Towards European Licensing of Small Modular Reactors

LW-SMRs main safety goals

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

Authors:

N. Playez, E. Courtin, L. Ammirabile, S. Israel

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	
LW-SMRs main safety goals	
Author(s) N. Playez (Framatome), E. Courtin (Framatome), L. Ammirabile (JRC), S. Israel(IRSN)	**Pages** 16/
Keywords SMR, Safety Systems, Safety Demonstration	**Report identification code**

Summary

One of ELSMOR goals is to create methods and tools for the European stakeholders to assess and verify the safety of light water small modular reactors (LW-SMRs) which would be deployed in Europe.

The objective of the work performed in the task 2.1 was to propose a set of requirements for LW-SMRs in terms of defence-in-depth, severe accident prevention reliability, limitation of radiological consequences for accidents without core melt and with core melt, resistance to hazards, approach for practical elimination of situations, plant autonomy, etc. for which adequate safety methodologies must be developed to evaluate whether the safety objectives are fulfilled or not. Requirements that are considered mandatory have been distinguished from those who are desirable.

Confidentiality	Public

Fontenay-aux-roses, September 23rd 2020

Written by	Reviewed by	Accepted by
Sebastien Israel, Leader	Nathalie Playez, Supervisor	Tulkki Ville, Coordinator in behalf of the Management Committee

Contents

1. Introduction

One of ELSMOR goals is to create methods and tools for the European stakeholders to assess and verify the safety of light water small modular reactors (LW-SMRs) which would be deployed in Europe /ELS 01/.

The review performed in the WP1 of the safety directives given by the European Union, IAEA, WENRA, ENSREG as well as by selected countries (EU and non-EU) showed, that the current regulation can be basically applied also for LW-SMRs. The EU safety directives establishes a high-level and technological neutral framework. Within the IAEA regulations, no explicit guidance for SMRs is given up to now, but the current documents can be used for SMRs. This is also the case for ENSREG and WENRA. The objectives given in /WEN 2/ apply also for SMRs: low frequencies for accident without core melt, practical elimination for accident with core melt (or implementation of measures to limit consequences), independency of Defence in depth levels and radiation protection under the concept of ALARP (as low as reasonable possible).

The work done in WP1 also showed that SMRs bring innovative features and potential challenges on the safety demonstration methods. This may lead to some adaptations in the way to apply some well-known historical safety principles and approaches that still shall be the basis of the demonstration of the safety of SMRs. On the other hand, SMRs specifics need to be properly taken into account in and may lead to some expectations.

The objective of the work performed in the task 2.1 was to propose a set of requirements for LW-SMRs in terms of defence-in-depth, severe accident prevention reliability, limitation of radiological consequences for accidents without core melt and with core melt, resistance to hazards, approach for practical elimination of situations, plant autonomy, etc. for which adequate safety methodologies must be developed to evaluate whether the safety objectives are fulfilled or not. Requirements that are considered mandatory (so-called “must”) will be distinguished from those who are desirable (so-called “want”). As far as possible proposed requirements will refer to existing high level safety goals from WENRA (/WEN 2/ /WEN 3/) or IAEA (/IAEA 4//IAEA 5/).

2. Generic requirements

Safety requirement GEN-01

General safety objectives as described in /WEN 2/ must be considered for the design of LW-SMRs.

Flexibility: Not negotiable

Higher safety goal reference: /WEN 2/

Justification / Further explanations:

As new reactors, SMRs have to meet WENRA Safety Objectives for new nuclear power plants stated in /WEN 2/[1]. Safety Objectives are recalled in appendix 1.

Safety requirement GEN-02

WENRA positions as described in /WEN 3/ must be considered for the design of LW-SMRs.

Flexibility: Not negotiable

Higher safety goal reference: /WEN 3/

Justification / Further explanations:

As new reactors, SMRs shall take due consideration of WENRA positions stated in /WEN 3/[2]. Topics of positions are recalled in appendix 2.

3. Requirements related to defence-in-depth

Safety Requirement DID-01

The design of LW-SMRs must be based on the concept of defence-in-depth for preventing accidents and mitigating their consequences by postulating a set of initiating events and the subsequent failure of systems regardless of their reliability.

Flexibility: Not negotiable

Higher safety goal reference: IAEA SSR2/1, INSAG-10, SO1-O3

Justification / Further explanations:

Defence in depth (DiD) is a fundamental principle of nuclear safety for preventing accidents and mitigating their consequences and remains fully applicable to SMRs.

Defence-in-depth consists in a hierarchical deployment of different levels of equipment and procedures in order to maintain the effectiveness of physical barriers placed between radioactive materials and workers, the public or the environment.

The strategy for defence in depth is twofold: first, to prevent accidents and, second, if prevention fails, to limit their potential consequences and prevent any evolution to more serious conditions. Accident prevention is the first priority, since preventing the degradation of plant status and performance generally will provide the most effective protection means. Should preventive measures fail, mitigation measures can provide the necessary additional protection of the public and the environment.

[1] In the report, SO1, SO2, SO3 and SO4 will refer to WENRA Safety Objectives O1 to O4 as described in /WEN 2/
[2] In the report, PO1 to PO6 will refer to WENRA positions 1 to 6 /WEN 3/

Defence in depth is generally structured in five levels. Each successive level is designed by postulating a set of initiating events and the failure of systems associated to the previous level regardless of their reliability. Should one level fail, the successive level comes into play.

Safety Requirement DID-02

The implementation of defence-in-depth in LW-SMRs must be exhaustive.

Flexibility: Not negotiable

Higher safety goal reference: IAEA SSR2/1, INSAG-10, GENIV BSA, SO1-SO3

Justification / Further explanations:

Complementary and essential characteristics that help improving the safety level, ensuring the effectiveness of the defence in depth concept and easing the safety demonstration call for an exhaustive defence, e.g. the identification of the risks (postulated initiating events and safety systems failures), which leans on the fundamental safety functions, should be comprehensive.

The corresponding scenarios identified to design and size the safety architecture provisions must be as exhaustive as possible. This calls in first instance for a systematic and comprehensive identification of postulated initiating events (PIE) and then for the successive assessment of the failure of systems. Enveloping situations, which are taken into account independently of their expected occurrence frequency (single failure criterion; margins; postulated combinations; etc.) are expected to compensate possible lacks of exhaustiveness coherently with the defence-in-depth principle.

Safety Requirement DID-03

The implementation of defence-in-depth in LW-SMRs must be progressive.

Flexibility: Not negotiable

Higher safety goal reference: IAEA SSR2/1, INSAG-10, GENIV BSA, SO1-SO3

Justification / Further explanations:

Complementary and essential characteristics that help improving the safety level, ensuring the effectiveness of the defence in depth concept and easing the safety demonstration call for a graduated, progressive defence: postulated accident scenarios should entail the progressive failure of each DiD level reducing the total likelihood of leading to core melt.

The graduated, progressive assessment of defence-in-depth aims in priority at identifying and correcting any “short” sequences leading directly from level 1 to level 4 and beyond without any possibility of restoring safe conditions at an intermediate stage. More generally, it aims at implementing a sufficient number of lines of defence for any initiating event, depending on the event frequency, and based on the deterministic assumption that any provision may fail.

The enhanced use of passive systems and all inherent safety characteristics in LW-SMRs that are provided by the design and credited in the safety demonstration should be duly substantiated against well-defined requirements and criteria.

The use of passive systems calls designer to address several new challenges, e.g.:

a) new innovative technologies without sufficient operational experiences,
b) uncertainties related to qualification and reliability assessments,
c) operational aspects as periodic testing, maintenance and in-service inspections.

Whereas this requirement remains fully applicable to LW-SMR, the specific design characteristics and safety features of these reactors are expected to provide alternative means to justify sufficient independence with limited means.

Safety Requirement DID-04

The implementation of defence-in-depth in LW-SMRs must be tolerant.

Flexibility: Not negotiable

Higher safety goal reference: IAEA SSR2/1, INSAG-10, GENIV BSA, SO1-SO3

Justification / Further explanations:

Complementary and essential characteristics that help improving the safety level, ensuring the effectiveness of the defence in depth concept and easing the safety demonstration call for a tolerant defence: small deviation of the physical parameters outside their expected range should not lead to severe consequences (i.e. no “cliff edges”, see IAEA SSR 2/1).

Basically this objective could be fulfilled by the application of conservative analysis rules, taking adequate consideration of uncertainties and pessimistic assumptions on systems performances, in order to bring adequate margins at each level of defence in depth.

Safety Requirement DID-05

***The implementation of defence-in-depth in LW-SMRs must be forgiving*.**

Flexibility: Not negotiable

Higher safety goal reference: IAEA SSR2/1, INSAG-10, GENIV BSA, SO1-SO3

Justification / Further explanations:

Complementary and essential characteristics that help improving the safety level, ensuring the effectiveness of the defence in depth concept and easing the safety demonstration call for a forgiving defence: assure sufficient grace period for possibility of manual intervention and repair during accidental situations.

The degree of tolerance to operator intervention delay is usually associated with dynamic characteristics, such as large thermal inertia or wide operating margins with respect to safety limits, which provide more time before corrective action is needed.

LW-SMRs are expected to provide an enhanced forgiving defence by means of a more favourable ratio between power and water inventory or broader operating margins.

Safety Requirement DID-06

The implementation of defence-in-depth in LW-SMRs must be balanced.

Flexibility: Not negotiable

Higher safety goal reference: IAEA SSR2/1, INSAG-10, GENIV BSA, SO1-SO3

Justification / Further explanations:

Complementary and essential characteristics that help improving the safety level, ensuring the effectiveness of the defence in depth concept and easing the safety demonstration call for a balanced or homogeneous defence: no specific accident sequence should contribute to the global frequency of the damaged plant states in an excessive and unbalanced manner.

With the likelihood of core damage being equal and (very) low, it is, nonetheless, preferable a design for which the total risk is made up of a larger number of small frequency scenarios than to have that risk dominated by one or two higher frequency scenarios. Designs that exhibit no dominant vulnerabilities reflect the desirable characteristic of balance.

The PSA is a useful tool to assess this characteristic, albeit a robust deterministic implementation of defence-in-depth should also aim at balanced design.

Safety Requirement DID-07

The levels of defence in depth must be independent as far as practicable.

Flexibility: Not negotiable

Higher safety goal reference: IAEA SSR2/1, INSAG-10, SO4

Justification / Further explanations:

The independence among DiD levels, as far as practicable, is universally considered to be an important requirement to enhance the effectiveness of defence in depth.

Independence between systems, structure and components can be achieved by means of diversity, physical separation, structural or by distance and functional isolation. The sufficient independence of DiD levels should be assessed sequence by sequence (a system can be called at different DiD levels for different accident sequences).

The lower power levels in LW-SMRs call for the possibility of an extended use of passive and/or inherent safety systems. A robust safety demonstration of independence of defence-in-depth levels to LW-SMRs design can rely on the optimal combination of active, passive systems and inherent

Safety Requirement DID-08

The safety demonstration of implementation of defence-in-depth concept to LW-SMRs design must be primarily based on a deterministic approach, complemented by probabilistic insights.

Flexibility: not negotiable

Higher safety goal reference: IAEA SSR2/1, INSAG-10, GENIV BSA, SO1-SO3

Justification / Further explanations:

The deterministic approach remains the primary method for the implementation of defence-in-depth in LW-SMR. As for large reactors, PSAs should be used for SMRs to complement the deterministic approach.

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 sufficiency of the number of levels of defence implemented and the independence between them. 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.

PSA could indeed assess if the implementation of defence-in-depth is balanced against the individual contributors to the global risk.

Methods to deal with passive features and with multi-module issues in PSAs should be investigated or enhanced.

Safety Requirement DID-09

The emergency planning zone should be defined consistently with the radiological objectives applied in severe accidents.

Flexibility: negotiable

Higher safety goal reference: IAEA SSR2/1, INSAG-10, GENIV BSA

Justification / Further explanations:

The EPZ should be defined so that out of this zone, no radiological release should occur that would require protection measures for the population, in any plant accident condition.

The possibility for LWR-SMRs design to have enhanced safety performance through inherent, passive, and novel safety design features could constitute a robust basis to reinforce the prevention and mitigation of some incidents and accidents.

The exclusion or limitation of some postulated initiating events (e.g. loop breaks) can be considered as an important reinforcement of the DiD levels 1 and 2. It may also affect the definition of the representative core melt scenario considered in the design. Similarily the possibility to use a combination of active and passive systems or inherent safety features can reinforce the independence among DiD levels and the protection of design basis accidents (DID level 3) and the mitigation of severe accidents (DID level 4). Such LW-SMRs features can also affect the size of the EPZs and generally contribute to its reduction.

It is worth considering, however, that the limited operating experience of some innovative systems and their associated reliability could also constitute a challenge to the safety demonstration and need to be tackled opportunely against a well-defined set of safety requirements and criteria.

4. Requirements related to Design Basis Conditions

Safety Requirement DBC-01

The list of Postulated Initiating Events that could affect a module must be justified.

Flexibility: Not negotiable

Higher safety goal reference: SO2, PO1, PO2

Justification / Further explanations:

Some designers would claim that some postulated initiating events (PIE) are excluded by design on SMRs compared to the one for large reactors. If some of these exclusions seems to be obvious (for example: breaks on primary loops for integrated SMRs), some have to be justified (for example: loss of primary flow for SMRs without primary coolant pumps). If SMRs design can allow to exclude some events, some new events could raise. The list of PIE shall be justified. Besides the list of PIE should be comprehensive enough to prove that any credible challenge to the plant safety functions is suitably addressed.

Safety Requirement DBC-02

When listing the Postulated initiating events, it must be considered whether this PIE could affect several modules within the installation.

Flexibility: Not negotiable

Higher safety goal reference: SO2, PO1, PO2

Justification / Further explanations:

Some PIE could affect several units in the installation (for example Loss of offsite power-LOOP). Impact of multi-units events should be analyzed, in particular regarding consequences on plant autonomy and availability of shared systems.

Safety Requirement DBC-03

For each Postulated initiating event, it must be proved with a high level of confidence that the safety criteria are met.

Flexibility: Not negotiable

Higher safety goal reference: SO2, PO1, PO2

Justification / Further explanations:

Safety criteria shall be defined so to ensure that the safety objectives are met. The design-basis condition analyses shall follow analysis rules that ensure the conservatism of the analyses. To ensure that the safety criteria are met with a high level of confidence, the analyses rules shall consider credible failure modes of safety systems. In general, the single failure shall be applied to active components. If specific failure mode are ruled out, adequate justifications shall be provided (e.g failure of passive components). These justifications shall include a cliff-edge effect analysis of the consequences of the failure excluded, with less conservative assumptions and methodologies; DEC-A rules may be appropriate for this purpose.

5. Requirements related to Design Extension Conditions without core melt

Safety Requirement DECA-01

Prevention of core melting accident must be proved with a high reliability in level 3 of defence in depth based on an adequate combination of simple accident sequences (DBC) and complex sequences (DEC-A), consistently with core damage frequency probabilistic targets.

Flexibility: Not negotiable

Higher safety goal reference: SO2, PO3

Justification / Further explanations:

For each initiating event, the frequency of core melting accident depends on the frequency of the initiating event itself and the reliability of the mitigation systems credited in the analysis. For the most frequent DBC, it is expected that, even with high reliability safety systems, common cause failures could result in unacceptable core damage frequency. Therefore, DEC-A complex sequences have also to be analyzed and, possibly, DEC-A mitigating provisions have to be implemented, in order to improve the core melt prevention.

Safety Requirement DECA-02

DEC-A complex sequences resulting from either:

- ***a DBC combined with a common cause failure on a redundant safety system***
- ***a Common Cause Failure of a redundant safety systems used in normal operation, including support system.***

must be considered to demonstrate the core melting accident prevention.

Flexibility: Not negotiable

Higher safety goal reference: SO2, PO3

Justification / Further explanations:

Deterministic failure of passive safety systems used for the limitation of DBC consequences should be considered in principle, in particular due to functional failure (uncertainties on physical phenomena). Exceptions could be claimed by proving:

- a physical impossibility
- a very high reliability (decades higher than redundant active safety systems), including the consideration of all the uncertainties on physical phenomena.

Safety Requirement DECA-03

The list of DEC-A sequences must be deterministically defined by considering all relevant combination of common cause failure of any safety system, including support system, with normal operation or initiating event

Flexibility: Not negotiable

Higher safety goal reference: SO2, PO3

Justification / Further explanations:

A comprehensive review of all systems credited in normal operation or DBC should be performed in order to identify credible common cause failures and relevant plausible complex sequences. Unlikely combinations belonging to the residual risk can be discarded. The list of DEC-A should remain limited and the relevant sequences to be analyzed are the most challenging ones regarding the function affected by the common cause failure.

Safety Requirement DECA-04

For DEC-A analysis main dominant parameters must be reasonably penalized, and the other parameters can be best-estimate values.

Flexibility: Not negotiable

Higher safety goal reference: SO2, PO3

Justification / Further explanations:

Robustness of DEC-A demonstration. A definition of "Best-estimate approach" is provided in the IAEA guide SSG-2. The dominant parameters are parameters which have a major impact on the result of the analysis. Rationale shall be provided to list the dominant parameters for each DEC-A analysis.

Safety Requirement DECA-05

A feature credited in DEC-A sequence must be sufficiently diversified from the system that is postulated to be affected by a common cause failure in this sequence.

Flexibility: Not negotiable

Higher safety goal reference: SO2, SO4, PO3

Justification / Further explanations:

DEC-A sequences consider the possibility of common cause failure of safety features used in normal operation or used to mitigate frequent DBC sequences. Alternative means to address these sequences have to be sufficiently diversified in order that their failure due to the same common cause failure is not credible.

Safety Requirement DECA-06

Sufficient independence of DEC-A features from the systems credited in normal operation and DBC should be proved sequence by sequence.

Flexibility: Not negotiable

Higher safety goal reference: SO2, SO4, PO3

Justification / Further explanations:

DEC-A sequences consider the possibility of common cause failure of safety features used to mitigate frequent DBC sequences.
It is acceptable to credit DBC features to mitigate a DEC-A sequence provided that these DBC features are not affected by the CCF postulated in the DEC-A sequence.

It is generally not advised to credit normal operation system as DEC-A features because any DEC-A sequence is meant to cover a large range of initiating events combined with a given CCF and then it could be difficult to prove the independence of the DEC-A feature with the initiating event itself. Note that the list of initiating events covered by a DEC-A sequence is not expected to be explicit.

Safety Requirement DECA-07

For installation with several modules, for any initiating event with an impact on several modules, a CCF on DBC features for all modules should be considered as a DEC-A situation.

Flexibility: negotiable

Higher safety goal reference: Safety Requirement DECA-01 and DECA-02 extended for multi-units specific aspects

Justification / Further explanations:

The typical example is the LOOP. For a LOOP event the common cause failure of EDG shall be considered. Nevertheless, this requirement could be discussed depending on the reliability of the DBC features and the type of common cause failure. For example, the possibility of passive common cause failure on different modules should be analyzed.

Safety Requirement DECA-08

For installation with several modules, the common cause failure of independent normal operating system for several modules should be considered as a DEC-A situation.

Flexibility: negotiable

Higher safety goal reference: Safety Requirement DECA-01 and DECA-02 extended for multi-units specific aspects

Justification / Further explanations:

The common cause failure case is considered to check the possibility to fill the safety function on different modules in the same time, even if normal operating systems are not shared between several modules. A typical example is a common cause failure of a support system, like heat sinks.

6. Requirements related to Design Extension Conditions with core melt

Safety Requirement DECB-01

The severe accident defined as the whole core melting accident must be considered and mitigated by Defence-in-depth level 4 measures

Flexibility: Not negotiable

Higher safety goal reference: SO3, PO1

Justification / Further explanations:

Despite scale and power reduction, whole core melting accident remains physically possible if the fuel elements are not drastically modified (as compared to conventional cores). **Excluding the whole core melting accident must rely on physical impossibility**.

As an example, in the HTR concept, core melting accident is excluded, considering that the fuel cladding tightness preserves fuel from degradation, even in case of loss of cooling.

Safety Requirement DECB-02

The systems used to mitigate the consequences of a severe accident situation must be independent as far as practicable from the systems used in any other plant condition.

Flexibility: Not negotiable

Higher safety goal reference: SO4, PO2, PO4

Justification / Further explanations:

A claim of the high reliability of a passive system won't be enough to justify its use in all levels of defence in depth. Only the physical impossibility of the function failure could be considered.

This independence requirement gives a more comprehensive structure of mitigation features. Nevertheless, when this independence is not reasonably achievable, the mitigation features should at least be independent from systems whose failure may have led to the situation (including support systems).

Safety Requirement DECB-02

In case of a severe accident, confinement must be ensured over a mission time ensuring that the effective doses stay below doses compatible with protective measures limited in time.

Flexibility: Not negotiable

Higher safety goal reference: SO3, PO4

Justification / Further explanations:

WENRA O3 objective states that the protective measures shall be limited in time, as such, requiring a second sheltering after the loss of confinement is not considered as acceptable.

Safety Requirement DECB-04

Energetic phenomena that would lead to unmanageable severe accident conditions that have to be practically eliminated must be prevented by conception (natural behaviour) or by DEC-B features.

Flexibility: Not negotiable

Higher safety goal reference: SO3, PO4

Justification / Further explanations:

This requirement permits to ensure that in case of energetic phenomena like hydrogen deflagration, steam explosion or RPV breakage do not lead to unmanageable severe accident conditions like for example a loss of the confinement

7. Requirements related to Practical elimination

Safety Requirement PE-01

Accident conditions with core meltdown which radiological consequences could not be reasonably managed by the provisions implemented for DEC-B situations must be identified and practically eliminated.

Flexibility: Not negotiable

Higher safety goal reference: SO3, PO3, PO4

Justification / Further explanations:

WENRA O3 objective states that accidents with core melt which would lead to early or large releases have to be practically eliminated. The possibility of certain conditions occurring is considered to have been practically eliminated if it is physically impossible for the conditions to occur or if the conditions can be considered with a high degree of confidence to be extremely unlikely to arise. The justifications for these measures shall be based on a deterministic analysis, consolidated where relevant by probabilistic evaluations, taking account of uncertainties due to the limited knowledge of certain physical phenomena. Specific attention shall be paid on conditions leading to significant radioactive releases that develop too rapidly to allow deployment of the necessary population protection measures in due time.

8. Requirements related to Plant autonomy

Safety Requirement AUT-01

With regard to the autonomy of its electrical power supply and the heat sink, the installation must be able to control/manage the long duration design basis and design extension conditions affecting one or several modules or the fuel assembly storage pool, including those affecting both simultaneously.

Flexibility: Not negotiable

Higher safety goal reference: IAEA SSR2/1

Justification / Further explanations:

The autonomy of the plant shall be consistent with the management of DBC and DEC.

Safety Requirement AUT-02

The installation must be able to operate autonomously for a time period compatible with the response possibilities of resources external to the site.

Flexibility: Not negotiable

Higher safety goal reference: PO6

Justification / Further explanations:

SMRs could be settled in remote region. It could take some time before external resources could be provided on site, especially in case of external hazards, including extreme external hazards.

9. Requirements related to hazards

Safety requirement HAZ-01

An internal or external hazard should not lead to an accident.

Flexibility: Negotiable

Higher safety goal reference: PO6

Justification / Further explanations:

When designing the installation, it should be sought that hazards will not lead to an accident. If not possible (for example when a hazard is also an initiating event (LOCA)), it should be demonstrated that the systems required to mitigate the accident are not affected by the hazard.

Safety requirement HAZ-02

A internal hazard should not affect simultaneously several modules of the installation.

Flexibility: Negotiable

Higher safety goal reference: SO1

Justification / Further explanations:

Because of the proximity of modules in the installation, a hazard could affect several modules. This impact should be prevented as far as possible. For example, a fire should not affect two independent systems operating in two different modules. Nevertheless, hazard impacting shared systems between modules could affect simultaneously the process of several modules.

Safety requirement HAZ-03

For installation with several modules, it must be considered that an accidental situation affecting a module could be a hazard for other modules.

Flexibility: Not negotiable

Higher safety goal reference: SO1, PO6

Justification / Further explanations:

Because of the proximity of modules in the installation, an accidental situation in a module could affect the other ones. To the extent practicable, this should be avoided.

Safety Requirement HAZ-04

In case of extreme external hazard (post-Fukushima situation), the severe accident must be:

- **either prevented with a high confidence level**
- **or mitigated**

Flexibility: Not negotiable

Higher safety goal reference: SO3, PO6

Justification / Further explanations:

Accident sequences with core melt resulting from external hazards which would lead to early or large releases should be practically eliminated.

Safety Requirement HAZ-05

For installation with several modules, a situation of extreme external hazard (post-Fukushima situation) impacting all the modules must be considered

Flexibility: Not negotiable

Higher safety goal reference: SO3, PO6

Justification / Further explanations:

Potential common causes of severe accidents in all modules should be considered. If the severe accident prevention cannot be achieved with a high confidence level, the mitigation of severe accident simultaneously in all modules shall be ensured.

10. Requirements related to multi-modules

The aforementioned safety requirements DBC-2, DECA-7, DEA-8, HAZ-2, HAZ-3 and HAZ-5, and the following MU-01 must be applied when designing SMRs with several modules operated in a unique installation.

Safety Requirement MU-01

If a system is shared among several modules, the use of this system on a module shall not impair it to perform its safety function for other modules when needed.

Flexibility: Not negotiable

Higher safety goal reference:

Justification / Further explanations:

The safety demonstration shall be provided for each module independently of other modules in the installation.

11. Summary

One of ELSMOR goals is to create methods and tools for the European stakeholders to assess and verify the safety of light water small modular reactors (LW-SMRs) which would be deployed in Europe.

The objective of the work performed in the task 2.1 was to propose a set of requirements for LW-SMRs related to the defence-in-depth, to the Design basis conditions, to the Design extension conditions without core melt, to the Design extension conditions with core melt, to the practical elimination of situations, to plant autonomy, to hazards and to multi-modules, for which adequate safety methodologies must be developed to evaluate whether the safety objectives are fulfilled or not. Requirements that are considered mandatory have been distinguished from those who are desirable.

References

/ELS 01/ ELMSOR, Proposal for call NFRP-2018, Horizon 2020, 2018

/WEN 2/ WENRA Statement on Safety Objectives for New Nuclear Power Plants, November 2010.

/WEN 3/ Safety of new NPP designs, WENRA RHWG Report, March 2013

/IAEA 4/ Specific safety requirements “Safety of Nuclear Power Plants: Design”, No. SSR 2/1 (Rev. 1), IAEA, Vienna, 2016.

/IAEA 5/ Defence in Depth in Nuclear Safety, INSAG-10, IAEA, Vienna, 1996

/GIF BSA/ GIF RSWG, Basis for the Safety Approach for Design & Assessment of Generation IV Nuclear Systems, Revision 1, 2008

APPENDIX 1 – WENRA SAFETY OBJECTIVES /WEN 2/

SO1. 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.

SO2. Accidents without core melt

- ensuring that accidents without core melt induce33 no off-site radiological impact or only minor radiological impact (in particular, no necessity of iodine prophylaxis, sheltering nor evacuation34).
- 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.

SO3. 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.

SO4. 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.

SO5. 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.

SO6. 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.

SO7. 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 re-sources 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.

APPENDIX 2 – WENRA POSITIONS /WEN 3/

Position 1 (PO1): Defence-in-Depth approach for new nuclear power plants

Position 2 (PO2): Independence of the levels of Defence-in-Depth

Position 3 (PO3): Multiple failure Events

Position 4 (PO4): Provisions to mitigate core melt and radiological consequences

Position 5 (PO5): Practical elimination

Position 6 (PO6): External hazards

Position 7 (PO7): Intentional crash of a commercial airplane