DEFENCE IN DEPTH INTERNALIZATION IN CAREM PROTOTYPE AND BASIS FOR SAFETY CLASSIFICATION OF STRUCTURES SYSTEMS AND COMPONENTS

M. GIMÉNEZ, P. ZANOCCO, D. QUIROGA

Nuclear Safety Group, Comisión Nacional de Energía Atómica
Av. Bustillo 9500, 8400 S. C. de Bariloche - Argentina

Email: gimenez@cab.cnea.gov.ar, zanoccop@cab.cnea.gov.ar, quirogad@cab.cnea.gov.ar

ABSTRACT

This paper discusses how Defence in Depth (DinD) is internalized in CAREM-25 design following WENRA approach [1]. It also presents the methodology developed to address Safety Classification of Structures, Systems and Components (SSCs), in harmony with IAEA and IEC [3], [5].

CAREM is a development project based on Light Water Reactors (LWR) technology coordinated by the Argentina's National Atomic Energy Commission (CNEA) in collaboration with leading nuclear companies in Argentina with the purpose to develop, design and construct innovative small nuclear power plants. CAREM is an integral type Pressurized Water Reactor (PWR) based on indirect steam cycle with distinctive features that simplify the design and support the objective of achieving a higher level of safety. The main characteristics are self-pressurization, core cooled by natural circulation, in-vessel control rod drive mechanisms, passive safety systems and a balanced and optimized design with a cost-effective internalization of safety. The prototype of CAREM (CAREM-25) has a thermal power of 100 MW (33 MWe) and is currently under construction.

DinD is a key concept to achieve the fulfillment of the Fundamental Safety Functions (FSF). In CAREM-25 DinD was internalized in the design since the project genesis and it was recently updated to give and adequate frame to systems originally provided to cope with multiple failure events. Level 1 prevention functions important to safety are categorized. Level 2 provides protection against anticipated operational occurrences by upgraded process and control systems called Enhanced Process Systems. The general strategy to cope with Postulated Events (PEs) within Level 3 is divided into two consecutive stages: the first one, called grace period (36 hrs), where the events are controlled by passive safety systems (no power electricity is required) to reach a safe state, and a second one where active systems are used to reach a final safe state. Level 3 is also divided, according to WENRA [1], into two sub-levels: Level 3A to cope with Postulated Single Initiating Events with systems that belong to the Main Line of Protection, and Level 3B to cope with Postulated Multiple Failure Events by means of a Diverse Line of Protection. Systems belonging to Level 3B and to the first stage are: Second Shutdown System which injects boron into the reactor in case failure of the First Shutdown System, and valves to depressurize the Reactor Pressure Vessel (RPV) to allow the injection of the Low Pressure Accumulators, in case of a Loss of Heat Sink (LOHS) with failure of the Passive Residual Heat Removal. Fails during the second stage are also postulated (station black-out longer than 36 hr, failure of the emergency supply), in this case the grace period can be extended by simple systems supported by fire extinguishing system or external pumps that provide core and containment cooling and RPV refilling. DinD Level 4 is dedicated exclusively to control accidents with core melt to limit off-site releases. Provisions are considered for hydrogen control in the containment and for RPV lower head external cooling for in-vessel corium retention.

Safety classification of SSCs is based on identification of low level safety functions (LLSF) -derived from the FSFs- and safety functional groups of SSCs that fulfill those functions. Criteria for safety categories assignation to LLSF and classes to SSC are obtained from the way the principle of DinD is internalized in the design to cope and mitigate the initiating events. Three categories and classes are defined. Category A, B and C are required for preventive functions (Level 1) depending on their importance to safety. Category A is applied to functions required in Level 3A/Grace Period, Category B for functions in Level 3A after the grace period needed to reach the final safe state and Category C: for some function required in Level 2 and in Level 4. Class reduction can be applied to SSC that constitute the Diverse Line of Protection. Also in this process probabilistic considerations are also taken into account. This methodology provides a clear assignation of design rules and requirements to systems important to safety and its SSCs.

Internalization of the DinD principle in the design of the CAREM-25

Introduction

The Principle of Defense in Depth (DinD) establishes a series of consecutive measures, framed in the prevention and early detection of deviations or failures of systems to reduce the probability of occurrence of failures, and in the control and mitigation of their consequences if the prevention fails. This series of measures are materialized through multiple physical barriers and levels of protection, aiming to fulfill the Fundamental Safety Functions (FSF) in the reactor and in the spent fuel pool: control of reactivity, removal of heat and confinement and / or limitation of releases of radioactive material. The frame proposed by WENRA for the Principle of DinD [1] is the one that has been adopted in the Project CAREM-25.

Prevention of Postulated Initiating Events

The **First Level of Defense in Depth** aims at the confinement of radioactive material, the prevention of faults and of abnormal operations. The failure of this level implies that an Initiating Event (IE) has occurred. Particularly in CAREM-25, regarding this Level, a reduction of the frequency of occurrence or elimination of certain typical Light Water Reactors (LWR) IEs has been implemented, using appropriate engineering solutions:

- Location of the hydraulic drives of the Rapid Extinguishing System and Control System within the Reactor Pressure Vessel (RPV) in order to eliminate the event of insertion of reactivity by ejection of absorbent elements.
- Elimination of neutron absorber dissolved in the coolant (boron) for the control of reactivity in all the operational states, in order to eliminate the event of insertion of reactivity by boron dilution.
- Adequate arrangement of the primary circuit to provide cooling capability by natural circulation in nominal conditions, in order to eliminate the initiating event of loss of cooling flow in the core.
- Limiting the diameter of the connection to the RPV at 38.1mm, in order to reduce its impact on loss of coolant events and on the requirements of the Safety Main Protection Line. In this way, the large loss of coolant event (LOCA), typical of PWR designs, is eliminated, excluding some complex characteristic phenomena, such as the fast emptying of the core and the consequent occurrence of Departure of Nuclear Boiling (DNB). On the other hand and associated to the saturation condition of the fluid in the hot branch, it will also avoid the existence of severe pressure waves that compromise the integrity of the internal components of the RPV.
- Location of the RPV penetrations at the highest possible level, above the Steam Generators (SGs) active zone, in order to minimize loss of liquid coolant. For the same purpose, the pipes that carry out the RPV and extend inside it, must have devices to avoid, as far as possible, the loss of liquid refrigerant below a given level.

Safety Strategy against Postulated Events

Figure 1 presents the conceptual basis for defining the overall **strategy for implementing the Defense in Depth principle to control and mitigate Postulated Events (PE)**. There it shows the structure of the different levels of defense and temporary stages, which reflect the characteristics of the CAREM-25 design.

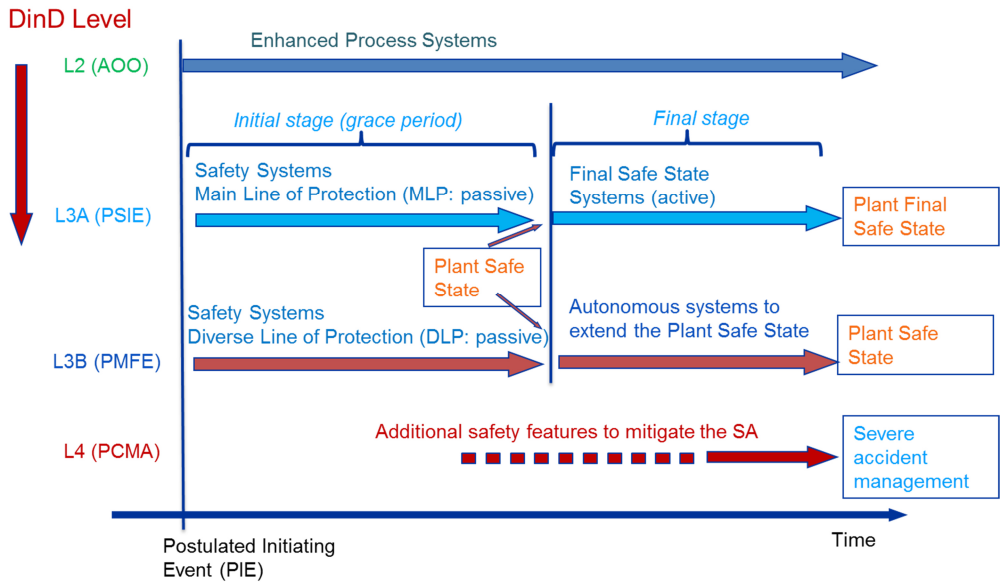


Figure 1 - Conceptual basis used for the definition of strategies for the fulfillment of the FSFs against PEs and PCMAs

The **Second Level of Defense in Depth** is aimed at fault detection and control of abnormal operations, to prevent them from being escalated and diverted to more severe conditions, so as to return to the operation of the plant as soon as possible once the fault is corrected. The IE to be controlled at this level are the **Anticipated Operational Occurrences (AOO)**, where functions related to refrigeration are fulfilled by systems used in the normal operation of the plant (Enhanced Process Systems). The AOOs include both events that can be controlled with maneuvers that do not require reactor extinction, and events that do require it, called Postulated AOOs (PAOO). These last events are those considered as part of the Postulated Initiating Events (PIE) group and to be addressed in the safety assessments.
This level is implemented by specific actions of the control system and other means of assistance available for the normal operation of the plant. As far as the extinguishing action is concerned, this is not necessarily fast. The First Shutdown System (FSS) can be acted on by the First Reactor Protection System (FRPS) at specific Level 2 events.
Systems that perform functions at this level and that are hierarchized especially by design, are called Enhanced Process Systems. Traditionally, they are not classified as Important Safety Systems, but it will be used in the AOOs control strategies in such a way as to strengthen safety-related performance by design. These systems will be considered as important to safety and will be assigned a safety rating. This selection can be made by evaluating the importance of these systems in the results of Probabilistic Safety Analysis (Level 1), and will therefore have the objective of reducing risk.
The **Third Level of Defense in Depth** aims to control both **Postulated Single Initiating Events (PSIE)** and **Postulated Multiple Failure Events (PMFE)** in order to avoid by design the damage of the fuel elements and the pressure boundary (if it was not affected by the PE), maintaining the effectiveness of the barriers (including containment) and fulfilling FSF. In both cases, the objective is to limit the release of radioactive material and prevent the escalation of such events to severe accident conditions. Given that there is a clear distinction between these events, in terms of the means and conditions for achieving the stated objective, it is that this level is divided into two sub-levels: 3A and 3B.

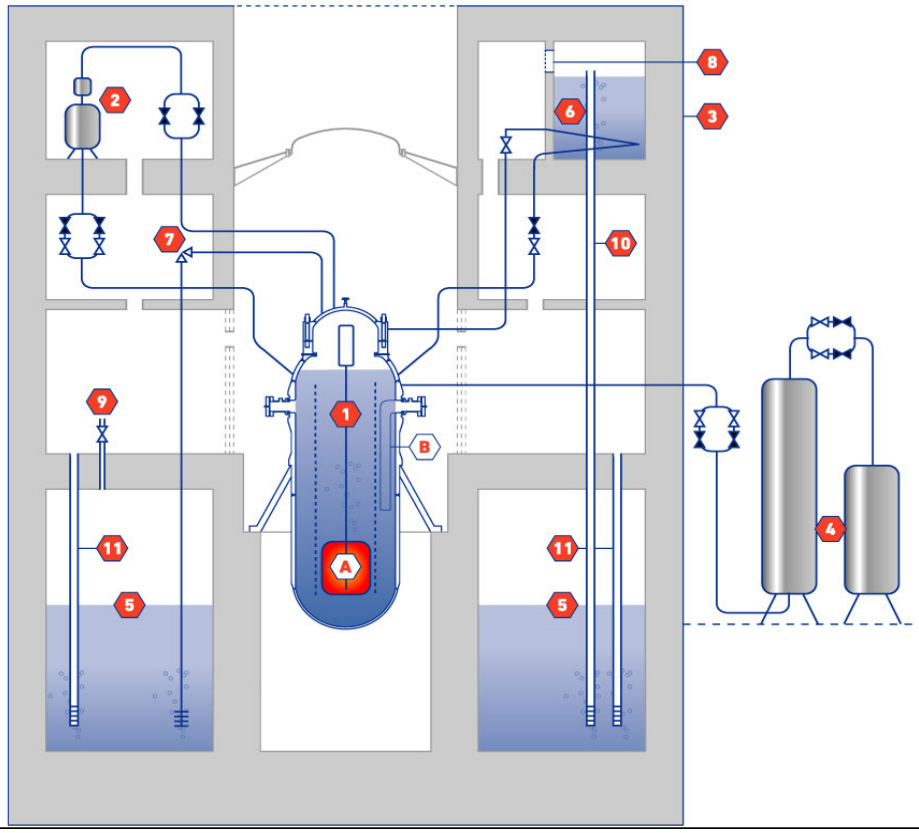
- **Sub-level 3A**: The objective of this sub-level is the control of PSIE to prevent its escalation to severe accident conditions. The strategy established in CAREM-25 for the control of these events is presented in two stages, the objectives of which are:
    - *Initial Stage*: reach and maintain the plant in the **Plant Safe State**, where the FSFs for an extended period of time, called the grace period (36 h), are fulfilled through the Safety Systems - Main Line of Protection (MLP).
    - *Final Stage*: to achieve and maintain the plant in the **Final Safe State** for as long as necessary, through active systems called Final Safe State Systems (FSSS), once reached the safe state.
- **Sub-level 3B:** the objective of this sub-level is the control of PMFE to prevent its escalation to conditions of severe accident. For its internalization in the CAREM-25 design, in this Level in particular two conditions associated with system failures are defined to control the events in initial or final stage:
    - Failure of Safety Systems - Main Line of Protection (Sub-level 3A failure, during initial stage): the objective is to bring the reactor to the safe state, where the safety functions during the grace period, are fulfilled by Safety Systems - Diverse Line of Protection. These systems do not require electric power supply.
    - Failure of FSSS or support systems (common cause failures) (Sub-Level 3A failure, during final stage): the objective is to maintain the plant safe state through Plant Safe State Extension Systems (SSES) and other Systems Related to Safety (SRS), supported by autonomous external means that allow to extend the Plant Safe State until the recovery of the FSSS. This objective can be achieved by extending the range of the Safety Systems – Main Line of Protection, recovering the level in the RPV and / or cooling the containment.

In this way, for the Level 3 of DinD, the systems defined as Safety Systems - Main Line of Protection (MLP) Sub-Level 3A, Initial Stage, in CAREM-25, are: First Reactor Protection System (FRPS) (responsible for detecting IE and demanding the performance of the rest of the MLP), the First Shutdown System (FSS), Passive Residual Heat Removal System (PRHRS), Safety Injection System (SIS) (for cooling and injection functions, respectively), the containment system and valves of Heating, Ventilation and Air Conditioning (HVAC) isolation and Steam Generators (radionuclide confinement function). These systems fulfill their respective roles in the Initial Stage of DinD Sub-Level 3A.
The systems defined as Safety Systems - Diverse Line of Protection (SS-DLP) Sub-Level 3B, Initial Stage, in CAREM-25, are: Second Reactor Protection System (SRPS) (in charge of detecting IE and demanding the action of the SSS), the Second Shutdown System (SSS) (for the extinguishing function), and the RPV Safety and Depressurization Valves (the first one for pressure boundary protection and the second, to allow cooling through injection functions, from SIS due to PRHRS failure). Figure 2 shows a schematic of some systems related to the MLP and DLP.
As mentioned above, the functions related to extinguishing, cooling and confinement are carried out in a passive fashion -without need of electricity supply- during the grace period (36h), initial stage, bringing the plant to the Safe State, where the energy removed from the Primary System is stored in the pressure suppressing containment. The Safety Systems that belong to the MLP will act against PSIE (PIE where the failure of the Enhanced Process Systems is postulated or they exceed the control capacity within the Level 2 of DinD). The Safety Systems that belong to the DLP will act on the occurrence of PMFE, e.g. PIE with additional faults postulated in the Main Line of Protection.

After the grace period, and once reached the Safe State, the goal is to bring the plant to the Final Safe State, by means of active means (sub-level 3A, Final Stage). For this purpose, the FSSS are used, which are: suppression pool cooling system and containment spraying system. These systems can be powered by the emergency power supply (with support of diesel generators) that also belong to this level. The enabling actions of these systems for the transition from the safe state to the final safe state will be carried out by the operator, except for the diesel generators, which is automatic in the case of failure of the normal electricity supply bars (the latter is for the Enhanced Process Systems actuation).
In the event of a failure of the FSSS, either due to its own fault or to a situation of total loss of long-term power supply (in normal and emergency bars) beyond the grace period, systems or means are provided for autonomously continue with the safe state beyond this period. For this purpose there are connections for autonomous external means to refill inventory to the RPV and to refill and cool the pool of the PRHRS and the containment suppression pool. These systems are called Safe State Extension Systems (SSES) and belong to DinD Sub-level 3B, Final Stage.
The **Fourth Level of Defense in Depth**, supposed the Level 3 failure, has as general objective to provide mitigation actions in severe conditions of core damage to control, as reasonably possible, the progression of the accident, in order to reduce the release of the radioactive material into the environment.
The design of this level, composed by Severe Accident Mitigation Systems, tend to significantly reduce the likelihood of early containment failure in postulated severe accident scenarios,:

- There is a system that ensures the depressurizing of the RPV at an early stage of the event to reduce as much as is reasonably practicable the direct damage of the containment by failure of the pressure vessel at high pressure.
- It include devices for the control of hydrogen in the various containment areas and auxiliary buildings, in order to reduce as far as reasonably practicable deflagrations and / or detonations (hydrogen control system).
- It includes an external refrigeration system of the RPV to avoid its breaking in case of severe accident, practically eliminating the possibility of corium-concrete interaction (an external spray of the lower head of the RPV).
- It includes a system of alkalization of suppression pool, to increase the retention of fission products in the Suppression pool.

Figure 1 presents the systems, in their generic name, assigned to each level of Defense in Depth to control the PEs (PAOO; PSIE; PMFE) and to mitigate the Postulated Core Melt Accidents (PCMA).
Other safety related systems not included in the previous subgroups can be mentioned, as the stand-by auxiliary support systems of the MLP or DLP (which are framed as Level 1 of DinD systems).
For the **Spent Fuel Pool**, it has been implemented the **Level 1 of DinD** by means of an adequate monitoring of water level and temperature of the pool and a corresponding system of alarms and interlocks. In the **Level 3 of DinD** the design implements an inventory of water in the pool that stores the heat generated by the fuels housed there (refrigeration by passive means), without reaching a condition such that, before the grace period, cooling by active means is needed. The mentioned grace period has a duration greater than that defined for reactor cooling. Beyond that stage, equivalent to the core, there are active systems available for the extraction of the heat generated by the stored irradiated fuels elements and transfer the heat to the final heat sink.



References			
A	Core	6	Passive Residual Heat Extraction System (PRHRS)
B	Steam Generators	7	RPV Pressure and Depressurization Limit Valves
1	First Shutdown System (FSS)	8	Containment system: relief membranes of the PRHRS enclosure
2	Second Shutdown System (SSS)	9	Containment system: relief valves of the Suppression Pool enclosure
3	Containment building	10	Containment system: relief ducts of the PRHRS enclosure
4	Safety Injection System (SIS)	11	Containment system: relief ducts of the dry enclosures
5	Suppression pool		

Figure 2 - Schematic of some MLP and DLP and other related components

A correct and clear assignment to each level strength the design and save regulatory problems.

General safety classification criteria of Structures, Systems and Components and Technical Requirements

Safety classification of SSCs is based on identification of Low Level Safety Functions (LLSF) - derived from the Fundamental Safety Functions (FSF) and Safety Functional Groups (SFG) of SSCs that fulfill those functions. Criteria for safety categories assignation to LLSF and classes to

SSC are obtained taking into account the descripted methodology for DinD internalization in the design, in order to cope and mitigate the initiating events.
The classification of SSCs is carried out in order to define the functional and **safety requirements**. The safety classification, to be assigned to SSC, is based taking into account the importance of the role they play in the safety of the plant, defined according to the DinD Principle [2] in the design of the plant.
The final objective is to establish requirements associated with each Level of DinD and Category-Class to establish rules that ensure the functionality and quality of the SSC in all expected conditions of the reactor as in all operating states, Postulated AOO, PSIE, PMFE and finally as much as possible in Postulated Core Melt Accidents (PCMA). In this way an adequate robustness of the design is established through a solid implementation of the Principle of DinD.
These requirements, together with additional engineering requirements and specific to the technical area involved, establish in a precise and documented manner in which the involved SSC must be designed and constructed.
Finally, this design process must be consolidated by implementing the principle of Safety Culture in the Design, Construction, Start-up, Operation and Decommissioning phases.
The Safety Classification process involves categorizing of LLSF. They must be categorized according to their importance in the different operational states of the plant both to prevent and to control and mitigate PEs and PCMA. In order to do so, criteria is established based mainly on how the DinD Principle for the prevention, control and mitigation of PE and PCMA are internalized in the design, their importance on a deterministic basis. For example, the following factors are taken into account: impact of the failure of the safety function, the frequency this function will be required, the time available after the IE for such a function to be required. For this purpose, the design and acceptance criteria established for PEs must also be taken into account. Three levels are considered for this categorization.
Later, SSCs are identified as those needed to fulfill the LLSF –the defined as SFG-. These are classified with the ultimate purpose of establishing differentiated requirements [2], [3], [5]. These classes allows the establishment of system-level requirements such as single fault, physical separation, type of power supply and periodic testing; and at component level, the environmental conditions for its operation and the use of codes and standards for its design and manufacture.
For the identification of the set of SSCs needed to fulfill the LLSF –SFG-, it is adopted as a criterion to include all systems that intervene directly or indirectly in the fulfillment of a given safety function (within the same level of DinD); this aims to avoid inconsistencies in certain international norms and standards, which has led to a restructuring that is taking place in recent years [3], [5] with a new approach, which aims to join the present work. This applies to actuation systems and support equipment, as will be explained later. The set of systems, sub-systems and components, both the main / front and the support ones, that make the fulfillment of a given safety function, compose the Safety Functional Group (SFG).
Finally, the assignment of Safety Classes to each SSC belonging to the SFG is performed. In order to do this, they define guidelines that take into account, firstly, the Category assigned to the related LLSF, the impact of the failure of the SSC on the fulfillment of the mentioned function, the existence or not of other systems that also fulfill the function, the time available for the demand of the mentioned SSC and the possibility to take alternative actions.

Identification of Low Level Safety Functions

According to the Argentinian Nuclear Regulator (ARN, for its acronym in Spanish) regulations and applicable international standards and recommendations, for a nuclear installation to be considered safe, the FSFs must be complied with, both in normal situations and in case of postulated initiating events within the context of the Principle of DinD [1], [2]:

- Reactivity control in the reactor and storage of fuels.
- Removal of the heat generated in the reactor core and in the pool of irradiated fuel elements.
- Confinement of radioactive material, radiation shielding, control of planned radioactive releases, and limitation of accidental radioactive releases.

Since these functions are of a very high level, in order to be able to identify plant engineering solutions that comply with them, the Plant Level Safety Functions (PLSF) [4] have been derived, which have an intermediate degree of detail.
The PLSFs depend on the type of reactor technology, and have been developed following international guidelines, reactors of similar technology and taking into account the particular characteristics of CAREM-25, source of radioactive material (reactor or Fuel Elements pool), and plant conditions (normal conditions or control of PEs). However, a degree of generality is maintained that allows comparison with other standards.
Besides, additional PLSFs, called transversal PLSFs, are identified that are functions that can directly relate to more than one FSF and may be related to both prevention and control or mitigation of PE. From the PLSFs, the LLSFs are derived. To this end, it is considered a greater degree of openness and specificity in the implementation in the central of each PLSF, according to the general strategy proposed for the implementation of the Principle of DinD, considering essentially the intrinsic characteristics of the design of the reactor CAREM-25.
Finally these LLSF are the ones that must be categorized.

Criteria for categorizing LLSF

Based on international bibliography taken as reference [5] it is considered sufficient to establish four functional Safety Categories: SF-A, SF-B, SF-C and SF-NC.
For the assignment of a Safety Category to a LLSF, criteria are identified for each of the categories. These criteria arise from the way in which the Principle of DinD is internalized in the design, and reflect the severity of the failure or failure of such LLSF, the frequency of its demand and the time, after the PE or PCMA occurred, from which it is required.
These criteria thus reflect the characteristic and distinctive features of the CAREM-25 concept, such as the existence of a prolonged grace period, where safety functions are fulfilled, upon request of the First Reactor Protection System (FRPS) or Second Reactor Protection System (SRPS), with passive Main and Diverse Protection Lines, the latter to control PMFE, and which take the plant to a Safe State. Then, once this condition is reached, the plant can be cooled by active systems called Final Safe State Systems, in order to fulfill the safety functions and reach the Final Safe State.

Guidelines for Assigning Safety Classes to SSC

In order to recognize the importance for the safety of the SSCs that contribute to the fulfillment of the different LLSF previously categorized, safety classes are established. Safety classes represent the capability, availability and level of robustness that will be required to design, build and operate the SSC [5].
SSC classes are set according to the following guidelines:

- SC-1 class: SSCs that play a major role in implementing SF-A functions.
- SC-2 class: the SSCs that play a major role in implementing SF-B functions, constitute the diverse protection line to the principal in the implementation of SF-A functions or contribute to the fulfillment of an SF-A function.

- SC-3 class: SSCs that fulfill an SF-C function or contribute to the fulfillment of an SF-B function, when there is already a system capable of fulfilling said function classified as SC-2.
- SC-NC class: SSCs not included in previous classes.

Conceptual summary of the Systems Important to Safety general Classification

In Figure 3 a synthesis of the correspondence of Categories for Functions and Classes to SSC is presented, carrying out the internalization in the CAREM-25 design of the DinD principle Levels 2 to 4. There it can be seen the conceptual basis of the CAREM-25 design in terms of the overall strategy of implementing the DinD principle to control PEs and mitigate severe Accidents, and its structure according to different levels of protection and temporal stages, reflecting characteristics of the CAREM-25 design.

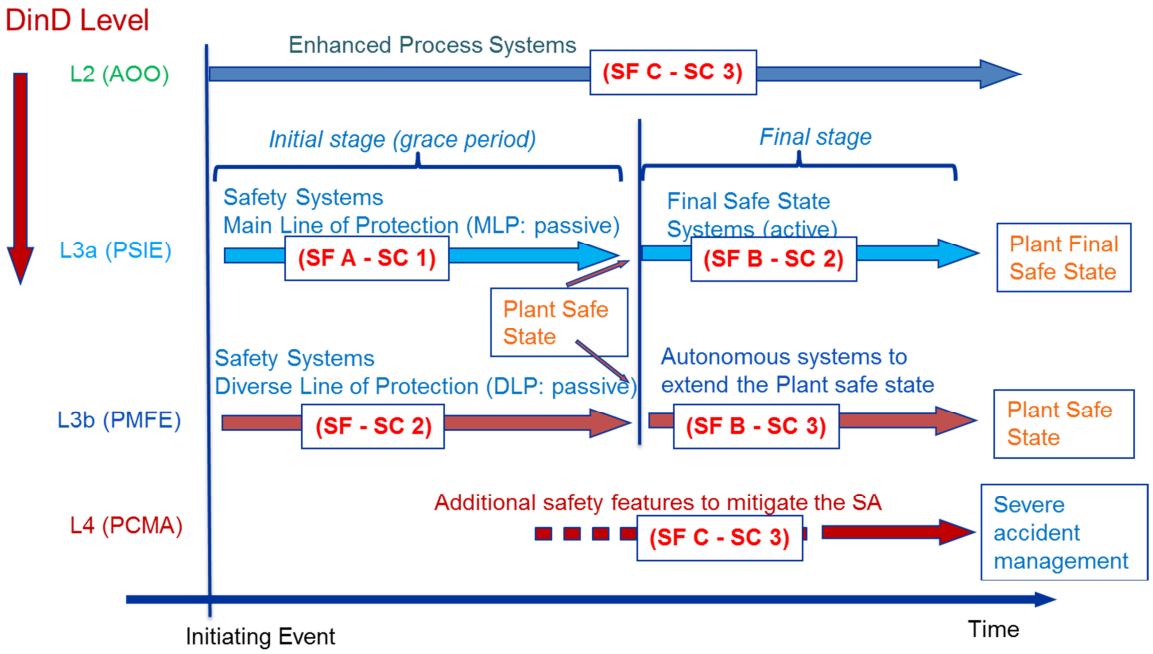


Figure 3 – Categories and Classes assigned to each level and stage defined in the strategies for control of PEs and PCMAs

Safety Technical Requirements for Systems and Components

In order to ensure the functionality of Systems and Components (SC) from a safety point of view, it is fundamentally necessary to have a clear set of functional requirements and design specifications against which SCs must be verified during design, manufacture, installation, commissioning and operation, and should be used as a reference for any subsequent modification. These requirements are established considering the DinD Level and the Category assigned to the LLSF and the Class assigned to the SCs of the SFG.

In particular, these requirements are established to ensure adequate capacity, reliability and robustness to each SC. Capacity is understood as the quality of each SC to perform its designated function, as required; reliability, the quality of an SC to perform its required function with a sufficiently low probability of failure consistent with the safety analyzes; and robustness, to the quality to ensure that no operational load or caused by the PEs adversely affect a SC to perform its function with the required reliability.

Because the structures have specific functions differentiated from mechanical, electrical and I&C components, generally referred to as SC, only the requirements for the latter will be defined in this document. Following the structure presented in [4], the requirements will be grouped in:

- General requirements for functionality,
- System-specific requirements,
- Specific requirements at the level of equipment and components,
- General requirements on quality management.

A clear and consistent assignment of category and class facilitates the regulatory process and the development of engineering, which also provides a basis for cost evaluation.

References

[1]. Safety of new NPP designs, Study by Reactor Harmonization Working Group, Western, European Nuclear Regulators Association (WENRA RHWG), August 2013.

[2]. IAEA Safety Standard: “Safety of Nuclear Power Plants: Design” – Specific Safety Requirements, SSR-2/1 (Rev. 1), Vienna (2016).

[3]. Safety Classification of Structures, Systems and Components in Nuclear Power Plants. IAEA Standards, SSG-30, Vienna (2014).

[4]. Instrumentation and Control Systems Important to Safety in NPP, Safety Guide NS-G-1.3, IAEA, Vienna (2002).

[5]. Nuclear power plants – Instrumentation and control systems important to safety – Classification of instrumentation and control functions, International Standard IEC 61226, Third Edition, 2009-07.