NUCLEAR SAFETY AND DEFENCE IN DEPTH IN CAREM25

M.O. GIMÉNEZ, P. ZANOCCO, D.A. QUIROGA, M.S. GRINBERG, F. MEZIO

National Atomic Energy Commission (CNEA)
San Carlos de Bariloche, Argentina
marcelogimenez@cnea.gob.ar

Abstract

The paper discusses the technological strategy adopted in CAREM to fulfil the Defense in Depth Principle (DiD) and its assessment by Deterministic and Probabilistic Safety Analysis (DSA, PSA). The strategy defined for levels 3A and 3B is based on two stages, using passive and active systems. Moreover, the implemented DiD strategy is the basis for safety functions categorization, following with structures, systems and components (SSCs) classification, and finally setting technology-specific criteria. DiD strategy provide the graded significance for the different safety functions, in agreement with the high-level criteria –not technology oriented- proposed in SSG-30. According to the proposed methodology, safety classification process is executed beginning from the Fundamental Safety Functions (FSF) and by using attributes Low Level Safety Functions (LLSFs) including monitoring ones are constructed for each DiD levels and stages. Next, Safety Functional Groups -set of SSCs that fulfill a LLSF- are identified for each LLSF. Finally, categories and classes have been allocated. PSA and DSA have been used to support this process, evaluating the SSCs relative significance. Moreover, both methodologies have been used to provide design feedback on DiD Levels 2, 3 and 4, evaluating alternative proposals to cope with postulated initiating events. Findings are presented. The integral approach, founded on the defined DiD strategy, has supported the engineering progress and the licensing process, providing a comprehensive assessment of systems design and a balanced integration into the plant.

1. INTRODUCTION

In the context of achieving the safety goals posed by the project, regulatory body and international standards, DiD [1] aids to define and structure the strategy to prevent and control the postulated initiated events and to mitigate the postulated severe accidents. The consecutive protective DiD levels and their specific objectives provide the framework for defining systems design and human actions, what is named as DiD internalization strategy. The fulfilling the FSF in the nuclear plant (reactor and spent fuel pool) -control of reactivity, removal of heat and confinement of radioactive material [2]- shall be applied at each level. Designers have adopted different strategies considering engineering solutions for systems allocated on each level. CAREM25 DiD strategy for levels 1 to 4 has been developed in an early stage of the design. PSA and DSA, as complementary tools, have been used to assess the correct DiD implementation, providing, in some cases, feedback to the design of systems important to safety. On the other hand, the defined DiD strategy has been the foundation to develop a methodology for Safety Classification of SSCs, in order to specify graded engineering requirements with a functional approach. The interaction between DiD strategy, DSA, PSA and Safety Classification is shown in Fig. 1.

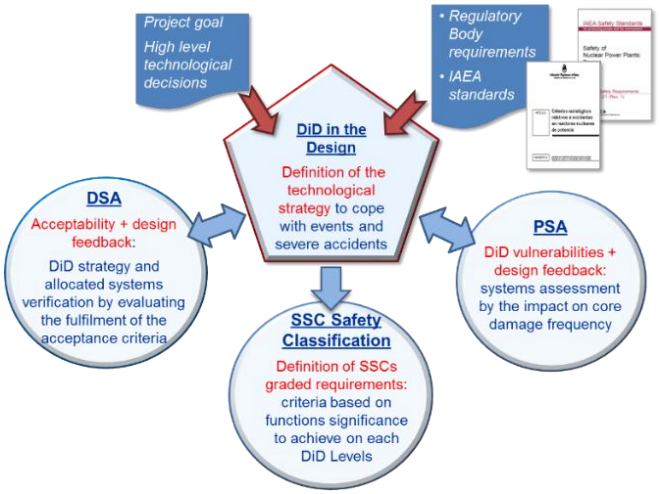

FIG. 1. DiD assessment in CAREM25 design.

This overall approach for DiD implementation has been used as an essential part of the design with high degree of integration for requirement coming from different areas. It has provided a balanced design among inherent-safety requirements, passive and active systems. Inherent safety characteristics aims to exclude some postulated initiating events in PWR and to reduce the probability of events escalation from one level to the next. By this way a proper consolidation of DiD has been achieved. Following, the mentioned elements are described, providing examples of feedbacks to the plant design.

2. DID STRATEGY IMPLEMENTED IN CAREM25 DESIGN

CAREM25 project has adopted the levels definition proposed by WENRA for the application of DiD principle [3] and therefore their conceptual basis. Independence is required, [3], as far as possible and with proper justification otherwise, between the SSCs that perform functions in following groups of DiD levels: 1 and 2; 3A; 3B; 4. In particular and as a complement, for the instrumentation and control systems, reference [4] that distinguishes the layered architecture has been taken into account. Regarding Level 1, in CAREM25 design, some of the classical initiating events postulated in Light Water Reactors have been eliminated due to high-level requirements like integrated reactor cooling system, self-pressurization and core cooling by natural circulation [6]. For instance, large loss of coolant, control rod ejection, boron dilution, primary system pump trip, are excluded as initiating events. Control of Anticipated Operational Occurrences (AOO) on Level 2, is achieved by selected systems which are classified in CAREM25 as safety related to be credited in safety evaluations. For example, the Chemical and Volume Control System (CVCS) can cope with a loss of coolant and loss of heat sink events. The control of both Postulated Single Initiating Events (PSIE) and Postulated Multiple Failure Events (PMFE) on DiD Level 3, aims to prevent damage to the radioactivity barriers, such as cladding, pressure envelop and containment, preventing escalation to severe accidents conditions. On the other hand, there is a clear distinction between these events (PSIE and PMFE) in terms of the means and conditions for achieving the same stated objective. Consequently, following WENRA [3], this Level is divided into two sub-levels 3A and 3B. Diversity is applied as a measure to reduce the probability of common cause failures between levels 3A and 3B. It is worth mentioning that the concept of Design Extension Condition A is equivalent to level 3B, and Design Extension Conditions B to level 4 [2].

Sub-level 3A strategy to cope with PSIE by the Main Line of Protection:

- Reactor shutdown function: executed in a single stage with the goal of reaching and maintain the Plant Safe State, by the First Reactor Protection System (FRPS) and First shutdown system (FSS)
- Reactor heat removal function: implemented into two temporal stages associated with Controlled State and Safe State:
  - First Stage: systems with passive actuation, grace period with one out of two redundancies: 36h for LOCA and larger than 72h for Loss of Heat Sink (LOHS). Objective: to reach and maintain the Plant Controlled State, by the First Reactor Protection System, the Passive Residual Heat Removal System (PRHRS) and the Safety Injection System (SIS).
  - Final Stage: active systems with support of emergency power supply, Safe State System (SSS). Objective: to achieve and maintain the Plant Safe State, once reached the Controlled State.
- Radioactivity confinement function: achieved by the containment isolation (isolation valves of the Heating Ventilation and Air Conditioning system and of Steam Generators main steam lines); in the long term by active radioactivity removal systems (in the event loss of coolant, the occurrence of the spiking phenomenon is expected at most, due to core-uncovery is not acceptable by design, and relatively low depressurization ramps are anticipated).

Sub-level 3B, strategy to cope with PMFE (AOO or PSIE with an additional postulated failure of a level 3A system) by means of the Diverse Line of Protection Systems:

- A postulated failure of a Safety System (FSS or PRHRS) during the grace period, goal: to bring the reactor to the Controlled State, where the safety functions during the grace period are fulfilled by the: Second Reactor Protection System, Second Shutdown System or Safety valves and Depressurization System (RPV-DS). No emergency power supply is required within this stage. No diverse line is required to cope with loss of coolant events due to the its low frequency and integral type design.
- A postulated failure of SSS active systems (common cause) during the final stage, goal: to extend the plant Controlled State until SSS recovery through simple systems supported by external water supply.

Level 4, aims mitigating the Postulated Core Melt Accident (PCMA) by means of the Severe Accident Mitigation Systems. The objective is to reduce the likelihood of an early containment failure. Provisions to mitigate core melt and radiological consequences have been implemented for hydrogen control, external RPV cooling, alkalization of suppression pool, containment venting and RPV depressurization.

Fig. 2 summaries the conceptual strategy adopted in CAREM25 to fulfil the control of reactivity function: reactor shutdown and sub-criticality on levels 2, 3A, 3B and 4. FIG. 3 summaries the conceptual strategy to achieve the control of reactor heat removal function.

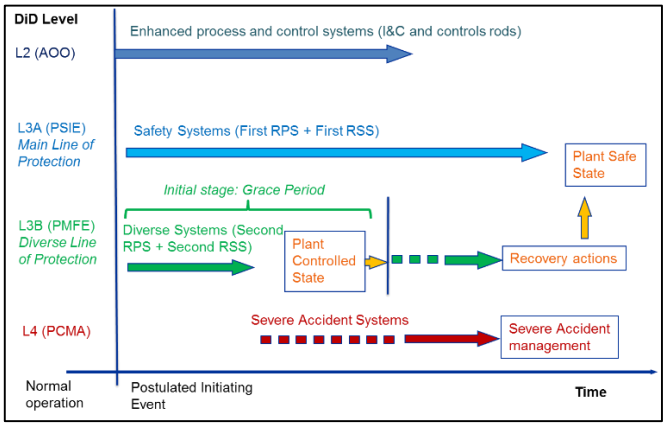

Fig. 2. General strategy for DiD levels 2 to 4 implemented in CAREM25 for the reactor reactivity control function

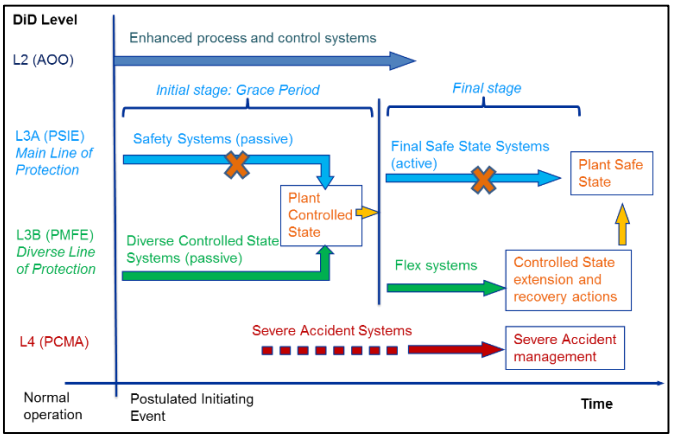

FIG. 3. General Strategy for DiD levels 2 to 4 implemented in CAREM25 for the reactor heat removal function

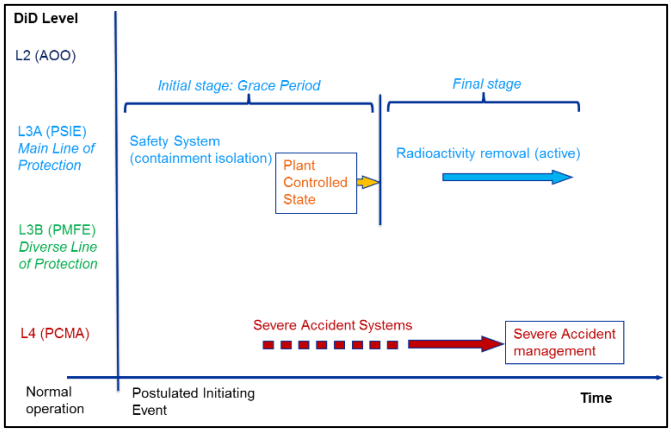

FIG. 4. General strategy for DiD levels 2 to 4 implemented in CAREM25 for the reactor radioactivity control function

FIG. 4 summaries the conceptual strategy to limit incidental or accidental radioactive releases. It is clear and well posed in [3], that on each level the confinement safety function shall be fulfilled. This safety function is accomplished by the use of the containment and associated systems. The containment is an example of a structure

used on different levels and for which it would not be reasonably practicable to require independence for different levels. Once an initiating event occurs, the automatisms –well implemented-, will act depending on the impact on the plant following the hierarchy of systems given by DiD levels, if additional failures arise. Finally, it is important to clarify that during an initiating event, a given safety function can be achieved on a DiD level, while other one can be fulfilled on another level. Therefore, within this thought, it is important to emphasise that the concept of Levels of DiD be conceived in the frame of a given safety function.

3. DID ASSESSEMT BY PSA AND DSA

The strategy and allocated systems on each DiD level, has been evaluated using probabilistic and deterministic modelling as complementary tools, to ensure their proper internalization in CAREM25. PSA Level 1 has been utilized to assess various strategies and systems, employing core damage frequency (CDF) as the figure of merit. DSA has been used to verify systems effectiveness by simulating the plant response to postulated events. Plant inertia, time available to demand systems, systems capability and others performance indicators have been evaluated by verifying margins to the deterministic acceptance criteria for each DiD level. The set of Postulated Events (PEs) are classified, having their frequency of occurrence as reference, as anticipated operational occurrence (AOO), allocated to Level 2, postulated single initiating events, to Level 3A, postulated multiple failure events, to Level 3B and postulated core damage accidents, to Level 4. These PEs and accidents establish the "plant design envelope". The deterministic modelling approach is conservative for levels 2 and 3A, while a best-estimate one is used for levels 3B and 4. PSA and DSA have been used to verify acceptability but also to assess to assess the reached independence between the levels of DiD, complemented by engineering judgement and plant vulnerabilities, providing appropriate feedback to the design based on the evaluation of selected performance indicators. Following, examples are described.

Regarding Level 2, the Chemistry and Volume Control System (CVCS) has been evaluated:

- By PSA, to control LOHS or a loss of coolant event –with reactor shutdown-. A relevant reduction CDF been observed, considering also the case with support of emergency supply considering a coincident loss of of-site power.
- to remove the decay power in case of a LOHS. It has been demonstrated its capacity to limit the RPV pressure increase, thereby avoiding the demand of the PRHRS.
- to avoid core-uncover in case of the design basis loss of coolant event (despite this postulated event belongs to Level 3). It is observed that with two CVCS operating pumps (one running and other in stand-by condition at the time of the event), the water level in the RPV remains above the core with sufficient margin. Enough time is provided by the CVCS tank to allow operators maneuvers to refill it with water from the containment suppression pool.

Concerning Sub-level 3A the following aspects have been assessed:

- the strategy based on passive safety systems and their capacity to bring the plant to the Controlled State during the grace period: to shutdown properly the reactor, to keep the negative reactivity margin and to cool and depressurize the RPV to a condition that allows the active systems to achieve the Safe State.
- Passive systems evaluation included the impact of uncertainties in engineering, operational and modeling parameters on their performance. Classical studies by fault and event trees have been enriched with the functional unreliability quantification. Functional unreliability is defined as the failure probability of a system to fulfill a given performance requirement, due to uncertainties. PRHRS removal power capacity has been assessed in case of a station blackout (SBO). The functional unreliability has been calculated having as failure criterion "the opening of the RPV safety valve". Additionally, the case of a loss of coolant event has been evaluated considering the influence of plant uncertainties, including the PRHRS uncertainties to depressurize the RPV and on the accumulator uncertainties (during its stand-by and on demand conditions) to avoid the core to uncover. The failure criterion for quantifying the functional unreliability, was an early uncovering of the core caused by a delay in water injection. As a result of this assessment and aiming to decrease the functional unreliability by one order of magnitude, the accumulator injection pressure has been increased by twenty percent. A good performance has been observed, providing a wide margin to the acceptance criteria. Recent evaluations done with a CAREM-like model, incorporating a new set of parameters

with uncertainties that affect the accumulators during the stand-by condition, prior to the rupture disk opening. This analysis has been developed within the framework of the Coordinated Research Project I32010, launched and supported by IAEA, entitled "Design and Performance Assessment of Passive Engineered Safety Features in Advanced Small Modular Reactors"

— the identification of functional dependencies in stage 2 (Safe State Systems) by PSA Level 1.

About Sub-level 3B (diverse line of protection the following strategies have been evaluated:

— a Second Shutdown System to extinguish the reactor in case of a reactivity insertion event with failure of the FSS. Its impact on core damage frequency has been quantified, justifying its implementation. Through deterministic evaluation, the system performance has been evaluated.

— a RPV depressurization system in case of PRHRS failure to drive from a LOHS to a small loss of coolant event to allow the accumulators injection. The impact of this system on core damage frequency was quantified, and its implementation has been justified by an increase safety and minimal impact on the plant design. Through deterministic evaluation, it has been calculated that the available time for manual intervention to demand this system to prevent core uncovering is greater than 45 minutes.

— Autonomous systems in case of failures on active final stage systems, in order to anticipate and facilitate the use of self-powered systems to perform mainly heat removal safety functions.

Concerning Level 4, the following features have been evaluated based on a conceptual PSA Level 2 and a PSA Level 3 focused on quantifying Individual Radiological Risk for members of the public:

— a RPV Depressurization System for practical elimination of core meltdown scenarios at high pressure.

— a RPV lower plenum Cooling System for in-vessel corium retention. This strategy has been proposed to keep the corium inside the RPV, supported by the low ratio between corium heat generation and RPV lower head area. Its performance was confirmed.

— the influence of uncertainties on the onset of core degradation and onset of core relocation into lower plenum. The time available quantification will be an input to support the development of Severe Accidents Management Guides. This task, using a CAREM-like model, has been accomplished due to the participation on the Coordinated Research Project I31033, IAEA, entitled "Advancing the State-of-Practice in Uncertainty and Sensitivity Methodologies for Severe Accident Analysis in Water-Cooled Reactors".

Regarding Level 5, the following topic has been considered:

— Emergency Planning Zone (EPZ) sizing. As figure of merit it has been proposed the Individual Radiological Risk (IRR) definition (probabilistic approach), combined with dose calculation (deterministic approach). The aim is to explore if a probabilistic approach could provide a novel criterion for EPZ sizing. This evaluation is being developed in the context the Coordinated Research Project I31029, IAEA, "Development of approaches, methodologies and criteria to determine the technical basis of the emergency planning area for the deployment of small modular reactors".

Finally, and in the context of gaining experience in modelling and analysing multi-units site dependencies, a hypothetical SMR case (a CAREM25-like was assumed) with two units and a common spent fuel pool has been analysed thought a Multi-unit PSA (MUPSA) approach. The study included a simplified and oriented probabilistic models to explicit relevant aspects of MUPSA methodology that included PSA Levels 1, 2 and 3, the last oriented to IRR calculation. A grace period for each unit was assumed where the Controlled State is achieved. After that time, active systems are required in order to achieve the Safety State or to extend the Controlled State. The postulated multi-unit initiating event was the loss of off-site power. The evaluated risk metric is based on the IRR on individuals of the public. Functional dependencies between units have been modelled and the results allow identifying engineering feature improvements, in order to reduce the associated IRR. Within the scope of this case of study it can be concluded that despite the limited human actions modelled, it is evident their criticality during management of share equipment (flex systems) among units. MUPSA is a complementary analysis to the traditional PSA, and its development has allowed to analyse the DiD strategy in different framework. This study has been accomplished due to the involvement in the Coordinated Research Project I31031, IAEA, entitled "Probabilistic Safety Assessment (PSA) Benchmark for Multi-Unit/Multi-Reactor Sites".

4. SAFETY CLASSIFICATION OF SSC BASED ON DID STRATEGY AND SAFETY FUNCTIONS

Safety classification of SSCs methodology has been developed to define graded safety technical requirements. Classification process is based on safety functions relative significance, given by the DiD Levels strategy internalized in the design and the umbrella of the high level safety goals [6]. It reflects the characteristic and distinctive features of CAREM25. For instance, a grace period after the initiating event covered by passive systems to achieve the Controlled State followed by a second stage to achieve the Safe State through active systems. This methodology has been developed using as reference the standard IEC-61226 [7]. IAEA SSG-30 [5], that was released in 2013 has a similar functional approach. The last, provides high level criteria, no technology dependant. Its application requires interpretation and evaluations by nuclear safety experts in order to translate those criteria into more plant specific ones, in order to be used by engineers of different specialities. Moreover, in the standard, there is not a criterion clearly mentioned for Level 1 functions. The explicitly mentioned functions in [5] are those focus on reaching a controlled/safe state after AOO/design basis accidents and to limit consequences of design extension conditions. In CAREM methodology Level 1 is explicitly incorporated. Monitoring functions are also considered and classified. They are built considering the following five monitoring purposes: planned manual actions, fundamental functions, DiD barriers, systems performance and detection of potential releases of radioactivity functions. Additionally, criteria have been obtained for allocation categories to LLSFs and classes to SSCs. The graded approach to classification has been based on the risk concept (probability of occurrence times consequences in case of failure). The criteria reflect the characteristic and distinctive features of CAREM25 design. For instance, a grace period after the initiating event covered by passive systems to achieve the Controlled State followed by a second stage to achieve the Safe State through active systems. The concept of Safety Functional Groups (SFG) –set of SSCs required to achieve a safety function-, is used which shall include, if applicable, initiator, frontal and support systems, belonging to the main and diverse lines of protection.

Three category ranks for LLSF and three classes for SSCs have been considered adequate. The allocation of Safety Classes to each SSC belonging to a SFG was performed taking into account the associated LLSF Category and the impact of its failure on the accomplishment of the mentioned function. Class reduction can be applied considering the existence of other systems that also fulfil the function and the time available to demand the SSC [6]. Safety requirements are settled in terms of "DiD Level-LLSF category-SSCs class". FIG. 5 summarize the criteria for Categories allocation to LLSF and Classes to SSCs in relationship with the overall strategy adopted by design for Levels 2 to 4, including the two stages for Level 3.

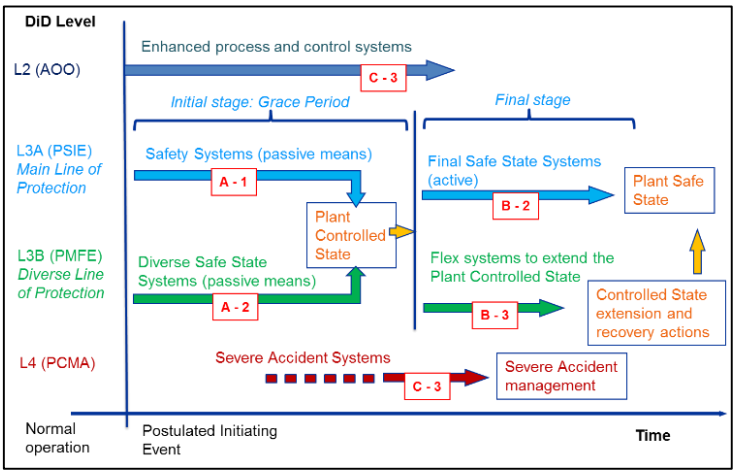

FIG. 5. Categories and Classes relationship with each DiD level and stage (adapted from [8]) for heat removal function.

The highest Category (A) and Class (1) are allocated to functions and SSCs respectively, that belong to the initial stage of level 3A, Main Line of Protection, as they are requested just after de initiating event. Category B and class 2 have been associated to the final stage in Levels 3A, given credit to the grace period cover by passive means (initial stage). The same categories are applying to level 3B initial and final stages, nevertheless SSCs class reduction corresponds as they belong to the Diverse Line of protection (lower probability to be demanded). Category C and Class 3 are reserved for Levels 2 and 4, distinguishing between them precisely by the DiD level. The central objective of Safety classification is establishing graded technical-safety requirements in terms of valid

combinations of DiD level–Category-Class. These requirements are clustered at system-level ones, such as single fault, physical separation, type of power supply and periodic testing; at component level ones, like codes and standards for its design and manufacture, environmental conditions, seismic grade, between others. In the event that by design a single SSC performs a given function in more than one of the defined groups of DiD levels to require independence, the assigned category and class must be the most stringent, and therefore the requirements.

Summarizing, the process of Safety Classification starts with building the Low Level Safety Functions (LLSF) from the Fundamental Safety Functions [1] (FSF), including the transversal ones that are directly related to more than one FSF, like monitoring functions. The LLSF are constructed applying attributes to the FSF, such as the radionuclides source, plant operational states and the DiD level and stage (Controlled Sate/Safe State) where the function has to be accomplished. Next, the process involves to set up the SFG and associated SSCs to each LLSF. Subsequently, LLSF are categorized and SSCs are classified accordingly. As result of this process, about one hundred LLSF have been identified, including monitoring ones, and nearly thirty systems important to safety have been classified. A correct allocation of functions and systems to each DiD level has facilitated the design process, with a clear and consistent category and class allocation to SSCs with the associated graded requirements. This process has guaranteed, founding rules to ensure the functionality and quality of SSC in all the operational states, and under the conditions prevailing during the postulated AOO, PSIE, PMFE and PCMA.

5. CONCLUSIONS

Given the high-level of safety required, and under the concept of reasonable practicability, DiD Principle forms the basis for achieving a well-balanced and cohesive plant design. Within this framework, a comprehensive methodology has been developed to integrate DiD into the design of CAREM25 plant, encompassing both the reactor and the spent fuel elements pool, aimed at managing the postulated events and to mitigate fuel damage. The following elements have demonstrated by what means DiD principle has been contemplated in the design: firstly, the definition of a strategy for DiD technological internalization in an early stage of the design; secondly, the utilization of DSA and PSA to verify the correct internalization of defined DiD strategy facilitating the identification of vulnerabilities and providing feedback to the design process by employing different figures of merit to evaluate their practical feasibility; and finally the use of DiD as the foundation for the methodology of SSCs safety classification. An early definition of DiD strategy, safety functions and associated systems has allowed setting clear design rules and requirements. As result of the function-oriented Safety Classification process, a set of technology-specific criteria was obtained for categorizing LLSF and classifying SSCs. This methodology serves as an interface with high-level criteria, such as those from SSG-30. This approach has facilitated the application of design rules and requirements by engineers from various disciplines. Additionally, it has promoted a thorough understanding of the DiD principle within the team. Finally, it is worth to mention, based on our own experience, a correct and clear allocation of safety functions and SSCs to each DiD level, facilitates the engineering process and inter-area relationship. This, in turn, has reinforced the design and has facilitated the licensing process.

ACKNOWLEDGEMENTS

The methodology for quantification passive system functional unreliability and cases of study, severe accidents uncertainties impact on figures of merit, EPZ sizing and MUPSA case of study, mentioned along this document, have been accomplished thanks to the guidelines and effort of CRPs I32010, I31033, I31029 and I31031 coordination teams and participants from several countries.

REFERENCES

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, Fundamental Safety Principle, IAEA Safety Fundamentals No. SF-1, IAEA, Vienna (2006).

[2] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Nuclear Power Plants: Design, IAEA Safety Standards Series No. SSR-2/1 (Rev. 1), IAEA, Vienna (2016).

[3] WESTERN EUROPEAN NUCLEAR REGULATORS ASSOCIATION, Safety of new NPP designs, Study by Reactor Harmonization Working Group, WENRA, (2013).

[4] INTERNATIONAL ATOMIC ENERGY AGENCY, Approaches for Overall Instrumentation and Control Architectures of Nuclear Power Plants, Nuclear Energy Series NP-T-2.11, Vienna (2018)

[5] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Classification of Structures, Systems and Components in Nuclear Power Plants. IAEA Standards No. SSG-30, IAEA, Vienna (2014).

[6] GIMÉNEZ, M.," Defence in depth internalization and basis for safety classification in CAREM-25", TopSafe 2017 Conference, Proc. Int. Conference TopSafe, 2017, ENS Conference, Vienna (2017).

[7] INTERNATIONAL ELECTROMECHANICAL COMMISSION, Nuclear power plants – Instrumentation and control systems important to safety – Classification of instrumentation and control functions, International Standard, IEC 61226, Third Edition (2005)