Safety assessment of next generation nuclear systems: methodology development and case studies on fission and fusion devices

Abstract

The current research activity in the nuclear field focuses on the development of nuclear facilities able to satisfy the four objectives identified by the Generation IV International Forum (GIF IV) in its Technological Roadmap in order to advance nuclear energy in its next generation: sustainability, safety and reliability, economic competitiveness, proliferation resistance and physical protection. The nuclear energy systems must be designed so that, during normal operation or anticipated transients, safety margins are adequate, accidents are prevented and off-normal situations do not deteriorate into severe plant conditions. Therefore, safety assessment and risk analysis are recognized as an essential priority in the development of these advanced systems.

My research activity aims at the definition and the application of an innovative approach to the risk analysis of next generation nuclear systems. The advanced technologies and the preliminary design of these concepts claim for a modernization of the traditional safety assessment, posing numerous safety-related challenges to be overcome in order to develop a holistic and comprehensive safety demonstration, therefore an efficient licensing framework.

For this purpose, the Integrated Safety Assessment Methodology (ISAM) proposed by the Risk and Safety Working Group (RSWG) in 2011 was selected as the basis methodology: it is constituted by several risk analysis tools to be applied in sequence and iteratively, in order to support the PSA, the final objective of the methodology. The ISAM was reviewed to better reflect the International standards/rules and to suit the peculiar case of new generation reactors. An inspirational philosophy was found in the IEC EN 61508, which constitutes a milestone for safety-driven design in the many engineering fields. Its major idea is that the systems safety must be studied and pursued from the early design by risk analysis tools through the definition of Safety Instrumented Functions to be analyzed in order to understand the effective risk reduction needed in terms of safety systems and additional safety requirements. Well-established practices to apply this functional safety approach to conceptual and innovative nuclear systems do not exist, therefore the idea is to enrich the ISAM with other risk analysis tools in order to select a list of hazards as complete as possible and improve the efficiency of the analysis and the detailed design definition. After a bibliographic survey on risk analysis operational tools, nuclear international standards, including also the process industry standards and best practices, three of them were integrated in the ISAM: Functional Failure Modes and Effects Analysis (FFMEA), Master Logic Diagram (MLD) and Lines of Defense (LOD).

Along with five other concepts, the Molten Salt Fast Reactor (MSFR) was selected by the GIF IV due to its promising design and safety characteristics and it is studied in the framework of the European project SAMOFAR, with the objective to advance its design and perform its safety

demonstration. MSFR consists of a cylindrical vessel with diameter and height of 2.25m filled with a circulating liquid fuel salt under ambient pressure at operating temperature of 750°C. Its peculiarities mostly derive from the circulating molten salt, acting as fuel and coolant contemporarily, and the fast neutron spectrum. Some consequences are the possibility of a passive reconfiguration of the core geometry in case of incident/accident, the frequent adjustments of the fuel composition allowing low reactivity reserves in core, a higher risk of reactivity insertion accident during loading and the fact that a significant part of the fissile matter is outside the core. Moreover, the design is still on-going, therefore a safety assessment performed at the components level is not useful since their architecture will evolve; instead, a functional approach allows to identify, since the early design, the functional deviations challenging the system and, consequently, to include safety features in a holistic optics.

The implementation of the defined methodology started from the identification of deviations able to compromise system safety (in terms of Postulated Initiating Events PIEs, the most challenging conditions for plant safety), through two approaches implanted at the same time: the FFMEA, a bottom-up approach, focused on the identification of the functions of the system and the analysis of the consequences of the loss of each of them, and the MLD, a top-down approach, that after the selection of a top event identifies its possible elementary causes. A list of PIEs was produced and for each of them a brief description of plausible causes, consequences, involved components and preventive and mitigation actions was supposed. In addition to the identification of PIEs, the FFMEA and the MLD allowed to highlight the lack of information on some systems, procedures or phenomena, to point out potential limitations of the design and make suggestions to enhance the safety of the concept. A list of some open points was produced.

Successively, for selected accidental scenarios the LOD method was applied to ensure that every accidental evolution of the reactor state was always prevented by a minimum set of homogenous (in number and quality) safety features before a situation with potentially unacceptable consequences might arise. Each event was briefly characterized, identifying also plausible prevention measures. During the application of the LOD method, some input data regarding natural behaviour of the plant following the initiating events, with a preliminary evaluation of expected radiological consequences, were fundamental in order to define the number of safety provisions. While describing the plant natural behavior, all the protection systems were not considered, therefore could not influence the evolution of the transient; consequently, physical phenomena, such as the feedback reactions and fuel salt volume variations, completely drove the scenario definition. Successively, possible provisions able to cope with the event were identified and the preliminary outcomes of this method were analyzed. The LOD helped to realize that additional provisions could be necessary to ensure the complete management of the accident (e.g. the addition of a core catcher or equivalent) or recognize the importance of ensuring the availability of some existing components: in particular, from the analysis of the overcooling accident, the availability of the free levels to allow the fuel salt expansion resulted absolutely necessary. This point deserves to be deeply studied: a detailed analysis of all scenarios that might lead to free level unavailability (e.g. too much initial fuel salt pouring, blockages, salt pouring from the intermediate circuit through an intermediate heat exchanger leak…) would be worthwhile, in order to ensure a very high reliability of the components and appropriate design measures.

Part of the defined methodology was applied to some systems of the full-scale fusion reactor EU DEMO, in the framework of the EuroFUSION program for the safety assessment of the DEMO auxiliary systems. The FFMEA was performed for the Primary Heat Transfer System (PHTS) and the Balance of Plant (BoP) of the Dual Coolant Lithium-Lead (DCLL) blanket option. The analysis started from the study of the system components, materials and plausible physical phenomena that could challenge the system (especially chemical characteristics of the present fluids); it provided a list of 24 PIEs, analogously to the list of 27 PIEs provided for the similar study about the Water Cooled Lithium-Lead (WCLL) blanket option.

The risk assessment process for an advanced nuclear plant is proposed to be iterative rather than serial: as the design matures and more design details become available, the set of accident initiators will be updated and broadened to gradually address other systems and operational states. At the same time, the selected events will be studied through deterministic analyses in order to define more accurate events sequences. When the deterministic inputs are modified, the design changes and the risk assessment model evolves as well.

In parallel, a critical evaluation of the nuclear safety assessment procedure was carried on: the majority of current safety regulatory requirements is based on LWRs technology and necessitates changes to suit to a new spectrum of advanced nuclear plants that present a much larger range of risks variability (due different physical phenomena, plant responses associated with the reactor transients/accidents, use of different materials for the reactor fuel, moderator and coolant and to different safety design approaches for the implementation of radionuclides barriers). Moreover, methodological and conceptual open points were identified: for example, the LWR risk metrics (core damage frequency –CDF- and large early release frequency –LERF-), are neither relevant nor useful for many advanced nuclear reactors; as well concepts as physical barrier, the severe accident definition or the PSA role need to be reconsidered and represent important safety challenges for the acceptability of new generation plants.