed in DSA/PRA must be structured and presented in a manner that support the demonstration of independence.

2.3.4 Individual DiD level strength requirements

Individual DiD level strength requirements consists of a set of specific requirements which vary between different levels of DiD. These are more design rules than issues for a safety assessment. Only if some requirement is not fulfilled, justifying assessment is needed for that case.

Examples of types of requirements:

- redundancy, single failure tolerance
- physical separation between redundancies
- safety classification
- power supply arrangements
- environmental requirements
- mission time
- man-machine interface
- manual control, testing, inspections, maintenance.

Many of these requirements are safety function and system specific.

3. Passive safety features

3.1 Passive safety systems

To ensure adequate Defence-in-Depth, and on the other hand, to ensure economically viable design solutions, passive safety features are incorporated in the safety design of SMR. The passive safety features combine the advantage of simplicity, reduction of the need for human interaction and avoidance of external electrical power or signals.

The passive safety features are nothing new and they have been previously incorporated in the safety design of large power reactors. The large power reactors with passive safety features are called innovative or advanced nuclear power plants. In the advanced nuclear power plants, the systems with passive safety features are usually involved in safety functions focusing on: a) the removal of decay heat from the core after a reactor scram; b) the removal of heat from the containment and reduction of pressure inside containment subsequent to a loss of coolant accident.

In /1/ different types of passive safety systems considered for a) the removal of decay heat from the core are the following:

- Pre-pressurized core flooding tanks (accumulators)
- Elevated tank natural circulation loops (core make-up tanks)
- Gravity drain tanks
- Passively cooled steam generator natural circulation
- Passive residual heat removal heat exchangers
- Passively cooled core isolation condensers
- Sump natural circulation

And for b) the removal of heat from the containment and reduction of pressure inside containment the following:

- Containment pressure suppression pools
- Containment passive heat removal/pressure suppression systems
- Passive containment spray

Similar to the advanced nuclear reactors, the passive safety features of SMR are typically deployed by using one or more passive safety systems listed above.

3.2 Classification of passive systems

/2/ provides definitions for safety related terms as applied to advanced nuclear power plants. In the document, a passive safety system is defined as: *"Either a system which is composed entirely of passive components and structures or a system which uses active components in a very limited way to initiate subsequent passive operation."*

Due to this possibility to use active components in a very limited way makes the determining whether a system is considered an active or passive system quite ambiguous. To emphasis the passive features, and on the other hand, the significance of active components for the functioning of system a specific classification is given in /2/. In the classification, systems are divided into categories A, B, C and D. The degree of passivity decreases and the involvement of active components in the system's functioning increases from category A to D. The characteristics and examples of each category is described below.

Category A:

- No signal inputs of 'intelligence'
- No external power sources or forces
- No moving mechanical parts, and
- No moving working fluid.

Examples of passive features in the systems belonging to this category are physical barriers and static structures such as nuclear fuel cladding, pressure boundary systems and hardened building structures against external events. Core cooling systems relying purely on heat radiation and conduction belong to this category. Category A systems could be described as passive structures with no change of operating stage.

Category B:

- No signal inputs of 'intelligence'
- No external power sources or forces
- No moving mechanical parts; but
- Moving working fluids.

Examples of passive features in the systems belonging to this category are moving working fluids and the phase changes and chemical reactions of medium. Reactor emergency cooling systems based on natural circulation of water in heat exchangers belong to this category. Category B systems could be described as having passive functionality where the change of operating stage uses operating power from the process directly.

Category C:

- No signal inputs of ‘intelligence’
- No external power sources or forces; but
- Moving mechanical parts, whether or not moving working fluids are also present.

Examples of passive features in the systems belonging to this category are moving mechanical parts such as spring loaded check valves opening based on pressure difference. Emergency injection systems consisting of gravity driven accumulators, or storage tanks, and discharge lines equipped with check valves belong to this category. Category C systems could be described as having passive functionality where change of operating stage uses stored operating power initiated by operating power from the process.

Category D:

- Signal inputs of ‘intelligence’ to initiate the passive process
- Energy to initiate the process must be from stored sources such as batteries or elevated fluids
- Active components are limited to controls, instrumentation and valves to initiate the passive system
- Manual initiation is excluded.

Examples of passive features in the systems belonging to this category are passive execution of stored energy based on active actuation. Emergency core cooling and injection systems based on gravity that are initiated by battery-powered electric or electro-pneumatic valves belong to this category. Category D systems could be described as having passive functionality where change of operating stage uses stored operating power initiated by active operating power.

In practical applications, there may be hybrid systems where passive features of different categories are implemented in the same system. In such cases, the system is classified under the lower passivity category.

3.3 Challenges in safety assessment of passive systems

Passive systems are based on application of laws of nature, such as gravity and stored energy. The idea is that they perform their accident prevention and mitigation function by using driving forces of nature. The natural forces that drive the operation of passive systems are normally small. Therefore, the counter-forces and other adverse effects can be of comparable magnitude and have to be analysed thoroughly. There are typically considerable uncertainties related with the quantity of natural forces and on the factor they depend on, e.g. heat transfer coefficients and pressure losses, all of which are depend on how the system is configured. Another big source of uncertainties to natural driving forces is the effect of plant specific conditions and human actions. These may vary significantly between normal operation and possible accident situations.

The uncertainties of passive systems have been traditionally addressed in reliability assessments. Several reliability modelling approaches have been proposed over time and couple of approaches are discussed and compared for example in /3/. Based on the comparison, it has become evident that there are differences between the different approaches and the general consensus is that a more practical approach would be very helpful for further design and qualification of passive systems in advanced nuclear power plants.

From the licensing point of view, it is important to find consensus on the reliability modelling and reliability assessment methods for passive systems. It is almost as important to understand that the uncertainties are due to different sources and the solution is not necessarily just one, single reliability assessment method, but a combination of methods, which assess the uncertainties relevant for the DiD requirements. For this purpose, the creation of hierarchy of safety requirements for passive systems following the grouping of DiD requirements presented in the previous section is important. For the licensing purposes, the application of both deterministic (physical calculations with predetermined initial state) and probabilistic approaches is beneficial due to complex uncertainties involved with passive systems.

4. Requirement management

4.1 Requirement management principles

High-level safety requirements have been collected in /13/. In this report these high-level requirements are used to focus on key DiD requirements and implementation of these requirements for the NUWARD^{TM} passive safety systems. To limit the scope, only two essential high-level requirements regarding DiD are selected. The requirements and their background are listed below. The lower-level requirements present important aspects of passive safety features of SMRs are elaborated from these selected high-level requirements.

The identifiers of high-level requirements are the same as /13/. The coding of lower-level requirements follows the coding of upstream requirement and suffix "-n" is added. For example, if lower-level requirement is based on high-level requirement DID-04, the id of lower-level requirement is DID-04-L1.

4.2 High-level safety requirements

Two high-level safety requirements have been selected to serve as examples for the safety requirement process to be utilized in a safety assessment. These requirements serve as the main requirements for the system architecture, i.e. the plant level demonstration of safety. Lower-level requirements developed from them are used to build the complete assessment from the system and component level safety assessments.

As presented in Chapter 3.3, demonstration of reliable actuation and operation in a wide matrix of possible operational and environmental parameters can be challenging for passive safety features. Therefore the high-level safety requirement DID-04 should be given special consideration in the safety assessment process.

Requirement ID	Requirement text	Upstream requirement(s)
DID-04	The implementation of Defence-in-Depth in LW-SMRs must be tolerant.	IAEA SSR 2/1, INSAG-10, GENIV BSA, SO1-SO3

Passive safety features may be proposed to be utilized in multiple DiD levels, sometimes by utilizing the same system in multiple levels. In some cases, passive safety systems on different levels may be structurally different but rely on the same physical phenomenon. This may lead to challenges in demonstration of independence of the DiD levels. Therefore the high-level safety requirement DID-07 should be given special consideration in the safety assessment process.

Requirement ID	Requirement text	Upstream requirement(s)
DID-07	The levels of Defence-in-Depth must be independent as far as practicable.	IAEA SSR 2/1, INSAG-10, SO4

4.3 Lower-level safety requirements

In order to create a safety analysis process, the high-level safety requirements presented in Chapter 4.2 must be developed into lower-level safety requirements.

In this Chapter, three lower levels of requirements for safety analysis process are described. The focus is on passive safety functions and especially on functions designed to manage design basis accidents (DBC3, DBC4) as described in Chapter 5. The requirement examples given are generic by nature, and should be modified for the plant design and the system that is being analysed. For example, in order to utilize the requirement examples in demonstration of fulfilment of the high-level safety requirements for the NUWARD™ design, details of the NUWARD™ plant and system design should be taken into account.

Level 1 requirements reflect the demonstration of safety at the level of specific subsets of the system architecture, i.e. the plant design. Here the selected subset is the set of passive safety systems, for which a non-exhaustive list of example Level 1 requirements is presented in the following table.

Requirement ID	Requirement text	Upstream requirement(s)
DID-04-L1-01	Tolerance for deviations in actuation and operating parameters of the passive safety systems shall be demonstrated.	DID-04
DID-07-L1-01	Functional independence between passive safety systems performing the same safety function on different DiD levels shall be demonstrated.	DID-07

Level 2 requirements reflect the need to analyse behaviour of specific systems to demonstrate the aspect required in the Level 1 requirements. A non-exhaustive list of example Level 2 requirements is presented in the following table.

Requirement ID	Requirement text	Upstream requirement(s)
DID-04-L2-01	Effects of deviations from pre-defined system configurations for the actuation and performance of passive safety systems shall be analysed.	DID-04-L1-01
DID-04-L2-02	Effects of deviations from designed actuation parameters for the actuation and performance of passive safety systems shall be analysed.	DID-04-L1-01
DID-04-L2-03	Effects of deviations of operating conditions during the performance of passive safety systems shall be analysed.	DID-04-L1-01
DID-07-L2-01	Independence of equipment used in actuation of passive safety systems performing the same function on different DiD levels shall be demonstrated.	DID-07-L1-01
DID-07-L2-02	Effects of the failure of a passive safety system on the actuation and performance of passive safety systems performing the same function on different DiD levels shall be analysed.	DID-07-L1-01
DID-07-L2-03	Effects of a spurious actuation of a passive safety system on actuation and performance of passive safety systems performing the same function on different DiD levels shall be analysed.	DID-07-L1-01

Level 3 requirements reflect the need to analyse the behaviour of specific components of specific system or phenomena that are present in the operation of a specific system. A non-exhaustive list of example Level 3 requirements is presented in the following table.

Requirement ID	Requirement text	Upstream requirement(s)
DID-04-L3-01	Effects of system valve closing fully or partially during the performance of a passive safety system shall be analysed.	DID-04-L2-01
DID-04-L3-02	Effects of a single actuation parameter being outside the designed range for the actuation of a passive safety system shall be analysed.	DID-04-L2-02
DID-04-L3-03	Effects of operating parameters drifting outside the designed range for the performance of a passive safety system shall be analysed.	DID-04-L2-03

5. Design solutions of the French SMR NUWARD(TM)

5.1 Overall description

NUWARD^{TM} is a multi-module unit SMR design which utilises heavily integrated design. Thus, the main components of primary circuit such as reactor core, pressurizer and steam generators are all located inside the reactor pressure vessel. This means that there are no separate primary circuit loops. The metallic containment shell which houses the integrated primary circuit is immersed in a water pool which acts also as heat sink in case of accident. /14/, /12/

Safety of the NUWARD^{TM} design relies heavily on passive safety systems and features. The objective is that normal operation and the response to transients are robust. This is achieved by design margins, a larger primary inventory, boron-free operation and simplified systems.

Management of design basis accidents (DBC 3 and 4 conditions), relies on passive safety systems and features. Passive safety systems include the passive decay heat removal system RRP and the accumulators used as water makeup system RIS. In normal operation when the normal systems are operating (using normal compact steam generators), the passive heat removal system RRP are not operating (valves on secondary loops of RRP are closed and safety compact steam generators are just immersed in primary water). When the functionality of the RRP system is needed, the decay heat from the reactor is transferred via the RRP system loops to the heat sink (water pool) via the safety compact steam generators and the safety condensers located inside the containment. The RRP system is actuated by the safety I&C system based on measurements. The system starts operating when the parallel, diversified motor operated valves on secondary loops are opened.

Accumulators of system RIS are required to inject water inside the reactor pressure vessel in the medium term (~ 30 min) to compensate volume changes caused by evaporation. The actuation of the accumulators is based on the decreased primary pressure.

The autonomy objective for the passive safety systems is 72 hours which means that no operator actions are needed for 72 hours after initiation of DBC 3 and 4 conditions. The large water pool which acts as the heat sink is one of the aspects which ensure that operator actions are not needed in first 72 hours.

The emergency cooling chain consists of the following phenomena and systems:

- Natural circulation inside the reactor pressure vessel between the reactor core and the safety compact steam generators
- Natural circulation inside the secondary loops between the safety compact steam generators and the safety condensers
- Natural circulation inside the tertiary loops between the safety condensers and the water pool surrounding the containment vessel

In design extension conditions (DEC) active safety systems are needed to ensure the safety of the reactor. For example in case of an anticipated transient without scram (ATWS), an active system is needed for boron injection. Also in case of common cause failure of the RRP system and small break loss of cooling accidents (SBLOCA), an active water injection system is needed.

Severe accident management (SAM) is based on the concept of in-vessel retention (IVR). The reactor pit surrounding the reactor vessel, can be flooded with water using passive systems. The water used may come from LOCA event or the separate tank called the Heavy Neutron Reflector (HNR) inside the containment. Also there is an additional depressurization system to decrease the primary circuit pressure if needed. Risks created from hydrogen formation are prevented by injecting nitrogen into the containment. Design of the severe accident management systems is not yet finalised.

5.2 Design principles

Appendix 1 presents allocation of safety functions (systems) to Defence-in-Depth levels based on their objective (fundamental safety function). /14/

Systems implemented in different DiD levels are all designed to be independent. Redundancy principle is applied to systems on level 3a (i.e. systems designed for managing DBC 3 and 4 conditions, e.g. RRP and RIS systems). Diversity principle is applied to the actuation of the decay heat removal function. There are two independent safety I&C systems, protection I&C system and I&C diverse system. Diversified actuation parameters are also utilized (e.g. low water level vs high temperature or low pressure).

An estimation of the degree of passive safety of the NUWARD™ passive safety systems according to IAEA TECDOC 626 (see chapter **Error! Reference source not found.**) is presented below.

The passive decay heat removal system RRP can be evaluated to represent level D degree of passive safety. The evaluation is based on the reliance on the motor-operated valves which require both external actuation from the protection and diverse I&C systems and external electrical power to operate the valve actuators (i.e. batteries).

Accumulators of the makeup water system RIS can be evaluated to represent level C degree of passive safety. The system relies on check valves which actuate (i.e. open) when the primary pressure has decreased sufficiently.

The in-vessel retention function which basically means that reactor core is kept in the reactor pressure vessel and it is cooled from the outside. from outside. Typically this means that there are ducts to flood the cavity of the reactor pressure vessel and a system to circulate and cool the water. This function can be evaluated to represent levels D degree of passive safety. Design of the system is not finalized and therefore the actuation of the system is assumed to be based on an external manual command via the safety I&C systems. This manual command is assumed to be used to open valves which allow the water to flow into the reactor pit.

6. Safety assessment and uncertainties

6.1 Linking the requirement management approach with safety assessments of ELSMOR WP3 and WP4

The objective of a safety assessment is to verify the safety requirements by analysis, simulations and other means. The assessment should identify uncertainties and analyse their impacts in to the safety assessment results. It is especially important to assess the DiD level strengths and independence of individual DiD levels. For example, it should be analysed that a failure of a passive safety system in one DiD level doesn't affect systems in the next DiD level. Also, if a safety system is performing multiple safety functions (partly or totally) it should be analysed what happens if it fails.

As stated in Chapter 3.3, a hierarchy for the safety requirements of passive safety features should be defined. This helps to understand and analyse uncertainties and their impact more effectively. One way of defining the hierarchy for the safety requirements of passive safety features is given in Table 2.

Table 2. Safety requirement hierarchy

Level	DiD requirements	Uncertainty examples	Description
Plant	Independency between DiD levels. Independency within a single DiD level.	Passive safety features should not be disturbed by active systems. Performance of safety systems in abnormal conditions.	Depending on the concept there might be passive and active safety system on a same DiD level such as high pressure injection pumps and accumulators and these do not interfere with each other. In some concepts the main defence line (i.e. DiD level 3a) is based on passive safety features and active systems are backing these up. It should be noted, if active systems actuate at the same time as the passive safety features, they shall not interfere each other. Passive safety features should also work in abnormal conditions (plant states, states of other systems hazards changing environmental parameters, etc).
System	Strength of individual DiD level.	System reliability and system failures.	In some cases, passive safety features require certain active components to work, for example closures or openings of valves. Some lines need to be isolated and others opened to actuate the passive safety feature. If these fail or system functions only partly it might cause disturbances to passive safety feature.
Phenomena / parameter	-	Strength of phenomena of passive safety features;	Passive safety features rely on phenomena such as natural circulation, gravity etc.

Level	DiD requirements	Uncertainty examples	Description
		parameters such as temperature range, pressure range which can have effect on system and plant levels.	Demonstration of "once actuated" passive safety feature such as accumulator is rather straightforward. Instead, demonstration of continuous passive safety features such as decay heat removal based on natural circulation is not so straightforward. Also, some continuous safety features might be time-dependent. Natural circulation is based on gravity and driving force provided by density difference (i.e. temperature difference) and it is prone to disturbances. Also, temperature differences typically decrease as function of time; decay heat decreases and temperature of heat sink rises.

The DiD requirements discussed above are for the most part system level and system architecture level requirements. However, it should be noted that phenomena can affect plant and system level if all uncertainties are not recognised. In the design process, these requirements are implemented to actual system designs through functional and technical specifications.

The tasks performed in ELSMOR Work Packages 3 and 4 concentrate on the identification of significant thermo-hydraulic (T-H) phenomena relevant for passive safety features and on the validation of T-H models based on experimental data. The scale of the T-H models, i.e. if the modelling is done on system or equipment level, is not known. Also, the scale and conformity of experimental facility, i.e. the details of the facility where the experimental data is retrieved, with the actual NUWARD^{TM} design is not known at the stage of writing this report.

The design specifications given in Section 5 for NUWARD^{TM} are mainly on the system architecture level. Connecting these specifications directly to the work carried out in WP3 and WP4 is not straightforward. In spite of the unknown factors, the analyses of WP3 and WP4 can be used to support the requirement verifications of passive features of NUWARD^{TM} safety systems. One important area of support is the identification and documentation of uncertainties involved with passive safety systems.

6.2 Classes of uncertainties

The current state of the art in the reliability of thermal-hydraulic passive systems is discussed in a technical note by Burgazzi /10/. In the technical note the overall uncertainty relative to T-H passive systems assessment can be divided to the following classes:

1. uncertainties related to T-H analysis;
2. uncertainties related to T-H performance and
3. uncertainties related to the probabilistic analysis.

The first class considers uncertainties ranging from the approximation of the models characterising any physical phenomena, to the approximation of the numerical solutions, to the lack of precision of

the values adopted for boundary and initial conditions, and to the parameters used as inputs to the phenomenological models. From the plant safety design perspective, the class concentrates mainly on component level uncertainties.

The second class addresses uncertainties associated with factors on which the magnitude of the engaged forces and counter forces depend on (e.g. values of heat transfer coefficients and pressure losses). These factors are typically dictated by specific plant configurations and conditions at the time the system is called to perform, or during the performance of, its safety function. From the plant safety design perspective, the class concentrates mainly on system level uncertainties.

The third class refers to uncertainties related to the probabilistic risk analysis (PRA) model development and consists of the data uncertainty, the model uncertainty and the completeness uncertainty. Since PRA modelling is carried out all the way from component to plant level, from the plant safety design perspective this class can be used to give valuable insight on uncertainties associated with the design solutions of the system architecture level (i.e. plant level).

6.3 Uncertainty identification and documentation

The identification and documentation of uncertainties originating from phenomenological models and application of the information in PRA modelling is discussed in /11/. The report introduces a specific format for identifying, classification and evaluation of uncertainties, and for summarising results of uncertainties and sensitivity analyses.

The format consists of uncertainty documentation tables, in which each phenomenon or issue is considered. First the phenomenon is described and its significance for PRA, or decision under consideration, is evaluated qualitatively. In this connection, the decomposition of phenomenon and related accident sequences are documented, and the decompositions are justified. The relationships to other issues and other models are discussed. Next, the models or computer tools used in the analysis, and reasons to use them are discussed. The theoretical basis and the degree of validation of the models and tools are described. Furthermore, the use and role of formal or informal expert judgement is explained, and the sensitivity and uncertainty analyses together with applied methodologies and main results made are presented.

In addition to the above-mentioned general description each possible source of uncertainty is evaluated. In this connection both qualitative characterisation and, if possible, the impact of uncertainty to the final results is evaluated in a (semi)quantitative way. In some cases, it may be advantageous to evaluate whether the analysis is based on conservative, optimistic or "best estimate" assumptions. In order to direct additional analyses, the possibilities to reduce the uncertainty are presented.

In the documentation format, the sources of uncertainties to be covered include

- the inherent and knowledge uncertainties related to the phenomenon under analysis (e.g. randomness, turbulence, material properties)
- model uncertainties, including those originating from the scope of the analysis incompleteness
- uncertainties due to input data
- uncertainties due to boundary conditions applied in the model
- uncertainties in selection of initial states for calculations (e.g. initiating events, assumptions on the amount of certain substances in the system, the results from another model)
- uncertainties due to computational or numerical properties of the model (nodalisation, time steps).

These sources of uncertainties can be identified for the different levels of plant design (i.e. component, system and system architecture) and for different DiD levels. In the documentation, it is important to clearly express, which assumptions are made and why. Within an analysis, a best estimate may be used for some initial values while other parameters are based on conservative assumptions.

An example on the format and application of the documentation tables is given in /11/. The example presents an uncertainty analysis of hydrogen leakage and combustion from a BWR containment to reactor building rooms during a severe accident.

7. Conclusions

Similarly to large power reactors, the safety of SMR relies on the Defence-in-Depth principle. The fulfilment of DiD requirements will be essential for the licensing of SMR. However, unlike in the case of mainstream large power reactors, the passive safety features are incorporated extensively in SMR. This is the case also for NUWARD^{TM} design. Safety systems applying passive features are seen as a sustainable solution for two contradicting basic requirements: adequate safety vs. economical design. The passive safety systems help to ensure adequate Defence-in-Depth, and on the other hand, due to their simplicity they help to ensure economically viable design solutions. For passive features there are typically considerable uncertainties related with the quantity of natural forces and the factors they depend on. From SMR licensing point of view, it is important to find consensus on the reliability assessment methods evaluating these uncertainties.

ELSMOR Task 2.3 aims at developing an approach to elaborate high-level safety goals to more concrete requirements in a systematic and hierarchical manner. The approach aims to provide a framework for defining requirements of different levels of detail and creating tangible and traceable linking between the elaborated safety requirements and the safety assessment results. In ideal situation, the approach can be applied for the different types of safety assessments performed in WP3 and WP4.

In the report, a requirement management approach is presented. Practical demonstration on the approach is given using the conceptual design and passive safety systems of NUWARD^{TM} as an example reference design. Two high-level safety requirements, or safety goals, identified in /13/ are elaborated to lower-level requirements. The high-level requirements have been selected to represent important DiD strength and independence requirements on the system architecture level. The high-level requirements are elaborated to three lower levels of requirements. These requirements can be allocated for systems and components, and compliance to the requirements should be given in their technical specifications. The presented lower-level requirements are examples and cover only a portion of the assessment scope.

The tasks performed in ELSMOR Work Packages 3 and 4 concentrate on the identification of significant thermo-hydraulic (T-H) phenomena relevant for passive safety features and on the validation of T-H models based on experimental data. Connecting the system architecture and system specifications of NUWARD^{TM} directly to the work carried out in WP3 and WP4 is not straightforward. However, the work carried out in WP3 and WP4 can be used for the identification and documentation of uncertainties involved with the passive safety systems. Section 6.3 lists important sources of uncertainty, which could be considered in WP3 and WP4. The listing of potential uncertainties helps to evaluate the amount of work needed for the safety assessments. This information can be used later in ELSMOR Task 5.1a to identify aspects, which can ease or challenge SMR licensing compared to large power reactors.

Appendices

Appendix 1. NUWARD^{TM} concept Defence-in-Depth and fundamental safety functions

References

/1/ IAEA-TECDOC-1624, Passive Safety Systems and Natural Circulation in Water Cooled Nuclear Power Plants, IAEA, 2009.

/2/ IAEA-TECDOC-626, Safety related terms for advanced nuclear plants, IAEA, 1991.

/3/ IAEA-TECDOC-1752, Progress in Methodologies for the Assessment of Passive Safety System Reliability in Advanced Reactors - Results from the Coordinated Research Project on Development of Advanced Methodologies for the Assessment of Passive Safety Systems Performance in Advanced Reactors, IAEA, 2014.

/4/ IAEA Safety Glossary Terminology Used in Nuclear Safety and Radiation Protection, 2018 Edition

/5/ Fundamental Safety Principles, IAEA Safety Standards Series No. SF-1, IAEA, Vienna, 2006.

/6/ IAEA. 1996. Defence-in-depth in nuclear safety. INSAG-10. International Atomic Energy Agency, Vienna.

/7/ Safety of Nuclear Power Plants: Design, Specific Safety Requirements, IAEA Safety Standard Series No. SSR-2/1 (Rev. 1), IAEA, Vienna, 2016.

/8/ Safety of new NPP designs. Study by Reactor Harmonization Working Group RHWG, Western European Nuclear Regulators' Association. WENRA. 2013.

/9/ Holmberg, J.-E., Helminen, A. & Porthin, M., Using PRA to assess defence-in-depth — case study on level 2 of defence-in-depth, SAFIR 2018 - The Finnish Research Programme on Nuclear Power Plant Safety 2015–2018 (internal report), 2017.

/10/ Burgazzi, L., State of the art in reliability of thermal-hydraulic passive systems, Reliability Engineering and System Safety, Issue 92, 2007.

/11/ Pulkkinen, U. & Simola K., Identification and communication of uncertainties of phenomenological models in PSA, VTT Automation, 2001.

/12/ Kick-off meeting of Work Package 5 on 27 May 2020.

/13/ LW-SMRs main safety goals. ELSMOR project WP2. N. Playez, E. Courtin, L. Ammirabile, S. Israel. Revision 0. 23 September 2020.

/14/ Information from TechnicAtome (email on 11 September 2020 and meeting on 16 September 2020).

Appendix 1. NUWARD™ concept Defence-in-Depth and fundamental safety functions

Safety function	DBC1-2	DBC3-4	DEC-A	DEC-B
Reactivity control	Core design Boron-free CRDM control			
	Shutdown system (gravity driven)		Boron injection in case of ATWS	No criticality risk
Residual decay heat removal	Normal cooling system (condenser and VRA circuit)	Safety passive cooling system RRP Accumulators RIS	Depressurization system Water injection	Passive reactor pit flooding system ensuring corium cooling
Heat sink	Normal heat sink	Water wall up to 7 days Active cooling (if available) Passive water make-up after 7 days		
Confinement 1st barrier (cladding)	Integrity	Integrity (*no core uncovering*)	Integrity (*no core uncovering*)	Postulated core melting
Confinement 2nd barrier (primary circuit)	Integrity	Max LOCA:Φ 30 mm break	DBC3/4 initiating event Depressurization 2 x:Φ 30	RPV depress. < 20 bar before core melt Passive reactor pit flooding system
Confinement 3rd barrier (Metallic containment)	Integrity Static under pressure Cooling via normal heat sink	Integrity Pressure reduction via HNR tank when required Passive cooling and steam condensation via water wall		Integrity Additional confinement of leaks inside the water-wall Hall containment static / low flow venting
		H2 management with recombiners		Preventive N2 injection

Active systems highlighted in RED

Passive systems highlighted in BLUE