Doctoral Dissertation
Doctoral Program in Energy Engineering (31th Cycle)

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

By

Anna Chiara Uggenti

******

Supervisor:
Prof. A. Carpignano
Prof. S. Dulla

Doctoral Examination Committee:

Prof. Valerio Cozzani, Università di Bologna
Prof. Francesco Di Maio, Politecnico di Milano
Prof. Elsa Merle, LPSC-IN2P3-CNRS, UJF, Grenoble INP
Prof. Nicola Pedroni, Politecnico di Torino
Prof. Giovanni Sansavini, ETH Zürich

Politecnico di Torino
2019

Declaration

I hereby declare that, the contents and organization of this dissertation constitute my own original work and does not compromise in any way the rights of third parties, including those relating to the security of personal data.

Anna Chiara Uggenti

2019

* This dissertation is presented in partial fulfilment of the requirements for **Ph.D. degree** in the Graduate School of Politecnico di Torino (ScuDo).

E i tuoi bandi
io non credei che tanta forza avessero
da far sí che le leggi dei Celesti,
non scritte, ed incrollabili, potesse
soverchiare un mortal: ché non adesso
furon sancite, o ieri: eterne vivono
esse; e niuno conosce il dí che nacquero.
...
Tu dirai che da folle io mi comporto;
ma forse di follia m'accusa un folle.
(Sofocle, Antigone, 442 a.C.)

I did not think
anything which you proclaimed strong enough
to let a mortal override the Gods
and their unwritten and unchanging laws.
They're not just for today or yesterday,
but exist forever, and no one knows
where they first appeared.
If you think what I'm doing now is stupid,
perhaps I'm being charged with foolishness
by someone who's a fool.
(Sophocles, Antigone, 442 b.C.)

A Mattia e Francesca

Acknowledgement

I would like to express my sincere gratitude to my advisors Prof. Carpignano and prof. Dulla for the continuous support throughout developing and writing this thesis and for discreetly driving me during these years.

I would like to thank all the members of the doctoral examination committee and in particular the reviewers of my thesis, Prof. Di Maio and Prof. Cozzani, for the insightful comments and for the questions that helped me to look at my work from a different perspective.

I thank the Ph.D and M.Sc. students that I met in this time; I am glad that we shared experiences and stimulating discussions. Above all, I am glad that I had the opportunity of meeting interesting people, brilliant young researchers and even some friends.

I thank the Seadog team, all the people who worked and are still working in the laboratory. In particular, my sincere thanks goes to Prof. Gerboni, a precious model of researcher and human being.

I would like to thank my family: my parents and my brother and sister for always supporting me and my choices.

Last but not the least, I want to thank Mattia, my boyfriend, which continuously supported and encouraged me with love, patience and tenderness. We are growing together, trying to be the best version of ourselves.

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 framework.

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 to 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.

Contents

List of Figures

List of Tables

Nomenclature

Abbreviations

AEC	Atomic Energy Commission
AL	Acceptance Limit
ALARP	As Low As Reasonably Practicable
BB	Breeding Blanket
BP	Basic Principle
BoP	Balance of Plant
BSS	Back Supporting Structure
BWR	Boiling Water Reactor
BZ	Breeding Zone
CCF	Common Cause Failure
CDF	Core Damage Frequency
CDS	Coolant Detritiation System
CR	Criteria
CVCS	Chemical and Volume Control System
DBA	Design Basis Accident
DCLL	Dual Coolant Lithium Lead
DEMO	DEMOnstration fusion power reactor
DHR	Decay Heat Removal
DiD	Defence in Depth
DoE	Department of Energy
DPA	Deterministic and Phenomenological Analyses
DV	Divertor
EDS	Emergency Draining System
EDT	Emergency Draining Tank
EIA	Environmental Impact Assessment
EUC	Equipment Under Control
EV	Expansion Vessel
FBS	Functional Breakdown Structure
FFMEA	Functional Failure Mode and Effect Analysis
FoM	Figure of Merit

FP	Fission Product
FW	First Wall
GDC	General Design Criteria
GFR	Gas-cooled Fast Reactor
GIF IV	Generation IV International Forum
HTS	Heat Transfer System
HVAC	Heating, Ventilation and Air Conditioning
HX	Heat Exchanger
IAEA	International Atomic Energy Agency
IE	Initiating Event
I&C	Instrumentation and Control
IHS	Intermediate Heat Storage
IHX	Intermediate Heat Exchanger
IN	Indicator (for INPRO)
INES	International Nuclear and radiological Event Scale
INPRO	International Project on Innovative Nuclear Reactors and Fuel Cycles
INS	Innovative Nuclear System
ISAM	Integrated Safety Assessment Methodology
ITER	International Thermonuclear Experimental Reactor
LERF	Large Early Release Frequency
LFR	Lead-cooled Fast Reactor
LM	Liquid Metals
LOCA	Loss of Cooling Accident
LoD	Line of Defence
LWR	Light Water Reactor
MLD	Master Logic Diagram
MSFR	Molten Salt Fast Reactors
MTTR	Mean Time To Repair
NPP	Nuclear Power Plants
O&M	Operation and Maintenance
OPT	Objective Provision Tree
PAV	Permeation Against Vacuum
PBS	Plant Breakdown Structure
PDC	Principle Design Criteria
PFC	Plasma Facing Component
PHTS	Primary Heat Transfer System

PIE	Postulated Initiating Event
PIRT	Phenomena Identification and Ranking Table
PSA	Probabilistic Safety Assessment
PWR	Pressurized Water Reactor
QHO	Quantitative Health Objective
QSR	Qualitative Safety features Review
RSWG	Risk and Safety Working Group
SAMOFAR	Safety Assessment of the Molten Salt Fast Reactor - MSFR
SCWR	Supercritical Water-cooled Reactor
SFR	Sodium-cooled Fast Reactor
SG	Steam Generator
SIF	Safety Instrumented Function
SIL	Safety Integrity Level
SIS	Safety Instrumented System
SRS	Safety Requirement Specification
SSC	Structures Systems and Components
TBM	Test Blanket Module
UR	User Requirement
US NRC	United States Nuclear Regulatory Commission
VHTR	Very High Temperature Reactor
VV	Vacuum Vessel
VVPSS	Vacuum Vessel Pressure Suppression System
WCLL	Water Cooled Lithium Lead

Introduction

Nuclear power is recognized as an outstanding source for base load low-carbon electricity production and it is included in all energy scenarios in the European Energy Roadmap 2050. In particular, the development of new technologies and associated fuel cycles results fundamental to improve the utilization of nuclear fuel. After Fukushima-Daiichi accident, all European nuclear power plants underwent stress test and peer reviews and new generation nuclear reactors are expected to be designed with the highest safety standards from the beginning. The ultimate aim is to develop nuclear energy, which is inherently safe and does not produce nuclear waste other than fission products. In 2002 Generation IV International Forum (GIF IV) selected six systems from nearly 100 concepts as the Generation-IV fission nuclear plants: the Gas-cooled Fast Reactor (GFR), Sodium-cooled Fast Reactor (SFR), Lead-cooled Fast Reactor (LFR), Molten Salt Reactor (MSR), Very-High-Temperature Reactor (VHTR), Supercritical-Water-cooled Reactor (SCWR) (GIF, 2014); on the other hand the DEMOnstration fusion power reactor (DEMO) is foreseen to follow the advancements of ITER (International Thermonuclear Experimental Reactor) by 2050 (EUROfusion website).

The current research activity in the nuclear field focuses on the development of nuclear facilities able to satisfy the eight objectives identified by the GIF IV in its Technological Roadmap in order to advance nuclear energy in its next generation. They are divided into four goal areas: sustainability, safety and reliability, economic competitiveness, proliferation resistance and physical protection (GIF, 2014).

In particular:

- The **sustainability** goals aim at enhancing the effective fuel utilization, the long-term availability/reliability of the systems and the waste management, in order to conserve resources, preserve population and environment health, without jeopardizing the ability of the next generations to satisfy their own necessities (Sustainability 1 and Sustainability 2 goals) (GIF, 2002).
- The **Economics** goals aim at realizing competitive life cycle, cost of energy production and financial risk with respect to the other energy sources (Economics 1 and Economics 2 goals) (GIF, 2002).
- The **Safety and Reliability** goals aim at safe and reliable operation, minimizing the frequency and consequences of severe accident with the consequent reduction of off-site radioactive release and serious plant damage. The objective is to zero the necessity for an off-site emergency response, no matter the new technologies and physical conditions characterizing the innovative systems (Safety and Reliability 1, Safety and Reliability 2, Safety and Reliability 3 goals) (GIF, 2002).
- The **Proliferation Resistance and Physical Protection** goal aims at controlling and protecting nuclear materials and facilities and protecting them against terrorism acts (Proliferation Resistance and Physical Protection 1 goal) (GIF, 2002).

The attempt to answer this request with a fully innovative technology is the rationale associating all Generation-IV reactor designs and also the proposed concepts for a full-scale fusion reactor (DEMO). In particular, according to the Safety and Reliability goal area, innovative reactors have to be designed so that, during every operational mode (normal operation, start-up, shut-down, maintenance or anticipated transients), safety margins are appropriate, accidents are prevented and off-normal situations do not degenerate into more severe plant conditions. Moreover, all the major contributors to availability, reliability, inspectability, and maintainability have to be identified (GIF, 2002). Therefore, safety assessment and risk analysis are recognized as a priority in the development of these advanced systems.

The unique and various characteristics of new generation nuclear installations, the preliminary stage of the design, the incomplete knowledge of the physical behavior of the systems, the safety role widely accepted in other industrial fields challenge the traditional safety demonstration and ask for innovations. The innovative

systems call for a new safety approach based on technological neutral methodologies, always relying on the IAEA fundamental safety principles (IAEA, 2006): in particular, the definition of an **integral safety assessment methodology** and the demonstration of its applicability and efficacy. In addition, as a general engineering trend, the safety demonstration should proceed in parallel with the design evolution, aiming at influencing it since the earliest stages by giving useful feedbacks and guidance to the designer in order to achieve a safety that is "built in" rather than "added on" (GIF, 2008; IEC 61508, 2005).

Chapter 2 explains the context of this work; in particular, after a brief overview on the general concepts of the nuclear safety, it focuses on the limits of the current regulatory structure and on the safety challenges of new generation systems. This chapter focuses on the reason why a reconsideration, a modernization and an adaptation of the safety philosophy currently applied to the existing nuclear stations is necessary to properly fit the needs of non-traditional nuclear systems.

Chapter 3 proposes an overview on some safety assessment methodologies and standards that drive the safety demonstration of the traditional plants. In this chapter, it is presented a brief summary on the IAEA safety standards and on US NRC (Nuclear Regulatory Commission) regulations, focusing on what is directly applicable to new generation systems and what is specifically deduced for traditional plants. Successively, is presented the IEC EN 61508, a non-compulsory but widely accepted approach in many sectors (process industry, transportations, manufacturing industry, etc.): it constitutes a milestone for functional safety driving the design. Its philosophy inspired the IEC EN 61513, for the sketch of I&C architecture in nuclear power plants, even if the rigid traditional nuclear safety makes the 61513 misrepresenting the nature of the 61508. In the end, two methodologies, the ISAM (Integrated Safety Assessment Methodology) and the INPRO (International Project on Innovative Nuclear Reactors and Fuel Cycles), proposed by IAEA are presented. The two approaches take inspiration from the IAEA principles and aim at implementing the concept of safety driven design. This section focuses on their limits, mainly due to the fact that these approaches are inspiring philosophies that must be reviewed, completed and adapted, also using traditional risk analysis tools to suit the unique case of new generation installations.

Chapter 4 presents the methodology developed for supporting the safety assessment of new generation nuclear systems. It is based on a completely reviewed ver-

sion of the ISAM, taking into account all the inputs presented in the previous paragraphs and using some risk analysis operational methods traditionally accepted. This methodology constitutes a part of a potential operational framework for safety demonstration, which needs to be completed trough tailored criteria, requirements and consolidated safety assessment methods. This activity is a part of the European project SAMOFAR of the Horizon2020 program, which aims at furnishing the experimental proof of concept of the Molten Salt Fast Reactor (MSFR) and providing a complete safety assessment of the reactor (Flauw et al., 2018).

Chapter 5 presents the first application of the methodology to the case study of the Molten Salt Fast Reactor (MSFR). The outputs of this work are not only the expected results of the methodology, but also some open points to be properly evaluated and solved to allow the design to evolve (Appendix A and B). Also this activity is a part of the SAMOFAR project.

Chapter 6 presents the application of part of this methodology to several options of the DEMO blanket cooling systems. The methodology has been used to prepare a comparison between several solutions. The activity provided a support to the EuroFUSION program for the safety assessment of the DEMO auxiliary systems.

Chapter 7 summarizes the conclusions of this work.

1.1 Aim of the thesis

This work contributes to highlight the main safety challenges of new generation nuclear installations to be overcome to allow a safety demonstration of innovative installations.

The definition of a **methodology** suiting the innovative but preliminary design, based on functional analyses, is fundamental to guarantee a systematic and as complete as possible analysis, which can be useful also for other innovative installations.

One main objective of the safety assessment methodology is to give **feedbacks on the design**, and the proposed method also contributes to this purpose by highlighting some open options in the design and giving some indications on their potential impact from the safety point of view. The safety demonstration has to be pursued along the design development, in a risk-informed point of view. The predefined risk tolerability criteria have to be guaranteed during all the phases of the

project of the reactor and its auxiliary/protection systems. On the other hand the residual risk, which cannot be eliminated during the project, will be managed during the operational life with opportune O&M actions and procedures (according to the inspiring philosophy of the IEC 61508).

The methodology is applied to MSFR and to some parts of DEMO reactors to identify hazards and needed safety provisions and to help the enhancement of the design.

Chapter 1

Context: Safety challenges for new generation nuclear plants

2.1 Nuclear reactor safety

The IAEA fundamental safety objective is “to protect people and the environment from harmful effects of ionizing radiations” (IAEA, 2006) and it applies to all circumstances that could represent a source of radiations risks in all the nuclear installations. The **nuclear safety regulation** is the operative translation of this safety principle and its role is to permit the authority independent verification that a given nuclear design can safely operate with reasonable guarantees to safeguard public health and safety, and the environment.

Notwithstanding significant cultural, social and political differences existing between countries with a program for nuclear energy production, the regulatory agencies around the world have adopted basic principles similar to those described by IAEA and US NRC regulations. Therefore, the fundamental basis for demonstrating nuclear safety results sufficiently uniform among the different countries. It depends on the accomplishment of a set of **safety functions** that guarantee the control of the reactor during normal operation conditions with adequate safety margins; moreover, safety functions ensure that accidents are prevented, consequences are minimized, off-normal transients do not deteriorate into severe plant conditions (no domino effect) and the residual heat is removed during the reactor shutdown.

The safety functions to be guaranteed for *all the nuclear systems* include:

- The *control of the reactor reactivity* during all operational modes (startup, operation and shutdown);
- The *control of heat removal* to an ultimate heat sink;
- The *control of coolant inventory*;
- The *control of any chemically reactive or radiological materials*;
- The guarantee of an *ultimate confinement*.

The achievement of these safety functions aims at preventing or limiting to acceptable levels the radiological releases.

Nuclear installations must install **safety systems** and implement **procedures** with the objective to realize these safety functions: this means also to take into account all the life phases of the support systems (design, operation, maintenance and dismantling). If needed, the reactor design must ensure physical separation, independence, diversity and redundancy for protection systems in order to reduce the frequency of Common-Cause Failures (CCFs) or single point failures that could lead to dissatisfy a safety function. Finally, **defence in depth (DiD) and safety margins** reduce the possibility that an incomplete understanding of the reactor behavior can challenge the safety functions (MIT, 2018).

The worldwide park of the currently operating commercial nuclear reactors consists of 85% LWRs (IAEA, 2017), where the satisfaction of critical safety functions is ensured by a combination of active and passive systems and operator actions. Consequently, the regulatory and licensing structure properly suits the LWRs technology, physics and procedures.

For safely operating, **advanced reactors must ensure the accomplishment of the safety functions**: to fulfill this objective, a great importance is given to inherent and passive protection systems directly integrated in the design. The unique and innovative characteristics of the new generation nuclear installation, a wide range of different technologies, the preliminary stage of their design, the new safety role widely accepted in other industrial field, and the feedbacks from occurred accidents (in particular Fukushima Daiichi) challenge the traditional nuclear safety demonstration and demand renovations. The aim is to better suit a new spectrum of novel and advanced plants (Southern Company, 2017).

The following paragraphs present a panorama on the main intrinsic challenges of the safety assessment of new generation installations.

2.2 Safety challenges

The majority of current nuclear safety regulatory requirements is based on LWRs technology and necessitates adaptations for the new generation installations. A brief overview of the traditional regulatory framework is presented in Chapter 3.

Several authorities highlight the limits of the application of the current regulatory structure and propose updates for specific elements of the traditional safety assessment.

The Southern Company, sponsored by the Department of Energy (DoE) of the US government and other industry participants, led a project for the modernization of the licensing process based on the development and the use of a technology-independent and risk-based PSA (Probabilistic Safety Assessment) for new generation installation. The proposed methodology is intended to be firstly introduced at a very early stage of the design and to be repeatedly applied during the entire design definition (Southern Company, 2017).

An interdisciplinary MIT study reviewed the regulatory structure for nuclear facilities to assess its ability to drive the licensing process of advanced nuclear installations. It focused on best practices and possibilities of improvements for the licensing and regulating US framework (MIT, 2018).

The IAEA standards suit perfectly to traditional installations, nonetheless opportune standards for innovative systems, always derived from the fundamental safety principles (see paragraph 3.1), must be still developed.

Some design-specific safety elements, which were developed for safety assessment of LWRs, must be fundamentally different for advanced reactors: functional barriers for the retention of radioactive materials, risk metrics for risk quantification, success criteria, SSCs (Structures, Systems and Components) available for the implementation of the safety functions, final state of the event sequences, radioactive source terms, frequency calculation of multi-module plants, Design Basis Accidents (DBAs), etc. For example, the inconsistency of the design safety margins required by standards and good practices can result in underestimation or overesti-

mation of SSCs. The traditional safety margins do not take into account the peculiarities of the specific analyzed technology, which may be extremely different from the LWRs. Since these margins guide the implementation of the safety provisions, their adequacy results fundamental for the safety demonstration of a system. The new generation installations necessitate appropriate criteria, derived from the analysis of the major physical-chemical phenomena driving their behavior during transients (e.g. the distance from the boiling temperature for Liquid Metals -LM- cooled reactors) in order to efficiently direct the sketch of their safety architecture.

Another example is given by the traditional structure of PSA; the classical Level 1, 2, 3 structure can need substantial changes for several new generation nuclear installations: the design of some advanced reactors does not foresee a plant status equivalent to the one described in Level 1 and 2 PSA of LWRs; in fact, specific design characteristics preclude core damage states that have been defined for LWRs. For example, for the molten salt reactors the core melting accident is meaningless, being the fissile and fertile salt at the liquid state. Moreover, the advanced reactor PSA will manage also radioactive sources outside the reactor.

It results evident the importance of harmonizing the regulatory framework to provide prompt and timely licensing process. In the following paragraph there is a systematic description of some of the main issues for the safety demonstration of advanced reactors (Carpignano et al., 2018).

2.2.1 New materials, new technologies and design in development

The PSA is highly design, plant and site specific; this is true for any kind of reactor. In particular, dealing with advanced nuclear systems with very different technologies implies a much **larger range of risks variability with respect to a LWR** (Carpignano et al., 2018): physical phenomena and processes are different, as well as the plant responses to reactor transients and accidents. This is due to the use of different materials for the reactor fuel, moderator and coolant, to innovative technologies for energy production and to different safety design approaches for the implementation of radionuclides barriers (Southern Company, 2017). For example, in the view of the sustainability, advanced reactors plan to use thorium based fissile and fertile salts, different from the traditional uranium based fuel cycle of LWRs. Moreover, the fast reactors will not include moderator (whose main function is to slow down the neutrons energy from fast to thermal spectrum). Finally, while LWRs are cooled by pressurized water (Pressurized Water Reactors –PWRs- at ~155 bar and Boiling Water Reactors –BWRs- at ~70 bar), generation IV concepts

present a wide range of coolant, from liquid metals (lead and sodium) to supercritical water, from gas to molten salt. On the other hand, the fusion devices exploit completely different technologies. The use of generic models and approaches, especially if developed for LWRs, risks neglecting the design and technology specific safety issues.

Dealing with the safety assessment of an advanced reactor means to investigate **all the potential sources of radioactive materials** (in core, in the fertile blanket, in the cooling circuit, in the protection and control systems, in fuel handling and storage systems). The analysis should be performed in all the planned operation conditions (normal operation, start-up, shut down, maintenance, refueling, etc.), exploring all the combinations of components failures causing the non-fulfilment of a safety function. Furthermore, the quantification of the frequencies and consequences must be modeled, including systematic sensitivity analyses in order to study the risk as a function of the characteristics of SSCs and set appropriate requirements, therefore design and operational safety margins.

It is worth highlighting that many of the designs of the new generation installations, including fusion machines, are very preliminary and still in evolution. A safety assessment at the component level is not useful since the architecture will mature in time and the **risk evaluation can be only preliminary**. Moreover, the operational phases are not completely defined. Hence, a non-LWR PSA can be considered not as a punctual methodology but as an iterative process expanding the purpose and the detail level of the PSA with the advancement of the design definition and the knowledge of the physics and the behavior of the system.

The lack of knowledge on the plant increases the uncertainties in the estimation of accident frequencies and consequences. The **sources of uncertainties** should be identified, treated through available data, expert opinions and other objective evidences and, in the end, their impact on the risk results should be quantified to be used for the implementation of the DiD evaluations (Southern Company, 2017).

2.2.2 Risk metrics

Because of these differences (see paragraph 2.2.1), the LWR risk metrics, for instance the Core Damage Frequency (CDF) and the Large Early Release Frequency (LERF), directly linked to the core melting phenomenon, are neither relevant nor useful for many advanced nuclear reactors. Some plants, in fact, may not

involve the core damage state that was defined for LWR and, even in the case, its meaning and risk framework can be fundamentally different from LWR (INL, 2011). For example, the MSFR major characteristic is the liquid state of its core, playing at the same time the role of fuel and coolant; it is clear that the previously mentioned risk metrics and the core melting itself result inappropriate to this system. As well, the fuel for the fusion machines is gaseous and the completely different physics claim for completely different risk metrics, detached from the idea of solid fueled reactors.

It is important to highlight that the traditional classification of PSA Level 1, 2 and 3 starts from the concept of core melting and CDF and LERF; therefore, the update of the risk metrics involves a new modernized PSA concept. Consequently, PSA for advanced reactors may be structured differently than the traditional Level 1, 2 and 3 model for LWR PSA: it is expected to include out of core sources of radioactive material (especially in the case of online refuel, as for the MSFR and GFR) and to adopt adequate and more general risk metrics (INL, 2011). The latter may lead to an appropriate definition of severe accident, disconnected from the core melting concept (see paragraph 2.2.3).

The regulatory framework and the risk metrics, as its operative instrument, can be described in terms of **technology** (are the requirements generic or specific?), **risk** (how is it taken into consideration?), **prescriptive or performance based**. Nonetheless, the final purpose of the entire regulatory processes is always the same: the satisfaction of the fundamental safety objective (MIT, 2018).

Technology

The risk metrics can be *specific for a certain nuclear technology* or can *be applied to any kind of technology*.

The advantage of *technology-specific risk metrics* is that it is developed for a specific system and perfectly suits it. It is simple to be used by operators/applicants/regulator bodies along the licensing process. Therefore, it reduces the licensing efforts, using the lessons learned from previous experiences and smoothing the process; moreover, it aids the verification of the consistent application of the rules, with less uncertainties (Walker & Mazuzan, 1992). The main disadvantage of this typology of requirements is the inertia opposed to innovation: a stiff regulatory framework may discourage the introduction of updated or novel reactor concepts, especially if they present major modifications with respect to traditional plants (e.g.

MSFR). The natural consequence is that the innovative concept will face important challenges to adapt to the regulatory framework.

The main advantage of *technology-neutral risk metrics*, and, more generally, regulations apparatus, (MIT, 2018) is the facilitated arrangement of any innovative technology of new systems. As a drawback, the requirements often lack of specific indications to guarantee consistent, uniform and unique interpretation of rules (NRC, 2007). Consequently, the licensing process is slowed down.

A mixed framework can be evaluated (NRC, 2007): the technology neutral requirements/objectives can provide a guidance for developing and applying the necessary technology specific criteria. In this way, the licensing process for all the technologies can be properly supported, giving value to the previous licensing experiences and optimizing the process (MIT, 2018).

The definition of technology neutral risk metrics particularly suits the generation IV systems for several reasons: the preliminary design of some of the systems, the lack of information about the reactor behavior during transients (especially about the major driving phenomena) and the wide range of different proposed technologies do not allow, at this moment, for technology specific risk metrics. The latter ones may be developed in a later stage of the technology evolution.

The Risk

The risk evaluation implies the answer to three questions: “What can go wrong?” (Scenario), “How likely is it?” (Probability + uncertainties) and “What are the consequences?” (Damage + uncertainties).

In the regulatory framework, these aspects can be managed in three ways:

- The deterministic approach;
- The risk based approach;
- The risk informed approach.

The *Deterministic approach* focuses only on two of these questions: in fact, a set of design basis accidents (DBAs) is defined to answer the question “What can go wrong?”; then, the consequences of these events are deterministically evaluated in order to answer the question “What are the consequences?” and to include pro-

visions to prevent or mitigate the consequences. This approach establishes requirements for engineering margins and components quality, without proper quantitative evaluations of probabilities. This is the traditional regulations structure, largely used in the past.

The *Risk Based approach* focuses on the numerical results of the risk assessment, based on the evaluation of the scenarios probabilities and the consequences using best estimate values. The uncertainties are evaluated but there are not conservative assumptions. It is worth highlighting that this approach has never been completely authorized by regulatory body, even if some specific applications are recognized, e.g. the dose limits. For example, during the application of the IEC 61508 (see paragraph 3.3), both probabilistic requirements (component availability/reliability) and architectonic criteria (prescriptive criteria such as redundancies) must be guaranteed for the correct classification of the SSCs (SIL assignment, for major details see paragraph 3.3). Especially in case of publically available data utilization, the probabilistic assessment is not sufficient. An exception is the case when the analyst can demonstrate the quality of the used statistical data (e.g. classified internal data): in that case only probabilistic methods can be used for the assessment without any additional prescriptive requirements.

The *Risk-Informed approach* represents a compromise between the purely deterministic approach and the risk-based approach: sometimes it reduces the excessive and unjustified conservatism of the deterministic approach, other times it highlights the necessity of additional requirements or provisions. The safety requirements are based on deterministic requirements derived from a wider set of scenarios challenging the reactor. The sequences of interest are determined through a probabilistic approach and are prioritized through their risk importance. Then, the uncertainties are quantified and/or conservative hypotheses are made, coherently with the defence in depth concept (Vietti-Cook, 1999). This approach results the most suitable for innovative reactors whose design is still preliminary because it helps understanding the different scenarios' risk contributors, identifying criticalities. Moreover, it can drive design evolution, additional safety analyses, definition of suitable safety criteria, especially thanks to the insights obtained from the PSA and proper management of the uncertainties.

It is worth noting that the consequences of an accidental sequence are acceptable according to the deterministic approach only if their severity is sufficiently low, no matter the frequency of the event. On the other hand, if the safety demonstration is based on probabilistic analyses (risk-based or risk-informed approach), a higher

severity of the accidental sequence can be acceptable, if the associated frequency is sufficiently low (the base philosophy of the risk matrices).

Prescriptive or Performance Based requirements

The *prescriptive/proscriptive (or rule-based) technical requirements* indicate what to do and what to avoid doing to satisfy a safety objective (how to satisfy a specific objective). Conversely, the *performance-based requirements* present an objective to be pursued (which objective must be pursed) and the operator/applicant can decide the systems, procedures, techniques, good practices to reach the goal (Kadamabi, 2002).

The prescriptive/proscriptive requirements are simpler to be applied and reduce the uncertainties: in fact, the licensing criteria are clear for both applicants and regulators. Nonetheless, the attention is focused on the way to reach the objective rather than on the objective itself. This stiffness implies that innovations are disheartened and all the efforts are concentrated on the implementation of the method while less energy is put on guaranteeing that the final objective is actually reached.

The added value of the performance-based requirements is that all the efforts are focused on the fulfilment of the final goal. It is flexible and suitable to all the new technologies; it encourages innovation in safety, good practices and continuous enhancement and supports new technologies. On the contrary, it can result in uncertainties, needs the engineering judgement for the verification of the objective achievement, is not univocal and may slow down the safety demonstration.

Nuclear Power Plants (NPPs) traditional design is very standardized (see paragraph 2.2.6), in fact the 85% of the existing and operating reactors are LWRs, for the major part designed and built by Westinghouse and General Electric according to the American licensing structure (see paragraph 3.2). Consequently, their safety demonstration is tailored on the used technology, with prescriptive and proscriptive requirements, improving the efficiency and velocity of the entire safety assessment process. With the proliferation of a wide range of new technologies, the prescriptive approach loses its main advantage. On the other hand, the risk analysis nature is essentially performance-based and its primary objective is the safety demonstration of a specific (also unique) technology in a specific site, with specific procedures, management, etc. (see paragraph 6.3 on IEC 61508). In this sense, performance-

based requirements result the most adequate for new technologies, driving their design development and compensating the lack of information.

A mixed approach results complicated to be realized: the nuclear safety present framework is rigid and the addition of external elements (e.g. goal-based requirements) is misrepresenting, difficult and always limited to small parts of the entire system. The IEC 61513 is an attempt to realize a mix framework (prescriptive and goal-based at the same time) for LWRs I&C architecture. The specific case is analyzed in paragraph 6.4.

The update risk measures

Since the inadequacy of the CDF and LERF to represent the non-LWR reactors, ASME/ANS PRA Standards (ASME/ANS, 2013) suggested the use of technology neutral risk measures, listed below.

a) **Frequencies of event sequences individually and grouped into accident families having the same or similar plant response and offsite radiological consequences**. Consequences generally are calculated in terms of offsite health effects (immediate or delayed) and/or site boundary doses. The accidents belong to the same family because their consequences are ranged in the same category or because the accident initiator, the plant response and end state, and offsite radiological impact are similar.
b) **Integrated risks of a given consequence metric** (e.g. site boundary dose, number of early or latent health effects, etc.). It can be obtained by summing risk (calculated as the product of the frequency and damage) of each events sequence over the full set of events sequences.
c) **Integrated risks of individual fatalities**: it is an individual risk mapping to be calculated in the proper way to be easily comparable to the Quantitative Health Objectives (QHOs).
d) **Cumulative frequency of exceeding consequences** (e.g. large release, early or latent health effects, specific site boundary dose). This criterion follows the logic of the FN curve for social risk: F is the cumulative frequency of events whose consequences affect at least N people (Bedford, 2004). In order to build this curve, for each accidental event, judged reasonably possible, the number of affected people (e.g. fatalities) must be evaluated. From this calculation it is possible to find the cumulative frequency of a generic

accident able to cause N fatalities. Finally, the obtained results must be compared to the risk acceptability criteria.

It is interesting to notice that criterion a) is similar to acceptability risk criteria reported in the Seveso legislation, in particular in the DM 9/5/01 (Ministero dei lavori pubblici, 2001), about the compatibility of territorial categories with the operation of a plant involving major accident hazards. It is an accepted industrial practice (e.g. see reference (Canevaro & Cevrero, 2014)) to sum the frequencies of the sequences leading to a specific damage (e.g. high lethality, irreversible injuries, etc.) with a correspondent damage area and compare the obtained results with the compatibility criteria reported in the norm. Moreover, criterion d), and in particular the FN curve, is widely accepted in the industrial practice for the evaluation of the social risk (Carpignano & Tuninetti, 2004), and its use is suggested in the Italian transposition of the European offshore directive 2013/30/EU.

In addition to these general criteria, reactor-specific parameters will be defined. It is important to define the parameters that describe better the behavior and the criticalities of each specific technology: if only general metrics are used, the possibility to neglect important issues during the analysis is significant. For example, for the Sodium-cooled Fast Reactors (SFRs), the frequency of the Sodium boiling represents a specific issue of the system to be evaluated.

In the definition and in the calculation of the risk metrics, the multi-modules and multi-reactors plant must be properly modeled. In fact, the parameters associated both to a single module/reactor and to the entire plant must be evaluated. Moreover, possible common cause failures and dependencies must be assessed, for example in case of shared systems or structures.

The most common way to evaluate the acceptability of a certain analyzed scenario is the frequency-consequence curve criterion (the Farmer curve, see fig. 2-1, proposed by INL in 2011). This is a plausible application of criterion a). The frequency and consequence of the specific scenario (expressed as a certain measure, e.g. a specific site boundary dose) are calculated in the form of mean values and uncertainties percentiles (5^{th} and 95^{th} percentiles) and compared to the frequency-consequence evaluation criteria.

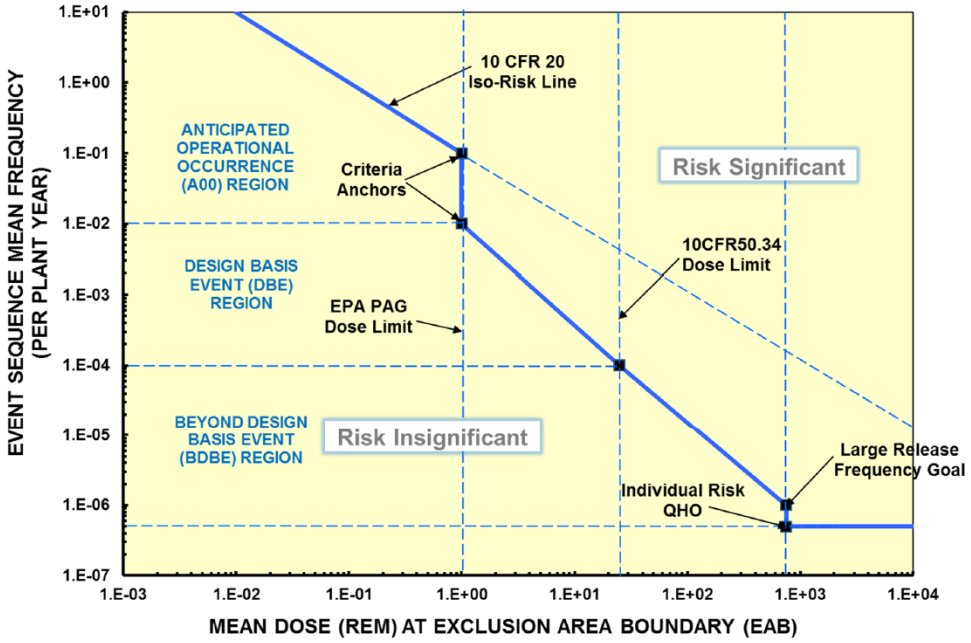

Figure 2-1 Frequency-Consequence Evaluation Criteria (INL, 2017)

According to the "Basis for the Safety Approach for Design & Assessment of Generation IV Nuclear Systems" (RSWG of the GIF, 2008), the rationalization of the advanced design should be pursued through the implementation of the ALARP (As Low As Reasonably Practicable) principle applicable to the full spectrum of design conditions. The ALARP region is defined by the UK Health and Safety Executive (HSE) as the tolerability zone between the acceptable and unacceptable risk regions. In order to define if a risk reduction measure is "reasonably practicable", a comparison between the benefits of the analyzed measure, in terms of risk reduction, and its implementation cost (comparison between advantages and drawbacks) has to be carried on a quantitative or qualitative basis (UK HSE, 2001). This optimal risk reduction is translated in the implementation of innovative provisions looking for further risk reduction (prevention of the initiators and consequences mitigation) on a cost-benefit basis (RSWG of the GIF, 2008).

It is worth to note that the curve represented in fig. 2-1 is not definitive, because the ALARP area is not represented. In a frequency-consequence graph, as the one represented in fig. 2-1, a range of values forms the ALARP zone, which in this case degenerates into a line. Because of the uncertainties due to the design still in development, the predictability of the reactor behavior, the knowledge of the main physical phenomena and the safety demonstration itself, the ALARP criteria, together

with the defence in depth, should constitute a cornerstone for the definition of the acceptability criteria (Carpignano et al., 2018).

Furthermore, the integrated risk evaluation of the entire plant is performed taking into account four evaluation criteria (INL, 2017):

- The total frequency of exceeding a site boundary dose of 100 mrem shall not exceed 1/plant-year according to the annual exposure limits in 10 CFR 20;
- The total frequency of a site boundary dose exceeding 750 rem shall not exceed 10-6/plant-year according to NRC Safety Goal Policy Statement on limiting the frequency of a large release;
- The average individual risk of early fatality within 1 mile of the Exclusion Area Boundary (EAB) shall not exceed 5×10-7/plant-year according to the NRC Safety Goal QHO for early fatality risk;
- The average individual risk of latent cancer fatalities within 10 miles of the EAB shall not exceed 2×10-6/plant-year according to NRC safety goal QHO for latent cancer fatality risk.

At the end of this section, it is important to remember that the traditional classification of PSA Level 1, 2 and 3 starts from the concept of CDF and LERF, therefore the update of the risk metrics implies a modernized PSA concept (Carpignano et al., 2018).

2.2.3 Severe accident

The term '**severe accident**' or 'core melt accident' for a LWR refers to an accident where the reactor fuel is significantly degraded, even melt. After Fukushima accident, the severe accident is not related only to the reactor core, but also to other systems, e.g. the pools used for spent fuel storage. This expanded definition (for example including fuel storage facilities) suits well LWRs, but may become problematic when applied to other reactor concepts. For example in the MSFR, the core state is at the liquid state during normal operation, making the notion of fuel degradation difficult to define. The concept of severe accident must therefore be expanded.

The definition given by the French institute for Radiological protection and Nuclear Safety (IRSN) in its review of generation IV nuclear energy systems (IRSN,

2014) may be of interest: "*A severe accident in a nuclear reactor is an accident during which the nuclear fuel radioelement confinement function is significantly degraded, regardless whether the fuel is inside the reactor, being handled or in a storage area".* This is only a definition reported in the previously mentioned report and it is not considered a general reference definition. Moreover, the notion of "significantly degraded" should be deepened with additional research activities (precise criteria). For example, for the EPR, a severe accident is considered to be initiated by a core outlet temperature in excess of 650°C or by a high dose rate measurement inside the containment. On PWR or SFR, the severe accident is also associated with loadings on the confinement. There is thus the notion of an accident potentially challenging the confinement.

Correlated to the notion of the severe accidents there is the notion of "**practical elimination**". It was introduced at the beginning of the 90's during the definition of the general safety objectives for the future PWR to be built in France and Germany. At the international level, in 1999, (IAEA, 1999) it was indicated: "[…] *Another objective for these future plants is the practical elimination of accident sequences that could lead to large early radioactive releases, whereas severe accidents that could imply late containment failure would be considered in the design process with realistic assumptions and best estimate analyses so that their consequences would necessitate only protective measures limited in area and in time*". In this definition there is a clear distinction between severe accident scenarios which can lead to an early containment failure which have to be "practically eliminated" and severe accidents leading to a late containment failure for which the implementation of design provisions to limit their consequences is possible. The latest international texts state that "practical elimination" should be applied to situations likely to lead to early or large releases (WENRA, 2013; IAEA, 2016), thus widening the range of situations potentially concerned. As of today, the "practical elimination" concept is a subject of on-going discussions at an international level, where a consensus has not been reached.

In the framework of this analysis, the severe accidents are considered as the situations potentially leading to large early radiological releases, e.g. situations where it seems impossible to define realistic and demonstrable measures to limit their consequences given the current knowledge and available techniques (e.g. fast and very energetic phenomena). This allows to identify and to pay a specific attention to the severe accident situations bearing the highest risk.

The decision to consider these situations or not in the design is very structuring for a new reactor concept. In fact, they have to be identified and analyzed from the initial design stages of a new reactor type. From a safety point of view, the practically eliminated accidents can lead to an early failure of the containment, therefore their occurrence must be prevented through sufficient protection measures. Since these sequences constitute a weak point of the system, for innovative concepts, the need for practical elimination by dedicated safety provisions should be strongly limited.

2.2.4 The cumulative frequency

While the traditional LWR risk assessment was developed following the "one-reactor-at-a-time" approach, in next generation nuclear plants the risk associated to multi-unit sites becomes certainly relevant and, especially after the Fukushima Daiichi accident, even dominant (Fleming, 2017). Advanced non-LWRs are expected to be constituted by several modules, located in the same site: this increases the possibility of common cause failures/domino effects, due to the sharing of systems and structures among several modules or hazards involving more than one reactor (e.g. external hazards) or human actions. The multiple modules structure augments the probability of scenarios affecting only one module and creates potential scenarios involving more than one module, and consequently potential release sources from more than one reactor. Therefore, integrated risks for advanced non-LWRs include event sequences involving two or more modules or radionuclides sources especially when the design includes a modular reactor concept. This influences the traditional frequency-consequence tolerability criteria (see paragraph 2.2.2).

One of the main challenges of new generation nuclear plants safety demonstration is a properly modelling of multi-units and multi-modules plants, quantifying all the radiological sources.

2.2.5 The role of PSA

A major difference between LWRs and next generation nuclear plants regulatory framework is the role played by risk assessment methodologies (e.g. PSA). For traditional installations, the safety analyses and the PSA are performed only after the definition of the detailed design and of the site and licensing process: in this case, if the tolerability criteria are not fulfilled, it could be necessary to modify also

the preliminary design. Therefore, the risk-informed applications are limited to additional systems or provisions for installations already built (for example in US, plants can be built even if the licensing process is not completed, see paragraph 3.2) and maybe operated. On the other hand, for advanced systems, the risk assessment tools aim at supporting and driving the design evolution and at widening the domain of the risk-informed choices (Southern Company, 2017). The safety tools will be applied at various discrete points of the design process. Moreover, their early application provides input for the development of reactor-specific design criteria and for the design of SSCs performing safety functions. As the design evolves and more details and data become available, the PSA purpose will expand as well in order to demonstrate the capability of the plant to meet the safety requirements. The analysis' scope is accomplished only when all the design information, the experimental data and tests are included and confirmed and a plant, site, design specific PSA is performed. The early introduction of the PSA pursues the objective to minimize the successive and expensive design updating.

2.2.6 No pre-defined methodologies

In the 1950s and 1960s, in US a huge number of nuclear systems were designed and built, due to the enormous government and population's support to the nuclear energy. The regulatory authority, which during those years coincided with the body enhancing and developing nuclear energy, the AEC (Atomic Energy Commission), licensed one by one all the technologies, basing on few experimental data, very limited practical experience and engineering judgement. The safety demonstration was based on four strategies:

- *Remote siting*: the reactor had to be located far away from populated areas;
- *Containment*: the structures had to contain the consequences of accidents, especially accidental release;
- *Low reactor power*: each reactor could represent a smaller source of radioactive materials;
- *Engineering margins*: the uncertainties were taken into account through additional engineering margins during the design (Mazuzan & Walker, 1985).

In 1971, the first general design criteria were formalized. In the meanwhile, the LWRs started their first commercialization. From this moment on, the general criteria became more and more specific and optimized for the LWRs peculiar case, with the aim of reducing uncertainties and improving the licensing process. As a side effect, also the size of the reactor increased (MIT, 2018).

Similar processes occurred all around the world, except for Canada and United Kingdom, whose main technologies are Heavy Water Cooled Reactors (CANDU) and Carbon Dioxide Cooled Reactors; therefore, their regulatory frameworks were optimized for these technologies.

Due to their standardization, the LWRs safety assessment, and consequently their safety architecture, are stiff and should be modernized and adapted to allow efficient safety assessment for new generations nuclear reactors. In fact, the use of models developed for LWRs may lead to neglect specific safety issues caused by the innovative design and technology of new generation installations.

Additionally, the LWRs' regulation framework is prescriptive (what to do) and proscriptive (what to avoid doing), since historically the safety process standards are rules-based. The variegate nature of the next generation nuclear facilities imposes safety process standards to be simple and based on stable, general principles. Risk informed and performance-based standards focus on the final objective of the safety assessment (what is necessary to achieve) and suits to new technologies (not only nuclear ones) better and more cost-effectively, by exploiting all the potentialities and the versatilities of the risk analysis. Certainly, gaps must be fulfilled in this updating process, as well as revisions of technical language and approach and a major flexibility.

2.2.7 Licensing's burden

It is well known that one of the main difficulties of licensing is its cost and the associated time (Finan, 2016). Historically, licensing costs (i.e. the fees billed to NRC in US) "have been in the order of $100 million for a complete design certification review and $25-$50 million for a site-specific combined operating license" (US NRC, 2015). Moreover, it is important to add the costs of eventual design work required for license application or to answer the questions of the regulatory body. Consequently, the **licensing's burden must be considered a criticality for the new advanced systems**.

The current licensing process (see paragraph 3.2) is not suitable for next generation plants. It must be tested for this new purpose in order to promptly identify

licensing criticalities, to trace a pathway and to train the operative staff. Several issues are highlighted:

- The regulatory readiness for many typologies of different reactors;
- How to assess the quality and completeness of the applications, when to require additional tests or analyses;
- The cost, the duration, the uncertainties of the process (maybe a long and expensive process is carried on for a reactor that will never be built);
- The training of the regulatory staff to appropriately review the applications and to solve technical questions during the process and appropriate management, taking into account the unavoidable gap of knowledge;
- The improvement of the efficiency of regulators/applicants interactions;
- Etc.

All the additional issues may increase the cost and the time consumption.

The regulatory body should define a more rapid licensing process for prototype reactors, which nowadays have to provide several additional safety features with respect to traditional reactors. For example, several experimental tests and data to be provided can be agreed in advance in order to speed the process. Moreover, a phased licensing approach should be evaluated with a costs-benefits analysis.

The renewed prototype licensing process must suit to all the reactor technologies.

2.2.8 Considerations

The regulatory agencies around the world agreed on IAEA basic principles (see paragraph 3.1) (IAEA, 2006). The implementation of these principles in the national regulations led to some differences, both philosophical and practical. From a philosophical point of view, the requirements can be technology specific (e.g. US) or technology neutral (e.g. Canada), deterministic (e.g. China, even if probabilistic evaluations may be required to support the results) or risk-based/informed (e.g. Canada), prescriptive (e.g. China) or performance-based (e.g. United Kingdom, Canada). From a practical point of view, there are also issues on the frequency of review of the licenses: 5 years in Canada, 10 years in France, 20 years in US (MIT, 2018).

For new generation systems, it is highly recommended (MIT, 2018) “to standardize and ensure a high level of safety worldwide”. The environmental and socio-political effects of the operation of nuclear systems should ensure certain basic standards, nevertheless national differences on safety framework and culture. Since the harmful effects of nuclear plants malfunctions cross the national boundaries and are experienced physically and psychologically all around the world, it is desirable an international agreement on the updating of nuclear safety regulations, in particular, on peculiar issues (e.g. the blackout protection systems) and shared methodologies for defining design criteria and for licensing evaluations.

Chapter 2

Overview of safety assessment methodologies and standards

The purpose of this chapter is to delineate a panorama on the prior activities, policies, standards, and requirements supporting the design and the licensing on nuclear reactors. The chapter starts from the IAEA safety standards (that inspire the national nuclear safety regulatory frameworks) and the NRC regulations (see paragraph 3.1 and 3.2), which constitute the milestone of the traditional NPPs safety demonstration all around the world. Nuclear safety assessment results a rigid and prescriptive process, tailored on LWRs; several processes are on-going to update the current framework for the innovative systems, but the process is only at the beginning. In this sense, the functional safety, the key concept of the IEC 61508 (developed for non-nuclear technical applications, see paragraph 3.3) could be inspiring and help the accomplishment of Generation IV requirements (see Chapter 1). The IEC 61513 (see paragraph 6.4) is a first example of a very specific application of the 61508 for nuclear purposes; nonetheless, it applies to a very small portion of the total domain, while the rest of the safety evaluation in not influenced by its presence. Finally, are presented two methodologies specifically developed for innovative concepts in the IAEA framework, the ISAM (Integrated Safety Assessment Methodology, see paragraph 3.5) and the INPRO (International Project on Innovative Nuclear Reactors and Fuel Cycles, see paragraph 3.6). They are not adaptations of already existing standards developed for other purposes, but are thought to help the innovative concepts design, while performing the safety demonstration of the analyzed systems. Their application is not always trivial; as well, the

interpretations of the included requirements is not always unique. Nonetheless, the ISAM has been chosen as the basis methodology for this work, after an adaptation process including some functional safety key concepts.

3.1 IAEA Safety Standards

IAEA (International Atomic Energy Agency) standards are considered the **global reference** for protecting people and environment from the harmful effects of radiations. They constitute an integrated comprehensive and consistent structure that provides the fundamental principles, requirements and recommendations to ensure high –level nuclear safety (IAEA, 2006).

The purpose of the Safety Standards is clearly expressed in **fundamental safety principle** (IAEA, 2006), "*The fundamental safety objective is to protect people and the environment from harmful effects of ionizing radiation*".

The IAEA standards must be clear, logical, harmonised and based on a unified safety philosophy. They must ensure transparency, an efficient feedback mechanism and user-friendliness, and always promote the safety culture. They are hierarchically organised, as shown in fig. 3-1.

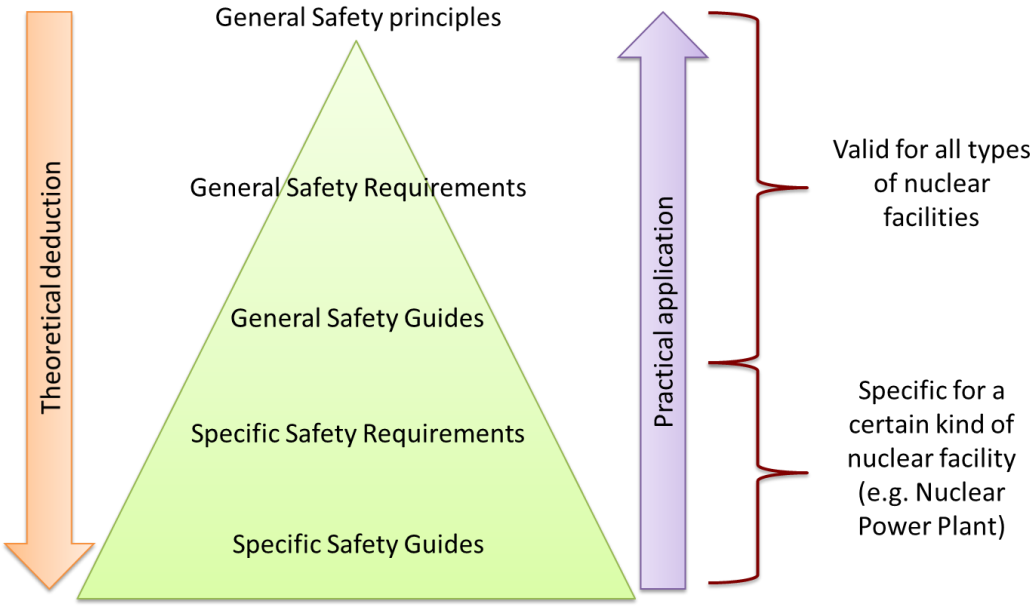

Figure 3-1 Hierarchical structure of IAEA safety standards

The fundamental safety principle is detailed in **ten safety principles** (IAEA, 2006), that represent the basis to develop all the safety requirements and, therefore, to implement the safety measures in all nuclear facilities and activities, during the entire lifecycle (e.g. planning, siting, design, manufacturing, construction, commissioning, operation, decommissioning, transport and management of radioactive waste).

These safety principles express the **basic concepts** for the entire structure of the IAEA Safety Standards. They are listed below (IAEA, 2006).

- *Responsibility for safety*: the first step is to understand who owns the responsibility to ensure the safety; the owner or the organizations responsible for the nuclear system must be clearly identified. All the activities must be licensed.
- *Role of government*: the nuclear activities must rely on a properly established system of regulatory bodies and regulations;
- *Leadership and management for safety*: in each activity the safety leadership and management must be clearly expressed, must be efficient and must always guarantee the respect and improvement of the safety culture, the continuous check of safety performance and the implementation of lessons learned from experience;
- *Justification of facilities and activities*: it must be demonstrated that the benefits of a nuclear installation are higher than the implied costs (in terms of radiological risk);
- *Optimization of protection*: the safety provisions can be considered optimized only if the facility can be safely operated without disproportionate limits;
- *Limitation of risks to individuals*: nobody must be exposed to unacceptable radiological risk; the dose must continuously be measured, and the protection systems must be efficiently operated and optimized;
- *Protection of present and future generations*: the risks connected to nuclear installations are not limited in space and time; in fact, the possible consequences of an accident are not limited by the national borders and can bother the future generations; therefore, these aspects must be appropriately considered;

- *Prevention of accidents*: all practical safety measures must be implemented for accident prevention and mitigation. The defence in depth concept is the first protection against the accident escalation;
- *Emergency and preparedness and response*: a response plan must always be ready in case of accident in order to mitigate any consequences for human life and health and the environment and avoid consequences escalation;
- *Protective actions to reduce existing or unregulated radiation risks*: the risk of an excessive exposure to radiations is always possible; in these situations, protection actions must be foreseen to reduce immediately the dose and mitigate the consequences.

These general principles give guidelines to be oriented among all the other IAEA documents.

They are deeply analyzed and explained in a set of seven "General Safety Requirements" reports, where different aspects and key points are examined; in particular, it is specified the "What" and "Who" for each requirement and "Why" each requirement exists.

Each "General Safety Requirements" report is supported by a "General safety Guide" that aids in accomplishing its objectives, explaining the "How".

The general safety principles, general safety requirements and general safety guides are valid for all nuclear facilities: nuclear power plant, fuel cycle facilities, research reactors, radioactive waste disposal facilities, milling and mining, application of radiation source, transport of radioactive materials.

The "General Safety Requirements" and the "General Safety Guide" are declined for each technical area into a certain number of "Specific Safety Requirements" and of "Specific Safety Guides" that provide all the guidance necessary for implementing the general principles.

For example, in the specific case of a nuclear power plant, there is a whole set of specific safety requirements divided into different categories corresponding to different phases of the life cycle of the system (e.g. the site evaluation, the design, the commissioning and operation …). For each of these specific safety requirements, there are several specific safety guides. For example, about the requirements for the design of nuclear power plant, there are specific directives about the design of the core, the design of the containment system, the safety classification of structures, systems and components in nuclear power plants and so on.

While the ten safety principles are general enough to be applicable also to non-LWRs, all the other documents and standards are referred specifically to LWRs (Carpignano et al., 2018)**.**

An equivalent well-articulated system of standards for new generation nuclear systems does not exist yet. Nevertheless, some methodologies suitable for innovative facilities and inspired by the general principles are available, such as the INPRO methodology (paragraph 3.5) and the ISAM methodology (paragraph 3.6).

Moreover, for advanced reactors, IAEA provides ARIS (Advanced Reactors Information System), a web-accessible database that collects balanced, comprehensive and up-to-date information about advanced nuclear plant designs and concepts. It constitutes a platform for the Member Stater to have access to information and development trends. (ARIS website)

3.2 NRC: US licensing

Similarly, the Nuclear Regulatory Commission (NRC) regulations, and in particular the Part 50 and Part 52 of the Title 10 of the Code of Federal Regulations (10 CFR 50 and 10 CFR 52) (USA NRC, 2017), establish Principal Design Criteria (PDC) derived from the General Design Criteria (GDC) that are specifically referred to LWRs (Appendix A of 10 CFR 50). In US, the licensing process can be performed into two ways:

- A **staged process**: each phase of the system design, construction and operation must obtain a formal approval; this process is described in 10 CFR 50. The applicants can submit a preliminary safety report to obtain the construction permit; then, they can start building the plant without the guarantee that the reactor will be actually licensed to operate. The final documents will be submitted when the reactor is almost ready. This method has been used to license all the commercial reactors in the US prior to 2012 (MIT, 2018).
- A **one-step process**: all the life phases of the systems obtain a single approval; this process is described in 10 CFR 52. The entire documentation must be furnished to the regulatory body before beginning of the construction. This method has been used to license 11 reactors in US, two of these (AP1000) are under construction (MIT, 2018).

The one-step approach is particularly suitable for systems with high design and operational maturity. In fact, it requires furnishing all the information years before the start of the construction; even if it is highly probable that modifications will be made during the entire process that will claim for updated of the licensing procedure, for very standardized systems, it is extremely probable that at the end the reactor will be actually operated. Nevertheless, a final verification will be necessary, with the possibility of unexpected criticalities. Moreover, a staged approach is currently used in many engineering fields (non-nuclear), e.g. the Seveso III, the EIA (Environmental Impact Assessment), the European offshore directive, etc.

The interest in advanced reactors poses the problem of their licensing. Since the last US commercial non-LWR was shut down in 1989 (Fort St. Vrain, a HTGR), the update of these processes is challenging (Carpignano et al., 2018). This is due to lack of specificity in the technology, lack of maturity of design and the unavoidable technical skills gap (Lee, 2016).

Different approaches have been proposed and they demonstrate that the licensing process can be defined using the existing tools and strategies and can be adapted to different and innovative technologies. Up to now, a staged process with smaller and frequent approvals seems to guarantee flexibility, transparency and continuous feedbacks between the applicants and the regulatory body, even on smaller portions of the design. Nonetheless, the formal approval cannot be given until all the "pieces" are evaluated together (even if each part has already been approved singularly, the entire project has to be approved too). As a drawback, the process can slow down, because the different phases of the process have to proceed in series. Moreover, it is worth noting that, up to now, the formal approval of each piece requires the fulfilment of prescriptive requirements, while the risk-informed and performance-based approach, which seems the most adequate to treat the innovative system, does not appear in the 10 CFR 52. The key point is the efficient communication between the applicants and the regulatory body (MIT, 2018).

For innovative systems, a staged licensing approach seems to be more convenient; nonetheless, an update is needed: a set of non-LWRs design criteria must be defined. In particular, to ensure flexibility to the design process, they should be technological-neutral, risk-informed and performance-based (see paragraph 2.2.2). The definition of technology-specific design criteria could be a part of the pre-licensing process.

Several studies about possible licensing pathways are on-going, such as the DOE Advanced Reactor Option Study (Petti et al., 2017) about commercial reactors, commercial prototypes reactors, test reactors and research reactor. Nonetheless, a new regulatory framework for advanced systems (a formal "Part 53" of Title 10) is foreseen and will need several years to be available.

3.3 IEC EN 61508

Nowadays a widely accepted approach in the process industry is the one described in the standard IEC EN 61508 (IEC 61508, 2015) and in the principles of functional safety there defined. Its major idea is that the safety of systems must be studied and pursued from the early design by risk analysis tools and must be addressed considering the entire system life cycle (design, integration, operation, maintenance, modification and decommissioning), guaranteeing a mix of prescriptive and performance-based requirements. It is worth highlighting **the tight link between the design evolution and the safety demonstration**, which proceed together. Even if it is not mandatory, its application is highly recommended in several local, national and international regulations.

The 61508 is a generic standard common to several industries: other specific standards have been developed for other industrial fields and for specific applications, e.g. 61511 refers to process industry, while 61513 (described in the next paragraph 3.4) applies to nuclear industry. The specific standards (e.g. 61511 and 61513) complete the general standard 61508; this means that each specific application of the functional safety approach foresees the implementation of the 61508 and the correspondent specific standard at the same time.

The first step of the procedure is to list all the Equipment Under Control (EUC), successively a preliminary risk assessment is performed in order to identify all their potential hazards. Then, the IEC 61508 is centred on the definition of the Safety Instrumented Functions (SIFs) and Safety Integrity Levels (SILs).

The Safety Instrumented Functions (SIFs) must be fulfilled in order to obtain acceptable risk. The risk reduction can be obtained through additional safety-related systems (SISs, Safety Instrumented Systems, both hardware and software), additional risk reduction facilities (e.g. redundancy and separation) and additional safety requirements, technical and operational.

The Safety Integrity Levels (SILs) are parameters indicating the class of probability that must characterise a system so it can properly perform a specific SIF within a predefined period of time and respecting defined technical, functional, architectural and design parameters (IEC 61508, 2015).

The standard suggests several possible techniques to support the SIL allocation, mainly:

- Quantitative approach by detailed QRA;
- Semi-quantitative approach by Safety Layer Matrix Method;
- Qualitative approach by Calibrated Risk Graphs;
- Qualitative approach by Risk Graph;
- Semi-quantitative approach by Layer of Protection Analysis (LOPA).

Following the previous steps, a set of Safety Requirement Specifications (SRSs) must be established for each identified SIF and for the related SISs that will implement it. The SRSs shall provide a basis for design, and the document shall be further developed and maintained through all lifecycle phases of the SIS. The SRSs may be quantitative requirements (SILs), functional (e.g. response time, draining tank capacity, etc.), architectural (e.g. redundancy, separation, etc.), operational, procedural, etc. For example, if for a specific SIF a certain SIL has been allocated and must be guaranteed, it is necessary a low failure probability of the implemented SISs. This implies to operatively define specific procedures or components characteristics, such as a low test interval for components characterized by undetectable failures and adequate maintenance procedures (sufficient resources, immediately available spare parts, etc.) for components characterized by detectable failures, in order to ensure a Mean Time To Repair (MTTR) as low as reasonably possible.

To summarize, the IEC 61508 is based on the definition of risk acceptability criteria, which can regard population health, environment, asset and production, reputations, etc. To fulfil the requirements, it is foreseen to identify a set of SIFs and the corresponding SISs satisfying them. Finally, the SILs are allocated to make the risk tolerable. This approach integrates the risk analysis since the early phases of the design, and the safety demonstration accompanies the entire project evolution, conditioning also its operational life and the maintenance procedures. This standard enhances a good distribution of the safety investments, endorsing actions on the major risk contributors and both hardware and software SISs are evaluated and implemented.

A schematic representation of the risk reduction activities is shown in fig. 3-2.

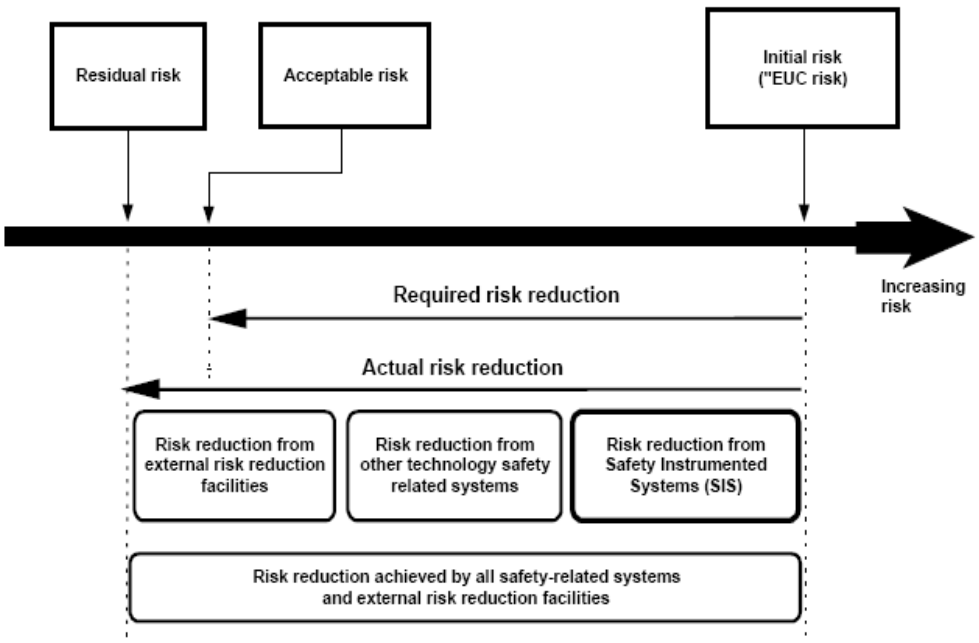

Figure 3-2 Framework for risk reduction (IEC 61508, 2005)

Functional safety assessment in the context of IEC EN 61508 constitutes a milestone for safety to drive the design (IEC EN 61508, 2005). Moreover, the standard introduces the concept of management of Functional Safety, i.e. all activities needed to guarantee that the functional safety requirements are met and that safety integrity requirements are identified, designed and maintained during the entire lifecycle of the system: recalling the previous example about the SIL to be properly guaranteed, during the design phase the level is established to fulfil the identified tolerability requirements, then adequate components and procedures must be practically defined and applied to ensure the SIL, finally during the entire operational life of the plant the SIL must be kept at least the same as it was at the beginning (e.g. monitoring the components aging, respecting the maintenance procedures, etc.).

The objective of this approach is to coherently link project, operation and maintenance choices, strategies and procedure to keep the risk level acceptable; in this sense, the final control of the satisfaction of the tolerability criteria will not highlight major criticalities in the detailed design that will not be modified substantially: all the major issues should have been solved already in the previous phases, with saving of time and money.

The following fig. 3-3 shows a schematic application of this standard.

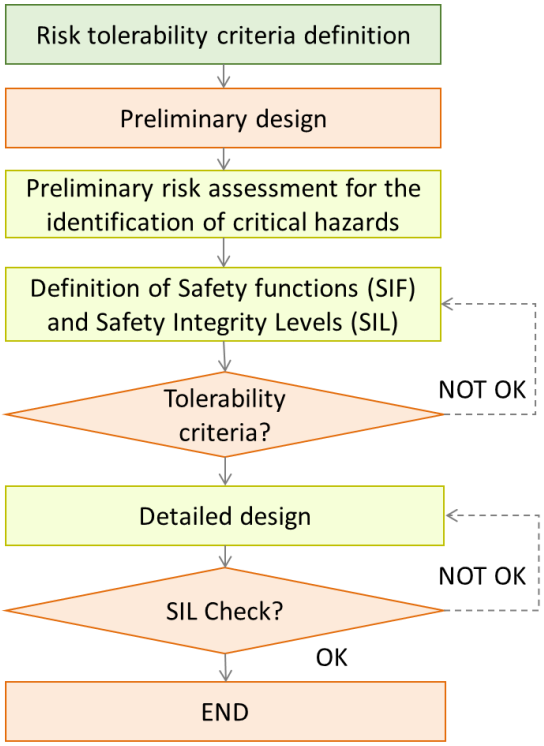

Figure 3-3 Schematic application of the IEC 61508

3.4 IEC EN 61513

The IEC EN 61513 (IEC EN 61513, 2013) standard aims at transposing the general requirements of 61508-1, 61508-2 and 61508-4 to nuclear application sector.

It focuses on Instrumentation and Control (I&C) important to safety in Nuclear Power Plants (NPP). It provides requirements and recommendations for the overall

I&C architecture (hard-wired equipment, computer-based equipment or a combination of the two) (IEC EN 61513, 2013). As the IEC EN 61508, it refers to the concept of a safety lifecycle for both the whole architecture and the individual systems, highlighting the relations between the safety objectives of the NPP and the requirements for I&C architecture (Carpignano et al., 2018).

This standard does not specifically discuss the plant safety assessment nor identify the means of guaranteeing the adequacy of the performance and reliability requirements arising from the analysis (e.g. SILs allocation). In fact, according to the nuclear sector practice, the plant safety assessment has to be performed according to specific stiff and prescriptive regulations (e.g. IAEA standards and their operative translation in national regulations or NRC regulations) that are outside the scope of this standard. The safety assessment process defines the initiator events, their sequences, the DiD concept of the plant and the categorisation of functions required to provide the defence. On the other hand, this standard identifies the input information necessary so that I&C designer may guide the subsequent design of I&C systems and its safety assessment.

The application of this standard is an iterative process (see fig. 3-4) constituted by major steps (inspired by the 61508 philosophy):

- Definition of the NPP safety goals, coming from IAEA standards;
- Definition of comprehensive requirements for the overall I&C architecture;
- Definition of comprehensive requirements for the individual I&C systems;
- Definition of requirements for integration, commissioning, operation and maintenance.

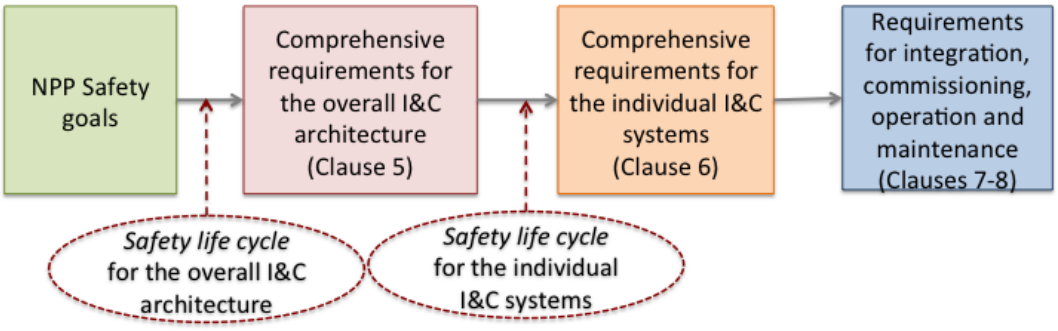

Figure 3-4 Schematic application of the IEC EN 61513

Even if the 61513 standard starts from the previous IEC EN 61508, the former substantially differs from the latter because it follows international standards (IAEA standard in Europe) and refers to systems important to safety as they are defined for nuclear power plants. The need to maintain the stiff traditional safety approach for nuclear applications makes the 61513 misrepresenting the nature of the 61508; instead, it represents an intermediate step included into a rigid process that was developed for and it is still suitable to LWRs, but difficult to apply to concepts of the next generation.

Figure 3-5 shows where the 61513 is located along the safety demonstration of traditional reactors in a simplified representation of this stiff process.

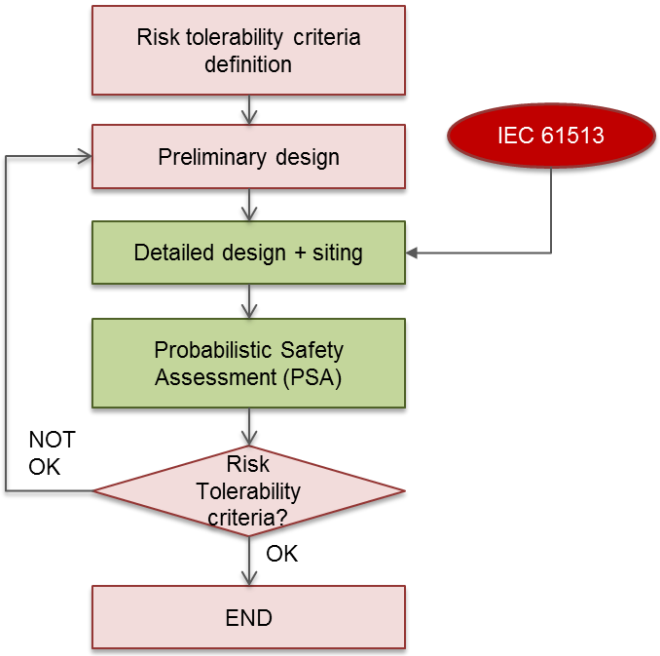

Figure 3-5 Schematic representation of the risk assessment process of a traditional NPP (Carpignano et al., 2018)

It is worth noting that the 61513 itself is not valid only for traditional reactors and there are not specific elements preventing its application to innovative systems. Nevertheless, the standard here described is a small part built a posteriori to adapt to a long, complex and rigid process, optimized for traditional reactors.

In conclusion, the philosophy of the 61508 (described in the previous paragraph 3.3) and its practical application described in 61513 can inspire the safety assessment of advanced nuclear plants, but outside the strict framework defined for LWRs.

3.5 INPRO methodology

The following review of the INPRO (International Project on Innovative Nuclear Reactors and Fuel Cycles) method is largely inspired by deliverable 3.5 of the SARGEN_IV project (SARGEN-IV, 2012). The INPRO was born in 2000 in IAEA context with the aim of promoting communications between international experts and regulators to build new sustainable energy capacity in a long-term horizon.

Among the other applications, INPRO developed a "*Guidance for the Application of an Assessment Methodology for Innovative Nuclear Energy Systems*", always inspired by the IAEA general principles but at the same time aiming at implementing the concept of a safety driven design.

This approach aims at providing a tool to analyze an innovative system in order to:

- Assess if the new nuclear installation is compatible with the sustainable development of energy production;
- Compare different systems to tailor the solution to the needs of a specific region or a State;
- Identify potential improvements.

During the comparison phase, it is essential to consider the uncertainties, considering the design detail.

The INPRO assessment (IAEA, 2008) is a stepwise approach with a hierarchic structure (see fig. 3-6):

- Basic Principles (BP);
- User Requirements (UR);
- Criteria (CR).

The **criteria** must be fulfilled by an Innovative Nuclear System (INS) to prove its sustainability.

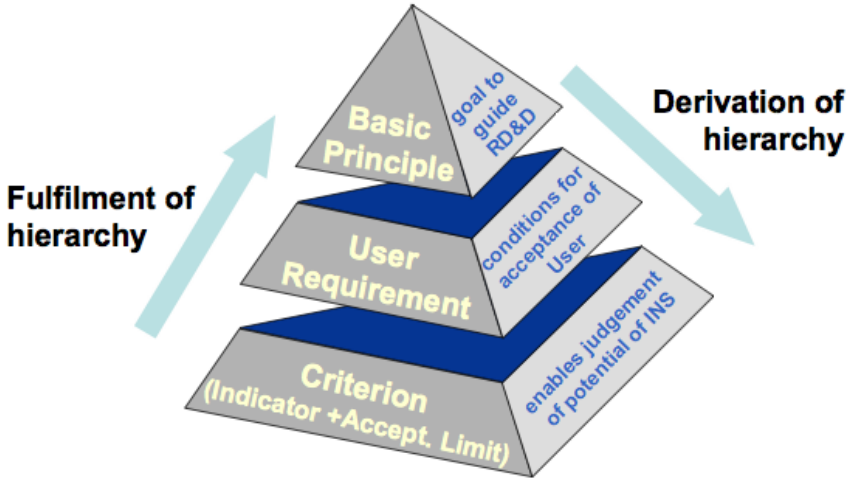

Figure 3-6 INPRO methodology hierarchical structure (IAEA, 2008)

The highest level in the INPRO structure is constituted by the **Basic Principles** (BPs); it is a statement of a general goal for the INS, hence it is a strong guidance for its design evolution. The INPRO BPs apply to 8 competence areas: economics, infrastructure, waste management, proliferation resistance, physical protection, environment, and safety. For the safety, they are directly derived from the IAEA Safety Standards. To demonstrate the sustainability of an innovative systems, all the BPs must be completely satisfied in all the areas considered by INPRO.

The second level in the INPRO hierarchy is constituted by the **User Requirements** (URs). They must be satisfied to achieve users' acceptance of a given INS. The users are all the stakeholders (i.e. the designers, the investors, the public, international organizations). URs represent the instrument to realize the BPs.

Finally, the Criteria (CR) are indicators to understand if and how well an UR is fulfilled by an INS. They can be single parameters, aggregate variables or a status statements. Each criterion consists of an indicator and an acceptance limit (IN and AL).

In fig. 3-6, the pathways of derivation and fulfilment of the hierarchy are shown. On one hand, the hierarchy derivation is a top-down process, starting from the general statements (Basic Principles) to arrive to the operational and technology-specific criteria. On the other, the hierarchy fulfilment is bottom up process: to fulfill a criterion the IN must compliant with the correspondent AL; to fulfill an UR all

the derived CRs must be satisfied; to fulfill a BP all the corresponding URs must be fulfilled. The satisfaction of all the BPs proves the sustainability of an INS.

Since this methodology has been developed for new generation nuclear systems and some of them are at a very preliminary design stage, during the application some data are missing or are very general. For ALs definition, the ALARP concept is accepted to correctly manage these uncertainties. As shown in fig. 3-7, for each Criterion two ALs must be defined: the Basic Limit and the Basic Objective; then, the IN and its uncertainty must be compared with these two limits. The Basic Limit is the minimum value that the IN must assume to abandon the unacceptable risk zone; the Basic Objective is the minimum value the IN must assume to enter in the acceptable risk zone. Between the Basic Limit and the Basic Objective there is the ALARP zone. If the IN is in the ALARP zone, the risk should be reduced through appropriate measures (e.g. protection systems, preventive measures, further analyses to reduce the uncertainty, etc.) until the cost will become strongly disproportional with respect to the gained advantage.

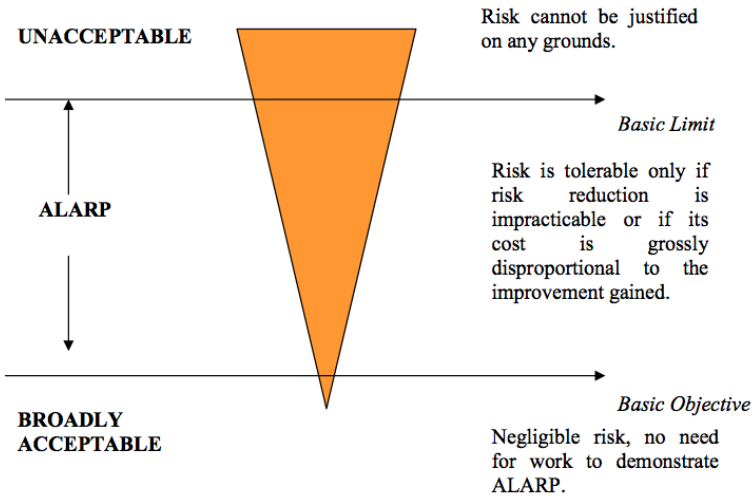

Figure 3-7 Three zones of risk: acceptable risk, ALARP zone, unacceptable risk (IAEA, 2008)

The described process is iterative, with alternative top-down (derivation of hierarchy) and bottom-up approaches (Fulfilment of hierarchy). In fact, if after the application of the methodology the analyzed INS results unsustainable or as non-compatible with the set standards, it can be archived, or the design will be improved through new R&D activities. In the last case, when the new design will be available,

the INPRO methodology will be applied again, after checking that the technology-specific criteria are compatible with the design modifications.

As said before, during the implementation of the methodology and in particular during the comparative phase, the uncertainties must be evaluated, especially the design state (if it is pre-conceptual or fully developed). In fact, in the case that an INS does not satisfy an IN, but it abundantly satisfies the others, it can be preferred to other INSs anyway, for several reasons, for example some indicators may be judged more important than others, the design may be at a previous phase, etc.

One of the major outputs from an INS assessment is the major risk contributors, i.e. the areas where a given INS needs to be improved.

3.6 ISAM methodology

The ISAM developed in the 2011 GIF report (RSWG of GIF, 2011) is meant to provide *"valuable insights into the nature of safety and risk of Gen IV systems"* contributing to the realisation of Gen IV safety objectives (see chapter 1).

The word "Integrated", present in the ISAM acronym, can be explained through two complementary meanings (RSWG of GIF, 2014):

1) The safety demonstration of an INS is supposed to support and evolve with the design during its entire lifecycle; the objective is that safety should represent an "integrated part" of the project since its earliest stages, rather than be added only after the definition of the detailed design. This methodology will try to give a safety-related perspective, shaping the design development and reducing costs and time.
2) The ISAM is composed by five tools that complement and support one another with mutual interactions in order to achieve a more comprehensive understanding of the safety issues and a safety assessment of the INS as robust and complete as possible.

The five complementary analytical tools are listed below:

- Qualitative Safety features Review (QSR);
- Phenomena Identification and Ranking Table (PIRT);
- Objective Provision Tree (OPT);

- Deterministic and Phenomenological Analyses (DPA);
- Probabilistic Safety Analysis (PSA).

According to the GIF, these tools guarantee enough flexibility "*to allow a graded approach to the analysis of technical issues of varying complexity and importance*" (RSWG of GIF, 2011). In addition, the methodology can be applied at any stage of design.

Figure 3-8 presents how these tools are interconnected among them and with respect to the relevant stages of design evolution.

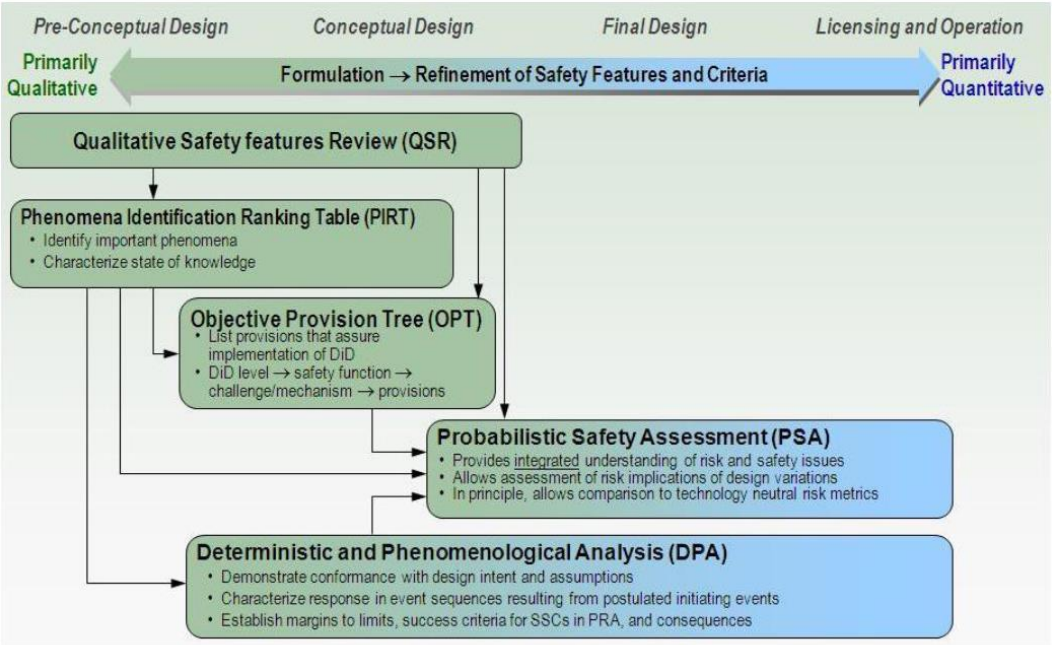

Figure 3-8 Proposed ISAM task flow (RSWG of GIF, 2011)

3.6.1 The QSR (Qualitative Safety features Review)

The main objective of **QSR** is to furnish to the designer a checklist of "good practices and recommendations" in order to help identifying the assets and vulnerabilities of a design, as early as possible (RSWG of GIF, 2011).

The checklist should be as complete as possible and based on the existing standards and practices. The GIF report gives the examples of recommendations formulated by the Risk and Safety Working Group (RSWG) as well as other reference

documents (e.g., the IAEA standards, the INSAG, INPRO guidelines) (RSWG of GIF, 2011). The elements of the checklist are collected and organised in 4 classes: generic and technology neutral (class 1), detailed and technology neutral (class 2), detailed and technology neutral for a specific safety function (class 3); detailed and technology specific (class 4). In each class all the levels of defence in depth are explored. The ISAM provides tables for the first 3 classes, and for all 5 levels of defence in depth.

A designer willing to use the QSR tool as presented in the ISAM should browse all these tables and check whether the characteristics of his design have a favourable, neutral or unfavourable influence on each element of the list.

For example, the methodology has been partially applied to a pool-type SFR (Stratified REDAN). For the prevention level of the DiD, class 3, with respect to the Decay Heat Removal (DHR) safety functions, the first level of the table is "Prevention of abnormal operations and failure". This first level requirement is specified more and more up to arrive to the specific criteria to be checked. Among many others, a specific element is to "Minimize the number of components per system": the stratified REDAN results "Unfavourable" with respect to this element, since it foresees a significant number of electromagnetic pumps (Typical element for the primary circuit of liquid metals cooled reactor). On the other hand, with respect to the element "Simplify the thermo-hydraulic for the safety of DHR" the analysed system is judged "favourable", since the geometry and the disposition of the elements of the hydraulic loop help establishing and maintaining the natural convection and are significantly simplified (RSWG of GIF, 2014).

Through this qualitative approach the designer should be helped in identifying the characteristics to be implemented, and in prioritizing the ones requesting more R&D efforts to reduce their drawbacks (RSWG of GIF, 2011).

3.6.2 The PIRT (Phenomena Identification Ranking Table)

The main objective of **PIRT** is the identification of all plausible phenomena affecting the outcome of an accident and the consequent generation of ranking tables identifying correspondent contributions to risk and gaps in the knowledge to be fulfilled by R&D work (RSWG of GIF, 2011).

It is largely based on expert and engineering judgement. Once the phenomena are identified, they are ranked basing on their relative importance with respect to

the accidental scenarios and the associated state of knowledge. This step is the most delicate.

In order to determine the importance of each phenomenon, a Figure-of-Merit (FOM) is established. It represents the evaluation criterion to judge the relative importance of each phenomenon. Thus, phenomena are ranked according to their effect on the FOM (usual scale: high, medium, low or insignificant). The second part of the ranking process concerns the level of knowledge available for the phenomena. The adequacy of the available knowledge and the correspondent uncertainties have to be assessed and documented. Then, an expert judgment is made to rank the phenomena (fully known/small uncertainty, known/moderate uncertainty, partially known/large uncertainty, very limited knowledge/uncertainty cannot be characterized) (RSWG of GIF, 2011). For example, for the stratified REDAN, with respect to the scenarios of the primary pumps run down, one of the chosen FOM is the "Transient thermal loadings on the core structure". In this scenario, one of the analyzed phenomenon is the transient thermo-hydraulic response of the core region, referring to the natural convection; the importance of this phenomenon is ranked "High" because the establishment of the natural convection helps the minimization of the thermal loadings on the core structure (FOM). The status of knowledge is ranked "Known", according to the relative state of the art (RSWG of GIF, 2014).

The PIRT exercise generates ranking tables (see fig. 3-9).

Knowledge Base Gap Determination				
Adequacy of knowledge	Rank of Phenomenon			
	H	M	L	I
(4) Fully known; small uncertainty				
(3) Known; moderate uncertainty				
(2) Partially known; large uncertainty	GAP	GAP		
(1) Very limited knowledge; uncertainty cannot be characterized	GAP	GAP	GAP	

Figure 3-9 PIRT, gaps identification (RSWG of GIF, 2011)

The PIRT is useful during the pre-conceptual design phase as an early "screen" to identify, categorize, and characterize phenomena that are potentially safety-relevant. Successively, it is applied iteratively throughout the development process.

The list of design open points identified for the MSFR and reported in "Appendix A" constitutes a good input for the implementation of this tool.

3.6.3 The OPT (Objective Provisions Tree)

The objective of the OPT is to help sketching the design safety architecture identifying all provisions necessary to guarantee the safety functions, after the identification of all the potential hazards posed by the plant (RSWG of GIF, 2011).

It is constituted by two consequent phases. The aim of the first phase is the identification of all the potential hazards of the plant as exhaustively as possible (for this purpose they are called "challenges/mechanisms"). The aim of the second phase is the identification of all the safety provisions (both preventive and mitigative) useful to preliminary design safety architecture based on the identified hazards. Hence, this step allows the definition of essential measures to ensure successful prevention, control or mitigation of phenomena that could potentially harm the nuclear system (RSWG of GIF, 2011).

According to the ISAM methodology, the OPT exercise should be done for each safety function at each level of defence in depth (DiD). This represents one of the key characteristics of the OPT. A graphical presentation of the OPT results is proposed and consists in a tree-shaped hierarchical structure where events are connected through the Boolean logic operators (as shown in fig. 3-10). From the top to the bottom, it includes:

- The considered level of DiD (generally from 1 to 5);
- The objectives to be achieved and the barriers to be protected for this level;
- The safety functions to maintain or to perform successfully (usually control of reactivity, heat removal and fuel confinement);
- The possible challenges (i.e. hazards) to the safety functions;
- The plausible mechanisms that can cause these challenges;
- The provision/provisions to implement in order to prevent, control or mitigate the consequences of the challenges/mechanisms (RSWG of GIF, 2011).

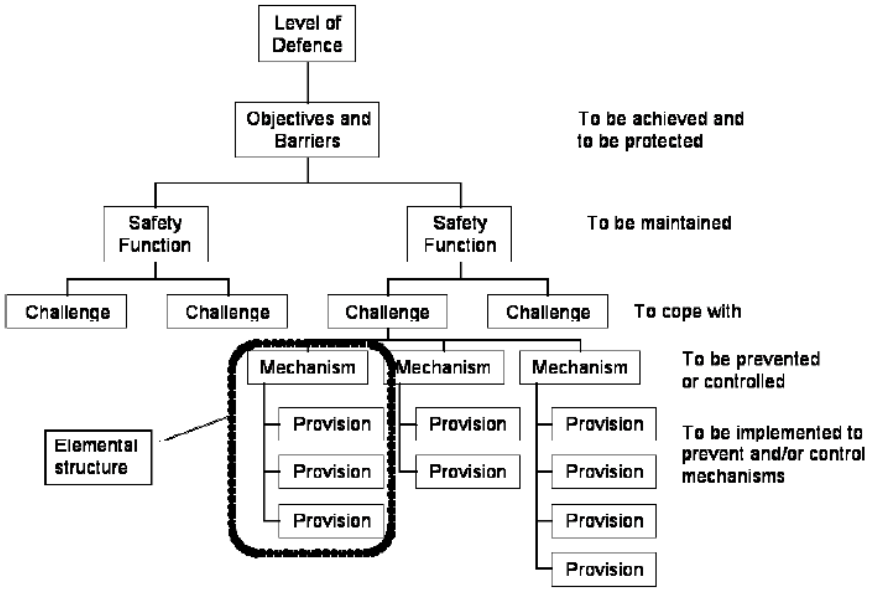

Figure 3-10 – Hierarchy Structure of OPT (RSWG of GIF, 2011)

As the PIRT, the OPT should be applied early in the pre-conceptual design phase, and iteratively through conceptual design.

3.6.4 The DPA (Deterministic and Phenomenological Analyses)

They help analyzing and quantifying the aspects/phenomena/transients important for the design development; hence, they are essential for the system safety demonstration. Through DPA, physical transients of accident scenarios are modeled and calculated; the appropriateness of selected provisions is assessed; the requirements and criteria for SSCs are defined (also necessary for PSA); sensitivity analyses are performed with the aim of establishing safety margins and reducing imprecision and uncertainties in current parameters at the design stage (RSWG of GIF, 2011).

The deterministic and phenomenological analyses include neutronic analyses, thermal-hydraulic analyses, thermo-mechanical calculations, reactor physics anal-

yses, materials behavior models, structural analysis models and accident simulations. The DPA simulation codes and analytical models must be verified and validated (RSWG of GIF, 2011).

3.6.5 The PSA

The PSA is the final objective of the ISAM and the entire methodology is structured to facilitate its implementation; it shares interfaces with each of the other tools that are developed in the view of its final achievement. Consequently, PSA is not integrated in the ISAM as an alternative to DPA, but rather as a containment where deterministic analyses are one kind information, together with all other outputs coming from the other tools. The major objective is to check the achievement of safety objectives, as required by ISAM (RSWG of GIF, 2011). It is worth noting that the ISAM general framework is not deterministic, neither risk-based (see paragraph 2.2.2), but it uses elements from both the approaches in a more comprehensive risk-informed point of view.

PSA is a rigorous, systematic and comprehensive tool with the aim of identifying the events (or sequences of events) that can cause the loss or the damage of complex engineered systems and to estimate their frequencies. Furthermore, it studies the potential interactions between identified hazards (in terms of technological failures) and the reliability/availability of safety provisions.

It provides a structured means of answering three basic risk analysis questions:

- What can go wrong?
- How likely can it go wrong?
- What are the consequences if it does go wrong?

PSA is historically considered meaningful if applied to a design that has reached a sufficient level of maturity and detail, often after the plant is actually licensed and operating (see paragraph 2.2.2). Nowadays the concept of a “living PSA” is becoming more and more accepted: since the earliest stages of the design process, the PSA is considered a decision tool, whose outputs can drive the design by taking into account the highlighted safety vulnerabilities and their potential for risk reduction. Regulators widely recognize the value of this technique (also along the licensing process); therefore, it is a powerful tool for communication and information sharing among different national nuclear regulators. Finally, during the plant operation, PSA is used in many ways to improve plant safety, manage plant operations and facilitate interactions with regulation bodies.

As seen in paragraph 2.2.5, the traditional role and structure of the PSA must be reviewed and updated to suit specifically to Gen IV systems.

3.6.6 Additional remarks on ISAM

In conclusion, the ISAM (RSWG of GIF, 2011) is meant to combine both probabilistic and deterministic tools, both quantitative and qualitative methods and evaluations, some focusing on high-level issues, others on more detailed issues. It aims at providing a robust guidance, based on a good understanding of risk and safety issues, contributing to the achievement of Generation IV safety objectives.

A big advantage of this methodology is the constant reference to the defence in depth. Unfortunately, the direct implementation of some of the tools of the ISAM results difficult to be applied to some innovate concepts, given the preliminary stage of their safety demonstration and design. The DiD levels, as well as the entire methodology, depend on the definition of the severe accident (see paragraph 2.2.3), risk metrics (see paragraph 2.2.2) and physical barriers (see Appendix B) that represent still an argument of discussion for many concepts (e.g. MSFR). To overcome these difficulties, it has been chosen to rather use the ISAM as a guideline to formalize the objectives to be achieved, with a critical analysis for each of its tools in the view of its utilisation for the conceptual systems (see Chapter 4).

3.7 Considerations

In this chapter, a panoramic view over some standards and methodologies of interest for the following analyses is presented.

At the beginning of the chapter, a brief summary of the fundamental safety principles and the structure of the IAEA standards and NRC licensing pathways is illustrated, highlighting what is applicable to all kinds of reactors and what is specifically derived for LWRs. It is worth highlighting that the major part of the practices has been defined for LWRs, as it is properly explained in paragraph 2.2.6. The safety demonstration of traditional NPPs is performed according to specific stiff and prescriptive regulations, which means IAEA standards and their operative translation in national regulations or NRC regulations. The regulation is generally prescriptive/proscriptive, in order to be efficiently applied to already well-known

technologies. On the contrary, their direct application to innovative systems results complex and needs a modernization process. This process has already started but it is still long, since it regards some of the most sensible concepts of nuclear safety (the risk metrics, the severe accident definition, the role of the probabilistic assessment, etc.): several studies all around the world critically analyze the possibility of an adaptation of the current regulatory framework for new generation reactors, or delineate the necessity of new standards and methodologies specifically developed for the innovative technologies, such as the Part 53 for NRC regulations. Some help can arrive from non-nuclear sectors, in particular from the standard IEC 61508, which systematically introduces the concept of functional safety and its management. The standard contains a mix of prescriptive and performance-based requirements that aim at helping the design evolution, implementing the safety assessment from the beginning of the life of the project. Since the standard has been widely accepted in the non-nuclear engineering applications for years, an important experience is already available. A preliminary declination of the 61508 for nuclear applications is constituted by the standard IEC 61513. It applies to the I&C architecture of traditional NPPs. The standard does not contain explicit reference to LWRs, but it represents a small performance–based contribution in a well-developed, rigid and prescriptive process, tailored for traditional plants, misrepresenting the 61508 philosophy.

For advanced concepts, in the IAEA framework, two methodologies have been developed: the ISAM and the INPRO. They are performance-based, technology neutrals and risk informed; nevertheless, their application, especially for the ISAM, is not always trivial and the interpretation is not unique. They represent guidelines that must be reviewed, completed and adapted, if necessary, also using traditional risk analysis tools. They define an inspiring philosophy but do not constitute an operational framework; in fact, tailored criteria, requirements and consolidated operational safety assessment procedures have to be defined for new generation installations in order to guarantee a more efficient implementation of the methodology and a unique interpretation of its requirements (Carpignano et al., 2018). For example, the ISAM conserves some LWR-specific concept, as Level 1-2- 3 PSA, that are difficult to apply to some of the innovative nuclear installations, as already explained in paragraph 2.2.5. Moreover, the role of a high-level simplified PSA in driving the conceptual design development is not explicitly identified and explained. Regarding the risk metrics, even if in the ISAM technology-inclusive risk metrics are considered necessary, the ISAM tries to adapt the core damage frequency (CDF) to make it applicable to all kinds of nuclear installations, which is

tricky for some INS, especially MSFR and fusion devices (see paragraph 2.2.2). The CDF acceptance criterion has been established particularly for large LWRs and it cannot be transposed to different nuclear installations, even if a core damage status can be "easily" defined. A more practical example is given by the implementation of the OPT tool: in the methodology it is said that the mechanisms challenging the safety functions have to be identified, but it is not explicit how to achieve this objective, the level of detail, how to define the safety provisions (objective of the second phase of the OPT) starting from the result of the first phase of the OPT.

Both the ISAM and the INPRO are high-level methodology, with all the advantages and all the disadvantages of their performance-based nature. Notwithstanding these issues, the ISAM is the chosen methodology for this work because it represents a robust guidance for the identification of risks and safety relevant aspects, considering the Generation-IV safety requirements, the international safety standards, the available return of experience and the peculiarities of INSs. In order to cope with the ISAM lack of operability, the methodology has been completely reviewed and integrated, as described in Chapter 4.

Chapter 3

The methodology

This chapter describes the methodology, which supports risk assessment of new generation nuclear systems and takes into account the Generation-IV safety requirements, the international safety standards, the available return of experience and the peculiarities of the analyzed reactor with the help of available risk analysis tools.

The objective is to guarantee that the design evolution is guided by safety analyses, in order to achieve a comprehensive understanding of safety related design vulnerabilities and the resulting contribution to risk. This may lead to new safety provisions or design improvements as well as R&D needs.

The methodology here proposed is based on the Integrated Safety Assessment Methodology, ISAM (see paragraph 3.6). As already explained, ISAM constitutes a kit of different analysis tools for Gen IV systems, which turn out to be useful at any stage of the design maturity. This diversity and complementarity help to provide a robust guidance based on a good understanding of risk and safety issues.

In this work, the ISAM tools are reviewed, completed and adapted, when needed, to better reflect the European standards/rules and the available return of experience. Useful inputs come from other global safety assessment methodologies (e.g. INPRO, see paragraph 3.5) developed for Gen-IV reactors, as well as standards commonly used in the process industry (e.g. IEC 61508, see paragraph 3.3).

Moreover, a wide survey on risk analysis operational methods (HAZOP, FMEA, etc.) is performed in order to study how they can be integrated within the

ISAM framework and to define a complete and operational methodology that well suits to advanced reactors analysis. Finally, the methodology is adapted to the specific analyzed system (Flauw et al., 2018).

4.1 ISAM review

Each ISAM tool is reviewed in order to identify the elements that should be added, adapted or modified to best fit the purpose of the work. Table 4-1 collects the main outcomes of the review process (Flauw et al., 2018).

Table 4-1 Review of ISAM tools

ISAM tool	REVIEW (criticalities/adaptations/..)
QSR	• It should be highlighted the compliance of the checklist criteria with the international standards. • The checklist tables result very complicated: tables should be simplified through the selection of subjects specific to different levels of DiD.
PIRT	• Since the preliminary design stage of some advanced concepts, the selection of the phenomena and scenarios to be analyzed through this tool results critical (lack of knowledge). • The PIRT can be used only after the application of other safety analysis tools allowing the definition of a list of relevant accidents.
OPT	• The ISAM methodology proposes to apply the OPT at each level of the DiD. At a first step of the analysis, the identification of hazards could be performed without defining the DiD level concerned; whereas, in a later stage, the completion of the OPT with DiD level identification could be of help to ensure the safety architecture is well balanced. • The OPT consists in a top-down approach. It is useful to complete the hazard identification step through a complementary bottom-up approach (see paragraph 4.3.1), to guarantee a list of IEs as complete as possible.

DPA	• In the ISAM, the DPA are considered as a support tool for the application of the OPT and the PSA. It is proposed to emphasize the role of the deterministic analyses, as a conservative and pragmatic safety approach for this early design phase.
PSA	• The entire ISAM methodology aims at performing the PSA, in this conceptual design phase the role and the weight of this tool must be redefined and lowered with respect to the DPA: the PSA will represent a support for the deterministic analyses.

In general, the explicit relationship of the ISAM with the various DiD levels represents one of its major advantages; nonetheless, these levels, therefore the whole methodology, depend on the definition of the risk metrics, the severe accident and physical barriers that are considered still an open topic for many new generation advanced systems (see paragraphs 2.2.2, 2.2.3 and annex B). Hence with very conceptual design and safety analysis some of the tools of the ISAM and in particular the direct link with the DiD concept cannot be fully exploited. Nonetheless, in the view of an iterative risk assessment, it will become useful in the next phases of the project when keeping a common framework should help speeding up the process. Therefore, in this preliminary phase of the project (where safety-relevant concepts have still to be defined and safety-relevant issues have to be solved) it has been considered preferable to use the ISAM structure as a guideline to formally define the objectives to be reached.

In particular, it has been chosen to perform the identification of the hazards without defining the DiD level concerned; nevertheless, in a later stage, the completion with the DiD level identification could help to ensure that the safety architecture is well balanced, consistently with the OPT analytical tool reckoned in the ISAM.

4.2 The safety assessment process

Figure 4-1 shows the flowchart elaborated in SARGEN IV project (SARGEN IV, 2012) and updated through the previous paragraph considerations. It schematically illustrates the implementation of the global safety assessment process.

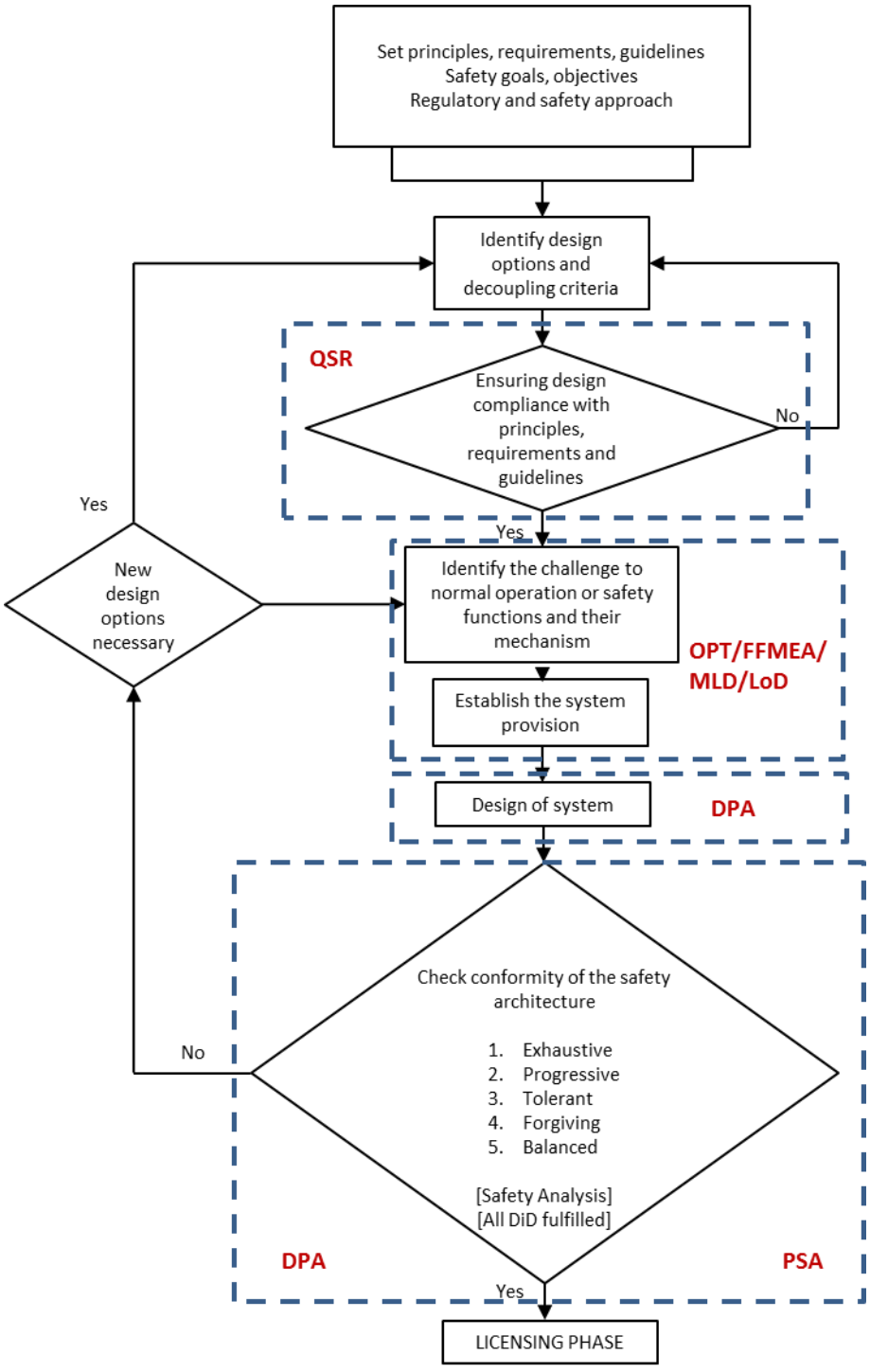

Figure 4-1 Flowchart of the implementation process of the global safety assessment and relevance of the different tools: the flowchart was developed of the framework of SARGEN IV project (SARGEN IV, 2012) (black lines) and updated through the previously explained considerations (coloured parts).

4.2.1 The safety principles, requirements and guidelines and the safety goals

For the definition of the **safety principles, requirements and guidelines**, at a very general level, the IAEA standards provide extensive references. Among the others, the work performed by the GIF, WENRA and the OECD MDEP can be consulted, too. It is worth to remind that, for some new advanced concepts, the requirements present in the available standards may be not exhaustive to account their technology-oriented aspects. In this situation, a case-by-case analysis is necessary for an adaptation to the reactor technology (see paragraph 2.2).

The **safety goals** are defined at the early stages of a new installation with the aim of guiding the design process and have to be ambitious and reasonably achievable at the same time. Driving the continuous improvement of safety, the safety goals have to be reviewed every time there is a major accident; in particular, big improvements were made on the basis of Three Mile Island, Chernobyl and Fukushima Daiichi accidents feedback. Moreover, the definition of safety requirements, and in particular the definition of operative safety margins, such as the frequency of Sodium boiling for SFRs, at a conceptual design stage can be a possible source of conflict. Since the limited available and reliable information on the design, the phenomena influencing the reactor behaviour and major risk contributors, the criteria might misrepresent the objectives whose achievement they should prove. They could be partial or even misleading, driving the design evolution in the wrong direction. Moreover, the development of the system might be slowed down, delaying the definition of the complete installation, especially in its non-nuclear part. In fact, the definition of the criteria itself represents a complex issue, consuming time and resources. This could constitute a safety issue since, especially in the nuclear field, the design and the safety demonstration are always focused on the nuclear island, while less attention is given to the "traditional part of the plant" and to the auxiliary and protection systems, which paradoxically result less protected. In the end, if the requirements are excessively ambitious or strict, the process of design definition might be stiffened, or the complexity of the system could be immoderately increased to fulfil the criteria, or the criteria themselves could represent an obstacle for the research of innovative solutions.

In this framework, the definition of the safety goals for advanced systems can start from different documents: for example, the GIF technology roadmap (GIF, 2014), "*Basis for the Safety Approach for Design & Assessment of Generation IV*

Nuclear Systems" (GIF RSWG, 2008), "*WENRA Statement on Safety Objectives for new Nuclear Power Plants*" (WENRA, 2008).

In particular, WENRA defines 7 safety goals for new nuclear power plants; however, they are not always well adapted to the specificities of the new generation reactors (e.g. an accident with core melt has no meaning for MSFR technology) (WENRA, 2008). Moreover, these goals are formulated in a qualitative manner to drive design enhancements for new plants with the aim of obtaining a higher safety level compared to existing plants. For these reasons, WENRA safety goals have to be detailed, adapted and completed.

The following non-exhaustive list represents an example of safety goals, which may be applied to new generation systems:

- Safety in operation (plant complexity, organizational and human factors);
- Independence of the levels of DiD, in particular levels 3 and 4;
- Plant autonomy;
- Consideration of external hazards, combination rules (natural and human hazards);
- Plant robustness with regards to the station blackout or heat sink loss;
- Accidents affecting the fuel treatment unit;
- Accidents affecting simultaneously the reactor and the fuel treatment unit;
- Events impacting multiple units on the same site;
- Severe accidents management in the long term;
- Accessibility, functionality, habitability of the control room and of the emergency response center; accessibility of local control points; reliability and functionality of the on-site and off-site communication systems, equipment measuring releases, radiation levels and meteorological conditions (Flauw et al., 2018).

4.2.2 Compliance of the design with safety principles, requirements, guidelines and safety goals

After the definition of the safety principles, requirements and guidelines and the safety goals, the **compliance of the design** with these criteria must be checked. The **QSR** is the ISAM instrument dedicated to realizing this step.

The QSR checklist has already been partially developed (RSWG of GIF, 2011), at least in its general sections. Nevertheless, it can be simplified, at least for systems with a conceptual design. In fact, the exercise can be performed in an early design phase with the aim of becoming aware of the safety issues so that they can drive the design rather than giving a final and punctual answer for the safety demonstration of the reactor. The same exercise (with the same objective) may be carried out for the successive updates of the design taking into account the feedback of the previous applications.

In particular, the QSR points dealing with safety goals or principles, study rules which are not linked to a specific level of DiD (integration of the principle of DiD itself, single failure criterion, materials qualification, separation, diversification…) may be ignored for the application of the QSR tables in the framework of conceptual systems, but they have of course to be considered in the safety assessment process.

4.2.3 Identification of risks, elaboration of a list of initiating events and definition of safety provisions

The successive step of the safety assessment foresees **the identification of hazards and the compilation of a list of initiating events**. For systems whose design is still in the conceptual phase, suitable methods shall be identified. For the purpose of this work, it is proposed to use both top-down and bottom-up approaches for identification of hazards and elaboration of a list of initiating events, in order to guarantee a list of initiators as exhaustive as possible.

The combined use of Master Logic Diagram (MLD, top-down approach) and Functional Failure Mode and Effect Analysis (FFMEA, functional bottom-up approach) will thus be considered. Both methods should be used at reactor level in a first time, and more generally in the whole plant in a second time, including the fuel treatment unit, with due considerations for the different plant states.

After completion of MLD and FFMEA, a review by experts will be needed to complement the hazards identification with available experience feedbacks gained from previous studies. As stated in paragraph 3.6.2, the use of PIRT could further be of help to study in more details the phenomenology of some relevant accidental

scenarios defined thanks to the previous methods and may complement and consolidate the hazards list. The identification of the initiating events will stand for the first step of the OPT method as referred to by the ISAM.

Among all the identified initiating events, an analysis will be performed to select a unique list of relevant items to be considered as Postulated Initiating Events (PIEs). At this stage, some events may be grouped to shorten the list. A preliminary classification of initiating events (incidental, accidental…) may be suggested on the basis of experts' judgment and available experience.

Once a list of initiating events is defined, the next step of the methodology is to preliminary **sketch the safety architecture**. To do so, it is proposed to use the Lines of Defence (LoD) methodology. This step can stand for the second part of the OPT method (identification of safety provisions). Compared to the OPT, and given the very preliminary stage of some designs, these safety provisions will not be arranged according to the defence in depth at this stage and the focus will be put on their correct identification in terms of number and quality. At a second stage, the association of the safety provisions to the different defence in depth levels could be done, taking profit of the fact that the LoD method forces to put in place independent provisions for a given risk, and complies well with the defence in depth principle.

The risk to be prevented should at least include:

- Loss of main safety functions;
- Severe accident and practically eliminated situations (if any).

Number and quality of LoD required for each risk should be defined considering potential consequences associated to each risk.

Since this step of the methodology represents the core of the present work, the operational path and each risk assessment tool (FFMEA, MLD, LoD) is exhaustively explained in paragraph 4.3.

4.2.4 Conformity of the safety architecture

Starting from a preliminary safety architecture, deterministic calculations need to be performed to refine the design of safety provisions and check the adequacy of the safety systems. The process is again iterative and design enhancement could be required to ensure satisfactory behaviour of the reactor.

The safety assessment should first concentrate on deterministic studies to achieve a sound and robust safety design. In a later stage, probabilistic insights may be used to identify potential weak points of the safety architecture and reinforce them, to further identify complex accidental sequences to be taken into account, and to consolidate the safety demonstration by finally giving insurance that the design is well balanced and allow achieving high reliability performances (Flauw et al., 2018).

4.2.5 PSA level 1 implementation

Different levels of PSA (level 1, 2 and 3) are available for different stages of the design process. Since the preliminary design stage, a fully quantitative PSA cannot be envisaged. A simplified and semi-quantitative/qualitative PSA level 1 would be feasible, while a PSA level 2 makes sense only after the definition of all the barriers and support systems and a PSA level 3 is feasible after the site evaluation.

For the MSFR, after the identification of the whole set of PIEs (through the already described risk analysis methods, FFMEA and MLD) and the identification of the necessary safety provisions (through the LoD method) with their plausible and postulated unreliability and unavailability (not calculated - that become constraints for the successive detailed project steps), the PSA would be performed to evaluate the risk from the frequency and the damage estimation. Both of them can be classified in macro-categories according to experts' judgements.

The risk evaluation can be useful to allow the detailed design to reach an acceptable level of risk, using a semi-quantitative risk matrix. This analysis should be completed by deterministic accident analyses that are crucial to properly characterize physical phenomena that can occur, to quantify parameters and technological constraints due to the design and/or materials, to quantitatively define all the provisions required to guarantee the safety functions, to ensure the independence of the provisions and to take into account eventual common cause failures. PSA is meant to check whether these safety provisions are robust enough in terms of effectiveness, availability and reliability and it will be used mainly as a verification tool at the conclusion of the entire safety evaluation (Flauw et al., 2018).

More advanced evaluations (fully quantitative PSA level 2 and level 3) will be performed successively at more mature stages of the design.

The inputs for PSA level 1 will come from the other tools of the ISAM methodology (PIRT, OPT), while its expected outputs will drive the deterministic analyses (DPA).

4.3 The operational path of the work

The aim of this paragraph is to define the operational methodology that guides the performed analyses. It corresponds to the third step of the global safety assessment methodology as described in paragraph 4.2.

Starting from the ISAM general framework, three risk analysis methods, which are appropriate for systems at the early stage of the design, are chosen to be integrated into it in order to define a complete and operational methodology. Moreover, since this analysis has been developed in the framework of the European project SAMOFAR, WP partners selected tools whose implementation for INS was already experienced. In particular, the methods are listed below.

- **The FFMEA (Functional Failure Mode and Effect Analysis)**: it is a *bottom-up methodology* suitable to define the possible accident initiators when there are not sufficient design details to allow more specific evaluations at the component level. The loss of the function is postulated rather than the specific failures of systems and components; in this way, it is possible to overcome the lack of information in the design (Pinna et al., 2015). The outputs of the FFMEA can give suggestions for the elaboration of other ISAM tools, i.e. the PIRT and the OPT. The methodology is described in detail in paragraph 4.3.1.
- **The MLD (Master Logic Diagram)**: it is a *top-down deductive approach* for the identification of the possible initiating events. It is particularly appropriate for projects in early design phases as the identification of hazards derives from the process main characteristics and phenomena and is not linked to detailed design assumption (Papazoglou, 2003). Outputs from the MLD will notably contribute to the elaboration of the "Objective Provision Tree" through a top-down approach, as requested in the ISAM. The methodology is described in detail in paragraph 4.3.2.
- **The LoD (Lines of Defence)**: it ensures that every accidental evolution of the reactor state is always prevented by a minimum set of homogenous (in number and quality) safety features - called Lines of Defence - before a sit-

uation with potentially unacceptable consequences may arise. It suits preliminarily designed projects as it can be used as a pragmatic guidance for sketching the architecture of the safety components and systems and for the classification of accidental sequences (Lo Pinto et al., 2017). Outputs from the LoD will contribute to the elaboration of the second step of the OPT, the sketch of the safety architecture, as requested in the ISAM. The methodology is described in detail in paragraph 4.3.4.

Furthermore, the MLD has a long tradition in the nuclear field; some other tools (e.g. LOPA, the calibrated graphs of the IEC 61508) were proposed to fulfill the same objective of the LoD, which has been preferred due to the experience of its application for the risk assessment of INSs.

The integration of these tools in the ISAM is shown in fig. 4-2.

The FFMEA and the MLD represent the operational instruments allowing the fulfilment of the first objective of the OPT: the identification of the operational hazards posed by the plants and the list of the accident initiators. The two methods are selected and employed separately in order to be as exhaustive as possible, being the exhaustiveness in the identification of possible hazards a major safety issue.

On one hand, these outcomes drive the successive deterministic and phenomenological analyses, which, on a first approach, will be performed in priority on the accidents, which are more likely to arise safety concerns. The deterministic and phenomenological analyses represent the quantitative safety assessment with direct effect on safety margins definition and design evolution. Therefore, the hazards identification through FFMEA and MLD will be the foundations of the safety demonstration of the MSFR.

On the other hand, a list of open points (Appendix A) has emerged from the application of the methodologies, regarding systems or procedures to be further defined and phenomena to be further investigated. It points out the potential limitations of the design and makes suggestions to enhance the safety of the concept. The implementation of these tools helps focusing on the available information about design, phenomena, procedures, etc. and the correspondent weak points. In fact, the identification of the hazards and their consequent categorization and ranking aid the designer to localize the sensible areas of the installation, to be further studied and

protected or drive the experts to research different solutions for increasing the availability/reliability of the system always fulfilling the safety functions (e.g. need of redundancies, empowerment of protection systems, additional safety barriers, etc.). Moreover, since the design is preliminary, it continuously evolves and many aspects have to be defined, many options are still available. These methods help to systematically point out the open issues and give preliminary information about the comparison if several solutions are available.

The LoD method receives the list of initiating events as an input and accomplishes the second objective of the OPT: to define a set of provisions to sketch safety architecture on the basis of the identified hazards to be prevented or controlled; the DPA has to validate these results or highlight plausible deficiencies. The experts' elicitation and the exploitation experience will be taken into account as a complementary contribution to the events identification. This part of the analysis is the clearest example of the expression "the safety driven design". The outcomes of the LoD method will practically influence the number of safety provisions (protection systems, procedures, safety criteria) and their characteristics (failure rate, maintenance policies, etc.).

The analysis here presented focuses on the fuel circuit and the systems in direct interaction with it, e.g. the fertile blanket, the intermediate circuit, the wall cooling system, the gas bubbling system and the sampling system, in normal operation conditions during power production.

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 plant systems and operational states (Gérardin et al., 2019). 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 intended PSA model evolves as well.

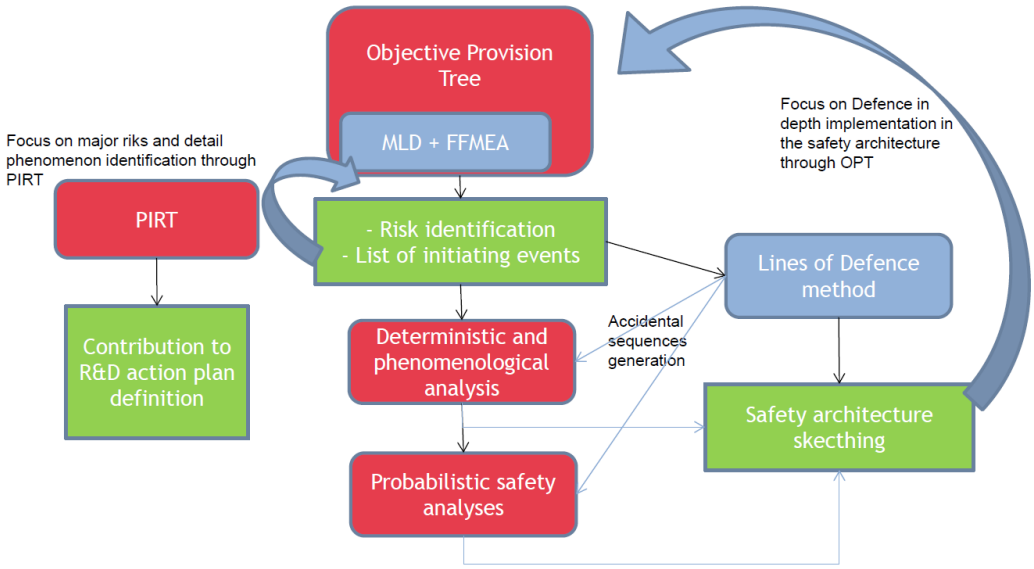

Figure 4-2 Schematic representation of the safety assessment methodology

4.3.1 Functional Failure Mode and Effect Analysis (FFMEA)

The Functional Failure Mode and Effect Analysis (FFMEA) aims at defining possible accident initiators when the design detail is not sufficient to allow more specific evaluations at the component level (US NRC, 2009). Therefore, it is particularly suitable to perform new systems safety assessment, notwithstanding their preliminary state of design. The objective is to identify **functional deviations** able to compromise the reactor safety, to list the PIEs and to recognize major risk contributors, lack of information and/or criticalities of the design and need of additional safety provisions.

The methodology is composed by different consequent steps, which are listed below:

- The first step is to **list all possible systems and main components of the plant**, thanks to the available design information and intents. Then, each system is decomposed into subsystems that can be considered functionally independent. At the end of this step the first version of the **plant breakdown structure (PBS**) is defined.

- The second step is to identify the main functions (process functions, safety functions, investment protection functions, etc.) of the system and specify them in sub-functions through the **functional breakdown structure (FBS)**. Then, each function/sub-function is correlated to one (or more than one) component performing it, creating a link between the PBS and the FBS.

- The third step is to compile the **FFMEA table**, postulating the **loss of functions**, rather than specific failures of systems and components. In this way, through the functional approach, the lack of information in the design is managed. However, in order to highlight causes and safety consequences the relation between functions and components is always highlighted, as much as possible. Furthermore, possible improvements, prevention and mitigation actions are recommended.

The objective of the FFMEA is to provide a **list of potential accident initiating events (IEs)** as exhaustive as possible and give suggestions for improving the overall safety of the system/reactor.

- The last step is to select **a set of postulated initiating events (PIEs)** from the complete list of IEs: for this work, the PIEs are defined as the most severe events challenging the safety of the plant. Each elementary IE is associated with the related PIE. In this way, safety analyses focus on the most relevant accident sequences.

These steps are schematically represented in fig.4-2.

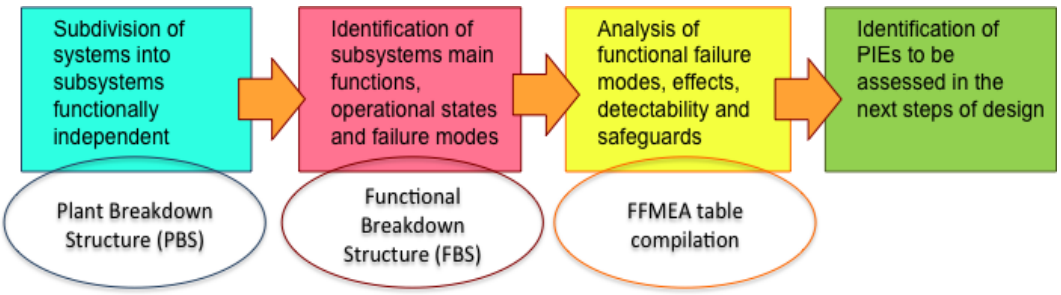

Figure 4-3 Steps of the FFMEA methodology

This methodology should be **iteratively applied**, as the design evolves; similarly, the list of the PIEs will be updated when new design details are available and the physical-chemical phenomena governing the behaviour of the system are investigated through deterministic analyses. Therefore, the objective of this tool if to influence the concept development from its earliest stages.

The results of the first three steps of the application of the FFMEA methodology are reported in paragraph 5.2.1 for the MSFR. The results of the identification of the PIEs are reported in paragraph 5.2.5 for the MSFR and in paragraph 6.1.3 and 6.2.3 for DEMO.

4.3.2 Master Logic Diagram (MLD)

The Master Logic Diagram (MLD) is a qualitative risk analysis method that aims at identifying the hazards and possible initiating events of a system in a deductive and systematic way. This top-down approach is adequate for projects in early design phases; in fact, the tool does not analyze the specific components of the reactor but focuses on physical phenomena and general considerations. Moreover, it helps highlighting the correlations between different functions/phenomena, proving to be an advantage in the study of complex systems such as NPPs. It has been widely used in nuclear industry as well as in other engineering fields such as chemical plants and processes (Papazoglou et al., 2003).

The main steps of the method can be summarized as follow:

- Identification of the **top event**, i.e. the situation to be prevented.
- Decomposition of the top-event into detailed sub-events, which are **possible causes** of the considered top-event. The decomposition continues a sufficient level of detail is achieved (for example statistical data are available for the identified causes, e.g. failure rates, MTTR, etc.) and the events directly challenging the safety functions are identified. In this step, the completeness in the consideration of all physically possible phenomena is crucial for the efficacy of the approach, even if the link with the design is not explicitly defines in a first time.
- Identification of the **initiating events**, i.e. the basic events that cannot be further decomposed into sub-events.

The diagram is usually presented in the form of a qualitative fault tree, beginning from the top event, where the sub-events are linked through the Boolean logic and the lowest levels of the tree show the elementary failures.

These steps are schematically represented in fig. 4-4.

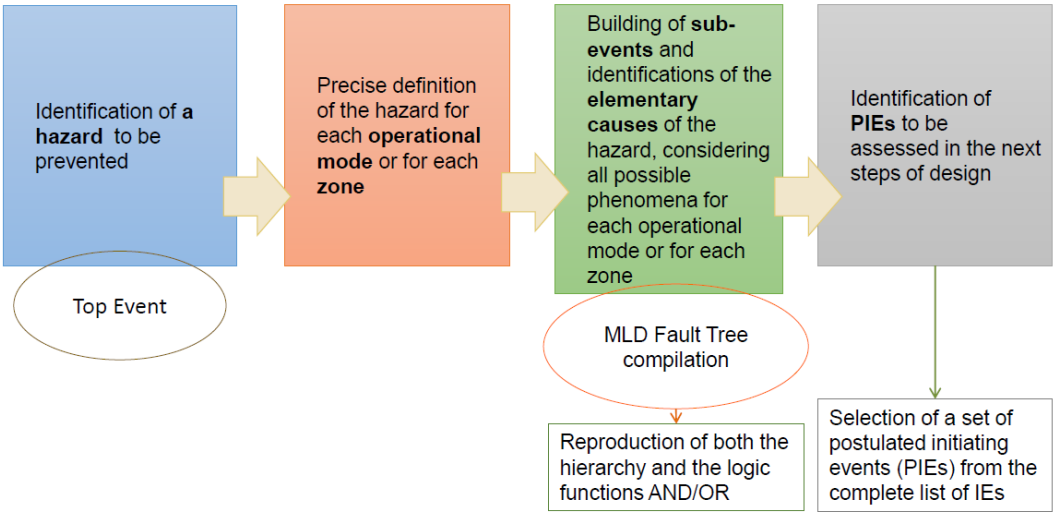

Figure 4-4 Steps of the MLD methodology

4.3.3 Compilation of the list of PIEs

In order to identify the PIEs (Postulated Initiating Events), all the IEs (the elementary failures that compromise process functions with safety related consequences obtained from the application of both the FFMEA and the MLD) are collected in a single list. Then, they are grouped into families. In order to group them, it can be useful to answer the following questions (Pinna et al., 2015):

1. What is the plant status after the IE, without considering the further accident propagation?
2. What are the mitigating actions (lines of defence) to be provided to avoid the accident propagation to the environment?
3. What are the mitigating actions (lines of defence) to be provided to limit the accident consequences to the environment?

The IEs can be assigned to a certain family, basing on criteria of similarity of their consequences and of the plant response (e.g. the triggering of preventive and mitigating actions). Therefore, all the events presenting similar answers to the three questions listed above can be grouped into the same family. Hence, based on preliminary engineering judgement, for each family, the event with the most severe consequences is selected as a PIE (Pinna et al., 2015). Since the very preliminary design stage, it is not simple or evident to identify the most severe events; therefore, in a conservative point of view, many events are selected as PIEs. In the future,

when new data and design information will be available, the list can be updated and optimized.

As final result of the work, each identified PIE has to be studied to define the possible accidental sequences; deterministic analyses shall be performed to verify the plant capacity to mitigate the consequences, to check the compliance with safety limits and to drive the design choices (Pinna et al., 2017).

It is also underlined that at this stage some PIEs are selected independently from their likelihood, with the purpose to guarantee the analysis of all phenomena of potential interest (for example: for the MSFR analysis the fuel salt freezing scenario, the postulated prompt critical power excursion with induced shockwave…). Some of them may be later found not to be possible in the future studies and thus eliminated from the PIEs list.

The common practice is to define incident and accident categories with associated occurrence frequency ranges. Therefore, not only the low probability cases with potentially severe consequences (bounding events) should be identified, but also the "not so low probability events" (the relevant events) for which criteria will be more stringent. Nevertheless, the evaluation of the expected frequency for each PIE is not performed in detail at this stage of the analysis given the premature state of the current design, and only very preliminary considerations on the probabilities have been made (distinguishing frequent events, rare events, and very rare events), based on engineering judgement.

If it is evaluated that some events do not cause safety concerned consequences, they can be classified as not relevant from the safety point of view (N/S). Nonetheless they can be important in the future when Reliability, Availability, Maintainability and Inspectability (RAMI) analysis will be performed (Pinna et al., 2015) (e.g. they can result critical from the production point of view).

4.3.4 Lines of Defence (LOD)

The Lines of Defence (LoD) method aims at ensuring that every undesired evolution of the reactor state is always prevented by a minimum set of homogenous (in number and quality) safety provisions - called Lines of Defence – in order to avoid situations with potentially unacceptable consequences. Therefore, the tool helps the

designer to assess the adequacy of the present safety features to manage the analysed accidental situation.

This method is deterministic and compliant with the internationally accepted safety principles. It suits well the early design phases, since, it can guide the design of the architecture of the safety components and systems. The method helps to identify and classify accidental sequences (Lo Pinto et al., 2017).

The LoD method steps

The safety demonstration of nuclear installations depends on the accomplishment of a set of safety functions, that guarantee the control of the reactor in all the operational modes with adequate safety margins, ensure accidents prevention, avoid that the small deviations from normal operation degenerate into severe accidents (domino effect) and ensure that the residual heat is constantly extracted during the reactor shutdown (GIF, 2002). Nuclear installations must realize these safety functions with systems and procedures during all the life phases of the systems.

The initiators (identified in the previous steps of the analysis) challenge the reactor integrity and the safety functions; they are grouped into families depending on their possible consequences on the reactor (Gérardin et al., 2019). For each family, are selected specific **initiating events** (IEs) to be further analysed. In this work, the LoD tool is applied to some of the identified IEs.

An *initiating event* initiates the accidental sequence. The *accidental sequence* is the evolution of the accident from the initiating event until the final consequences and damage. The *consequence* is the effect in physical terms of a particular accident and the *damage* represents the last impact of failures/accidents on the population, the environment, structures/assets, and reputation (in this work it is quantified in terms of availability of the system, investment loss or radioactive release). The prevention and mitigation of the accidental sequence is given by the implementation of LoDs.

For a given accidental situation to be prevented (typically, the situation of loss of the main safety functions or severe accident is generally considered here), the main steps of the LoD method are:

1. **Define the number and quality of LoDs** to be provided for prevention of this accidental situation (if several safety functions are interested, the method should be implemented for each of them);

2. For each IE, **ensure an adequate set of LoD** (in terms of number and quality).

It is worth to note that at the early design stages (when the safety provisions are not defined yet) the method provides a guidance to sketch the safety architecture; when a more detailed safety architecture is defined, the tool checks its adequacy, and allows the classification of accidental sequences upstream accident analyses.

One of the essential points in the application of this method is to ensure the **independency and the diversification** of the LoDs implemented for each IE in order to minimize the risks of CCF (Lo Pinto et al., 2017).

Lines of Defence definition

There are three types of LoDs: the measures aimed at preventing the occurrence of the IE (in fact, the low occurrence frequency of an initiating event may stand by itself for a LoD), the measures aimed at limiting the consequences of the IE by means of specific equipment, and the intrinsic behaviour and natural resistance to the progression of the accident.

The lines of defence are classified according to their expected reliability and availability:

- Strong LoD, type "a" (failure rate of approximately 10^{-3} to 10^{-4}/year or solicitation);
- Medium LoD, type "b" (failure rate of approximately 10^{-1} to 10^{-2}/year or solicitation) (Lo Pinto et al., 2017).

From the experience, it is possible to distinguish strong and medium LoDs as described below:

- **Strong LoD** ("a"): for example active systems designed respecting the standards of the nuclear industry and including internal redundancies; passive equipment (e.g. confinement barriers) respecting the standards of the nuclear industry; intrinsic behaviour ensuring a long grace period to perform human corrective actions.
- **Medium LoD** ("b"): for example active systems without internal redundancy; actions by the operator.

Two medium independent LoDs may be considered equivalent to one strong LoD (Lo Pinto et al., 2017).

Use of the LoD method within the advanced reactors safety architecture definition process

Once a list of IEs is defined, the hazardous situations to be prevented should at least take into consideration:

- **Loss of main safety functions**: it usually includes the risk of loss of the *reactivity control,* the risk of loss of the *decay heat removal* function; the risk of relevant *releases* in the environment;
- Occurrence of a **severe accident situation** or a practically eliminated situations situation (if any).

The quantity and quality of LoD required for each situation should be defined considering its potential consequences. If a risk of important or early radiological releases is supposed, three LoDs are generally considered necessary. This means that, for each IE potentially leading to a severe accident or a practically eliminated situation, two strong LoDs and one medium LoD ("2·a + b"), which can operate with a different order, shall be available and reliable (it is reminded that the low occurrence frequency of an initiating event can stand for one LoD by itself).

Chapter 4

Results - Case Study: the MSFR

The aim of this chapter is to summarize the main results obtained from the application of the previously defined methodology (see paragraph 4.3) to different advanced systems. In particular, in this chapter, the entire methodology is applied to the Molten Salt Fast Reactor (MSFR), whose design is described in paragraph 5.1, as reported in the deliverables of the SAMOFAR project (Allibert et al., 2017).

5.1 Description of the system

Along with five other concepts (see Chapter 1), MSFR was selected by the GIF-IV due to its promising design and safety characteristics (GIF, 2014).

The MSFR, object of this analysis in the frame of the SAMOFAR project, is a 3000 MW_{th} reactor based on the thorium fuel cycle. The MSFR can be operated in the full range from breeder to burner reactor and is flexible in terms of operation (load-following capabilities…) and design choices (core geometry, fuel composition, specific power level…), but very different from solid-fuel reactors in terms of design and safety characteristics (Gérardin et al., 2019).

Figure 5-1 shows a schematic representation of the MSFR plant. It includes three circuits involved in the power generation: the fuel circuit, the intermediate circuit and the power conversion circuit. These circuits are associated to other systems composing the whole power plant: the emergency draining system, the routine draining system to the storage areas and the reprocessing units.

It is worth to note that the design is still conceptual; design activities are currently on-going with the aim to establish if MSFR can satisfy the **goals of Generation-IV** reactors in terms:

- Sustainability (U-233 breeding from Th-232):
- Non-proliferation (integrated fuel cycle, multi-recycling of actinides);
- Resource saving (closed Th/U fuel cycle, no uranium enrichment);
- Safety (e.g. as far as regard the following MSFR characteristics: no reactivity reserve, strongly negative feedback coefficient);
- Waste management (potential actinide burner).

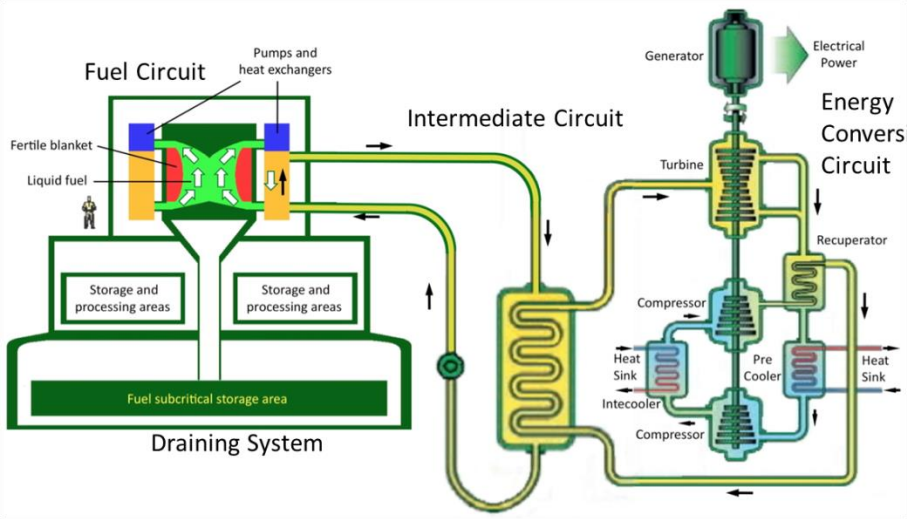

Figure 5-1 Schematic representation of the MSFR plant (GIF, 2014)

5.1.1 The fuel circuit

In its preliminary design, the core of the MSFR is a single compact cylinder (2.25m high x 2.25m diameter) where the nuclear reactions occur within the liquid fluoride salt acting both as fuel and as coolant. The fuel salt flows from the bottom to the top of the core cavity (Allibert et al., 2017).

A schematic representation of the fuel circuit is shown in fig. 5-2.

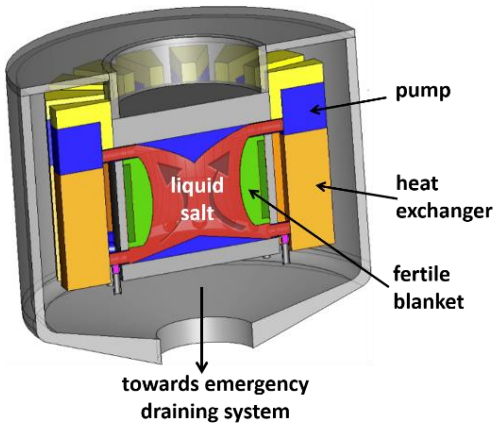

Figure 5-2 Schematic representation of the reference MSFR fuel circuit (Allibert et al., 2017)

The major components of the MSFR are listed hereafter.

- Core: The core or 'active region' corresponds to the salt volume where most of the nuclear fissions take place. It includes the flowing salt in the central cavity, the injection zone (at the bottom of the core) and the extraction zone (top of the core). The MSFR core does not include any solid internal support structure except for the wall materials. The reference concept is designed with a salt temperature rise preliminarily fixed at $\Delta T = 100$ K. The operating fuel temperatures are in the interval [650°C-700°C] (inlet salt temperature) and [750°C-800°C] (outlet salt temperature). The lower limit is set in order to have a safety margin from the salt melting point (585°C) while the upper limit is imposed by the resilience of the structural materials (limited to 800°C with a thermal protection envisaged). The core operating parameters were defined after various parametric studies (Mathieu, 2005; Mathieu et al., 2009; Merle-Lucotte, 2008; Brovchenko, 2013; Heuer et al., 2014; Laureau, 2015a); their purpose is to minimize neutron losses, reflector irradiation and in-core fissile inventory, while maintaining a fuel salt volume in the heat exchangers large enough to ensure a $\Delta T = 100$ K. The resulting core shape is roughly a cylinder, with 1/2 of the entire salt volume inside the core, the rest being located in the external fuel loops. This torus core geometry has been further improved to guarantee a stable flow in the core (Brovchenko et al., 2014; Dulla et al., 2014).
- Upper and Lower Reflectors: The lower and upper walls of the core are neutron reflectors. The upper reflector is submitted to mechanical, thermal

(the fuel salt mean temperature in the extraction area is around 750°C with possible spatial and time dependent fluctuations) and radiation constraints. The combination of high temperature and high radiation levels seems to be the biggest challenge for the proposed alloy so that the surface of the upper reflector may require a thermal protection. Due to the significantly lower inlet temperature with respect to the outlet temperature, the lower reflector is under reduced thermal stress. The lower reflector is coupled to the Emergency Draining System. The shape of these reflectors has been determined in studies aiming at ensuring a stable thermal flow in the core (Dulla et al., 2014; Rouch et al., 2014).

- Recirculation loops (called sectors): Each of these loops or external sectors is dedicated to the cooling of the fuel salt, from its extraction at the top of the core to its injection at the bottom. A sector consists in a pump, a heat exchanger block and the bubbling system (a bubble injection device in the cold leg and a salt/bubble separator in the hot leg), a blanket salt tank, and cooling equipment (which uses as coolant the intermediate fluid). When the sectors are in place, there is some play among them and between the sectors and the vessel. The spaces among the different sectors and between the sectors and vessel will be filled with salt which, during normal operation, is kept in the solid state (because of the temperature distribution). A pre-filling operation with an inactive salt may be necessary before the fuel salt filling in order to avoid the presence of fuel salt in dead areas (Allibert et al., 2017). Figure 5-3 shows a schematic representation of the sectors inside the reactor.

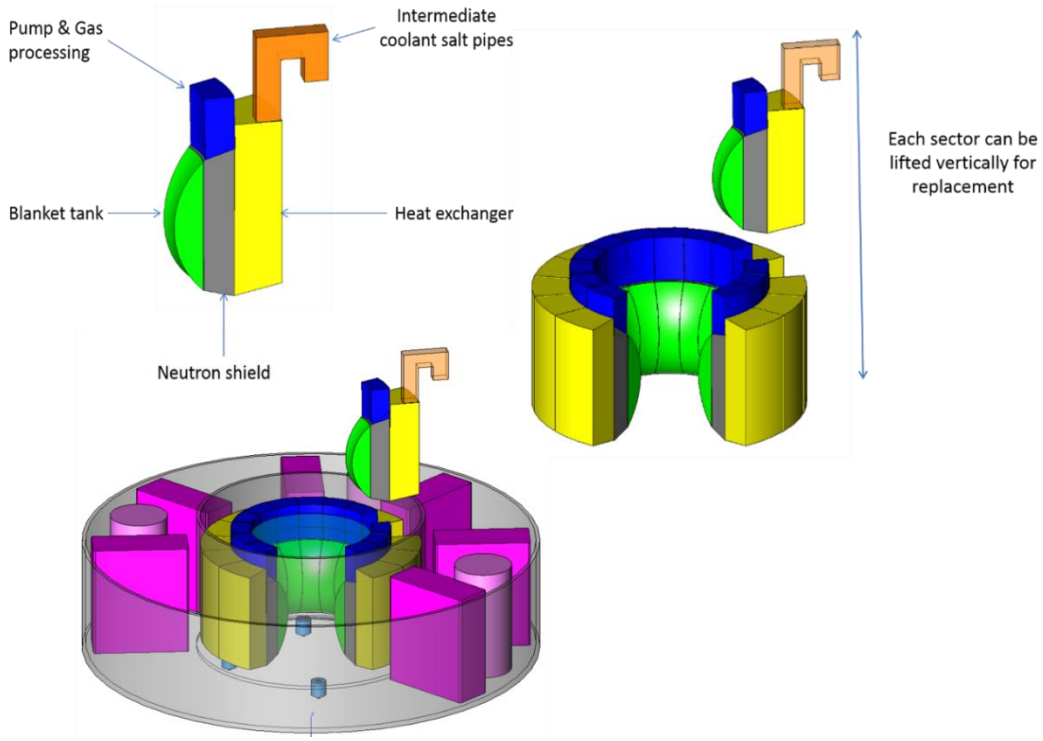

Figure 5-3 Schematic representation of the lower part of a sector showing the blanket salt tank (green), the neutron shield (grey), the intermediate exchanger (yellow), the pump with its salt collector and its distributor connected to the exchanger (blue) (Allibert et al., 2017).

- Heat Exchanger (one per sector): Each heat exchanger (HX) unit has to extract about 187 MW during normal operation. The HX design is challenging since a very compact design is needed (to reduce the volume of the fuel salt outside the core) but on the other hand the maximum compactness achievable is limited by considerations on the HX pressure drop, the maximum allowed salt velocity (to limit erosion phenomena) and the thermodynamic properties of the working fluids. A preliminary design has been developed based on a plate HX option, which represents a reasonable compromise between compactness (exchange area) and pressure drop. This preliminary design is adequate for the purpose of the present studies but will require further examination (in particular related to the geometry, materials and fabrication) for better optimization. The design of this component affects the heating (ΔT) in the core when both reactor power and total fuel volume are fixed (Allibert et al., 2017).

- Fertile Blanket: This component serves as a radial reflector and as a neutron shield to protect the external components of the fuel loops (pipes, heat exchangers). In addition to this protective function, the fertile blanket improves the breeding capabilities of the reactor. The walls of the blanket tank are made of a Ni-based alloy for corrosion resistance and are layered with B_4C on the outer wall to reinforce the neutron shielding. The salt in the blanket is of the same type as the one in the core but with 22.5 mol% Th and without any initial fissile material. Since the thorium in the fertile salt is exposed to the core neutron flux, it generates the ^{233}U fissile element by neutron capture. A small fraction of the ^{233}U produced in the blanket will fission, so that fission products are produced in the blanket and will have to be removed. In addition, the power arising from the ^{233}U fissions (estimated ~ 7 MW in the whole blanket volume) and from the captures on thorium (~24 MW) will heat the fertile salt in the blanket. It has been found that this heat cannot be evacuated through the blanket walls by natural convection so that an external cooling system is also necessary for the fertile blanket. If breeding is not required, the MSFR design could be simplified by replacing the fertile blanket with an inert reflector, similar to the axial reflectors. Optimized shapes of the fertile blanket may also be studied to improve the thermal flow in the core.
- Pump (one per sector): The salt is circulated in the reactor by 16 pumps (one for each recirculation loop). The fuel salt flow rate is about 0.28 m^3/s to ensure an adequate temperature rise in the core for the current core power level. The pump characteristics (static head) has an impact on the circulation time of the salt and thus on the temperature rise in the core since the produced power is fixed and proportional to the product of the fuel velocity in the core by this temperature rise.
- Bubbling system: The online bubbling system aims at removing the gaseous fission products (FPs), via dilution in a carrying gas, and removing the metallic particles dragged by the fuel salt, via capillary sticking to the bubbles.
  If the fission gases, especially Kr and Xe, are not extracted, the fuel reaches saturation rapidly. Gas bubbles grow in the fuel and in particular on the walls of the exchangers, since the solubility of the noble gases decreases with the temperature. In the absence of any special device, these gases escape via the fuel free surfaces: the expansion tank, the pumps, and any interstice with a free liquid salt surface. A gases extraction device must then be envisioned in order to control their behavior.

The non-soluble metals naturally deposit on the surfaces encountered in the course of their travel within the fuel salt. Therefore, they may cluster preferentially on the exchanger plates and in the bends, with occasional obstructions. A non-soluble metals extraction device must be envisioned in order to control their behavior.

There are different options to design the bubbling system, it can be in-core or out-core, and each solution presents advantages and drawbacks. The advantage of the in-core solution is its high FPs extraction rate, hence a short residence time in the fuel. The main drawback is the in-core presence of a complex separation device. Conversely, the out-core option is simpler to be realized, but it has a poorer extraction efficiency, with a longer FPs residence time in fuel.

For the in-core option, it is foreseen that the fuel reaches the top of the sectors, enters into a pipe that makes it swirl, and then a cyclone maintains the swirling motion. The central part of the swirled fuel salt is separated into a separation chamber. After the fuel-gas separation, the fuel salt is led back to the cyclone beneath the pump inlet. The separated gas is compressed by a liquid ring pump into the gas processing tank, where it stays about 1000s before being recycled.

Another function of the bubbling system is the control of the reactivity, independently on the FP extraction. In this case large bubbles are injected into the core to reduce the local fuel density. The void ratio could be up to 3% of the core volume, instead of 0.1 to 0.5% for FP extraction. Gas extraction has to be dimensioned accordingly.

The bubbling system has only been partially studied up to now. Some suggestions are presented in Appendix A to provide useful information for risk assessment associated to this component.

Figure 5-4 shows a schematic representation of the components of a sector.

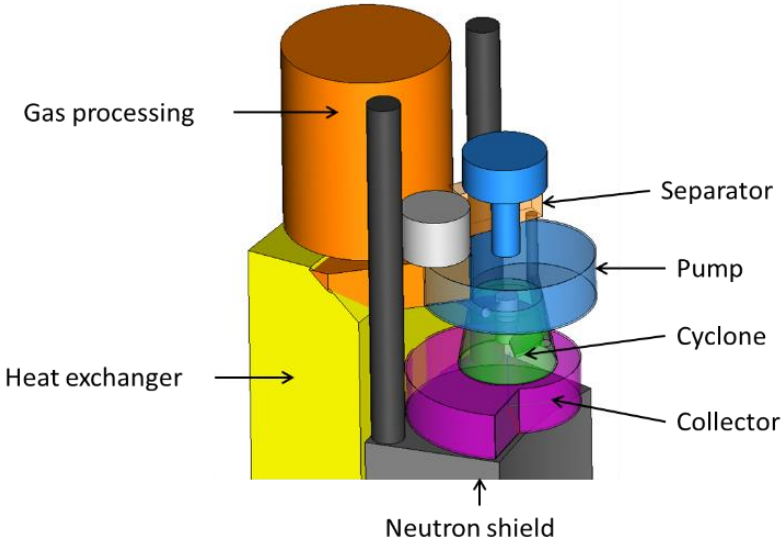

Figure 5-4 View of the top of a sector showing the pump (blue) and the two parts of the separation device consisting in a cyclone to concentrate the gas phase in the vortex center (collector & cyclone) and deriving this central part of the fuel stream to a separation chamber (Allibert et al., 2017).

- Pipes: The piping conveys the salt circulation between the core and the HX and pumps. The pipes are sized (diameter and length) according to two main constraints: reduction of the fuel salt volume outside the core and limitation of the maximum salt speed in the pipes to mitigate erosion. The pipe diameters affect the circulation period of the fuel salt in the system, and thus its heating in the core, if the power is fixed. Other considerations that will have to be analyzed in the future include optimization of the pressure drop, thermal fatigue (in particular in the upper pipes), pipe vibration, welding, seismic behavior, access for inspection, thermal shielding, etc.
- Reactor Vessel: The core and the reactor systems (components of fuel loops such as pipes, pumps, HX, etc.) described above are contained within a reactor vessel which is filled with an inert gas (e.g., Argon). The inert gas has a double function: it is used to cool the reactor components by maintaining the gas temperature at about 400°C, and it can be sampled for an early detection of any salt leak. Setting the gas temperature at 400°C guarantees that in the event of a small fuel salt leak, the leaked salt solidifies since its melting temperature is 565°C. The reactor vessel parameters (geometrical and material) do not directly affect the core performance (and thus are not needed for the optimization) but are necessary for the safety analysis.

The sectors contain all identical components that can be factory-made, in small quantities. They must be easily transportable and manageable, implying that they should be as small as possible. This requires a larger multiplicity of these components. Moreover, a failure in one of the sectors is the less damaging since the number of sectors is large. In this respect CCFs have to be evaluated.

The sectors are arranged in one row around the core vessel and they comprise a pump that ensures the fuel salt circulation. The bulk of the pump is likely to be the limiting quantity for the number of sectors. Furthermore, the intermediate circuit will probably comprise fewer circulation loops than sectors so that each intermediate circuit will feed several sectors. This means that the total number of sectors is a multiple of the number of sectors fed by each intermediate circuit circulation loop. Each sector is connected to an intermediate fluid circuit (4 circuits, each feeding 4 sectors, for example, can still cool the core if one of the intermediate circuits fails).

5.1.2 Intermediate circuit

The intermediate fluid cools down the core and heats up the Balance of Plant (BoP) fluid. Moreover, it cools down the fertile salt and the reactor walls. It is important to ensure the compatibility between the hot leg temperature and the maximum temperature manageable by the BoP fluid. The cold leg temperature must be high enough to eliminate any chance of solidifying the fuel salt in the intermediate exchangers. The intermediate fluid is not defined, yet. It may be a liquid metal (LM) or a salt.

The advantage of LMs (Na or Pb, essentially) is their very good thermal conductivity, which enhances the global thermal transfer coefficient with a smaller exchange surface. As a drawback, the cold leg temperature must be close to the fuel salt melting temperature (585°C), with corrosion issue for lead. The use of sodium involves several hazards, due to its high reactivity with air and water.

Among the salts, there are several options: FLiBe, FLiNaK, $LiFZrF_4$ or fluoroborate (8NaF-92NaBF4). The poor conductivity of the salt can be compensated by the fact that there is a temperature gradient at the interface between the salt and the wall, permitting a cold leg intermediate temperature significantly lower than the fuel salt melting temperature.

An online gamma spectrometry analysis of the intermediate fluid must be implemented to monitor any fuel salt leaks in the intermediate heat exchangers.

5.1.3 Expansion vessel and fuel sampling

The free levels are fundamental for guaranteeing the fuel expansion in case of temperature increases. Among the others, two of them are the most important: the gas-salt separation chambers (if the core bubbling option were adopted) and a specific expansion tank. The expansion tank may be used to remove and add fuel salt at a daily rate of 10 to 40 liters, in one or several batches. Remembering that the mean fuel volume is 18 m^3 and a mean temperature variation of ±10K has to be allowed (with a relative volume dilation coefficient around $2 \cdot 10^{-4}$/K), the total volume change is around ±36 liters. The current major idea is that the tank volume is to be dimensioned as the double of this volume variation (80 liters).

The expansion tank is placed in the center of the upper reflector with a vertical inlet for the insertion of new fuel in the core, for allowing the online refueling. Lateral pumping through radial pipes keeps the in-core fuel content constant. The tank walls are cooled and protected by a refractory lining because of the high fuel temperature and large decay heat. The tank is closed with a removable lid. In order to guarantee the nominal composition of the fuel, a pressurized sampling device is foreseen. During sampling, the lid is removed and replaced by a sampling vessel where the fuel can be transferred both ways by differential pressurization.

Figure 5-5 shows the upper reflector with the expansion vessel and the sampling device.

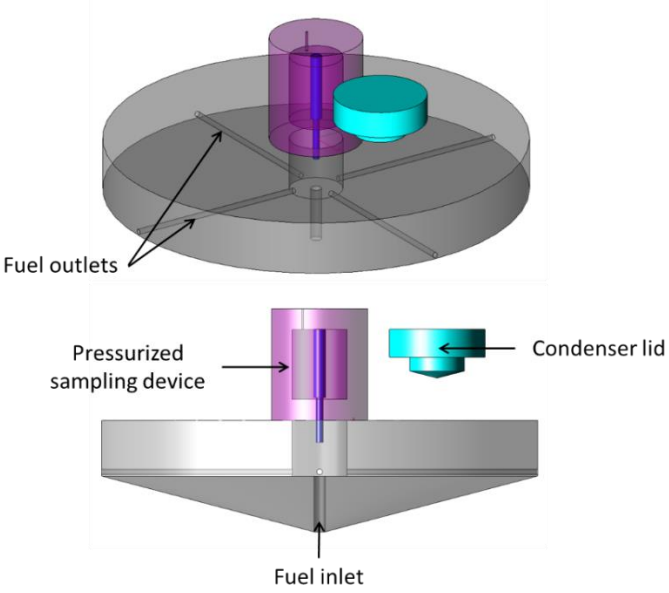

Figure 5-5 Illustration of an expansion vessel on the upper reflector fitted with a sampling vessel for fuel transfer (Allibert et al., 2017)

5.1.4 Draining systems

There are two foreseen draining modes, each operated by a different system:

- *Controlled routine draining*: Fuel salt is transferred to the actively cooled storage tanks, for routine maintenance procedures (a few days to a few weeks). They also ensure the fuel salt heating before the core filling. The routine draining is rather slow (e.g., one hour) in order to adequately reduce the fuel temperature before the draining. It is foreseen to perform this type of draining every 1 to 5 years, during sectors substitution.
- *Emergency draining*: in case of anomaly during operation, the fuel salt can be drained in the Emergency Draining Tank (EDT), either by active devices, or by passive means. This process must be rapid (e.g., less than 10 minutes) enough to limit the fuel salt heating in a loss of heat removal event.
  In case of emergency, the EDS triggering must be redundant and reliable: three opening systems are foreseen and depend on the reactor status. They are based on three different mechanisms and at least one of them will be passive (specifically, a fusible plug). The EDS orifices are short pipes (30

to 60 cm) that run through the bottom reflector. Their diameter (~10 cm) allows a 15 minutes draining with only one orifice open. The risk of spurious activation if the EDS limits the number of orifices. The fuel salt is drained to a funnel-shaped collector that ends into a vertical shaft, driving the salt into the passive storage reservoir (EDT), which guarantees a deeply subcritical core geometry. The collector can communicate with the core, in order to allow the gases to return into core. The design of the EDS is still on-going. One of the considered design is constituted by a system of cooling rods. The gaps between the rods is filled by the drained fuel salt, while the inside of each rod is filled with a thick layer of inert salt, leaving space in the central part for cooling channels. The cooling fluid has not been selected yet (Allibert et al., 2017).

In fig. 5-6, one of the design options for the EDS is shown.

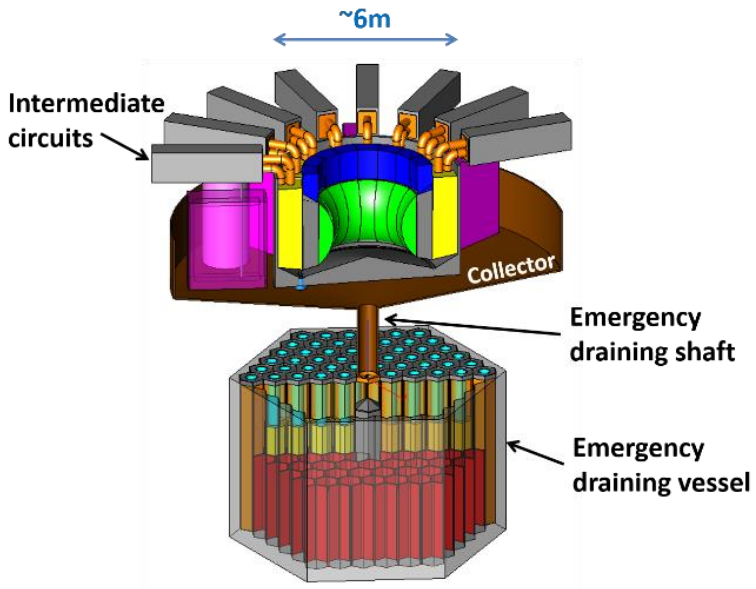

Figure 5-6 Schematic representation of EDS plausible design (Allibert et al., 2017)

For the successive analyses (especially during LoD application), it is useful to note that the fuel salt system has 3 kinds of free surfaces (see fig. 5-7) that can help to manage temperature increases and the consequent liquid fuel volume dilation, mainly in case of unavailability of the EDS:

- The central opening for the fuel periodical transfers, located in the upper reflector;

- The salt-gas separators with controlled pressurization, supposedly at low pressure for efficient degassing;
- The siphons, which are attached to the vessel, not to the sectors, and have their own pressurization. The inert gas is returned to the vessel during draining via the sampling opening in the expansion tank.

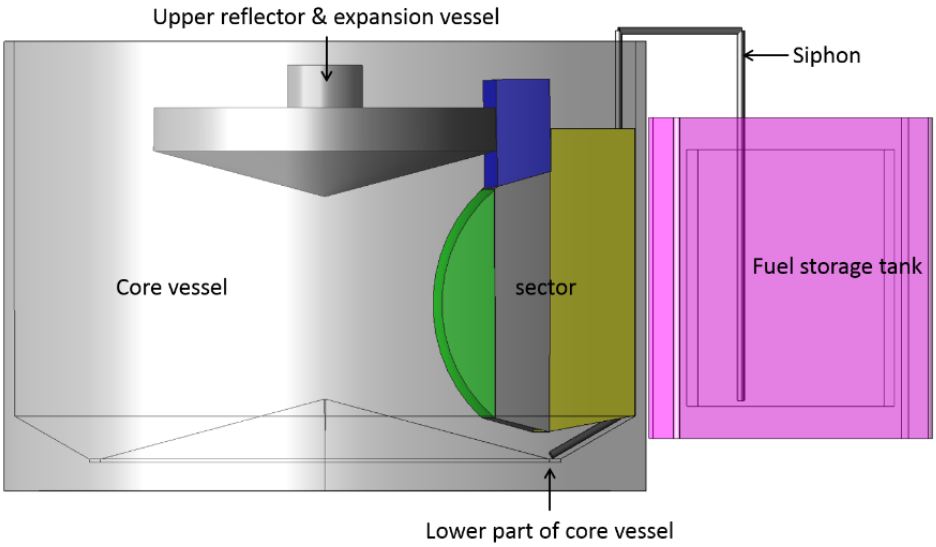

Figure 5-7 The fuel salt free surfaces are situated in the gas-salt separator (blue) and in the expansion vessel (gray). The bottom of the fuel storage tanks is approximately at the same level as the bottom of the core vessel (ends of the siphons) so as to allow complete draining without large pressure gaps (Allibert et al., 2017).

In conclusion, the MSFR unique characteristic is the circulating molten salt, performing as fuel and coolant contemporarily, and the fast neutron spectrum. Some consequences are the possibility of a reconfiguration of the core geometry in case of anomalies through passive systems, the regular adjustments of the fuel composition permitting low reactivity reserves in core, a higher risk of reactivity insertion accident during refueling and the fact that a significant part of the fissile matter is not in core (Uggenti et al., 2017).

Figure 5-8 shows the position of the different systems in the reactor building. In this figure, the HXs between the intermediate circuit and the energy conversion circuit are located within the reactor building. It has to be noted that other design

options are currently studied, where these heat exchangers are located outside of the reactor building. Their position is still matter of discussion.

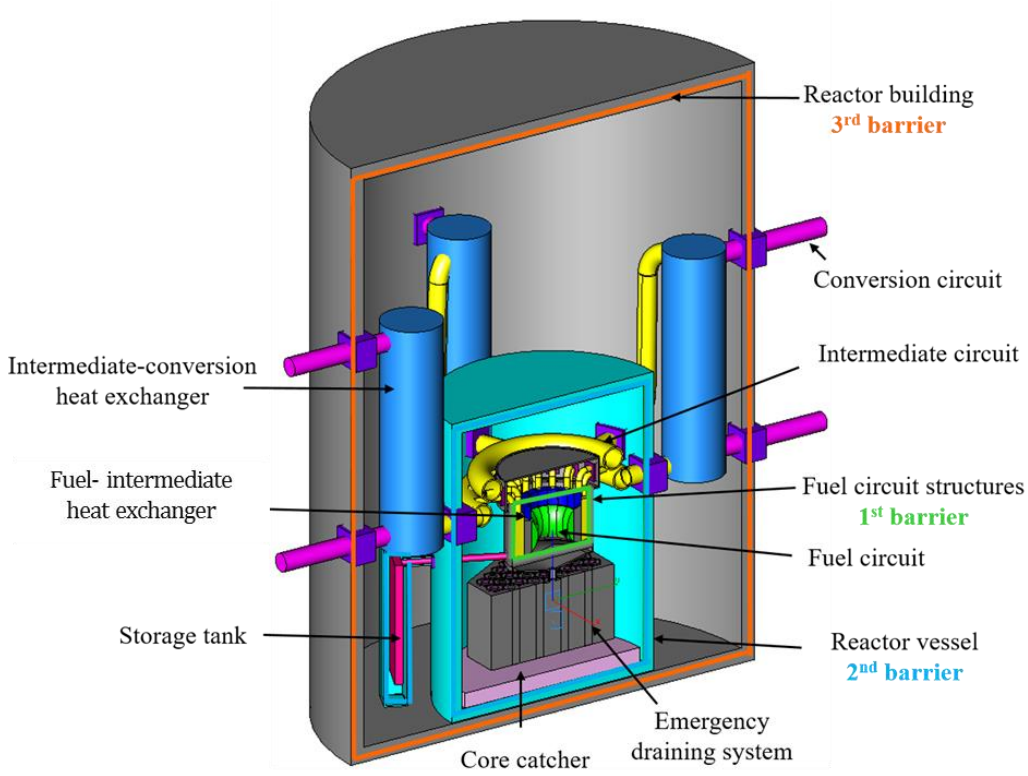

Figure 5-8 Schematic view of the main systems located in the reactor building; proposals for the confinement barriers are highlighted.

At the present stage, the design of the reactor is incomplete and in evolution. As it can be deduced from the systems description, there are many open points, on systems, components procedure and physical phenomena characterizing the reactor behavior. Annex A lists these open points and presents the different available options with the correspondent advantages and drawbacks.

5.2 Identification of Initiating Events for MSFR

The major safety analysis performed for the MSFR in the frame of this PhD work has been carried out on the reactor **during nominal power production** and

concerns the different MSFR systems involved. Some design evolutions and optimizations of the MSFR have also been suggested as a result of the safety analysis presented here as will be explained in the following.

The following **assumptions** and considerations drive the analysis:

- The design of the system is at a preliminary stage and still in evolution, therefore the outcomes of the study are not final, but could/will evolve with the design details;
- Only the core circuit and the immediately adjacent systems, interacting with it, are analysed, e.g. the fertile blanket, the intermediate circuit, the wall cooling system, the gas bubbling system and the sampling system, in normal operation conditions during power production;
- The analysed operational mode is the normal operation of the reactor during power production (P= 3000 MW_{th});
- Security issues are not taken into account during the study.

Moreover, in order to perform the analysis, the physical barriers able to prevent a radioactive release should be defined. In annex B, the issue is analysed and some proposals are presented. The following analysis is coherent with the third proposal (see paragraph 9.3.3), which is summarised in the following bullets:

- The first containment physical barrier is constituted by the fuel circuit and the EDS vessel (in green in fig. 5-8);
- The second containment physical barrier is constituted by the fuel casing (in sky blue in fig. 5-8);
- The third containment physical barrier is constituted by the reactor building (in orange in fig. 5-8).

5.2.1 FFMEA application to the MSFR

The Plant Breakdown Structure (PBS)

The PBS is the first step of the FFMEA methodology (see paragraph 4.3.1). It is a hierarchical structure that is created early in the project life cycle and that highlights what has already been designed and what has to be completed.

The system is subdivided into different subsystems that can be considered functionally independent and the PBS organizes items and materials that are necessary for the project. These components will be associated with the performed functions and become one of the inputs for the FFMEA table.

For the specific case of the MSFR, the list is organised into nine main parts, one for each main system/unit of the reactor according to the available design information.

The more developed sections are:

- The active fuel zone (section 1 of the PBS), which regards the components in direct contact with the fissile and fertile salts, no matter the operational phase (the Emergency Draining System is listed in this section);
- The intermediate salt circuit (section 2 of the PBS);
- The energy conversion circuit (section 3 of the PBS).

The other sections could not be completed yet because of the still preliminary design stage. This represents a clear example of the iterative nature of the methodology: the design data are inputs for the safety analysis whose results drive a more detailed design evolution, which allows the improvement of the accuracy and the completeness of the safety assessment.

A part of the PBS compiled for the MSFR is reported below. The different colours indicate the different levels of the list.

Example:

1. Active fuel zone
   1.1. Fuel casing system
      1.1.1. Reactor vessel filled by inert gas (e.g. Argon)

1.1.2. Fuel casing removable lid (for the change of fuel recirculation sectors)
1.1.3. Removable lid upon the expansion vessel system
1.1.4. Openings for the intermediate salt pipes
1.1.5. Valves to isolate the intermediate circuit
1.1.6. Support system for the reactor vessel
1.1.7. Support system for the core vessel
1.2. Fuel circuit containment structure
1.2.1. Core vessel
1.2.2. Upper and lower closure of the core cavity
1.2.2.1. Upper closure of the core cavity
1.2.2.1.1. Upper reflector
1.2.2.1.2. Expansion Vessel system
1.2.2.1.2.1. Expansion Vessel (fuel salt free surface)
1.2.2.1.2.2. Vertical inlet pipe for the fuel from the core to the expansion tank
1.2.2.1.2.3. Radial fuel outlet pipes (x4)
1.2.2.1.2.4. Removable condenser lid
1.2.2.1.2.5. Valve to isolate expansion vessel for exchanging condenser lid and sampling device
1.2.2.1.2.6. Pressurised sampling device
1.2.2.1.2.7. Gas injection for pressurized sampling device
1.2.2.1.2.8. Opening for fuel transfer through the upper reflector (Sampling and injection)
1.2.2.1.2.9. Connexion from the pressurised sampling device to the reprocessing unit through the reactor building (for fuel salt samples transfer-sealed system)
1.2.2.1.2.9.1. Pipes
1.2.2.1.2.9.2. Gates
1.2.2.1.2.10. Connexion between the fission product removal system and the expansion vessel
1.2.2.1.2.11. Valves
1.2.2.2. Lower closure of the core cavity
1.2.2.2.1. Lower reflector
1.2.2.2.2. Openings for fuel salt draining
1.2.2.2.3. Openings for the bubble injector for reactivity control
1.2.3. Cooling system circulating within the external walls (cooled by intermediate circuit fluid)
1.2.3.1. Pipes
1.2.3.2. Pumps
1.2.3.3. Heat Exchanger
1.2.3.4. Valves
1.2.3.5. Openings in the core vessel

… … … … …

The Functional Breakdown Structure (FBS)

In the standard IEC 61226 (IEC EN 61226, 2005), the function is defined as the specific purpose or objective to be accomplished that can be specified or described without reference to the physical means implementing it. There are different families of functions for a system, e.g. process, safety and investment protection functions.

The main objective of the **process functions** is to operate the plant/system and to demonstrate the feasibility of the power production from the system.

Safety functions should be guaranteed by the physical provisions and barriers, in order to prevent or mitigate nuclear and non-nuclear damages (radiological, chemical, electrical, magnetic, etc.) for workers, public and environment.

The main objective of the **investment protection functions** is to ensure that operations are performed safeguarding the investments, such as machinery and equipment, as well as to minimize operational costs (Pinna et al., 2015). The asset integrity, usually taken into account in the process industry analyses, manages the capability of a system to perform its function effectively and efficiently, always safeguarding population and environment with the aim to optimize the production, e.g. by proper maintenance policies. On the other hand, the investment protection applies to INS, whose major objective is the demonstration of the feasibility of the project rather than the availability/reliability of the plant. Moreover, it is highly probable that the first attempt to build an innovative system will be a prototype (one of a kind), whose costs are increased by the fact that there is not a scale economy for the components that are manufactured ad hoc.

The FBS is the second step of the FFMEA methodology and it systematically lists and organizes the functions, so that the higher-lever functions are more and more specified in lower-level functions, whose negations are one of the inputs for the FFMEA table. The highest-level process functions are 2: “to produce electricity” and “to produce fissile matter in the blanket sectors”; therefore, the FBS results to be composed by two complementary sections, each one referred to one of the main production objectives of the reactor (to burn and to breed).

These functions are specified more and more, taking into account all the complementary aspects necessary to accomplish them (operation, control, measurement, structure integrity, etc.).

A part of the FBS for the process of the MSFR is shown below. In the FBS, the utilization of different colours allows a clearer identification of the different levels.

Example:

1. To generate electricity
    1.1. To generate heat by realizing fissions in the core cavity
        1.1.1. To provide fuel salt inventory in the core cavity
            1.1.1.1. To keep and preserve the integrity and leak-tightness of the core cavity
            1.1.1.2. To keep and preserve the integrity of the fuel salt recirculation sectors
            1.1.1.3. To add fuel salt to the core cavity
            1.1.1.4. To remove fuel salt from the core cavity
            1.1.1.5. To manage pressure/volume of the fuel salt
                1.1.1.5.1. To preserve free surfaces in the active zone
                1.1.1.5.2. To manage the fission products presence (in terms of pressure and volume) in the active zone
        1.1.2. To maintain controlled and self-sustained chain reaction in the core cavity
            1.1.2.1. To maintain the core critical geometry and mass
                1.1.2.1.1. To keep and preserve the integrity and leak-tightness of the core cavity
                1.1.2.1.2. To keep and preserve the integrity of the fuel salt recirculation sectors
                1.1.2.1.3. To maintain the fuel recirculation sectors in the correct position
                1.1.2.1.4. To maintain the core cavity in the correct position
                1.1.2.1.5. To add fuel salt to the core cavity
                1.1.2.1.6. To remove fuel salt from the core cavity
                1.1.2.1.7. To manage pressure/volume of the fuel salt
                    1.1.2.1.7.1. To preserve free surfaces in the active zone
                    1.1.2.1.7.2. To manage the fission products presence (in terms of pressure and volume) in the active zone
            1.1.2.2. To ensure the fuel salt homogeneity in the core cavity
                1.1.2.2.1. To keep and preserve the integrity and leak-tightness of the core cavity
                1.1.2.2.2. To provide the fuel salt circulation in the core cavity

1.1.2.2.3. To provide the correct geometry and space for the fuel salt circulation
1.1.2.2.4. To provide fuel salt flow
1.1.2.2.5. To provide enough turbulence eddies in the core cavity
1.1.2.2.6. To maintain the fuel salt at a liquid state
1.1.2.3. To manage the reactivity of the fuel salt by the temperature
1.1.2.3.1. To maintain the correct temperature range in the core cavity (density/Doppler effect)
1.1.2.3.1.1. To transfer heat from fuel recirculation sectors to intermediate circuits (ref.)
1.1.2.3.1.2. To transfer heat from the structures to intermediate circuits (ref.)
1.1.2.3.2. To change power in the core cavity by heat exchangers temperature using reactivity feedback reactions (load following)
1.1.2.3.2.1. To provide intermediate salt mass flow variations
1.1.2.3.2.2. To transfer heat from fuel recirculation sectors to intermediate circuits (ref.)
1.1.2.3.2.3. To transfer heat from the structures to the intermediate circuits (ref.)

… … … … …

The FFMEA table

The third step of the FFMEA methodology is the compilation of the FFMEA table. The FFMEA table is a specific table that is suggested to report the results of the analysis.

The heading of the table refer to the following items (Pinna et al., 2015):

1. Selection of a function to be analysed (i.e. negated) from the process functions list (see table 5-1, column 1: “Process function”);
2. Identification of the systems and/or main equipment and/or components devoted to performing the function (see table 5-1, column 2: “PBS elements”);
3. Indication of the analysed operating mode (see table 5-1, column 3: “Op. Md.”);

4. Identification of the function failure modes (see table 5-1, column 4: “Failure mode”);
5. Investigation of the possible causes for the loss of function for each failure mode (see table 5-1, column 5: “Causes”);
6. Analysis of the possible consequences for the plant deriving from the loss of these functions, in terms of damage to the machine, of radioactive inventory mobilization through the different containment barriers and to the environment, and, finally, of possible damage to workers and population (see table 5-1, column 6: “Consequences”);
7. Possible actions/means set to prevent occurrence of the initiator and the progress of accident chains (e.g., detections and responses of the control system) if necessary. This column is not present in the extract of FMEA presented in table 5-1 due to space limitation.
8. Possible actions/means set to mitigate the consequences of the failure if necessary. This column is not present in the extract of FMEA presented in table 5-1 because of space limitation.
9. Representative PIEs for the elementary failure identified (see table 5-1, column 7: “PIE”);

The higher-level functions are automatically analysed through the lower level ones, being the relationship such that the failure of a lower-lever function causes the failure of the related higher-level function.

Table 5-1 shows an extract of the FFMEA table compiled for the process functions of the MSFR in normal operation conditions during power production.

Process function	**PBS elements**	**Op. Md.**	**Failure mode**	**Causes**	**Consequences**	**PIE**
P1 To generate electricity						
P1.1 To generate heat by realizing fissions in core cavity						

P1.1.1 To provide fuel salt inventory in the core cavity						
P1.1.1.1 To keep and preserve the integrity and leak-tightness of the core cavity	Core vessel	NOp -P	Loss of contain-ment leak-tightness	Leak/Rupture in the core vessel	The fissile fuel flows outside the core cavity; The chain reaction shuts down; The fissile fuel is collected in the collector; The fissile fuel is drained in the EDS and cooled down in order to remove residual heat; Etc.	Loss Of Liquid Fuel in the bottom part of the core cavity: Breach in the lower reflector

Table 5-1 *Extract from the FFMEA MSFR table*

5.2.2 MLD application to the MSFR

The MLD method (described in paragraph 4.3.2) is applied to the same conditions for the FFMEA. According to the assumptions listed in paragraph 9.3.3, the fuel circuit constitutes the first confinement barrier. Therefore, the fuel circuit degradation or fuel circuit failure is selected as top event in the current study. An extract of the compiled tree, produced with the Arbre-Analyste software (Clement, 2013), is presented in fig. 5-9, where the top event is decomposed according to the phenomena involved (thermal, chemical, mechanical, etc.); in fig. 5-10 the tree relative to the sub-event “Insufficient fuel cooling” is also reported. The second tree is just an example of analysis of a specific sub-event; in this case it is simple to highlight the initiating events that correspond to the last level of the tree, e.g. “Blockage of one or several sectors”, “Spurious stop of one or several fuel circuit pumps”, “Rupture of one or several fuel circuit pumps”.

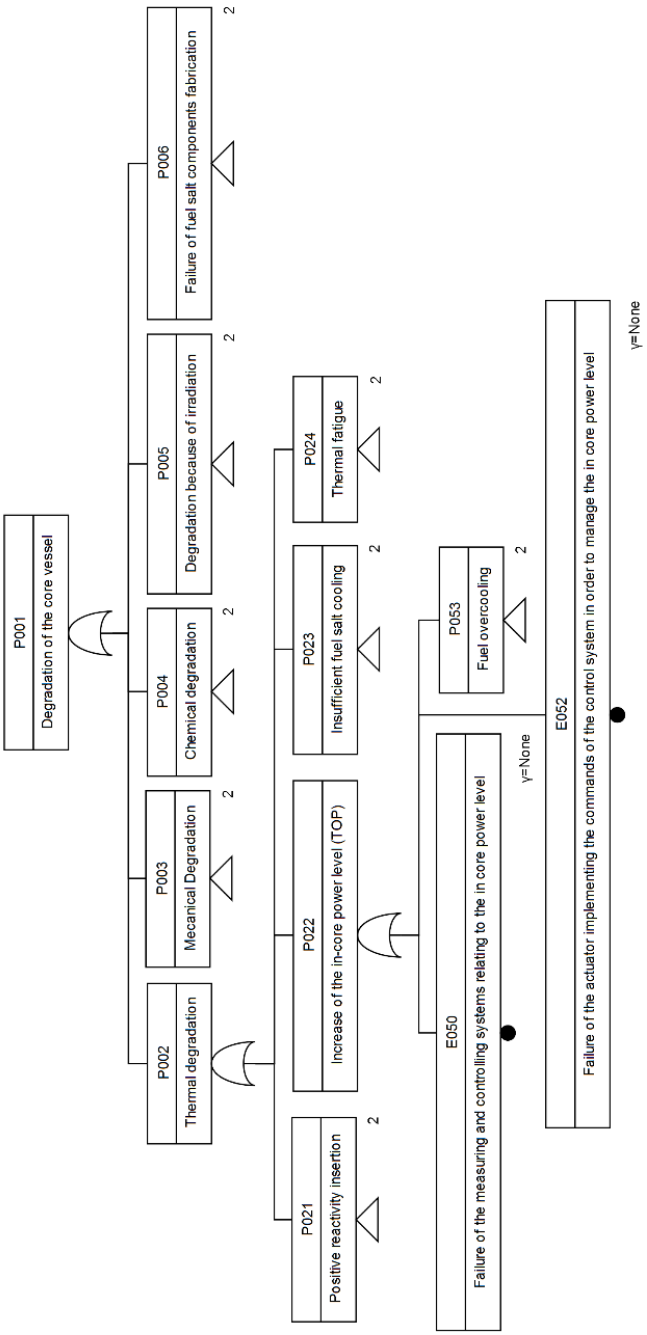

Figure 5-9 *Extract of the MSFR MLD*

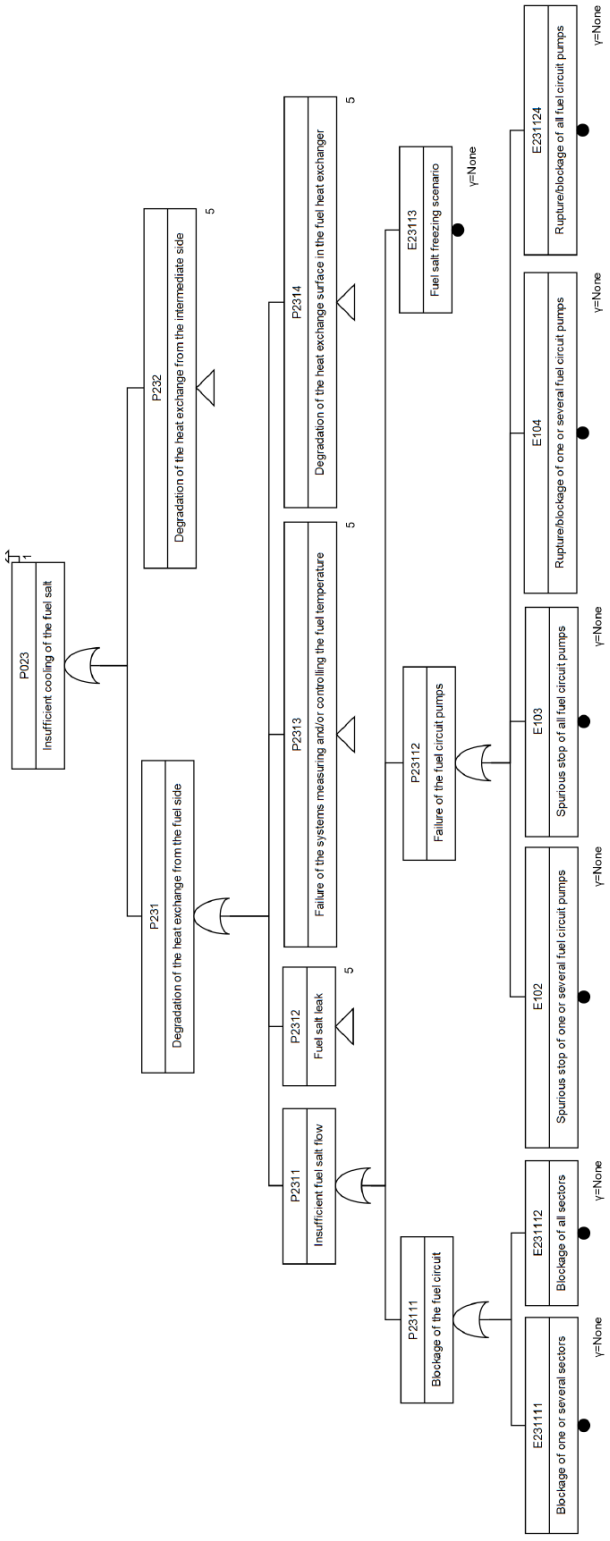

Figure 5-10 Part of the MLD related to the "Insufficient fuel cooling event"

5.2.3 Comparison of FFMEA and MLD

The FFMEA and the MLD methods are based on different approaches: with the FFMEA the user is led to reason from a functional point of view by searching for the possible causes of the loss of the functions of the system and their consequences. Instead, the MLD approach is more phenomenological and the user identifies the causes of phenomena that can lead to the physical degradation of the system. Both methods have proved to be relevant for the purpose, despite some lacks of precise data on the MSFR components, systems or procedures. In the FFMEA the identification of the postulated initiating events is due to the loss of functions rather than the specific failures of systems and components; similarly, in the MLD the hazards identifications derives from the process main characteristics and is not linked to detailed design assumptions. Indeed, in both methods the link with the component is made explicit only in a second time, making them more suitable to an application at early design phase. Moreover, the two methods are qualitative, while the semi-quantitative estimation of the frequency and consequence in terms of macro-categories is performed for the categorization of the initiating events and the selection of the postulated initiating events, which are mainly based on engineering judgement. More quantitative methods will be implemented when the design details will be sufficient for the purpose.

The two methods (FFMEA and MLD) gave similar results and many events were found redundantly. However, few events appeared only in one of the two analyses. For the application of the MLD to the MSFR, risks have been differentiated according to the physical phenomena involved and the method also revealed risks caused by external hazards or by the action of other systems of the plant (e.g. auxiliary systems). In table 5-2, the selected PIEs are listed, specifying if they have been identified through the implementation of the FFMEA, of the MLD or both. For instance, the event “Loss of Chemical Control: Chemical reaction between different fluids” only appeared through the MLD analysis: this represents a typical event identified by the MLD since its phenomenological approach. On the other hand, the FFMEA brought more details onto the failure modes thanks to the effort to link the loss of each function to one or more than one component or system failures. For instance, even if the breach in the upper reflector was well identified with the MLD, the FFMEA highlighted the fact that the breach could involve the rupture of the wall cooling systems and/or the expansion vessel system, according to its location and its deepness.

The FFMEA has the advantage to sketch a plausible accident evolution and to provide additional information on the systems or procedures used for detection, prevention and mitigation, while the MLD offers a good graphical tool to present the hazards and helps understand the logical connections (AND/OR) between them.

In conclusion, the combined use of the FFMEA and the MLD methods proved to be useful to ensure a more complete identification of the hazards and initiating events of the MSFR. This list cannot be considered final, but it will be updated, as new deterministic results are available, and the design is detailed. In addition, as a complementary result, both the methods helped to highlight the open points of the project, which are presented in Annex A and could be taken into account during next steps of the design, with their advantages and drawbacks, in the logic of a safety-driven design.

5.2.4 List of postulated initiating events

The first result obtained from the application of the methodology is a list of initiating events. Among the set of elementary events challenging the plant in similar way and producing equivalent fault plant conditions, the most severe accident initiators in terms of potential radiological consequences (given in particular the related solicitations on confinement barriers) are selected as PIEs, according to the methodology described in paragraph 4.3.3.

Table 5-2 lists the PIEs obtained through the implementation of the FFMEA and the MLD, accordingly to the design stage. The table contains many events, conscious that the list can be refined in a later stage of the design.

Table 5-2 List of Postulated Initiating Events. Selection made on the expected consequences of the events; if the code of the PIE contains an ‘F’, the event has been identified through the application of the FFMEA, if the code of the PIE contains an ‘M’, the event has been added to the list thanks to the application of the MLD, if the code of the PIE contains ‘FM’, the event was a result of both the methods (Gérardin et al., 2019).

PIE-F-1	Loss of liquid fuel in the upper part of the core cavity: Breach the upper reflector with rupture of the structure cooling system (without damages to the expansion vessel system)

PIE-F-2	Loss of liquid fuel in the upper part of the core cavity: Breach in the upper reflector with rupture of a radial fuel outlet pipe (without damages to the structure cooling system)
PIE-F-3	Loss of liquid fuel in the bottom part of the core cavity: Rupture of a pipe of the reactivity control system
PIE-F-4	Loss of liquid fuel in the bottom part of the core cavity: Breach in the lower reflector (with rupture of the structure cooling system)
PIE-F-5	Loss of integrity of the core cavity: Complete (internal + external) rupture of the pressurized sampling device
PIE-F-6	Loss of integrity of the core cavity: Breach of a heat exchanger plate/channel
PIE-F-7	Loss of integrity of the core cavity: Rupture of blanket tank wall between fuel and fertile salt with rupture of the cooling circuit for internal structures
PIE-F-8	Loss of pressure/volume control in the core cavity: Obstruction of the vertical inlet pipe for the fuel from the core to the expansion vessel
PIE-F-9	Loss of pressure/volume control in the core cavity: Rupture of the connection between the free surface of the fuel storage tank and the free surface of the core for the gas in the part between the core cavity and the valve
PIE-FM-10	Loss of liquid fuel flow: Complete rupture of the pump
PIE-FM-11	Loss of criticality control: Reactivity insertion accident: Accidental insertion of fuel
PIE-FM-12	Loss of criticality control: The welded joints taking the recirculation sectors in the correct position collapse

PIE-F-13	Loss of chemistry control: Rupture/obstruction of reactivity bubble injector
PIE-FM-14	Loss of chemistry control: Rupture of horizontal bubble injector for salt cleaning
PIE-F-15	Loss of chemistry control: External rupture of the gas separation chamber from the liquid part
PIE-F-16	Loss of chemistry control: External rupture of the gas separation chamber from the gases part
PIE-FM-17	Overcooling: overworking of one of the fuel salt pump
PIE-M-18	Overcooling of the intermediate circuit: conversion circuit pump overworking
PIE-FM-19	Overcooling: Over-working of the pump of the intermediate circuit
PIE-M-20	Loss of heat sink: Leakage of intermediate salt
PIE-M-21	Loss of heat sink: complete rupture of one or more than one intermediate pump
PIE-M-22	Total loss of electric power
PIE-M-23	Mechanical degradation: external aggression (e.g. earthquake)
PIE-M-24	Mechanical degradation: Ejection of a conversion system component in direction of the fuel circuit
PIE-M-25	Chemical degradation: Chemical reaction between different fluids (e.g. hot part of intermediate circuit and water)

If the code of the PIE contains an ‘F’, the event has been identified through the application of the FFMEA, if the code of the PIE contains an ‘M’, the event has

been added to the list thanks to the application of the MLD, if the code of the PIE contains 'FM', the event was a result of both the methods (Gérardin et al., 2019).

5.2.5 Selection according to the frequency and the consequences of the initiating events

An alternative approach has also been applied, where the IEs are categorized according to their occurrence frequency (in terms of orders of magnitude) and their consequences on the plant and the most representative events of each category are then selected as PIEs. This categorization is useful to determine the level of the safety studies that should be undertaken in the next steps of the safety approach. Indeed, it allows increasing the effort on the events that have a high probability of occurrence and high consequences and for which more stringent criteria should be used.

Method

This second approach used in order to classify the IEs (according to their frequency and consequences) and select a restricted list of PIEs is described below and is summarized in fig. 5-11.

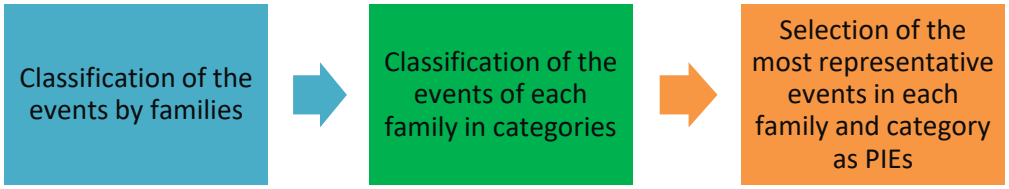

Figure 5-11 *Method for the selection of the PIEs*

As for the first approach, all the elementary IEs are listed in a unique document and are grouped into families, depending on their potential effects on the reactor. The families of events identified for the MSFR are currently:

- F1: Reactivity insertion
- F2: Loss of fuel flow
- F3: Increase of heat extraction/over-cooling
- F4: Decrease of heat extraction
- F5: Loss of fuel circuit tightness
- F6: Loss of fuel composition/chemistry control

- F7: Fuel circuit structures over-heating
- F8: Loss of cooling of other systems containing radioactive materials
- F9: Loss of containment of radioactive materials in other systems
- F10: Mechanical degradation of the fuel circuit
- F11: Loss of pressure control in fuel circuit
- F12: Conversion circuit leak
- F13: Loss of electric power supply

This list will be updated with the progress of the MSFR safety analysis if other phenomena are identified. Some events can appear in several families at the same time. For instance, the event "Detachment of the thermal protection" (to prevent the damage to the structures due to the high temperature in the fuel circuit) appears in the families "Reactivity Insertion'', "Loss of Fuel Flow" and "Fuel Circuit Structures Over-Heating".

Subsequently, event categories are defined with frequency ranges. Given the premature state of the current design and the large uncertainties on the frequencies of most of the events, only three macro-categories have been used for the classification:

- **Incidents** characterized by a frequency of occurrence higher than 10^{-2} event/reactor·year;
- **Accidents** characterized by a frequency of occurrence between 10^{-2} and 10^{-6}-10^{-7} event/reactor·year;
- **Limiting events** characterized by an extremely low likelihood; their frequency of occurrence is lower than 10^{-6} - 10^{-7} event/reactor·year or they can be postulated, based on the defence in depth principle.

Some scenarios or phenomena have been classified as "limiting events", even if no specific cause of the scenario/phenomenon have yet been identified, because they constitute bounding cases or specific risks for the concept. Thus, they should be documented in the next steps of the safety approach. The objective is to drive the analysis towards the consideration of all phenomena of potential interest (for example fuel salt freezing scenario, postulated prompt critical power excursion with induced shockwave, etc.). The classification of the events into categories is also linked to the expected consequences of the IEs. Since an event with a high occurrence frequency and large consequences is unacceptable, some dispositions should be taken in the design to diminish its consequences or to reduce its frequency and

bring it down into a category of lower frequency. Using different words, if a scenario has a frequency of occurrence higher than 10^{-2} event/reactor·year, it is classified as an incident and in order to be considered acceptable its consequences must be low enough; according to the INES scale (International Nuclear and Radiological Event Scale) introduced by IAEA in 1990, from a safety point of view even a serious incident cannot produce lethal health effect, otherwise preventive or mitigative measures must be implemented in order to reduce its frequency or its consequences. Similarly, if a scenario has a frequency of occurrence between 10^{-2} and 10^{-6}-10^{-7} event/reactor·year, it is classified as an accident; since the low frequency, lethal effects are considered tolerable according to the INES scale. If a scenario has a frequency of occurrence lower than 10^{-6} - 10^{-7} event/reactor·year or they can be postulated, it is classified as a limiting event, characterized by the worst tolerable consequences. At this point of the analysis, the INES scale is not the only possible option to distinguish incident, accident and limiting events and it only refers to effects on population and environment (radioactive release).

Due to the lack of information in this phase of the design, regarding in particular the normal and emergency procedures and the possibility to rapidly recover the fuel from the EDS, the consequences related to the operability of the reactor have not been considered.

The simplified Farmer diagram used for the MSFR safety analysis is presented in fig. 5-12. The evaluation of the event frequency and their categorization is based on expert judgment and available experience feedbacks, especially referring to the Oak Ridge reports (Haubenreich, 1968). As the occurrence frequency of a given event may be difficult to assess at this stage, considering an event in a given accident category may also be seen as an objective to be further aimed at design level and checked in future analysis (Allibert et al., 2018).

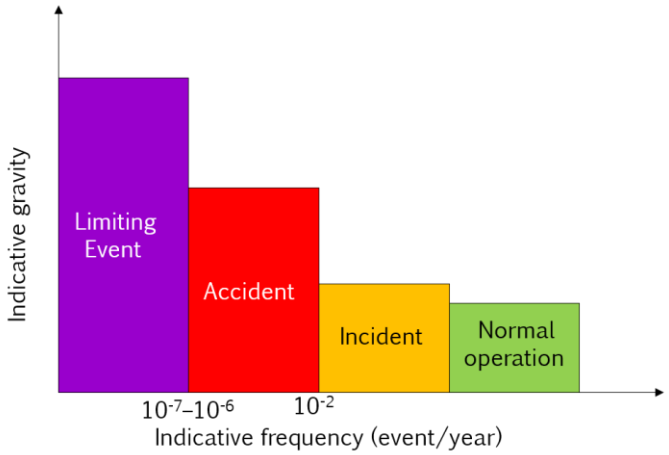

Figure 5-12 *Simplified Farmer diagram used for the classification of the MSFR initiating events*

Finally, PIEs are identified as the most severe events in a given family and a given category (i.e. in a given occurrence frequency range). Therefore, not only the low probability cases with potentially severe consequences should be identified, but also the "not so low probability events" for which criteria will be more stringent.

The classification of the events and the selection of the PIE is illustrated in table 5-3, applied to the «F2: Loss of Fuel Flow » family. Each initiating event/functional failure (in the first column) is classified in a category (in the second column) and associated to a PIE (in the third column). Events that are themselves selected as PIEs are written in bold. The PIEs selected with this approach are listed in the next section.

Table 5-3 Extract of the list of initiating events for the family "F2: Loss of Fuel Flow"

Functional failure	**Category**	**Associated PIE**
Failure of one or several fuel circuit Pump	Incident	Failure of one or several (up to all) fuel circuit Pump
Failure of all fuel circuit pumps	Incident	**Failure of one or several (up to all) fuel circuit Pump**
Spurious speed reduction of the fuel circuit pumps	Incident	**Failure of one or several (up to all) fuel circuit Pump**
Blockage of one or several sectors of fuel salt circuit	Accident	**Blockage of one or several sectors of fuel salt circuit**

Rupture of one or several fuel circuit pumps	Accident	**Rupture or blockage of one or several fuel circuit pumps**
Blockage of one or several fuel circuit pumps	Accident	Rupture or blockage of one or several fuel circuit pumps
Distortion of the geometry of the pipe that makes the fuel swirl	Accident	Blockage of one or several sectors of fuel salt circuit
Compression of a part of the fuel circuit	Accident	Blockage of one or several sectors of fuel salt circuit
Obstruction of HX pipes/plate	Accident	Blockage of one or several sectors of fuel salt circuit
Distortion of salt extraction from the core to the heat exchanger	Accident	Blockage of one or several sectors of fuel salt circuit
Distortion of salt injection from the heat exchanger to the core	Accident	Blockage of one or several sectors of fuel salt circuit
Rupture of the cooling system for the pump	Accident	Rupture or blockage of one or several fuel circuit pumps
Blockage of the cooling system for the pump	Accident	Rupture or blockage of one or several fuel circuit pumps
Fuel circuit pump speed reduction	Accident	Failure of one or several (up to all) fuel circuit Pump
Complete rupture of a fuel circuit pump with breach on the pump shaft at the level of the sector lid	Accident	Rupture or blockage of one or several fuel circuit pumps
Defect of sealing within the components of the sector	Accident	Blockage of one or several sectors of fuel salt circuit
Detachment of the thermal protection	Accident	Blockage of one or several sectors of fuel salt circuit
Rupture/collapse of the sector frame /support	Accident	Blockage of one or several sectors of fuel salt circuit
Rupture of the sector suspension system (welded joints taking the sector in the correct position)	Accident	Blockage of one or several sectors of fuel salt circuit
Fuel salt freezing scenario	Limiting event	**Fuel salt freezing scenario**
Rupture or blockage of all fuel circuit pumps	Limiting event	**Rupture or blockage of all fuel circuit pumps**

Blockage of all sectors of fuel salt circuit	Limiting event	**Blockage of all sectors of fuel salt circuit**

The classification of the initiating events (IEs) in terms of incidents, accidents or limiting events is performed on the basis of the available data, considering analogies with respect to operating reactors and the experts' judgement.

Among the incidents, the failure of one fuel circuit pump or the spurious reduction of its speed are considered. The contemporary failure of all the pumps is also classified as an incident because the event can be caused by common cause failures that still have to be analyzed, e.g. the loss of electric power. It is highly plausible that the consequences of the contemporary failure of all the circuit pumps are worse than the consequences of a single pump failure (partial or complete). Therefore, the former event will be analyzed rather than the latter. The consequences of this event must be accurately quantified in order to understand if they are acceptable (hence, the classification of the event as an incident can be kept) or if they must be reduced through modifications of the design (e.g. eliminating the CCF) or though preventive or mitigative actions to be included into the project. It is important to highlight that the pumps are equipped by a flywheel that allows a slow reduction of the fuel flowrate, rather than an abrupt stop, noting that this applies in case of spurious stop or failure of the pump. On the other hand, all the events implying the rupture or the blockage of the pump cannot profit of this inertia; therefore, they are considered more severe, due to the rapid transient. Different initiators are identified, e.g. broken pieces of the fuel circuit carried through the pump, or the distortion of the fuel circuit geometry. These events are considered less frequent than the failure of one or several pumps; hence, they are classified as accidents. Since at the current stage of the design and of the deterministic analyses it is hard to understand the differences between the blockage and the rupture of the pumps, the associated PIE is "rupture or blockage of one or several fuel circuit pumps". As before, a proper analysis for the identification of plausible CCF causing the contemporary rupture/blockage of all the fuel circuit pumps has not been performed yet. Nevertheless, the partial loss of fuel flow, classified as an accident, is distinguished by the total loss of fuel flow, classified as a limiting event. This classification is based on engineering judgement.

Moreover, the event "Blockage of one or several sectors of fuel salt circuit" is classified as a PIE. This is an example of possible excess of detail in the definition of the PIEs list; in fact, it is possible that in a later stage of the analysis the PIEs "Rupture or blockage of one or several fuel circuit pumps" and "Blockage of one

or several sectors of fuel salt circuit" will be merged together. Also in this case the blockage/rupture of one sector is distinguished from the event "Blockage of all sectors of fuel salt circuit" that in this analysis is classified as a limiting event.

For all the events previously mentioned, the role of the natural convection must be clearly defined relying on detailed deterministic simulations and experimental campaigns.

The event "Detachment of the thermal protection" is not considered a PIE for the family "Loss of fuel flow", but it will be selected inside the families "Reactivity insertion" and "Fuel circuit structures over-heating".

For the event "Fuel salt freezing scenario", no explicit causes are identified; nevertheless, this event is kept in the list since it can be interesting from a phenomenological point of view and it can result fundamental for the reactor dimensioning.

This analysis allowed identifying a certain number of events to be analyzed through DPAs for the safety demonstration. In the next paragraph, the PIEs for each family are presented, without the reference to the complete list of initiators.

Results

The next paragraphs list the selected PIEs, which are considered the most representative accident initiators in terms of frequency of occurrence and radiological consequences. The PIEs are presented by family of phenomena and then, inside each family, by category of frequency.

F1: Reactivity Insertion

The events listed in this family challenge one of the safety function "control the chain reaction". The reactivity variations can be caused by modifications of the fuel composition/density, of the core geometry and of the temperature of the fuel salt. It is important to notice that the events related to the variation of the heat extraction are treated in the families "Increase/Decrease of heat extraction" (F3/F4), the former causing a positive reactivity insertion, the latter causing a reactivity reduction. The events are listed in table 5-4.

Table 5-4 List of PIEs of the family F1 (Reactivity insertion)

Category	PIE
Incident	• Limited precipitation of fissile matter on cold parts and release in core • Involuntary/excessive addition of the fuel salt • Addition of fuel salt with a too high concentration of fissile matter • Addition of too cold fuel salt • Failure/spurious shut down of the bubbling system • Fuel circuit structures over-cooling • Fertile salt over-cooling • Insufficient addition/ involuntary removal of fuel salt - negative reactivity insertion • Addition of fuel salt with a too low concentration of fissile matter - negative reactivity insertion • Addition of too hot fuel salt - negative reactivity insertion • Too high bubbles injection - negative reactivity insertion
Accident	• Detachment of the thermal protection • Incorrect fuel salt composition (too high amount of fissile mater) and/or too fast loading • Addition of fuel salt in the fertile blanket
Limiting event	• Important deformation of the fuel circuit leading to an increased core volume (e.g. fall of a sector, deformation of fertile blanket wall, etc...) (PIE-FM-12) • Fertile blanket loading with fuel salt • Fuel salt freezing scenario • Bulk precipitation of fissile matter (e.g. inlet of water)

F2: Loss of Fuel Flow (LOFF)

This family has already been discussed in the previous paragraph where the method has been described. The events are reported in table 5-5 for the sake of completeness.

Table 5-5 List of PIEs of the family F2 (Loss of Fuel Flow)

Category	PIE
Incident	• Failure of one or several (up to all) fuel circuit Pumps
Accident	• Blockage of one or several sectors of fuel salt circuit • Rupture or blockage of one or several fuel circuit pump

Limiting event	• Fuel salt freezing scenario • Rupture or blockage of all fuel circuit pumps (PIE-FM-10) • Blockage all sectors of fuel salt circuit

F3: Increase of Heat Extraction/Over-cooling (OVC)

The major effect of the increase of heat extraction may be the overcooling of the fuel salt. Due to the feedback reaction, it implies a positive insertion of reactivity, therefore an increase of temperature. The major risks associated to the events of this family are:

- Too high temperature in the hot leg (especially inside the heat exchanger, where there is no thermal protection);
- Too low temperature in the cold leg, with the possibility of localized fuel salt freezing.

The PIEs associated to this family are listed in table 5-6.

Table 5-6 List of PIEs of the family F3 (Increase of Heat Extraction/Overcooling)

Category	**PIE**
Incident	• Over-working of one or several (up to all) fuel circuit pumps (PIE-FM-17) • Overworking of one or several (up to all) intermediate circuit pumps (PIE-FM-19) • Over-cooling at conversion circuit level (PIE-M-18) • Over-cooling of the structures cooling system • Over-cooling of the fertile blanket cooling system
Accident	• Over-cooling at loading or at low power

The overcooling of the fuel salt can be caused by the increase of the flowrate of the fuel salt or of the intermediate salt, due to an overworking of the fuel circuit pumps or of the intermediate circuit pumps. This implies a more efficient heat exchange between the fuel circuit and the intermediate circuit. Moreover, a malfunction of the BoP can cause an overcooling of the intermediate circuit, which influences the fuel circuit temperatures. The BoP cooling fluid has not been defined yet, so it is not possible to better detail this point.

In addition, an overcooling of the structures and fertile blanket cooling circuits can affect the fuel circuit temperatures, even if, at this point of the study, the effects are considered weak. However, further analyses are necessary to confirm this point, therefore the event is kept in the list of table 5-6.

The case of overcooling at low power is considered more severe, since there is more potential for overcooling at this state.

F4: Decrease of Heat Extraction

The events listed in this family challenge one of the safety function "The control of heat removal to an ultimate heat sink". It is important to notice that in this section are considered only the events related to the circuits cooling the fuel salt (i.e. the intermediate circuit and the BoP). The phenomena linked to the loss of fuel salt flow are considered in the family "F2: Loss of Fuel Flow".

The PIEs associated to this family are listed in table 5-7.

Table 5-7 List of PIEs of the family F4 (Decrease of Heat Extraction)

Category	PIE
Incident	• Loss of heat extraction at conversion circuit level • Unwanted closure of a valve/gate in the intermediate circuit • Failure/shut down of one or several (up to all) intermediate pumps • Loss of main heat sink (water)
Accident	• Inadvertent opening of a draining valve of the intermediate circuit • Leakage of the intermediate salt outside core vessel, in reactor vessel or reactor building (e.g. pipe rupture) (PIE-M-20) • Rupture/blockage of one or several (up to all) intermediate circuit pump (PIE-M-21) • Obstruction/Blockage of the intermediate circuit (e.g. freezing in conversion HX)
Limiting event	• Complete loss of the intermediate salt (e.g. complete draining, large breach) of all intermediate circuit

The loss of heat extraction can be caused by the loss of flow of the intermediate circuit. It can be due, for example, to the failure of one (or several) pump of the intermediate circuit, the spurious closing of an intermediate circuit valve, the obstruction of the intermediate circuit (e.g. because of a freezing in the heat exchanger between the intermediate circuit and the BoP or accumulation of corrosion products). Consequently, the heat exchange decreases up to the point where the temperatures of the fuel salt and the intermediate salt are equal. Then, both the temperatures increase. As discussed for the family "F2: Loss of Fuel Flow", the rupture/blockage of the pump is more severe than the failure, due to the loss of inertia ensured by the flywheel. In the case of pump failures, the role of the natural convection must be analyzed. As reported in the design description, paragraph 5.1, there are four intermediate circuits, therefore all the mentioned events regard only one circuit. On the other hand, the heat extraction from the fuel circuit can be zeroed in the case of complete loss of the intermediate salt (e.g. because of a spurious draining of the intermediate circuit or a catastrophic breach). This event involves all the four circuit. Its frequency is preliminary judged low enough to be classified as a limiting event.

Moreover, the loss of heat extraction can be caused by a loss of flow in the BoP or a loss of the ultimate heat sink. The components constituting these systems are non safety-relevant components, therefore their failure rates imply that the related initiating events are classified as incidents. The consequences of these events will be evaluated by future studies in order to understand if mitigating measures will be necessary (e.g. an emergency cooling system for the intermediate circuit alternative to the BoP).

F5: Loss of Fuel Circuit Tightness

The PIEs associated to this family are listed in table 5-8.

Table 5-8 List of PIEs of the family F5 (Loss of Fuel circuit tightness)

Category	**PIE**
Incident	• Spurious opening or failure to close the gate isolating the fuel circuit from the fuel salt sampling system • Spurious opening or failure to close the gate allowing the routine fuel salt draining

Accident	• Fuel salt leak – Spurious draining of the fuel circuit to the EDS • Fuel salt leak - Unwanted draining to storage tank • Rupture of a routine draining pipe • Rupture of the lower reflector (with rupture of the structure cooling system) (PIE-F-4) • Rupture of the upper reflector with possible damage to the structure cooling system and/or to the expansion vessel system (PIE-F-1/2) • Rupture of the fuel circuit in the gas part (e.g. fuel circuit lid) (PIE-F-5) • Rupture of the connection between the free surface of the EDS and the free surface of the core for the gas • Rupture of a heat exchanger plate/channel between the fuel circuit and the intermediate circuit (PIE-F-6) • Rupture of blanket tank wall between fuel and fertile salt with or without rupture of the structures cooling system. (PIE-F-7) • Rupture of the bubble injector of the bubbling system for fuel salt purification (PIE-FM-14) • Rupture of the gas processing unit (with possible leak of processing fluid) • Fuel salt leak - Rupture of the core vessel • Abnormal fuel salt inlet in the gas processing unit (through gas separation chamber) e.g. rupture of gas separation chamber (PIE-F-16)

The events of this family regard all the components in contact with the fuel salt in normal operation during power production:

- The pressurized sampling device: the "spurious opening of the gate isolating the fuel circuit from the fuel salt sampling system" can cause the exit of the gaseous FPs from the first barrier to the second barrier. Since this event is linked to the failure rate of a valve, it is classified as an incident.
- The routine fuel draining tanks: the "Spurious opening or failure to close the gate allowing the routine fuel salt draining" can cause, as before, the exit of the gaseous FP from the first barrier to the second barrier. Since this event is linked to the failure rate of a valve, it is classified as an incident. Other examples are the "Unwanted draining to storage tank" and the "Rupture of a routine draining pipe". The former event is interesting since the normal operation shutdown procedure foresees that the fuel salt remains in-core for

a while; in fact, the routine draining tanks are not dimensioned for evacuating the decay heat during the first phases after the stop of the chain reaction. The latter event is interesting since it does not involve a loss of salt until the routine draining process is trigger; thus highlighting the importance of the failure detection.

- The emergency draining system: for example, the "Spurious draining of the fuel circuit to the EDS" does not imply the exit of the fuel from the first barrier. On the other hand, the event "Rupture of the connection between the free surface of the EDS and the free surface of the core for the gas" involves the exit of the gaseous FPs from the first barrier to the second barrier. Both these events are classified as accidents by experts' elicitation. Several check-valves can be foreseen to mitigate the consequences of this IE.

- The online bubbling system: the events "Rupture of the bubble injector of the bubbling system for fuel salt purification" and "Abnormal fuel salt inlet in the gas processing unit (through gas separation chamber)" can imply the entry of the fuel salt into the bubbling system, and thus its degradation. Conversely, the event "Rupture of the gas processing unit (with possible leak of processing fluid)" can involve the exit of the processing fluid and its mixing with the fuel salt. Therefore, to demonstrate the compatibility of these fluids is fundamental. It is worth to note that the consequences of these events never cross the first barrier since the bubbling system and the gas process unit are entirely located inside it.

- The heat exchanger: the event "Rupture of a heat exchanger plate/channel between the fuel circuit and the intermediate circuit" implies the mixing of the fuel salt and the intermediate salt (also in this case the chemical compatibility of these two fluids needs to be ensured). The circulation of the salts helps the mixing process and the diffusion of the FPs in the intermediate circuit. The higher pressure of the intermediate salt with respect to the fuel salt delays the exit of the fissile matter from the first barrier, giving a certain grace time for the accident managing. The implementation of check valves can help limiting the effects of the failures to the involved sector, mitigating the consequences.

- The fertile blanket: the event "Rupture of blanket tank wall between fuel and fertile salt with or without rupture of the structures cooling system" involves the mixing between the fissile and fertile salt. As described in the previous paragraph, the fertile blanket pressure can be higher than the fuel

circuit, in order to maintain the fissile matter in-core. Nevertheless, fertile blanket is still inside the first barrier. Remembering that the fertile blanket has to be cooled down, it is relevant to consider the case if the rupture involves also the cooling structures, with a consequent mixing of the fuel salt, the fertile salt and the intermediate salt and the escape of the radioactive matter from the first to the second barrier.

- Structures of the fuel circuit: the consequences of the events of failure of the fuel circuit structures depend on the dimension of the breach. In case of a large breach, the fuel is drained in direction of the EDS, therefore the consequences are the same as the event "Spurious draining of the fuel circuit to the EDS", with a possible escape of the gaseous FPs; conversely, in the case of a small breach, the fuel salt can freeze in contact with the air and thus cover the failure. Moreover, if the failure happens in the lower reflector, it can involve also the structure cooling system, with consequences analogous to the one described in the previous paragraph. If the failure happens in the upper reflector, it can affect also the expansion vessel and the pressurized sampling device.

It is worth to note that, in all the considered cases, the radioactive products never exit from the second barrier. In many cases the fuel is drained in the EDS, where it is supposed to be in case of accident. Some IEs involve the mixing of fluids: this is a theme of research inside the SAMOFAR project, where the team focusing on the chemical risks works on the identification of the proper materials and fluids, also according to the reciprocal compatibility in case of accident.

F6: Loss of Fuel Composition/Chemistry Control

The events included in this family can affect the critical composition/temperature, produce unexpected chemical reactions, and worsen the corrosion processes.

The PIEs associated to this family are listed in table 5-9.

Table 5-9 List of PIEs of the family F6 (Loss of Fuel Composition/Chemistry Control)

Category	PIE
Incident	• Inability to control and adjust the fuel salt composition (via sampling system and reprocessing unit) • Failure of the system measuring the redox-potential • Failure/shut down of the bubbling system • Incorrect management of fuel composition in reprocessing unit

	• Release of particles (HX, filters, etc.) • Inlet of impurities in small quantities impacting redox potential (e.g. Fe3+, tracks of oxygen or humidity)
Accident	• Rupture of the gas processing unit (with possible leak of processing fluid) • Obstruction/blockage of the bubbling system for fuel salt purification (PIE-F-13)
Limiting event	• Inlet of water • Draining/inlet of the fuel salt in a tank containing water

The event "Inability to control and adjust the fuel salt composition (via the sampling system and the reprocessing unit)" makes the total inventory of fissile matter decrease and the FPs inventory increase, modifying the composition of the salt and consequently departing from criticality. Nevertheless, this process is slow because compensated by the breeding of Th-232. The event "Incorrect management of fuel composition in the reprocessing unit" can insert fuel salt with a too high or too low fissile concentration. The event "Failure/shut down of the bubbling system" makes the FPs inventory increase. The "Release of particles" (e.g. precipitates' clusters or corrosion products) can cause the local variation of the fuel salt composition.

The events involving the mix of different fluids impact the reactivity level, because of the composition modification. Moreover, the chemical compatibility of the missing fluids must be evaluated. The fluids that can potentially enter in the fuel circuit are:

- The fertile salt: since it is of the same nature as the fissile salt, the two are compatible; hence, no chemical reactions are expected but an effect on the system reactivity is anyway expected.
- The intermediate salt: even if the intermediate salt composition is not definitive, the plausible choices are all compatible with the fuel salt; further studies may be necessary to study its behavior at higher temperatures (i.e. the intermediate salt temperature increases when in touch with the fuel salt, with possible dissociation phenomena, to be further analyzed).
- The purifying fluid: even if this fluid has not been defined yet, a proposition is to use lead (as for the MOSEL concept, see (Kasten, 1964)). Lead and the fuel salt cannot mix; therefore, two separate phases will be formed. Moreover, the Pb density is higher than the fuel salt density; hence, it will descend

in the bottom part of the fuel circuit. Finally, the corrosive power of the Pb increases with temperature. The long-terms effects of this corrosion must be evaluated in order to understand if the involved risks are acceptable.

- Air (in particular the O_2): from chemical analysis, it has been demonstrated that the fuel salt does not react in contact with air. Therefore, this is not considered a PIE.
- Water: from chemical analysis, it has been shown that the fuel salt reacts with water producing HF and oxides of uranium and thorium, with a risk of vapor cloud explosion. The events involving a reaction between the fuel salt and the water ("Inlet of water" and "Draining/inlet of the fuel salt in a tank containing water") are classified as limiting events, even if their specific causes have not been identified, yet. In order to minimize the probability of these events, alternative EDS cooling solutions are explored.

The corrosion phenomenon is mainly driven by the redox potential. The IEs impacting it are "Failure of the system measuring the redox-potential", "Inlet of impurities in small quantities impacting redox potential (e.g. Fe^{3+}, tracks of oxygen or humidity)", "Failure/shut down of the bubbling system", "Obstruction/blockage of the bubbling system for fuel salt purification". Corrosion can challenge the integrity of the fuel circuit; therefore, corrosion detection methods should be put in place in order to optimize maintenance procedures.

F7: Fuel Circuit Structures Over-Heating

The PIEs associated to this family are listed in table 5-10.

Table 5-10 List of PIEs of the family F7 (Fuel Circuit Structures Over-Heating)

Category	**PIE**
Incident	• Failure of the circuit cooling down the structures (Obstruction, pump failure/rupture, etc.)
Accident	• Detachment of the thermal protection

The IEs considered for this family are only two:

- The "Failure of the circuit cooling down the structure" can have different causes, e.g. pump failure/blockage, pipe obstruction, etc. The structures

cooling circuit is not completely described, yet; nevertheless, this transient is expected to be slow due to the inertia of the system;

- The "Detachment of the thermal protection" can challenge the structures, especially in the location where the detachment actually occurs. A higher coolant flowrate must be foreseen to compensate the loss of this protection.

F8: Loss of Cooling of Other Systems Containing Radioactive Materials

The elements containing radioactive matter are the fertile blanket, the gas processing unit and the fuel salt reprocessing unit. These components must evacuate the decay heat (safety function). Among these systems, the decay heat associated to the gas processing unit is the highest. Nonetheless, the cooling of all the systems must be ensured. For example, the loss of cooling of the fertile blanket can be caused by the failure/rupture of a fertile circuit pump, the obstruction of the fertile circuit, etc.

The PIEs associated to this family are listed in table 5-11.

Table 5-11 List of PIEs of the family F8 (Loss of cooling of other systems containing radioactive materials)

Category	**PIE**
Incident	• Loss of Fertile salt cooling – Failure/rupture of the fertile circuit pump. • Loss of Fertile salt cooling – Failure of the circuit cooling down the fertile blanket (obstruction, pump failure/rupture) • Loss of Gas processing cooling – failure of the cooling circuit for the gas processing unit

F9: Loss of Containment of Radioactive Materials in Other Systems

The events of this family are associated to the same components containing radioactive matter and treated in the previous paragraph about "F8: Loss of Cooling of Other Systems Containing Radioactive Materials". These systems must guarantee the integrity of the circuit (second safety function). In addition, all the systems dedicated to the handling and re-processing of the fissile salt, the fertile blanket and gas have to be considered. It is worth to note that the consequences of these events are limited by the small quantities reprocessed daily (e.g., 40 liters of fuel salt).

The PIEs associated to this family are listed in table 5-12.

Table 5-12 List of PIEs of the family F9 (Loss of containment of radioactive materials in other systems)

Category	PIE
Incident	• Spurious opening or failure to close the gate isolating the fertile circuit from the fertile salt sampling system
Accident	• Rupture of the fertile salt sampling system • Rupture of the fuel salt sampling system • Rupture of a pipe of the intermediate circuit (outside core). • Rupture of the heat exchanger between the fertile circuit and its cooling circuit • Rupture of a fuel salt storage tank • Rupture of a fertile salt storage tank • Rupture of the gas sampling system

For the fertile blanket, the considered events are “Spurious opening or failure to close the gate isolating the fertile circuit from the fertile salt sampling system” and “Rupture of the heat exchanger between the fertile circuit and its cooling circuit”: analogous events are considered for the fuel salt circuit (see PIEs of family “F5: Loss of Fuel Circuit Tightness”). In particular, the second event implies the mixing between the fertile salt and the intermediate salt, hence the diffusion of the fertile blanket radioactive matter present into the intermediate circuit. Also in this case, the fact that the intermediate circuit is at a higher pressure than the fertile salt can mitigate the consequences.

Since the bubbling system is entirely in-core, the events of “Loss of Containment” of this system are already considered in the family “Loss of Fuel Circuit Tightness” and do not involve the failure of the first barrier. The failure modes of the gas process unit will be object of analysis of a forthcoming research project financed in the frame of the H2020 Programme, called SAMOSAFER.

The intermediate salt is constantly subject to neutron irradiation; therefore, its activation must be evaluated. The event “Rupture of a pipe of the intermediate circuit (outside core)” considers the loss of activated intermediate salt: this is interesting since it can occur at any point of the intermediate circuit, also in the heat exchanger between the intermediate salt and the BoP coolant. In the reference design, this component is located inside the reactor building, but other proposals place it

outside the reactor building, in order not to have a high-pressure component in the same building of the core. In this latter case, the considered event will cause a loss of radioactive material outside the reactor building.

Similar considerations are valuable for the fissile and fertile salt storage tank, since their position has not been defined univocally. In the reference design, they are located inside the reactor building, but it is possible that they will be placed in a dedicated unit. The related IEs "Rupture of a fuel salt storage tank" and "Rupture of a fertile salt storage tank" can produce their consequences inside or outside the reactor building according to the design evolution.

F10: Mechanical degradation of the fuel circuit

The mechanical degradation of the fuel circuit can cause the rupture of other components or structural elements and challenge the integrity of the fuel circuit (first barrier). It is generally due to pressure variations and erosion phenomena.

The PIEs associated to this family are listed in table 5-13.

Table 5-13 List of PIEs of the family F10 (Mechanical degradation of the fuel circuit)

Category	**PIE**
Incident	• Abnormal flowrate/pressure fluctuations
Accident	• Blockage of fuel circuit pump • Water hammer (or "salt hammer") in the fuel circuit • Presence of solid elements in the fuel circuit (extraneous elements, broken pieces of fuel circuit components, agglomeration of element etc.)
Limiting event	• Shock wave produced by prompt criticality

Among the pressure effects, the considered events are:

- "Abnormal flowrate/pressure fluctuations", which impose mechanical constraints on structures and components and can be caused by pumps malfunction or reactivity oscillations;

- "Water hammer (or "salt hammer") in the fuel circuit", which can be caused, for example, by the blockage of fuel circuit pump/sector;
- "Shock wave produced by prompt criticality", in fact, the increase of power induces the increase of temperature, which cause the dilation of the fuel and pressure increase.

Among the erosion effects, the considered event is "Presence of solid elements in the fuel circuit (extraneous elements, broken pieces of fuel circuit components, agglomeration of element etc.)".

F11: Loss of Pressure Control in the Fuel Circuit

Even if the fuel circuit is at ambient pressure, it is a closed system; therefore, in this family, all the events causing loss of pressure control in the fuel circuit are listed. In particular, the loss of control of the pressure of the fuel circuit is caused by the unavailability of the free levels causing the increase of pressure of the fuel salt.

The PIEs associated to this family are listed in table 5-14.

Table 5-14 List of PIEs of the family F11 (Loss of Pressure Control in the Fuel Circuit)

Category	**PIE**
Incident	• Abnormal flowrate/pressure fluctuations • Obstruction of the gas outlet pipes from expansion vessel
Accident	• Rupture of the expansion vessel • Gas sampling system discharge in fuel circuit • Obstruction of the vertical inlet pipe for the fuel from the core to the expansion vessel (PIE-F-8)
Limiting event	• Obstruction of all free levels • Inlet of water in the fuel circuit • Draining/inlet of the fuel salt in a tank containing water

As reported in paragraph 5.1, in the fuel circuit different free levels are foreseen, all connected. Therefore, the pressure of the gaseous phase at the free level has to be continuously monitored. Different IEs modify the geometry of the free level and reduce their availability, e.g. "Obstruction of the gas outlet pipes from expansion vessel", "Rupture of the expansion vessel", "Obstruction of the vertical inlet pipe for the fuel from the core to the expansion vessel". The prevented fuel

salt dilation will cause an increase of the fuel salt pressure. The "Obstruction of all free levels" is classified as a limiting event; in fact, in this case an important increase of pressure, due to an important increase of temperature will not have the necessary space to evolve. The consequences of this event must be analyzed in detail.

Some of the identified IEs cause an increase of fuel salt pressure: "Gas sampling system discharge in fuel circuit", "Inlet of water in the fuel circuit" and "Draining/inlet of the fuel salt in a tank containing water". For the first event, the increase of pressure is due to the production of gaseous FPs. For the other two events, the increase of pressure is due to the chemical reactions between the fuel salt and the water, already explained for "F6: Loss of Fuel Composition/Chemistry Control".

Some of the listed events challenge the integrity of the fuel circuit; hence, the exit of the radioactive matter from the first to the second barrier.

F12: Conversion circuit leak

The PIEs associated to this family are listed in table 5-15.

Table 5-15 List of PIEs of the family F12 (Conversion circuit leak)

Category	PIE
Incident	• Small leakage of the HX between the intermediate circuit and the energy conversion circuit • Leakage of the conversion fluid in/out of the reactor building (e.g. pipe rupture)
Accident	• Large leak of the heat exchanger between the intermediate circuit and the energy conversion circuit • Large breach of the conversion fluid in/out of the reactor building (e.g. pipe rupture)
Limiting event	• Ejection of a conversion circuit component (PIE-M-24)

IT must be stressed that the BoP design is still conceptual and no details are provided about this unit. Therefore, only very qualitative considerations can drive the analysis. For example, it is chosen to distinguish the small breach (that are considered frequent, therefore classified as incidents) from the large breaches (that are

considered less frequent, therefore classifies as accidents). Any breach on this circuit implies the loss of the heat sink, which is a safety function. Moreover, the BoP fluid has not been selected, yet: different fluids are proposed: helium, supercritical CO_2, supercritical water. Since the event "Small leakage of the HX between the intermediate circuit and the energy conversion circuit" implies the mixing between the BoP fluid and the intermediate salt, analyses of chemical compatibility must be performed. In addition, the BoP will be in pressure, while the intermediate salt is only weakly pressurized; hence, this kind of failure increases the intermediate circuit pressure. In case of a breach on the pipes entering the intermediate salt/BoP coolant heat exchanger, the component position results fundamental. In the reference design, it is inside the reactor building, which can be pressurized in case of failure.

Lastly, the high pressure of the BoP can cause the ejection of a component that can hit other components. During the safety demonstration of the MSFR, it is fundamental to demonstrate that this projectile can never affect the fuel circuit.

F13: Loss of electric power

The PIEs associated to this family are listed in table 5-16.

Table 5-16 List of PIEs of the family F13 (Loss of electric power)

Category	PIE
Incident	• Loss of electric power (grid)
Accident	• Total loss of power supply (PIE-M-22)

The consequences of these IEs are generally summarized as the spurious stop of all the pumps (fuel circuit, intermediate circuit, BoP). The event "Total loss of power supply" implies the loss of all the electrical systems (normal operation systems and protection systems). In the safety report, this is usually divided according to the duration of the event. In the case of this analysis, it is not possible to perform detailed analyses since the electrical systems are not designed yet.

5.2.6 Considerations

These methodologies can be iteratively applied, following the design development; similarly, the lists of the PIEs evolve with the detail of the design and the

investigation of the physical phenomena governing the behavior of the system, through deterministic analyses.

It can be noted that many events identified with the first approach (FFMEA) also appear with the second approach (MLD). Most of the time, these events are classified in the "limiting event" or "accident" categories. The list of PIEs obtained with the second method takes into account these events but also the events with high occurrence frequency and low expected consequences. This list has been used to perform the next steps of the safety analysis that are presented in the following sections.

In the next steps of the safety analysis, each identified PIE has to be discussed outlining the possible accidental sequences and deterministic analyses shall be performed to verify the plant capacity to mitigate the consequences, to check the compliance with safety limits and to drive the choices for the selection of the reference design.

Annex A contains a list of open points (about systems, components, procedures, phenomena, etc.) that have been highlighted as a complementary result during the implementation of the FFMEA and the MLD for the compilation of the list of PIEs.

5.3 Identification of Safety provisions: LOD application to the MSFR

5.3.1 LOD application for MSFR in the context where no severe accident is clearly defined at this stage

The LOD method has been applied to some PIEs judged relevant for the MSFR analysis.

Cliff-edge effects studies allowing to precisely define severe accident and situations to be practically eliminated for a MSFR, are still on-going and to be further continued. The following approach is thus employed in the first place:

- Identification of the most relevant initiating events (i.e., those who have the potential for major changes in the fuel circuit in terms of neutronic, chemistry, thermal hydraulic, mechanics…)

- Preliminary assessment of their consequences in the absence of any safety limitation feature, on the basis of previous studies, and considering on-going calculations in the SAMOFAR project,

- Preliminary allocation of the lines of defence in function of the expected consequences. The following preliminary allocation is proposed :

    - Sequences or situations which could significantly impair the reactor availability (meaning quick restart is not possible following the event), or which could lead to limited radiological releases but significantly exceeding normal operation releases (and order of magnitude could be value up to but below 1 mSv per event), should at least be prevented by one medium line of defence (b),

    - Sequences or situations which could significantly impair the reactor investment (meaning for example significant and expensive repair may be needed, with in some case uncertainty on the ability to restart the reactor), or which could lead to significant radiological releases but with no need for off-site confinement measures (and order of magnitude could be value up to but below 10 mSv per event), should at least be prevented by one strong line of defence (a),

    - Sequences or situations which could threaten safety, with potentially important radiological releases (which may need limited off-site measures such as confinement or even more significant measures) should at least be prevented by two strong and one medium lines of defence (2·a+b).

In the application of the LoD method, it is pointed out that input data regarding natural behaviour following the initiating events, with a preliminary evaluation of expected radiological consequences, is key to be able to define the required number of safety provisions. For the SAMOFAR project, the process should thus be iterative and the safety architecture refined as the evaluation of the MSFR natural behaviour and potential for radiological releases is assessed into more details.

5.3.2 Guidelines for practical MSFR studies

The occurrence frequency of an **incident** may be considered as an initial medium line of defence (if the equipment whose failure initiated the incident has a

failure rate in the 10^{-1}-10^{-2} /reactor·year range) or no line of defence at all. If the occurrence of an incident corresponds to a "b" (medium line of defence), then the following number of lines of defence are required for the limitation of its consequences:

- No additional line of defence strictly required if there are availability concerns only. Limited radiological releases may occur: the interest of additional LoD should still be studied here in an ALARP approach,

- At least one medium line of defence "b" with regard to investment concerns and risk of significant radiological releases,

- At least two strong lines of defence "2a" with regard to potentially important radiological releases.

The occurrence frequency of an **accident** may be considered as an initial medium line of defence (if the equipment whose failure initiated the accident has a failure rate around 10^{-2} /reactor·year) or a strong line of defence (if the equipment whose failure initiated the accident has a failure rate around 10^{-3}-10^{-4}/reactor·year). This second case is typical for active systems designed in accordance with the standards of the nuclear industry and comprising internal redundancies; or passive equipment, exploited like confinement barriers, designed in accordance with the standards of the nuclear industry (e.g., see the strong LoD definition).If the occurrence of an incident corresponds to an "a" (strong line of defence), then the following number of lines of defence are required for the limitation of its consequences:

- No additional line of defence is strictly required if there are investment concerns only. Radiological releases below safety targets may occur: the interest of additional LoD should still be studied here in an ALARP approach,

- At least one strong line and one medium lines of defence "a+b" with regard to potentially important radiological releases.

In addition to accidents, very rare events may be postulated, to ensure the avoidance of cliff-edge effects in terms of radiological releases, should they occur. For such "limiting events", only one medium line of defence "b" may be considered at a first stage, while the interest to consider additional LoD may be addressed at a second stage in the frame of an ALARP approach.

Figure 5-13 sums up the proposed guidelines for the LoD first application to MSFR.

Type of event considered	Equivalent in terms of LoD crossed	Minimal criteria to be respected	Supplementary LoD strictly needed to avoid availability concerns or limited radiological releases	Supplementary LoD strictly needed to avoid investment concerns or significant radiological releases	Supplementary LoD strictly needed to avoid important radiological releases
Incident	0	No significant impact on reactor availability Releases within normal operation values	b	a	2a+b
	b (*)	No significant impact on reactor investment Only limited releases (order of magnitude is <1 mSv/event)	-	b	2a
Accident	b	No significant impact on reactor investment Only limited releases (order of magnitude is <1 mSv/event)	-	b	2a
	a (**)	No important releases (order of magnitude is <10 mSv/event)	-	-	a+b
Limiting event	~2a	Verification that there is no cliff edge effect in terms of radiological releases	-	-	b

(*) if the equipment whose failure initiated the incident has a failure rate in the 10^{-1}-10^{-2} /reactor·year range

(**) if the equipment the failure of which initiated the accident has a failure rate around 10^{-3}-10^{-4}/reactor·year range, which is typically the case for active systems designed in accordance with the standards of the nuclear industry and comprising internal redundancies; or passive equipment, exploited like confinement barriers, designed in accordance with the standards of the nuclear industry (see strong LoD definition).

Figure 5-13 Guidelines for the LoD first application to MSFR

5.3.3 General considerations

Given the very preliminary state of MSFR design and studies, a lot of assumptions must be made when applying the LoD method, such that the method cannot provide a final statement on the acceptability in terms of safety but rather helps to identify relevant safety questions that need to be further addressed.

Therefore, at this stage, the goal is not to perform a full and final safety assessment but rather to apply the LoD method on few cases, to check that the method can effectively be used for the MSFR, and put forward some relevant insights for the future safety and design studies.

The few events selected for a first application of the LoD method, are the following:

- Loss of main heat sink,
- Overcooling at zero power
    - Note: although the list of PIE identified in SAMOFAR was focused on events arising from power operation, an overcooling event starting from a zero power condition is judged more interesting as involving a larger potential for reactivity insertion
- Addition of fuel salt with too high concentration of fissile matter
- Fertile blanket loading with fuel salt
- Leak of fuel circuit (lower and upper parts)
- Leak on the intermediate heat exchanger
- Leak of fuel salt storage tank

Note: although the list of PIE identified in SAMOFAR was focused on events arising from power operation, the event of a leak when the fuel salt is in the fuel storage tank is already identified as an interesting event to be analyzed.

As regards the evaluation of consequences of events and sequences identified, it is not always possible to provide a clear conclusion concerning the risk of challenging the reactor availability, the investment protection or even the safety (e.g. no evaluation of radiological releases has been performed up to now). Engineer judgment is thus provided on some cases. Besides, there can also be an interest in

identifying events or sequences that should be given high priority for further evaluations.

To evaluate the consequences of reactor transients, a common practice is also to define decoupling criteria (e.g. in terms of temperature and/or pressure values), the respect of which should ensure that availability, investment protection or safety concerns are appropriately dealt with (e.g. as regard safety, through preservation of safety systems such as containment barriers). Such decoupling criteria are still be defined for the MSFR. Nevertheless, some orders of magnitude are preliminary given here, to be further confirmed:

During an accident, the objective is to keep the fuel circuit Hastelloy N structures below 1100°C, for material structural limits, given the risk of leak-tightness loss or even loss of integrity.

5.3.4 Loss of main heat sink event (LOHS)

Characterization of the event

The loss of heat sink could result from a failure of the BoP circuit or failure to remove heat from the tertiary circuit, so that the heat removal from the intermediate salt circuit is no longer ensured. Conservatively, it can be assumed that the heat transfer from the intermediate salt circuits to the BoP circuits immediately stops at the beginning of the event.

Prevention of the event

The loss of main heat sink event is assumed to be frequent, as it may be caused by non-safety classified equipment from the tertiary circuit or in connection with this circuit. The occurrence of this event is therefore not counted as the crossing of a line of defence.

Natural behaviour of the plant

As the loss of main heat sink occurs, heat from the intermediate salt circuit, and consequently from the fuel salt circuit is no longer removed.

The temperatures in the fuel circuit tend to homogenize, and also to rise, due to the residual heat. The intermediate loops, unless drained, act as a thermal buffer, helping to attenuate the temperature rise. The fuel circuit mean temperature increases by 150°C in about 1000 s starting from a mean fuel circuit temperature of 725°C, while it would increase by 450°C without the buffering effect of the intermediate loops. The structures may thus undergo high temperatures so that their leak-tightness can be challenged, with a loss of investment and potential safety consequences in terms of releases (Gérardin et al., 2018). The 1100°C would not be reached on the Hastelloy N surface before one hour and a half. Indeed, leak in the bottom part of the fuel circuit may occur but also in other parts of the fuel circuits, such as the interface with the fertile blanket, the upper level in interface with the upper structure cooling circuit and the intermediate heat exchanger level.

At the intermediate circuit level, salt decomposition should occur at approximately 800-850°C with the formation of gaseous BF_3 –in case fluoroborate is retained- thus leading to the pressurization of the circuit. The material retained for the intermediate circuit is not decided yet, but may not be Hastelloy N. It is thus expected that the intermediate circuit fails before the fuel circuit.

There is a special concern if there is a leak at the intermediate heat exchanger also, given the risk of siphoning of the fuel salt and of confinement by-pass. Then, the relocation of the fuel salt must be studied. Concerns associated to fuel salt heating are also related to the release of fission products, and to their confinement.

A scenario with complete and long term loss of the fuel salt heat removal function has not been studied in detail up to now. It is assumed at this stage that such scenario is likely to be unacceptable, as it would lead to an increasing fission products releases from the salt by vaporization with pressure build up, and therefore a potential for further releases into the environment.

Possible lines of defence to cope with the event

A cooling system on the intermediate loops can be actuated to cool down the fuel salt when the tertiary circuit is lost, through exchange with air by natural convection. This system may be counted as a strong line of defence (“a”), considering several independent trains are provided on the different loops.

In the case of failure to limit the temperature rise in the fuel salt circuit, an automatic draining through redundant valves opening in the lower region of the

circuit is foreseen, accounted for as a strong line of defence (“a”). It has to be checked that the draining is fast enough so that the fuel salt temperature increase before draining completion is acceptable. Draining devices should also be designed to avoid any criticality risks during the overall transient.

Additionally, fusible valves (redundant and diversified compared to the automatic valves) can besides provide passive draining, accounted for as a strong line of defence (“a”) as regard the draining. Should all valves fail, a leak in the lower part of the fuel salt circuit could also provoke the fuel sat draining.

Once the fuel salt is drained, it would still be necessary to collect it and to ensure its subcriticality as well as its cooling. To do so, an emergency draining storage is provided, with redundant cooling circuits (able to operate in natural convection, with air as heat sink: to be confirmed), accounted for as a strong line of defence (“a”).

Lastly, in the case of fuel salt relocation in the EDS and subsequent failure of the EDS, further relocation of the fuel salt in the bottom part of the building may be considered. A system equivalent to a core catcher, along with a cooling system, is under investigation, which may stand for a medium or strong line of defence, to be further studied.

It is assumed that the fuel salt recovery from the EDS can be performed to start-up the reactor again in a second time, while the fuel salt at the core catcher level is considered to be lost, due to mixing with the sacrificial salt.

Event tree using the LoD method

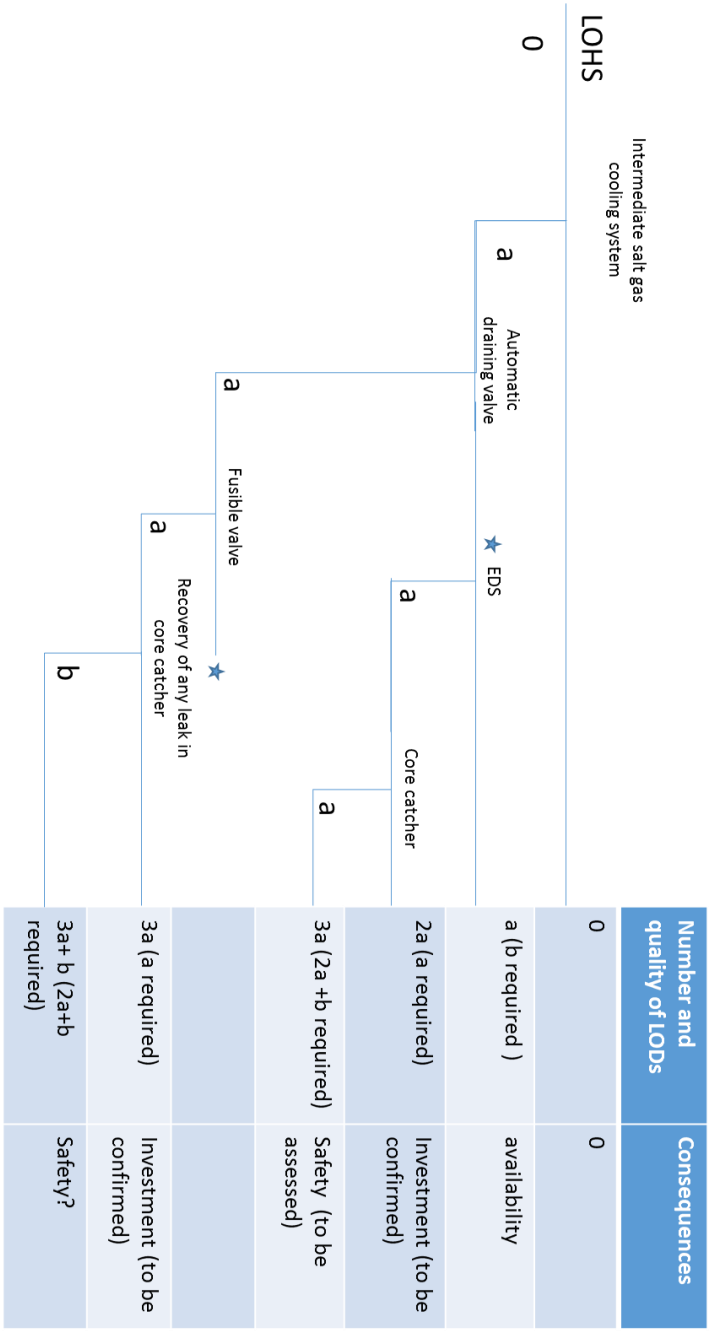

Figure 5-14 Schematic event tree of the loss of main heat sink event

Preliminary outcomes of the LoD method application

The situation where the fuel salt is drained in the EDS, with subsequent EDS failure, would need further evaluation, to check the avoidance of a cliff-edge effect. This situation may require the addition of a "core catcher" or equivalent, with a cooling circuit.

In case of failure of the tertiary circuit, only one system is considered for the fuel salt cooling in the fuel salt circuit. Should another system be considered, this could alleviate the need for both an EDS and a core catcher. More generally, the allocation of lines of defence may be different (3a at this stage could be lowered to 2a+b).

The LoD analysis performed here is very preliminary. To confirm the whole reliability of the different cooling systems, a more detailed analysis of their respective independency is needed, in order to check there is no credible common cause failure.

In the course of the accidental sequences, the risk of an IHX leak should also be further studied as it could influence the scenario, as it could be considered as a sensitivity case to check the avoidance of cliff-edge effect.

5.3.5 Overcooling event

Characterization of the event

During reactor start-up, it is assumed that both the fuel circuit and intermediate salt circuits are circulating at the mean fuel temperature of 725°C, while the heat extraction at the tertiary level suddenly increases from few kW up to nominal power. This event is preferred for the analysis as compared to the overcooling from nominal power, as it is judged more relevant as there is more potential for overcooling from a low power state.

Prevention of the event

The start-up procedure is not defined yet, for example progressive increase of the mass flow rate at the fuel salt and intermediate salt circuits' level, as reactor power is increased, may be privileged. In any case, the procedure will be such that the reactor power increase is progressive. It is assumed at this stage that the occurrence of the event is equivalent to one medium line of defence (i.e., the compliance with the start-up procedure).

Natural behaviour of the plant

Conservatively, it has been assumed in the evaluations that the cold leg of the intermediate salt is immediately cooled down at the beginning of the transient in proportion to the heat evacuated at the tertiary level. This leads to a cooling down of the fuel salt, with a positive reactivity insertion and therefore an increased reactor power. If the cold leg of the intermediate salt is lowered too rapidly, such that nominal power is evacuated after less than 30 seconds, prompt criticality can be reached. Considering instantaneous reactivity feedbacks, a prompt critical jump would be very short, such that the fuel salt temperature in the hot leg remains limited below 800°C (Laureau et al., 2017). This also implies that the fuel salt expansion, thanks to free levels in the upper part of the fuel circuit, is possible. The fuel salt temperature in the cold leg might also be lowered above the solidification point, an aspect which needs to be assessed. A prompt critical jump may also result in a pressure wave, to be verified by deterministic calculations. Should fuel salt expansion not be possible, this could result in a sustained prompt critical jump with sudden and significant energy release and pressure increase.

Possible lines of defence to cope with the event

Before reaching large reactivity insertions, detection measures can be put in place, based for example on the temperature decrease in cold leg of the fuel or intermediate circuits. The corrective measure could consist in valve closure on the intermediate circuit, to stop the heat transfer with steam generators and thus stopping the overcooling. Other measures such as an increased bubbling to lower the reactivity may also be considered. The efficiency of such measures will have to be checked, considering in particular the time constants (checking notably the possibility to detect sufficiently rapidly the event). At this stage, such measures are accounted only for a medium line of defence ‘b’, but this evaluation may be modified on the basis of further analyses.

The presence of free levels in the upper part of the fuel circuit allows to benefit from a largely negative reactivity feedback as fuel expands. It is assumed that the design, foreseeing one free level above each pump and a free level above the active core region, all communicating together, will be such that the availability of these free levels will be ensured with a high reliability, accounting for at least one strong line of defence ‘a’, or even more depending on the design evolution.

Event tree using the LoD method

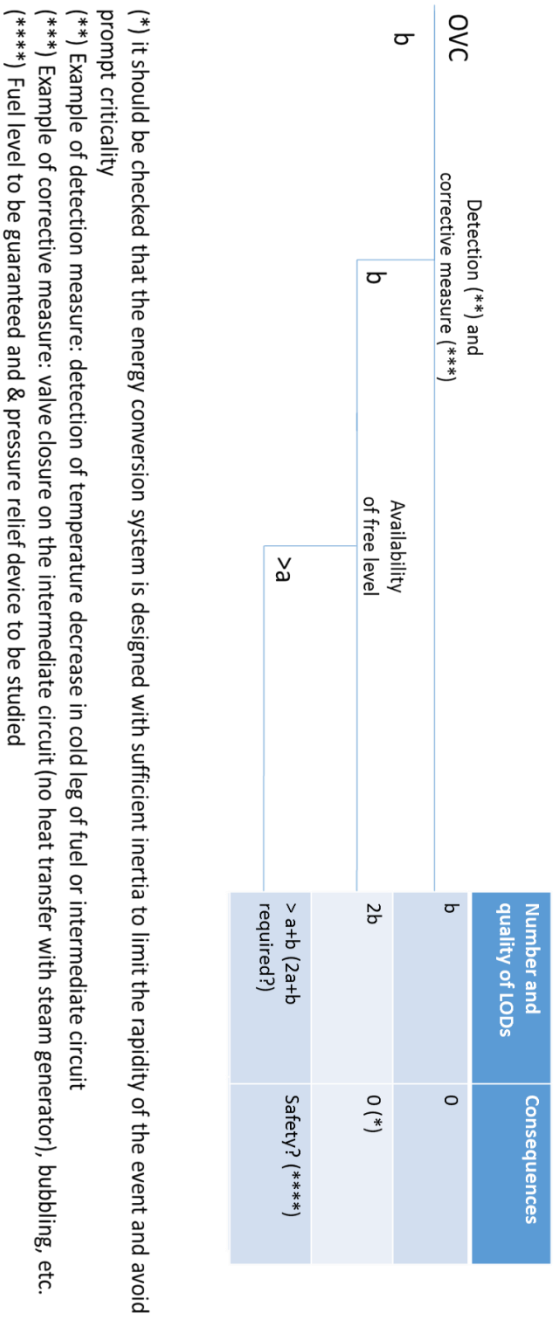

Figure 5-15 Schematic event tree of the overcooling event

Preliminary outcomes of the LoD method application

First, it should be required that the design of the reactor, and the energy conversion system in particular, and start-up procedure are such that even the worst

overcooling scenario possible evolves sufficiently slow (time constant for temperature decrease of the intermediate salt cold leg above 30 seconds).

With regard to rapid overcooling scenarios, there is an interest to look for detection and corrective measures allowing to limit the reactivity insertion, for example though valves closure on the intermediate circuit on a salt temperature decrease signal.

The availability of free levels to allow the fuel salt expansion is absolutely necessary. It may be accounted for as a strong line of defence, or even more. This point deserves to be studied more in detail: 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 IHX leak…) would be worthwhile, in order to ensure appropriate design measures are taken to ensure a very high reliability when it comes to free levels availability for fuel expansion. The interest of having pressure relief devices, should fuel expansion be limited, could also be studied.

5.3.6 Heat exchanger leak

Characterization of the event

Leak may occur at several locations depending on the intermediate heat exchanger design, typically at plate level or collectors, if foreseen. Leaks sizes are to be defined. The event studied hereafter is assumed to concern only one IHX, and therefore only one intermediate circuit out of four.

Prevention of the event

Prevention of leak basically relies on the design quality. Conservatively, a leak occurrence is assumed to be a frequent event here, with no line of defence credited. A design goal may be to sufficiently prevent the leak to make it an accidental case, then crediting the prevention of such a leak as a medium line of defence.

Natural behaviour of the plant

Should a leak on the IHX occur, the intermediate salt –which is at higher pressure- would enter into the fuel circuit. Consequently, the fuel circuit level will go up. The equilibrium level will depend on the respective pressure in both the fuel

circuit upper gas volume and the intermediate circuit gas volume. Conservative assumptions should be made regarding gas pressure regulations in both circuits. At the intermediate circuit level, two cases are possible: unavailability of the pressure gas regulation system or, on the contrary, sustained gas input in the intermediate circuit to maintain its pressure.

At some points, fuel salt may enter the gas circuits located in the very upper part of the fuel circuit, with a potential investment concern, noting however that confinement should still be ensured up to this level.

If the fuel circuit was to be completely filled with salt, with no more spaces for fuel salt expansion, it can be noted that the reactivity feedback due to fuel salt thermal expansion would no longer be available in case of reactivity transient.

In the fuel circuit, fuel salt should mix with the intermediate salt in turbulent flow areas. In case fluoroborate is retained, salt decomposition with the formation of gaseous BF_3 should still be avoided if the temperatures are below approximately 800-850°C, considering a normal core outlet temperature of 775°C.

Regarding reactivity, the lower intermediate salt temperature results in a positive reactivity insertion while the global dilution effect of the fuel salt is linked to a supposedly stronger negative reactivity effect. The power level should go down as only three loops out of four are still cooling the reactor down.

After pressure equilibrium, fuel salt diffusion toward intermediate salt may occur, thus leading to contamination of the intermediate circuit. It should be remembered that the heat exchangers with the energy conversion system may be located outside of the reactor building.

At the intermediate circuit level, a low salt level may also impact the intermediate pump, with cavitation risks.

Should a leak be induced in the fuel circuit or a draining toward the EDS be launched, then the salt mixture (with both the fuel salt and part of the intermediate salt) would enter the EDS. The EDS is currently sized to recover twice the volume of all the fuel salt, thus accounting for a capability to cope with $1/5^{th}$ on the total intermediate salt inventory (all loops). Anyway, at a certain time, the fuel salt circuit will have to be drained, a priori toward the fuel salt tanks, to allow the IHX repair

or replacement. After fuel salt draining, the IHX leak should be under gas atmosphere, with a priori low contamination potential transfer toward the intermediate loop, assuming a rather clean gas content during reactor operation (to be checked).

The above scenario would be quite different if the leaking intermediate loop was to be drained in the same time. In such case, the intermediate salt would mainly go in its dedicated tanks, together with a portion of fuel salt, with a possible siphoning effect) with a potentially much higher contamination of the intermediate circuits and decay heat to be managed at this level. There may be a concern with a potential for further radiological releases.

Possible lines of defence to cope with the event

Sector valves closure on the intermediate circuit (limitation of intermediate salt leakage, and confinement barrier recovery) upon detection could act as the first line of defence. Currently, one set of valves at each intermediate sector inlet and outlet is planned. Detection is needed upstream valves closure actuation, allowing to identify which intermediate loop is leaking. Besides measures at the fuel circuit level (e.g. salt level), it is likely that measures at the intermediate circuit level, such as pressure and/or gas inventory, will be needed. At some point, reactivity variation should be detected, but the link with the leakage and its location should a priori not be deduced from such variation. There may be an opportunity to detect a change in the salt composition, for example through on line monitoring of a small salt by-pass flow, through absorption spectroscopy, but this would not allow leaking loop identification if only made at a general fuel circuit level. Therefore, a medium line of defence is accounted for here, since more arguments are needed to take credit of a strong line of defence, considering the detection would rely on detection at the intermediate loop level (mainly gas pressure and/or inventory). Moreover, note that it may be needed to stop the intermediate pumps prior to valves closure to avoid hammer effects.

As regard the fuel salt level increase:

- Fuel salt draining should also be possible, e.g. upon detection of gas pressure elevation or free level increase in the fuel circuit. Such device might be credited as a strong line of defence.

- An overflow system may be implemented in the fuel circuit design, redirecting salt above a certain level toward the EDS. The design of such devices is still to be made, and could include a melting membrane. Such device might be credited as a strong line of defence (hypothesis made in the following).

As regard the risk of contamination in the leaking intermediate loop:

- Radioactivity detection would allow reactor vessel/building valves closure (if not made yet), possibly accounting for a strong line of defence (two sets of valves are currently planned: one set on the intermediate circuit at the reactor vessel crossing and the other one at the reactor building crossings).
- Fuel salt draining may besides further prevent the risk of fuel transfer toward the intermediate loop (only gas transfer could occur after draining).

Event tree using the LoD method

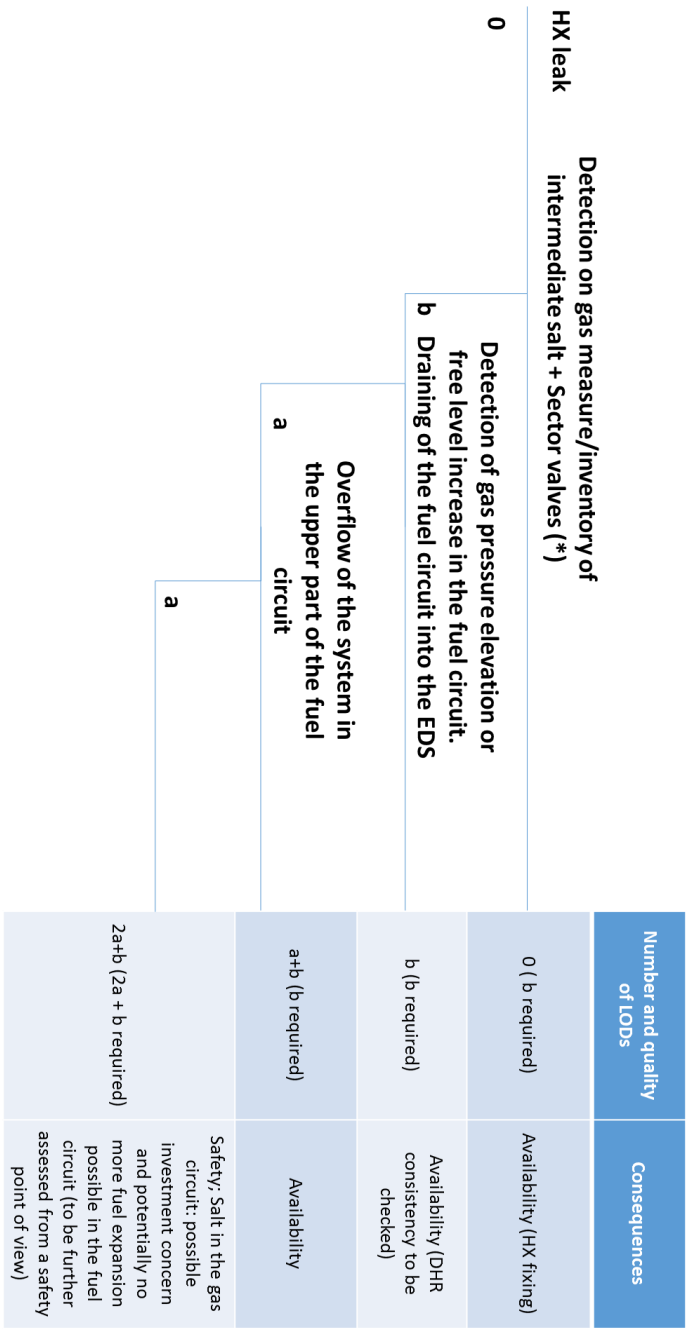

Figure 5-16 Schematic event tree of Heat Exchanger Leak event (fuel salt level increase)

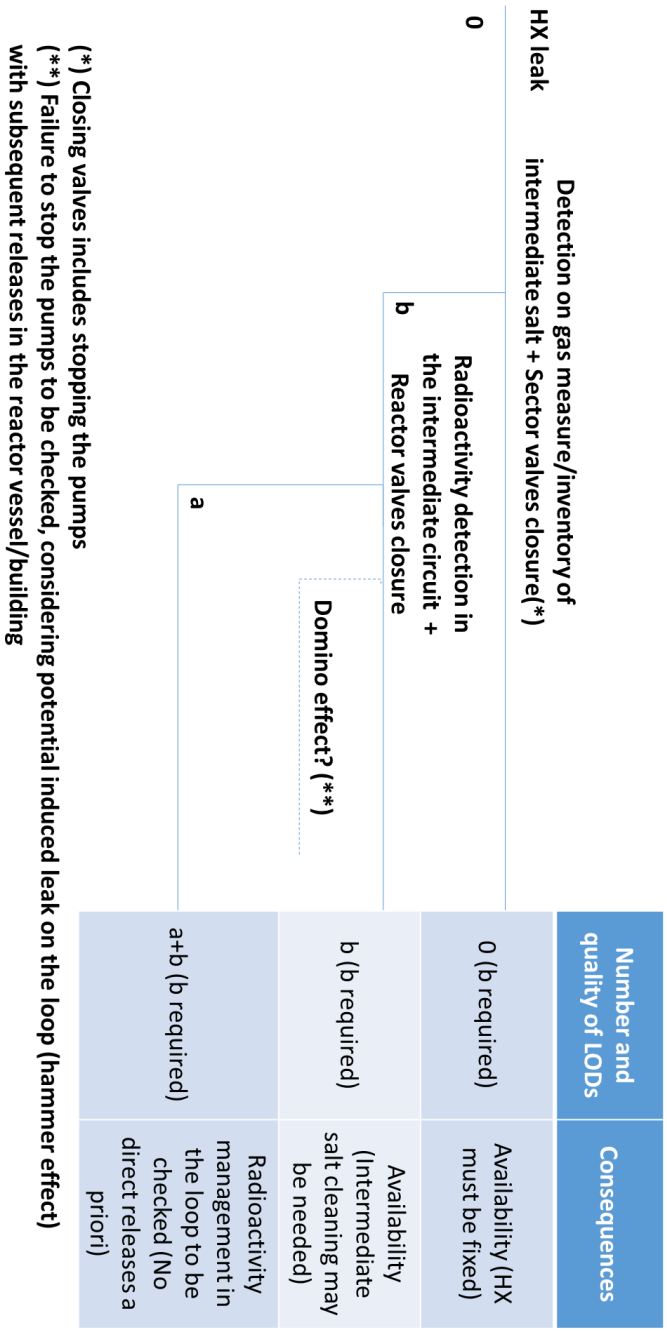

Figure 5-17 Schematic event tree of Heat Exchanger Leak event (Contamination risk)

Preliminary outcomes of the LoD method application

From a confinement point of view, the benefit of having several sectors is not strongly put forward here. In case of sectors valves closure, this would of course

allow to limit the amount of intermediate leaking salt. Nevertheless, unless the detection allows to identify which sector is leaking, the four sectors of a given loop would have to be closed.

Possibility to arrange efficient detection of free level variation in the fuel circuit should be further studied, as well as an overflow passive system.

Sufficiency of DHR systems for long term accident management should be checked, as regard fuel salt relocation in the EDS (at least a strong line of defence aimed at in the loss of heat sink event, before relocation of fuel salt in the EDS). A deeper focus could thus be made on the occurrence frequency of an IHX leak combined with a failure of the leak detection upon gas/inventory monitoring on the intermediate loop, this sequence being likely to lead in a second time to fuel salt draining in the EDS.

Regarding confinement issues, the need to have redundant isolation valves is confirmed. An optimisation between reactor vessel and reactor building valves may be studied, considering also that, in the end, it may be difficult to allocate more than a strong line of defence for all the valves together (sectors valves and reactor vessel/reactor building valves). The case of an IHX leak with failure to isolate the valves must be studied to confirm proper confinement management, due to the potential risk of contamination of the intermediate circuits by fuel salt or fission gas transfer.

In the isolation valves procedure, the case where the intermediate pumps would still be operating has to be checked, with the goal to avoid an induced failure / leak of the intermediate circuit, considering the risk of hammer effect.

As regard fuel salt relocation, typically in the EDS, proper volumes should be considered to allow also recovery of the additional salt volumes coming from the intermediate loop.

5.4 Considerations

5.4.1 Current safety and licensing context and changes required

The majority of current nuclear safety regulatory requirements is based on LWRs technology and necessitates changes to suit to a new spectrum of novel, advanced, next generation plants (Southern Company, 2017). In Probabilistic Safety Assessment (PSA), the risks associated with the reactor accidents are highly design, plant and site specific; this is demonstrated for any kind of reactor. In particular, dealing with next generation nuclear plants implies a much larger range of risks variability with respect to an LWR: fundamental differences in the physical processes are present, as well as in the plant responses associated with the reactor transients and accidents. This is due both to the use of different materials for the reactor fuel, moderator and coolant and to different safety design approaches for the implementation of radionuclides barriers (Southern Company, 2017). Because of these differences, the LWR risk metrics, for instance the Core Damage Frequency (CDF) and the Large Early Release Frequency (LERF), are neither relevant nor useful for many advanced nuclear reactors; some plants, in fact, may not involve the core damage state that was defined for LWR and, even in the case, its meaning and risk framework can be fundamentally different from LWR (INL, 2011). Consequently, PSA for advanced reactors may be structured differently than the traditional Level 1, 2 and 3 model for LWR PSA: it is expected to include out of core sources of radioactive material (especially in the case of online refuel, as for the MSFR) and to adopt adequate and more general risk metrics (INL, 2011); the latter may lead to an appropriate definition of severe accident, detached for the core melting concept. Additionally, while the traditional LWR risk assessment was developed following the “one-reactor-at-a-time” approach, in next generation nuclear plants the risk associated to multi-unit sites becomes certainly relevant in the safety assessment, notably after the Fukushima Daiichi accident (Fleming, 2017). Advanced non-LWRs may be constituted by several modules, located in the same site: this would imply proper evaluation of possible common cause failures/domino effects, due to the potential for sharing of systems and structures or hazards involving more than one reactor (e.g. external hazards). This could influence the traditional frequency-consequence tolerability criteria (Southern Company, 2017).

Finally, it should be bear in mind that there is no recent licensing experience of an MSR and the suitability of the existent regulations which were principally developed for light water reactors must be assessed. Safety regulations adapted to such

a concept will have to be developed and validated by the Safety authority of the country hosting the plant. However, the fundamental safety principles such as the defence in depth remain applicable but their application must be adapted.

5.4.2 Safety advantages identified for the MSFR concept

- With the liquid fuel and a fast neutron spectrum, a negative temperature feedback coefficient is obtained, whose action is immediate in the event of a salt temperature variation. This ensures an intrinsic safety with respect to reactivity accidents.
- The fuel unloading from the core zone is easier and faster as compared to the unloading of a solid fuel; this allows to maintain the salt subcritical and to cool the fuel.
- The fuel circuit is not pressurized and the fluoride salt is not likely to cause violent exothermic chemical reactions when in contact with the materials of the plant. Lithium fluoride does not react violently with air; it does not represent a fire hazard, and it should not react chemically with water either.
- Fission gases (and possibly some non-volatile and non-soluble fission products) are released from the fuel during operation, reducing the radiological salt inventory, in particular that of the gaseous fission products which are the most likely to be released in case of accident with a solid fuel. The fission products that remain within the salt, in particular cesium, are not significantly released in the event of an accident.
- The absence of fuel structures in the core such as cladding and subassemblies removes any risk of fuel compaction, a major risk of reactivity insertion in a fast neutron reactor with solid fuel.
- The intrinsic temperature feedback effect could eliminate the need of a control rod system for adjusting the operating conditions. Moreover, the amount of fissile matters dissolved in the critical zone of the fuel circuit is just necessary to maintain a critical state. Fertile matters are periodically injected in the core without needing to shut down the reactor. This allows to intrinsically reduce the risk of accidental reactivity insertion.

5.4.3 Safety related Challenges / R&D studies needed for the MSFR concept

- The safety analyses led until now must proceed more in depth to make sure the identification of risks is exhaustive. The current report presents some major achievements in that respect when it comes to identification of initiating events on the reactor during power operation. This risk identification exercise should be further continued, trying notably to encompass all initial states / operation modes (startup, shutdown phases etc.) and all the facilities, including the fuel treatment unit.
- Note that, as the fuel is in the liquid state, there is no accident similar to the severe accident of core meltdown as on solid fuel reactors, where the impact of such an accident on the safety functions is an important aspect for the reactor design and R&D. The definition and the studies of the severe accidents to be considered are in progress and must be continued, including a focus on the reactor behavior in case of a postulated prompt-critical jump.
- The prevention of corrosion of the structures in contact with the salt, especially the reactor vessel, must be shown to be sufficient. Suitable measures of surveillance are to be developed.
- The absence of risk of severe chemical reactions between the salt and the other materials employed is to be confirmed, especially the absence of risk of producing some hydrogen by the dissociation of water. Also, the consequences of a contact between salt and water need to be assessed, in particular the risk of steam explosion.
- The risk of precipitation and concentration of fissile matters in the salt, as well as generally speaking the criticality risk of the salt which is not in the reactor zone is to be further examined.
- Fission products extracted from the fuel circuit during operation are stored, in particular in the salt treatment unit. Associated risks (i.e., presence of a radiological source term, production of residual power, criticality risk) must be analyzed in detail.
- The monitoring of the reactor and the salt treatment unit, the features for in-service inspection and repair or replacement of equipment in contact with the salt, must be defined. It should be possible to monitor the envelopes containing the salt from the outside.

The work presents significant progresses as regard the definition of confinement barriers for fuel salts and fission products. Next steps could include the definition of their performances required as regards normal and accident conditions to consider.

Chapter 5

Results - Case Study: EU DEMO

The aim of this chapter is to summarize the main results obtained from the application of the previously defined methodology (see paragraph 4.3) to different advanced systems. In particular, in this chapter, it is described the application of part of the methodology (PIEs identification) to specific systems of the EU DEMO, as reported in EUROfusion project.

In PPCS (Power Plant Conceptual Study), four reactor concepts have been developed (Dongiovanni et al., 2014):

- Model A, Water-Cooled Lithium Lead blanket (WCLL);
- Model B, Helium-Cooled Pebble-Bed blanket (HCPB);
- Model C, Dual Coolant Lithium-Lead Concept (DCLL);
- Model D, Helium-Cooled Lithium Led concept (HCLL).

In particular, two blanket concepts have been taken into account: the WCLL (Water Cooled Lithium Lead), with and without an Intermediate Heat Storage (IHS) and the DCLL (Dual Coolant Lithium Lead), briefly described respectively in paragraph 6.1.1 and in paragraph 6.2.1.

6.1 The methodology implementation: WCLL blanket concept

6.1.1 WCLL description

The blanket

This WCLL blanket design refers to the information contained in the report (Aubert et al., 2013).

The blanket has three main functions: the cooling of primary heat source with a cooling circuit insuring power conversion efficiency; the tritium production system insuring tritium self-sufficiency; the shielding of the coils (realizing the plasma confinement).

The WCLL blanket is designed with modules of different sizes, attached together along the poloidal direction with a back supporting structure and fed with pipes at the rear of the modules (see fig. 6-1).

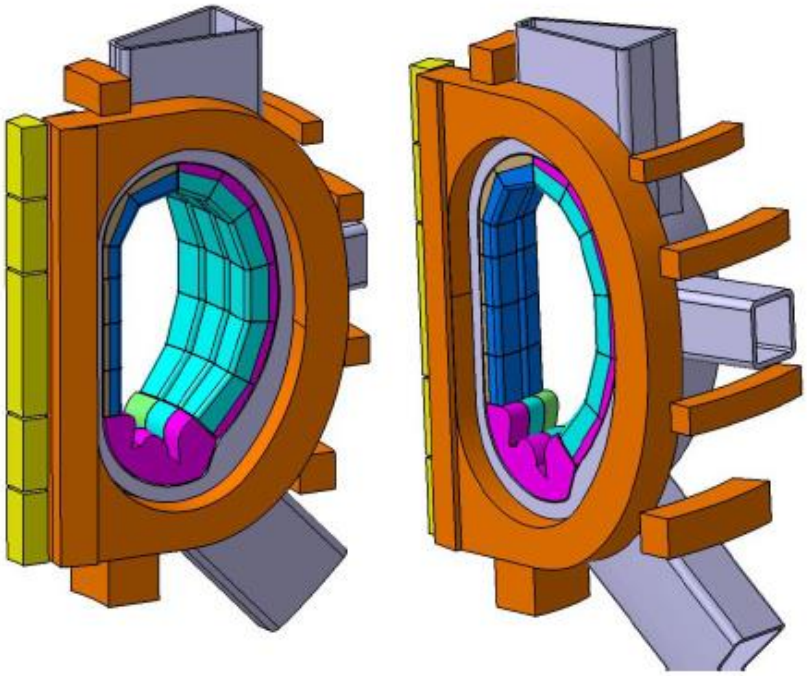

Figure 6-1 Several modules assembled in segments (Dongiovanni et al., 2014)

Each module is built with reduced activation ferritic-martensitic steel Eurofer as structural material, filled with liquid lithium-lead (LiPb) as breeder, neutron multiplier and tritium carrier and water at typical PWR conditions as coolant, i.e. nominal cooling water temperatures are 285°C at the inlet and 325°C at the outlet and nominal pressure of the cooling water is 155 bar. The lithium-lead inlet and outlet temperatures are above the (eutectic) lithium-lead melting point (235°C), and nominally 285°C (assumed), while the nominal pressure is 5 bar (Pinna et al., 2015).

The front part of the blanket module facing to the plasma is the First Wall (FW). Two independent cooling loops are envisaged: one for the FW and one for the breeder zone (BZ). This concept ensures the blanket cooling even in accidental situations, allows a separate regulation for the FW and the BZ and minimizes the pressure drops.

The Heat Transfer System without Intermediate Heat Storage

The PHTS (Primary Heat Transfer System) is outlined in six cooling loops connected in parallel to the reactor blanket BZ and FW, and two additional loops for cooling the divertor (DV) (see fig. 6.2). The conceptual design of the heat transfer systems of the DEMO WCLL blanket is on-going.

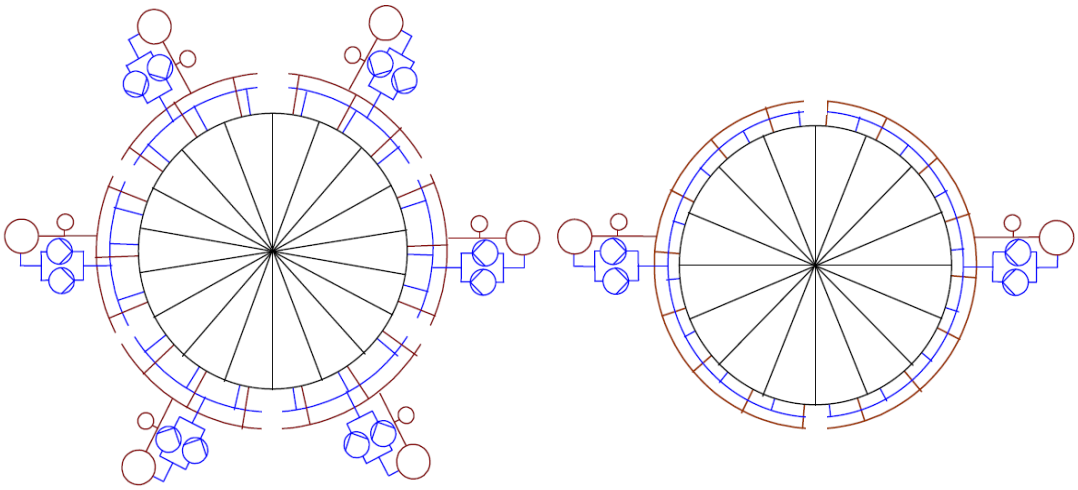

Figure 6-2 *Schematic of PHTS for FW and BZ (left) and DV (right) (Pinna et al., 2015)*

In the case without an Intermediate Heat Storage (IHS), each of the six BZ/FW cooling loops contains two parallel coolant pumps (LP), a pressurizer (PZ) and a steam generator (SG). Each loop serves 3 of the 18 tokamak sectors. During operation, the reactor coolant pumps circulate primary water through the coolant loops. The fluid is heated as it passes through the FW/BZ. Then, it flows to the steam generators, where the heat is transferred to the water/steam circuit and returns to the reactor coolant pumps to repeat the cycle (Pinna et al., 2015).

Other designs with a different number of cooling loops for the FW and for the BZ are investigated, but for PIEs identification this information is not relevant.

Table 1 shows the main parameters of the PHTS in the case without IHS (Del Nevo et al., 2014; Natalizio et al., 2014).

Table 6-1 Main parameters of the PHTS in the case without HIS *(Pinna et al., 2015)*.

Parameter	**Value**
Thermal power from the blanket BZ [MW]	3892
Thermal power from the blanket FW [MW]	1438
Primary water pressure [bar]	155
Primary water inlet T in SG [°C]	325
Primary water outlet T in SG [°C]	285
Primary water flowrate [kg/s]	9295
Primary water T from the divertor [°C]	167
Primary water T to the divertor [°C]	140

The divertor cooling system comprises two cooling loops, containing each of them two liquid pumps (LP), a heat exchanger (preheater) (HX) and a pressurizer (PZ). During operations, pressurized coolant is heated at the reactor and preheats water entering in the SG. After transferring the absorbed heat to the water/steam circuit, the primary water is pumped back to the reactor.

The pressurizer regulates the water pressure in the primary circuit, with heaters and water sprays, which maintain water and steam in equilibrium. A set of valves guarantees the meeting of safety requirements in abnormal reactor operations (Del Nevo et al., 2014).

The PHTS is also serviced by the Chemical and Volume Control System (CVCS) and the Coolant Detritiation System (CDS). These auxiliary systems are interconnected with the reactor coolant piping (Pinna et al., 2015).

It has been found that it could be possible that in case of failure of one of the cooling circuits, permanent damage of the in-vessel components could be avoided or reduced if independent circuits were used for BZ and FW. In fact, in case of failure of the FW circuit and consequent plasma shutdown, the BZ circuit would be able to remove the decay heat by conduction through the FW (or vice versa in case of fault in the BZ circuit) (Dongiovanni et al., 2014).

From now, for the purposes of the FFMEA application, the proposal of two independent PHT loops for the BZ and for the FW and a separate PHT loop for the divertor is considered as reference design.

It is assumed (Bubelis and Hering, 2014) that the operation of the EU DEMO will be pulsed (pulse duration ~ 2 h), with a dwell period of ~ 30 minutes needed to re-charge the central solenoid pulse. In consequence of that, the power transferred by the PHTS is characterized by a periodic evolution, ranging between almost zero and 100%. This could be a problem, both because of fatigue stresses of all components and because of the related difficulties of electric power injection into the grid. A solution can be the introduction of an IHS using molten salts. In particular the solar salt (60% $NaNO_3$ and 40% KNO_3) is the option considered in this work (Del Nevo et al., 2014; Natalizio et al., 2014).

As for the PHTS without IHS, in *the PHTS with IHS* there are two separate cooling systems for the FW and BZ and 2 cooling loops for the DV. Each primary circuit contains the same above-mentioned elements, but the SG is substituted by a heat exchanger (HX) between primary water and molten salt (Bubelis and Hering, 2014).

The Balance of Plant in the case without IHS

In the power plant conceptual study for WCLL concept, in the case without IHS, the primary water exchanges heat with the secondary water in the steam generators, producing steam. The steam is supplied to a turbine through a manifold collecting the steam produced in three or six SGs. The steam flow rate is about 3024 Kg/s. The power generator unit transforms steam's thermal energy into kinetic energy firstly and electric energy secondly. It is composed by the high-pressure turbine, the low-pressure turbine, the moisture separator re-heater and the generator. The high-pressure turbine operates at an inlet temperature and pressure of about 285 °C and 7.0 MPa respectively. The exhausted steam is cooled down by the condenser system and then pumped through the pre-heating system. In particular, the heat

coming from the divertor is used to pre-heat again the low-pressure water coming from the condenser. The temperature of the secondary water leaving the divertor cooling system is 247 °C, while the primary water inlet in the divertor preheater is about 267°C. As a result of a temperature difference of about 20 °C, the divertor pre-heater needs to be very large. The condensed water returns to the SGs by a distributor. The feed-water temperature is about 230°C (Pinna et al., 2015).

A set of valves (e.g. Relief and Safety valves, Steam Generator Safety valves, Main Steam Isolation valves) and by-pass lines are present in order to insure the safety of the plant.

The condenser is cooled by a third cooling circuit through a cooling tower.

The Secondary Water Cooling System is shared between the primary building and the turbine building: the Steam Generator, as well as the divertor pre-heaters, is contained into the primary building, while the collecting manifold, the power generator unit and the condenser system are contained in the turbine building (Pinna et al., 2015).

Design activities on the definition of the Balance of Plant (BoP) are in progress to define optimum solutions.

Figure 6-3 shows a schematic representation of the power conversion system, as it has been analyzed for the FFMEA purposes.

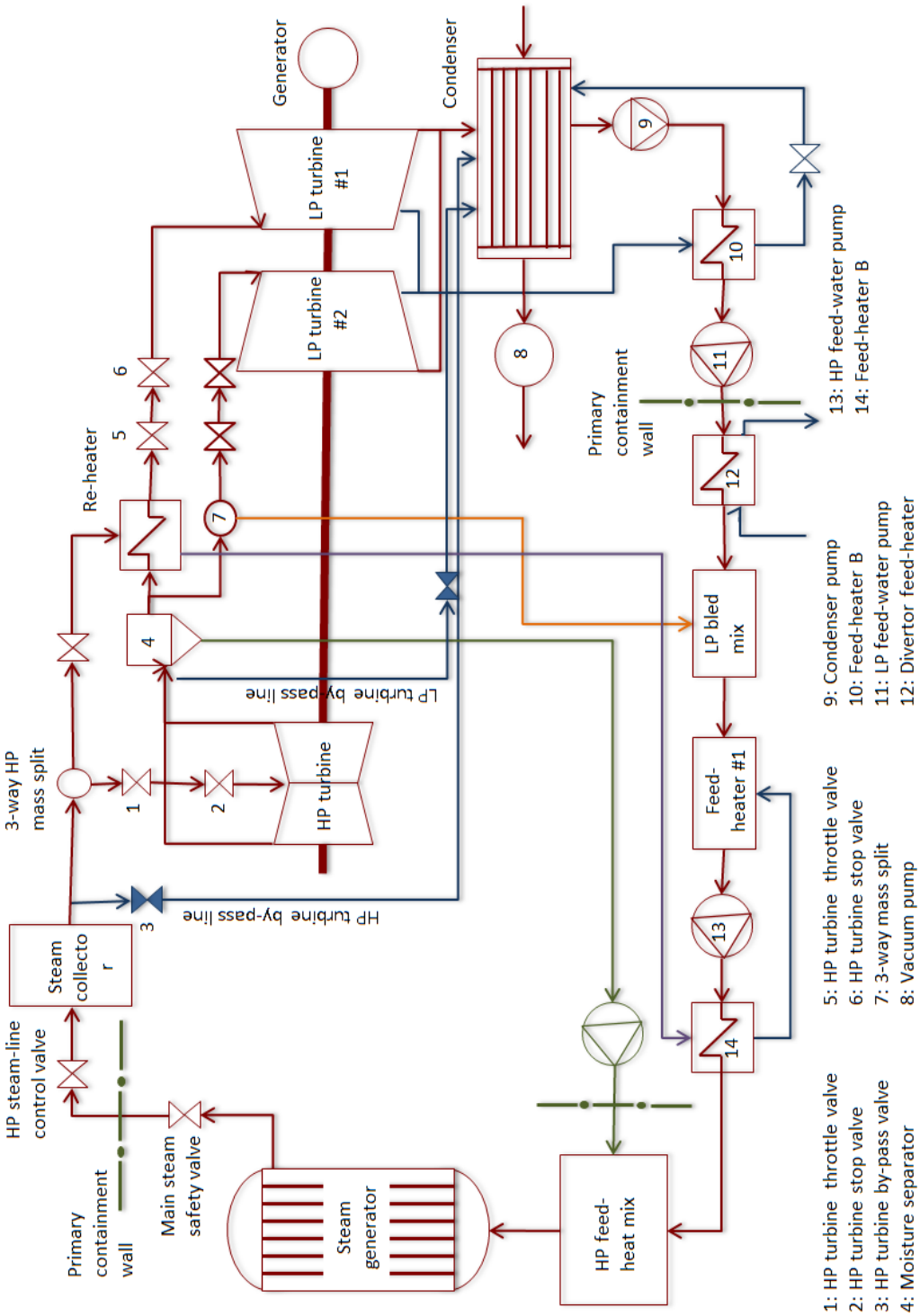

Figure 6-3 Secondary circuit for the WCLL cooling system (Pinna et al., 2015)

Figure 6.4 shows a schematic representation of primary circuit and secondary circuit in the case without IHS, including only one of the (6 FW + 6 BZ) cooling loops of the PHTS.

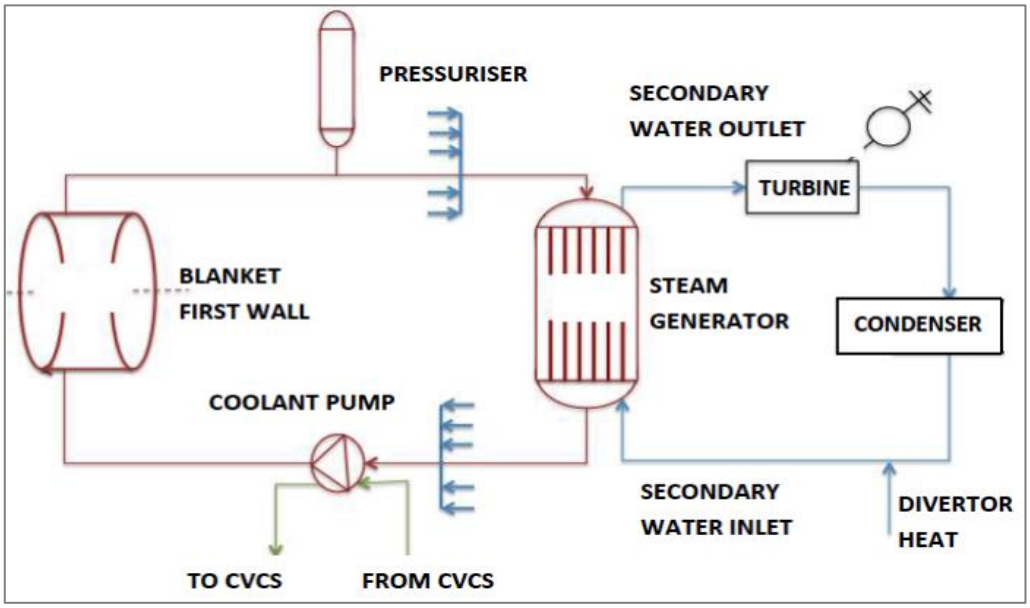

Figure 6-4 Sketch of the cooling loop in the case without IHS, including only one of the (6 FW + 6 BZ) cooling loops of the PHTS (Carpignano et al., 2016).

Table 6-2 shows the main parameters of the secondary circuit in the case without IHS.

Table 6-2 Main parameters of the secondary circuit in the case without HIS *(Pinna et al., 2015)*.

Parameter	**Value**
Steam pressure in SG [bar]	70
Steam T at the outlet of SG [°C]	285
Secondary water flowrate [kg/s]	3024

Molten salt circuit and WCLL secondary water circuit in the case with IHS

The molten salt intermediate circuit is characterized by one loop that contains two tanks, which are used to store energy to be used during the dwell period, when DEMO is not producing power. The hot tank is at an average temperature of about 320.7 °C, while the cold tank is at an average temperature of about 284.8 °C. Between the hot and the cold tank, there is the SG, where thermal energy is transferred to steam circuit and the economizer, which pre-heats the secondary water until saturation conditions before entering in the SG. A pump extracts molten salts from the cold tank to the HX with the primary water. The molten salt is at ambient pressure (1 bar).

The required storage capacity needs about 50800 t of molten salt: this means significant additional costs for both the molten salts and the additional circuit.

It is interesting to notice that the molten salt flowrate from the hot tank to the cold tank is 28000 kg/s, that is the 80% of the total flowrate (35000 kg/s), while the molten salt flowrate from the cold tank to the hot tank is equal to 35000 kg/s, that is the 100% of the total flowrate, during 100% power conditions, and it is equal to 0 during the dwell period *(Carpignano et al., 2016)*.

Table 6-3 and 6-4 summarize the main parameters IHS and BoP circuit, respectively (Bubelis and Hering, 2014).

Table 6-3 Main parameters of molten salt circuit in the case with HIS *(Carpignano et al., 2016)*

Parameter	**Value**
Molten salt melting T [°C]	220
Molten salt pressure [bar]	1
Hot tank T [°C]	320.7
Cold tank T [°C]	284.8
Total molten salt quantity [t]	50800

Molten salt flowrate (hot to cold) [kg/s]	28000
Molten salt flowrate (cold to hot in 100% conditions) [kg/s]	35000
Molten salt flowrate (cold to hot in 0% conditions) [kg/s]	0

Table 6-4 Main parameters of the secondary circuit in the case with HIS *(Carpignano et al., 2016)*.

Parameter	**Value**
Steam pressure in SG [bar]	64
Steam T at the outlet of SG [°C]	279.8
Secondary water flowrate [kg/s]	985.77

Figure 6-5 shows a schematic representation of the primary water circuit, the molten salt circuit and the BoP in the case with IHS, including only one of the (6 FW + 6 BZ) cooling loops of the PHTS.

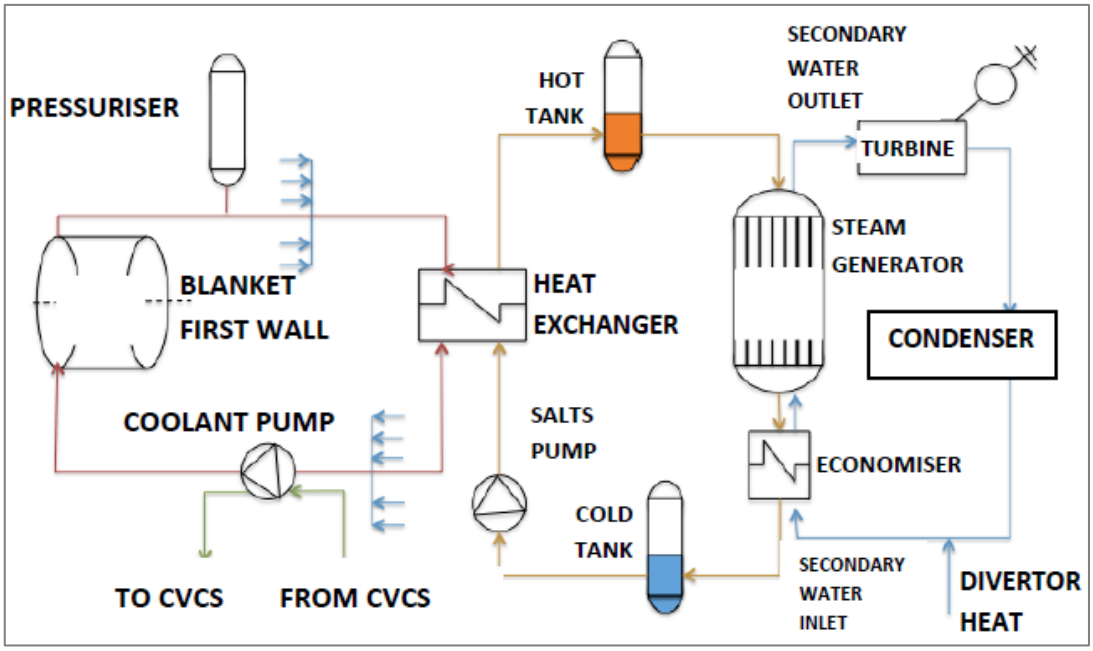

Figure 6-5 Sketch of the cooling loop in the case with IHS, including only one of the (6 FW + 6 BZ) cooling loops of the PHTS *(Carpignano et al., 2016)*.

6.1.2 The molten salt characteristics

One of the most peculiar aspects of the introduction of the intermediate circuit is the presence of the molten salt, which represents the possible cause of new PIEs and of the different evolutions of PIEs already identified in the study of the system without IHS (Pinna et al., 2015). Therefore, it is interesting to analyze some specific features.

Thermo-chemical characteristic

The storage material for thermal energy can be solid or fluid. It can utilize sensible or latent heat. The most important characteristics for a storing material are: a good capacity for storing, an efficient transfer of heat between the cooling fluid and storage material, mechanical and chemical stability because of the number of uploading/downloading cycles that it must guarantee, chemical stability at high temperatures, low vapour pressure, high density for compactness, chemical compatibility with other fluids and metallic components, low oxidation rate, low thermal losses, control and competitive costs (Gil et al., 2010a; Gil et al., 2010b).

In the EU DEMO (Herrmann et al., 2004), the selected storage material is at the liquid state, containing molten salts, because of the wide experience of molten salt utilization in solar applications (e.g. concentrated solar power plants), in chemical and metal industries and in agriculture. In particular, the solar salt is the first choice In fact, it is characterised by a good combination of properties: density (about 1900 kg/m^3), specific heat (about 1500 J/kg K), vapour pressure (< 0.01 Pa) and cost (about 0.49 $/kg). Moreover, it is liquid at atmospheric pressure if the temperature is above the freezing point; the proposed operating temperature allows the use of commercial high temperature and high-pressure steam turbines, with a good efficiency for the Rankine cycle. The solar salt is non-flammable and non-toxic (Gil et al., 2010a).

Since molten salts solidify at relatively high temperature, it is necessary to guarantee that the solar salt does not freeze during operation; consequently, routine freeze protection systems and operations increase the O&M (operation and maintenance) costs. For example, the installation of an electrical heater could be foreseen to avoid the solidification in emergency situations (Gil et al., 2010a). Additionally, thermal losses augment because of high temperature of the storage, implying the need of more expensive piping and materials (Carpignano et al., 2016).

Even if the solar salt is composed by two oxidizing agents (sodium nitrate and potassium nitrate) and the thermal fatigue increases the corrosion rate, the studies concluded that oxidation rate is sufficiently low and impurities have a small effect (Gil et al., 2010a). On the other hand, if nitrates are in contact with organic or combustible materials above the ignition temperature, reactions can proceed quickly enough to cause ignition, combustion or explosions; if water is inadvertently introduced into the molten salt bath, and a steam explosion can occur (Herrmann et al., 2004; Kitchen et al., 2004). Finally, the nitrates decomposition can catalyse precipitation phenomena and the consequent metallic parts scaling and possible pump and pipe plugging (Donatini et al., 2005).

Notwithstanding these criticalities, it has been concluded that there are not major technical issues preventing the realization of this concept.

Safety and operational issues or EU DEMO IHS

In this paragraph, some safety relevant issues from the FFMEA are summarized.

A superficial oxide layer, which is caused by corrosion, modifies physical, chemical and technological steel properties. In fact, the oxide is more brittle than the metal, increasing the occurrence probability of a brittle fracture (instantaneous and sudden). Additionally, the oxide layer transfers heat worse than the metal, decreasing the efficiency of the heat transfer between the primary water and the molten salt, and between the molten salt and the BoP fluid. It could be the cause of a slight overpressure and overheating in the primary circuit; as well, the efficiency of the Rankine cycle of the BoP is decreased, because of the increase of the thermal losses. Moreover, some oxide fragments, dispersed in the circulating salt can change also the thermal resistance between the molten salts and water circuits. These fragments enhance the corrosive-erosive nature of molten salt, scrubbing and further wearing down the steel surfaces. From these considerations, it is deduced the necessity of a molten salt purification system, especially for key and expansive components like the pumps. The last ones result the most sensitive components to the corrosion problem. Furthermore, preventive maintenance actions are fundamental, e.g. regular X-rays and ultra-sound inspections, implementing a risk-based inspection (RBI) approach, in order to keep constant the material properties (mainly ductility and maximal tensile stress).

The diffusion of molten salt particles in the metallic matrix is not negligible. In fact, it causes the embrittlement of the steel, which at the beginning is ductile. The molten salt particles represent the heterogeneities, acting as obstacles for dislocations movement. As a consequence, the steel is hardened and the occurrence probability of a brittle fracture is increased. On the other hand, since the molten salt is at high temperature (about 300°C), we can have a kind of compensating effect on material properties evolution. In fact, high temperature reduces hardness and Young modulus, and augments the maximal elongation. The sum of all these contributions (corrosion, diffusion and high temperature flow) result in lower fracture resistance.

A critical aspect of the solar salt is its oxidizing power. In particular, in case of an accidental contact with hydrogen produced in the primary circuit by hydrolysis mechanism, the reaction between $NaNO_3/KNO_3$ and hydrogen can be primed and it is always exothermic.

Finally, the probability of molten salt freezing must be evaluated. The liquid state of the salt must be guaranteed in all the points of the circuit, especially in critical components, i.e. pumps and HX (Carpignano et al., 2016).

6.1.3 PIEs identification

Table 6-5 summarizes briefly the results of the implementation of the FFMEA for the system without HIS, which led to a list of 27 PIEs (Pinna et al., 2015).

Table 6-5 List of PIEs identified by the FFMEA on HTSs of the DEMO WCLL reactor (Pinna et al., 2015).

PIE	Description
AOP	Loss of Off Site Power
FB1	Loss of flow in the primary cooling loop of the breeder material because pump trip
FB2	Loss of flow in cooling channels of breeding material in one blanket module because internal clogging
FD1	Loss of flow in the primary cooling loop of the divertor because pump trip
FD2	Reduction of flow in cooling channels of one divertor cassette because internal clogging
FF1	Loss of flow in the primary cooling loop of the FW and blanket structures because pump trip
FF2	Reduction of flow in cooling channels of FW and blanket structure of one module because internal clogging
FM1	Loss of LiPb flow in the liquid metal circuit because electromagnetic pump trip: the LiPb flow is lost in all blanket modules supplied by the LiPb circuit
FM2	Loss of LiPb flow in one blanket module because clogging of the outlet pipe

HB99	Loss of heat sink in all FW, BZ and divertor primary cooling circuits because trip of both HP and LP turbines due to loss of condenser vacuum
HB1	Loss of heat sink in one cooling train of the blanket module (either BZ or FW)
LBB1	Large loss of water from the FW cooling circuit inside breeder blanket box: Rupture of a sealing weld
LBB2	Leak of water from the FW cooling circuit inside breeder blanket box: Leak of a sealing weld
LBO1	LOCA (Loss of Cooling Accident) Out-VV (Vacuum Vessel) because large rupture of the BZ primary cooling loop in the water manifold feeder inside PHTS Vault
LBO2	Leak Out-VV because small rupture of the BZ primary cooling loop in the water manifold feeder inside PHTS Vault
LBO3	LOCA Out-VV from the breeder primary cooling loop because rupture of tubes in a Steam Generator
LDO1	LOCA Out-VV because large rupture of the divertor primary cooling loop in the water manifold feeder inside PHTS Vault
LDO2	Leak Out-VV because small rupture of the divertor primary cooling loop in the water manifold feeder inside PHTS Vault
LDO3	LOCA Out-VV from the divertor primary cooling loop (DV-PHTS) because rupture of tubes in the Heat Exchanger with the secondary loop
LDV1	LOCA in-vessel because large rupture of the divertor cassette
LDV2	Leak in-vessel because small rupture of the divertor cassette
LFO1	LOCA Out-VV because large rupture of the FW primary cooling loop in the water manifold feeder inside PHTS Vault
LFO2	Leak Out-VV because small rupture of the FW primary cooling loop in the water manifold feeder inside PHTS Vault

LFO3	LOCA Out-VV from the first wall primary cooling loop because rupture of tubes in a Steam Generator
LFV1	LOCA in-vessel because large rupture of the FW structure: Complete rupture of the FW
LFV2	Leak of FW cooling circuit inside VV
TWO1	Tritium and H_2 release in the room hosting the water detritiation system
N/S	Not Safety Relevant

In the FFMEA analysis for the system with IHS, some of these PIEs result the most influenced by the presence of the intermediate circuit:

- The loss of heat sink (*HB1, HB99*);
- LOCA in tubes of HX between PHTS and HIS, which in the case without IHS corresponds to the steam generator (*LFO3*).

In the subsequent paragraphs, the PIEs obtained in the analysis (Pinna et al., 2015) for the concept without IHS are described, in order to facilitate the comparison with the PIEs obtained for the concept with IHS, which are reported in paragraph 6.1.4.

HB99: Loss of heat sink in all FW, BZ and divertor primary cooling circuits

This PIE can be related to the loss of secondary flow or the loss of secondary confinement due to the blockage of a valve or piping leak/rupture or the loss of component cooling or turbine protection intervention, e.g. in case of over-speed, high vibrations or imbalance. Moreover it is assumed that DEMO reactor will be an inductive pulsed tokamak: consequently the turbine works in pulsed regime that can lower its reliability, leading to a higher frequency of trips than in stationary regime of conventional turbines (Pinna et al., 2015).

The reference event for the PIE is the loss of condenser vacuum for rupture of the condenser or of the interfacing lines. The PIE induces the unavailability of the heat sink to all the FW, BZ and divertor primary cooling systems of the reactor. The loss of condenser leak-tightness implies:

- Ingress of air into steam loop towards low pressure turbine;
- Loss of condenser vacuum;
- Turbines trip for protection intervention (high pressure control);
- Loss of saturated steam into turbine building once equalization of pressures;
- Building pressurization;
- Release into building of tritium permeated through steam generator;
- Direct release of tritium contained in secondary fluid towards the environment if HVAC (Heating, Ventilation and Air Conditioning) is not promptly isolated;
- Fast over-pressurization of primary and secondary loops if plasma is not promptly shutdown;
- Pressure relief in primary loops: it will assure heat removal from plasma facing components (PFCs) for a while, giving, even if very short, a period of time in order to operate the plasma shutdown;
- Leaks/ruptures in ex-vessel and in-vessel sections of primary loops can occur (other leaks/ruptures in secondary circuit can occur too);
- Plasma disruption and possible in-vessel break of FW of blanket modules;
- Vacuum vessel pressurization;
- Pressure relief to vacuum vessel pressure suppression system (VVPSS);
- VV radioactive products and tritium released into VVPSS room and vacuum vessel surrounding area through containment leaks;
- Possible loss of vacuum vessel penetration leak-tightness because the high overpressure inside the vessel (Pinna et al., 2015).

The following preventing and mitigating features/actions have been identified:

- Redundant control of operating parameters in secondary circuit
  - Condenser and vacuum line parameters,
  - Parameters of vacuum equipment dedicated to remove incondensable gases from the condenser,
  - Hot well and degasser parameters,
  - Pressure relief devices,

    - Turbine control against over-speed, over-load, vibrations, etc.,
    - Interlock plasma operation with turbine parameters ,
    - Closure of the high pressure stop valve and opening of the turbine by-pass valve.
- Pressure relief devices in primary circuits.
- Soft/Fast Plasma shutdown.
- Vacuum vessel rupture disk opening
    - Release of pressure to the VVPSS.
- Switch-on atmosphere DS into building.
- Start of the emergency cooling (e.g. vacuum vessel cooling circuit)
- Vent of cryostat to reduce the temperature in the vacuum vessel and its surrounding structures (Pinna et al., 2015).

HB1: Loss of heat sink in one cooling train of the blanket module (either BZ or FW)

This PIE can be related to the loss of secondary flow or the loss of secondary confinement due to piping leak/rupture or valve leak/rupture in the section of the circuit interesting only one SG (e.g. high pressure steam lines from steam generator to steam collection header or, main steam safety valves) (Pinna et al., 2015).

The reference event for the PIE is the unavailability of the heat sink to the FW primary loop cooling the FW of all blanket modules of the reactor. This could imply:

- Damages of the steam circuit;
- Loss of steam into the building and building pressurization;
- Release into the building of tritium permeated through the steam generator and following environmental releases due to building leaks;
- Direct release of tritium contained in secondary fluid towards the environment if HVAC is not promptly isolated;
- Reduction of the capability to remove plasma heat from FW segments;
- Fast over-pressurization of FW primary loop if plasma is not promptly shutdown;
- Pressure relief in primary loop (it will assure heat removal from FW for a while, giving, even if very short, a period of time in order to operate the plasma shutdown);

- Plasma disruption and possible in-vessel break of FW modules because of thermal and mechanical stresses;
- Vacuum vessel pressurization;
- Pressure relief to VVPSS;
- Vacuum vessel radioactive products and tritium released into VVPSS room and vacuum vessel surrounding area through containment leaks;
- Possible loss of vacuum vessel penetration leak-tightness because the high overpressure inside the vessel (Pinna et al., 2015).

The following preventing and mitigating features/actions have been identified:

- Redundant control of operating parameters in secondary circuit
  - steam generator parameters,
  - Pressure relief devices.
- Isolation of steam generator failed loop in secondary and primary side thank to a high efficiency isolation valves system;
- Pressure relief devices in primary circuits.
- Soft/Fast Plasma shutdown.
- Vacuum vessel rupture disk opening
  - Release of pressure to the VVPSS.
- Switch-on atmosphere DS into building.
- Start of the emergency cooling (e.g. vacuum vessel cooling circuit)
- Vent of cryostat to reduce the temperature in the vacuum vessel and its surrounding structures (Pinna et al., 2015).

LFO3:LOCA Out-VV from the SG of the first wall primary cooling loop

The reference event for this PIE is the large loss of water from the FW primary cooling circuit inside the secondary loop because rupture of tubes in the steam generator (Pinna et al., 2015).

As consequences of the initiator the following chain of accidents can occur:

- Release of primary water into secondary loop;
- Tritium and radioactive products contained in primary loop released into secondary loop (contamination of secondary loop);
- Release of radioactive products through secondary loop leaks;
- Equalization of pressure between the two loops;
- Decrease of water pressure and inventory inside the primary loop;

- Loss/Reduction of capability to remove plasma heat and heat produced by the neutron reaction from the FW;
- FW rupture because thermal and/or mechanical stress (plasma disruption can aggravate the thermo-mechanic load on the structures);
- In-vessel LOCA from FW of blanket modules;
- Vacuum vessel pressurization;
- Pressure relief to VVPSS
- Vacuum vessel radioactive products and tritium released into VVPSS room and vacuum vessel surrounding area through containment leaks;
- Possible loss of vacuum vessel penetration leak-tightness because the high overpressure inside the vessel (Pinna et al., 2015).

Redundant detection of primary loop parameters could be able to actuate automatic actions to get safe conditions in case of anomalies. The first action is the soft or fast plasma shutdown (Pinna et al., 2015).

Furthermore, as the BZ is cooled by an independent primary loop the damage and collapse of the FW could be prevented if safe mitigations are promptly activated (Pinna et al., 2015).

6.1.4 Differences found out for the system with IHS

All the PIEs identified for the case without IHS are valid also for the case that includes the intermediate molten salt circuit. The aim of the present paragraph is to highlight the differences between the design with and without IHS.

No major differences have been found concerning events occurring in the breeding blanket, first wall, divertor cooling loop, LiPb circuit and detritiation system, because the introduction of the IHS and its possible failure do not affect the functionalities of these components. Table 6-6 summarizes the systems affected by the presence of the IHS.

Table 6-6 Systems affected by the presence of the HIS (Carpignano et al., 2016).

System	Affected	Not Affected
Breeding Blanket		X

First Wall		X
Divertor		X
LiPb circuit		X
Detritiation system		X
PHTS	X	
BoP	X	

The PIEs, whose evolution is modified by the presence of the IHS circuit, are the loss of heat sink for the primary water circuit and LOCA in the tubes of the HX between primary and intermediate circuit. For each PIE, the major differences linked to the different nature of the two systems are summarized in table 6-7.

Table 6-7 Main differences in the PIEs due to the presence of the IHS (Carpignano et al., 2016).

PIE	Differences
Loss of heat sink (or of off-site power)	- Leakage of molten salt; - Need of collecting tanks; - Possible solidification of molten salts where heaters are not present.
LOCA in HX tubes	- Pressure difference between PHTS and intermediate circuit of about 155 bar; - Vapour formation; - Water-molten salt chemical reaction; - Contamination of molten salts; - Possible H_2 reaction.

PIE: Loss of heat sink

The loss of the heat sink for the FW/BZ can be due to different causes. Figure 6-6 shows a sketch of an example of rupture location in the system. It causes the leakage of molten salt in the containment building. The worst scenario corresponds to a leakage in the part of the storage circuit located inside the primary building,

even if the fluid is not in pressure, hence there is no building pressurization. Nevertheless, the molten salt must be recollected; therefore, containment tanks must be foreseen in order to mitigate this event. Moreover, even if the salt is non-toxic and non-flammable, it must be handled carefully, mainly because of its oxidizing nature in presence of hydrogen or other organic compounds (Carpignano et al., 2016).

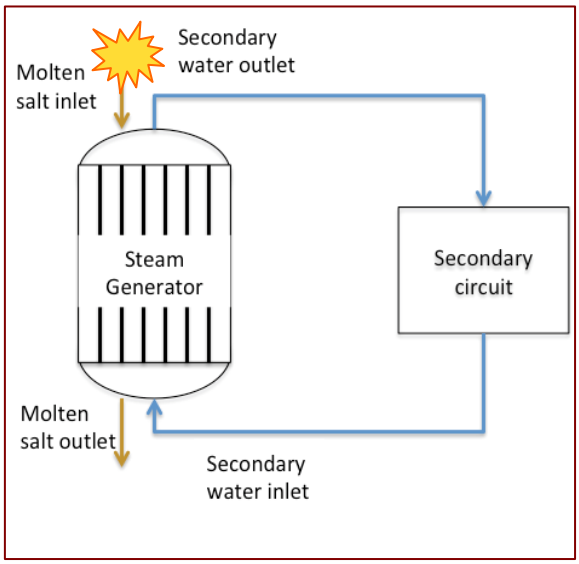

Figure 6-6 Sketch of the accidental rupture location, causing a loss of heat sink

Another potential cause of this PIE could be the partial/total failure of the molten salt pump. Since the molten salt flow is fundamental to prevent freezing, sufficient redundancies must be foreseen.

With respect to FW/BZ and VV (Vacuum Vessel), the consequences are similar to the case without IHS. They are mainly linked to over-pressure and over-temperature in the primary water, the necessity of a prompt shutdown of the plasma, eventual pressure relief in the primary loop and tritium release, possible leak/rupture in ex-vessel and in-vessel sections of the primary circuit because of thermo-mechanical stresses and possible radioactive release in VVPSS and VV surrounding areas through containment leaks.

The event of loss of off-site power should be considered. This can be caused by an external event (e.g. earthquake) or to a failure of the on-site electrical network. It can initiate a pumps trip, with the consequences already presented in the loss of heat sink PIE. Moreover, the loss of off-site power can make the molten salt solidify in pipes and components, complicating the post-accident procedures.

PIE: LOCA in tubes of HX between PHTS and HIS

In the study of a LOCA in the tubes of the HX between primary and intermediate circuit, it is important to remember that the primary water is in overpressure with respect to the intermediate circuit. In fact, while the primary water is at 155 bar, the molten salt circuit operates at atmospheric pressure. In case of rupture in the HX tubes, the primary water goes in the intermediate circuit at the sound speed and the primary water contaminates the molten salt. The water pressure decreases until the saturation pressure corresponding to the primary water temperature, then it evaporates instantaneously. An exothermic water-molten salt chemical reaction could be primed, involving fire or even explosion; the hydrogen, present in the primary water, can react with the salt that is an oxidizing agent, worsening the consequences.

Figure 6-7 shows schematically a representation of the accident position.

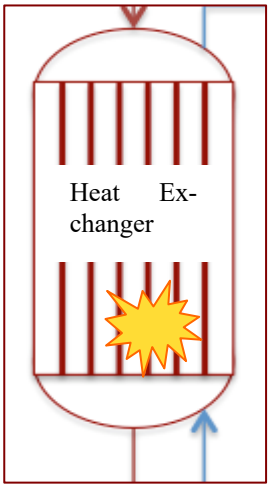

Figure 6-7 Sketch of the accident LOCA in the tubes of HX between PHTS and IHS

Some consequences of this PIE are similar to the case without HIS, especially the ones related to radioactive releases from the primary loop to the secondary loop and from the secondary loop leaks to the secondary building (supposing that the HX is not contained in the primary building). Furthermore, this PIE causes the loss/reduction of heat removal function (plasma heat and heat produced by neutron reactions in the BZ). Over-pressure and overheating are expected in the primary circuit with thermal-mechanical stresses and risk of explosion because of H_2 produced by radiolysis. Finally the opening of the pressure relief valve to VVPSS causes the VV pressurization. The soft or fast plasma shutdown can mitigate this accident.

As for the case of a LOCA in tubes of HX between PHTS and IHS, in the case of a rupture of a tube in the SG between IHS and BoP same problems are possible to occur.

6.1.5 Considerations

The thermal storage helps realizing a steady feeding of the SG and continuous regime of the turbine (reduced mechanical fatigue) and introduction of the steady state electrical power into the grid.

The FFMEA investigate systematically the concept and guarantees that only few systems are affected by the presence of the IHS: the ones heat with the storage, the PHTS and the BoP.

The PIEs interesting the PHTS and the resulting consequences for the case without IHS are still valid in the case with IHS, but the presence of the IHS introduces new criticalities connected to the physical-chemical characteristics of the molten salt. The presence of molten salt storage requires proper maintenance preventing actions by a RBI approach, to control the corrosive-erosive molten salt power, with respect to the steel structures (especially the pumps). In particular, the safety function of heat removal (ultimate sink) is influenced by this event. When the intermediate circuit is compromised, overpressure and overheating are likely to occur in primary circuit.

However no major safety/operational obstacles are found for IHS concept.

In future, a quantitative risk analyses will be performed after the definition of a more detailed design of IHS.

6.2 The methodology implementation: DCLL blanket concept

6.2.1 DCLL description

In the DCLL blanket, eutectic alloy LiPb acts as a breeders and coolant for the BZ and circulates slowly for limiting corrosion issues, while helium is used for cooling the FW and the reduced activation ferritic steel structure. The conceptual structure of the DCLL module for EU DEMO is shown in fig. 6-8. The LiPb flowrate inside each channel has been selected to maximize the heat extraction from the reactor and to avoid LiPb backflow in the poloidal ducts.

As shown in fig. 6-8, the LiPb enters the module through the annulus (external duct) of the concentric pipes located at the top of the module. It goes downwards through two rows of parallel poloidal channels located at the rear part. It turns 180º at the bottom through radial channels and then circulates upwards in parallel front poloidal channels. Finally, the LiPb goes outside through the internal duct of the concentric pipes.

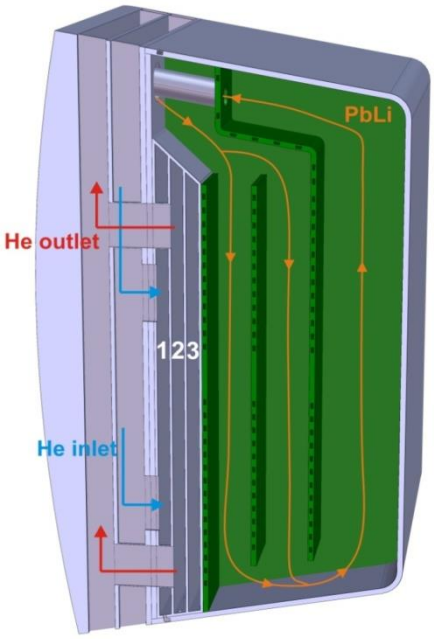

Figure 6-8 Section of cooling structure of the EU DCLL Breading Blanket module (Rapisarda et al., 2015)

A Back Supporting Structure (BSS) integrates all service connections for every module and also acts as shielding. It is composed by two long poloidal ducts covering the segment whole length where LiPb flows downwards and upwards, respectively. The concentric pipes feed the four independent LiPb circuits in each module and are connected to the general manifolds ducts. Two poloidal ducts with smaller dimensions are located close to the sidewalls, where helium flows downwards and upwards to feed the different modules. They are connected to the internal manifolds for helium distribution.

The DCLL system is constituted by the following subsystems:

- The breeder blanket segment: it includes the DCLL modules, the feeding pipes and the Back Supporting Structure (BSS)
- The LiPb loop: it provides circulation of LiPb inside the modules and outside the VV.
- The helium loop: it provides the circulation of the coolant from the modules to outside of the VV.
- The Tritium Extraction system (TES).

The following fig. 6-9 shows a schematic representations of the circuit.

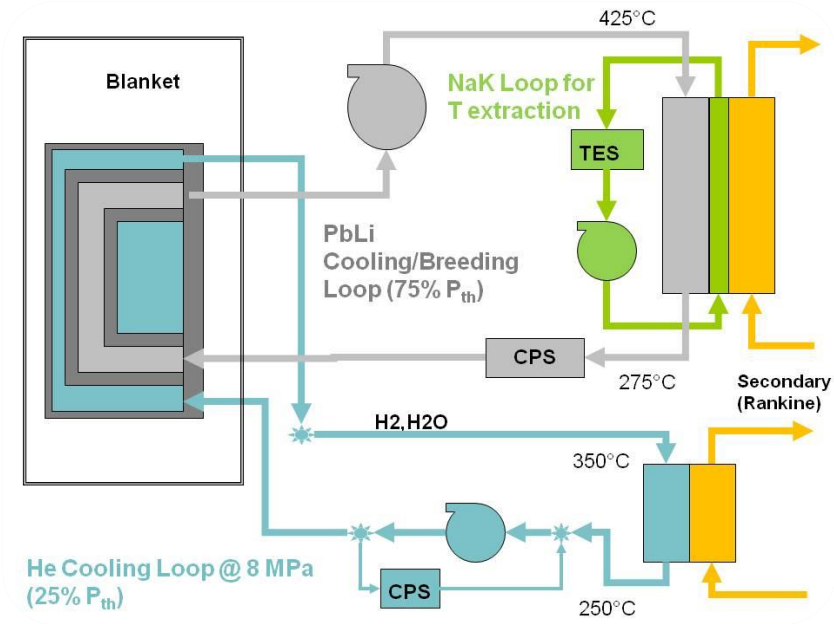

Figure 6-9 Schematic representation of the primary cooling circuits (Rapisarda et al., 2015).

He loop

Due to the lack of information, for these studies, the helium circuit designed for ITER DCLL test blanket module (TBM) is used as reference (see fig. 6-10).

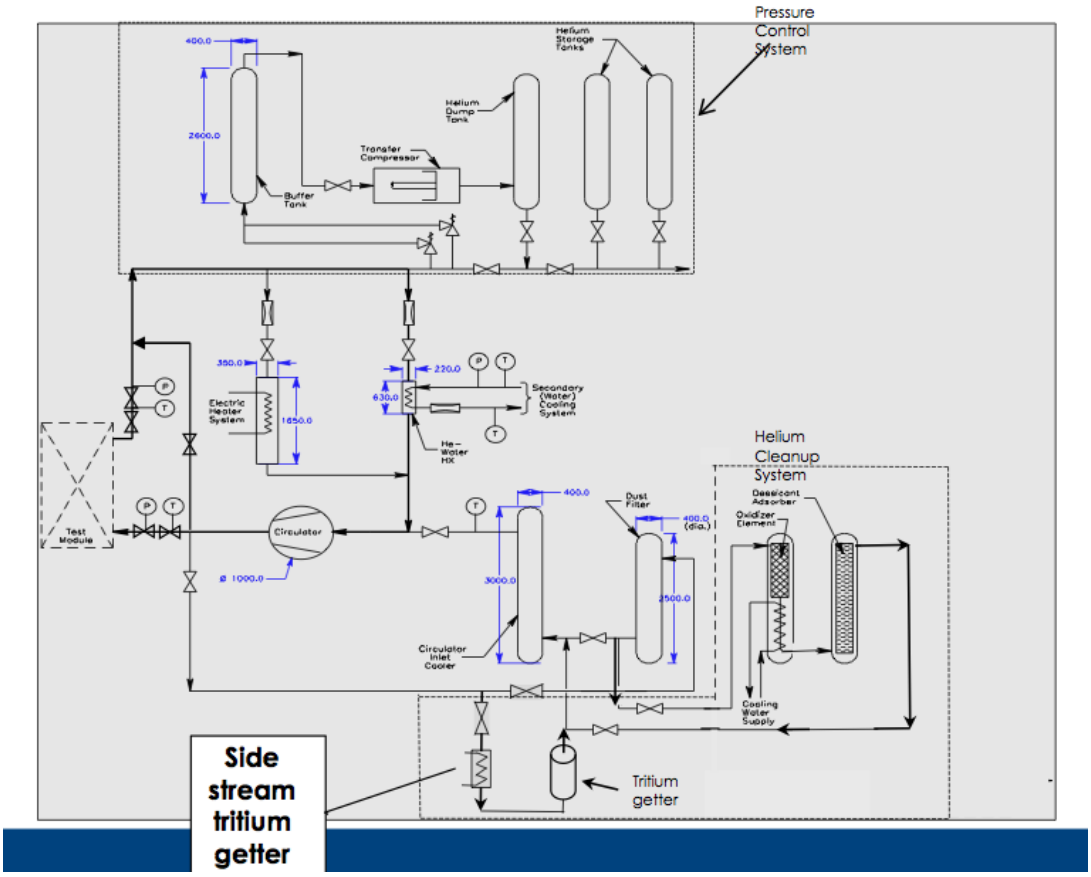

Figure 6-10 Simplified helium loop design for ITER DCLL TBM (Wong, 2010)

The Helium circulates at ~8.0 MPa and reaches the temperature of 395°C in the blanket module. It exchanges heat with the BoP coolant in the HX and it returns in the blanket module (no intermediate circuit is considered for this concept). A compressor helps the helium circulation. In case of need, an electric heater switches on in case to manage helium temperature and pressure.

For these preliminary studies, it has been considered that U-tubes constitute the helium circuit inside the blanket box. The cooling channels are disposed inside the Breading Blanket as shown in fig. 6-11 and fig. 6-12, where operational conditions are also indicated.

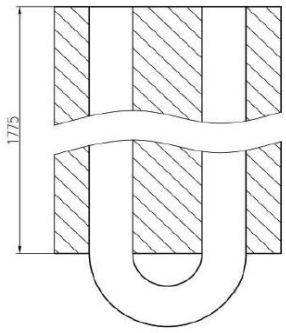

Figure 6-11 U-tube geometry used for He circuit analyses (Rapisarda et al., 2015)

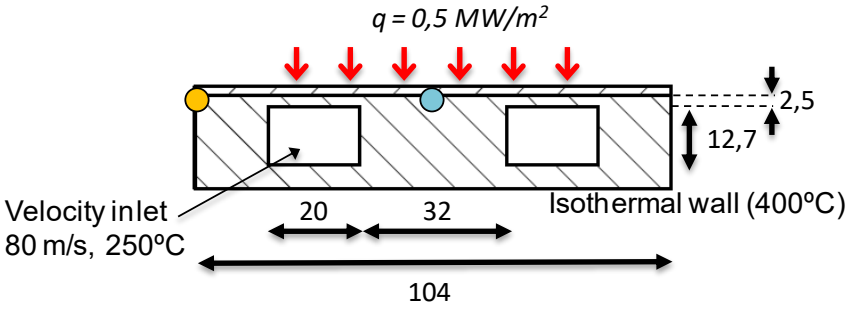

Figure 6-12: FW segment geometry (Rapisarda et al., 2015)

The helium loop is designed in order to maintain the EUROFER temperature below 550 °C, maximizing the helium outlet temperature (~395 °C) and minimizing the pressure loss. The limiting temperature of 550 °C is given by EUROFER/LiPb corrosion (Rapisarda et al., 2016).

LiPb loop

A preliminary proposal for the LiPb loop for the DCLL BB concept has been performed based on the input data and parameters available in 2014 (Reungoat & Vala, 2014). Main operational parameters are listed in the table 6-8 below; they have been considered to perform the preliminary safety assessment of the LiPb loop.

Table 6-8 Operating parameters for the 2014 DCLL BB concept 2014 (Reungoat & Vala, 2014)

Parameter	**Value**
Composition of LiPb coolant	Pb-15.7Li
Maximal temperature of LiPb [°C]	550
Minimal temperature of LiPb [°C]	300
Total LiPb mass flow rate for DEMO [kg/s]	46000
Max LiPb velocity in BB [m/s]	1
Helium pressure in BB [MPa]	8
BB material	EUROFER + alumina-sandwich for FCI
LiPb loop material	EUROFER
Corrosion rate of EUROFER [μm/year]	300–900 (TBC)
BB lifetime [years]	5–6
Magnetic field [T]	Maximum field on Nb3Sn-conductor: ≈ 12
Pressure drop due to MHD effect [MPa]	1.29 (TBC)
LiPb inlet/outlet position	On the top of the BB segment
Number of LiPb loops for DEMO	16 (one for each of the 16 sectors)
LiPb volume in one outboard BB segment [m^3]	11.8
LiPb volume in one inboard BB segment [m^3]	8.52

The LiPb loop includes the following components:

- Expansion tank (ET);
- Tritium Extraction System (TES);
- Pump (Permanent Magnet Pump or mechanical pump);
- Purification system (PS);

- Storage tank.

The BB and the HX are considered as interfaces for LiPb loop.

In a DCLL DEMO each sector is connected to one LiPb loop, in order to split the extremely high LiPb mass flow rate. This improves also the safety aspects; in fact, cooling the PFCs through independent primary circuits minimizes the impact of the failure of one of them, since the other cooling circuits will remain available, giving more time to get safe status of the reactor. The diameter of the LiPb loop pipes has been chosen in order to keep the LiPb velocity low and therefore to reduce the corrosion rate. It has been estimated to be 0.44 m/s.

Finally two different pumping systems have been proposed for the LiPb loop of the DCLL BB concept:

1. A permanent magnet pump (PMP); in this case it is located at the hot leg of the loop in order to prevent precipitation of corrosion products (favored by a combination of magnetic field and low temperature of LiPb);
2. A mechanical centrifugal pump; in this case the pump is located at the cold leg of the loop in order to limit the operating temperature of the component (Rapisarda et al., 2016).

A schematic representation of the LiPb loop is proposed in fig. 6-13 (Rapisarda et al., 2016).

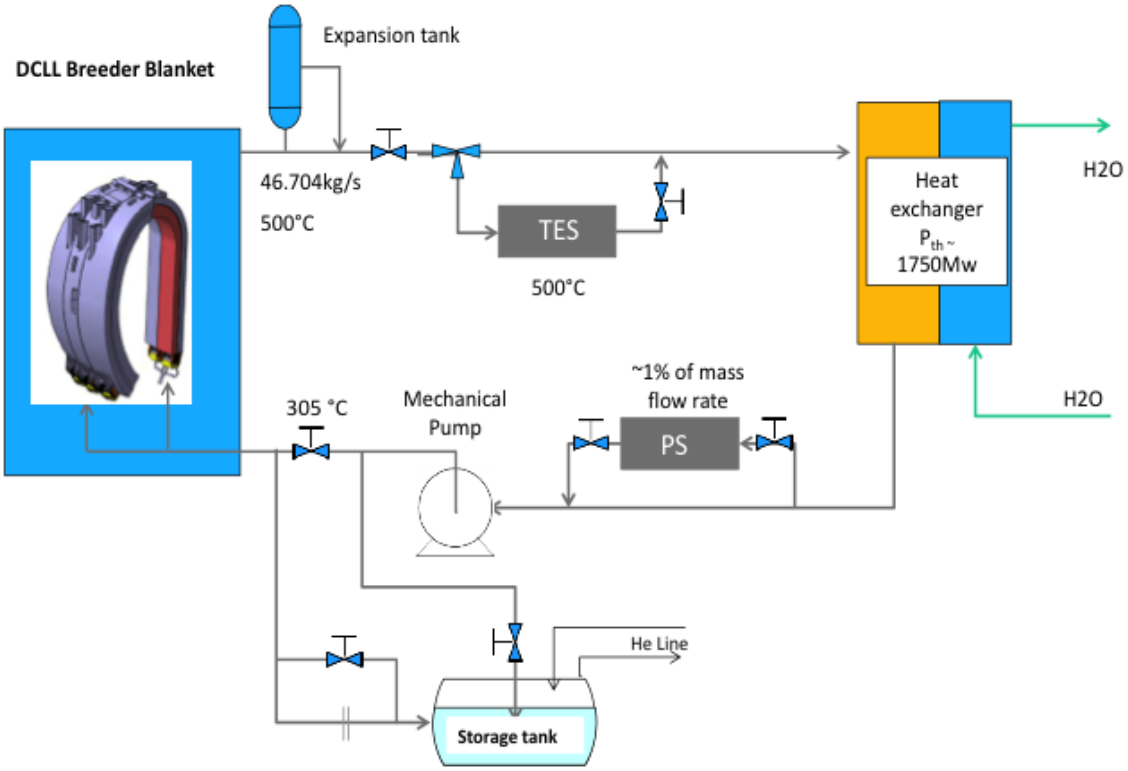

Figure 6-13 Proposed DCLL LiPb loop (Tincani et al., 2015).

6.2.2 Safety issues for the DCLL BB in EU DEMO

Chemical and physical properties of LiPb

The phase diagram of LiPb alloy is showed in fig. 6-14, where the variation of phases is described in terms of system temperature and alloy composition. The LiPb eutectic alloy, which is used in DCLL and many other different applications is characterized by a percentage of Pb equal to 83% (99.3 wt%) and melting point of 235 °C.

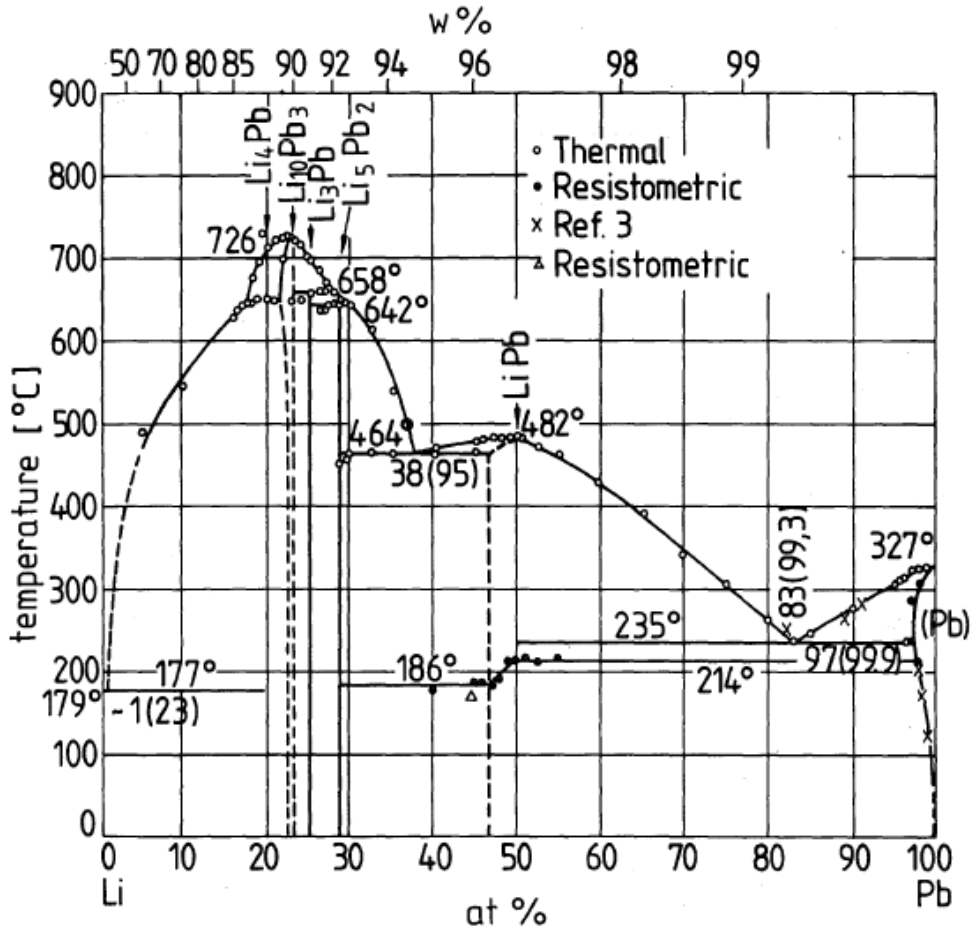

Figure 6-14 Phase diagram of LiPb alloy (Jauch et al., 1986)

The interaction between LiPb eutectic alloy and water are already studied in the frame of WCLL DEMO and ITER blanket.

With respect to the corrosion process of LiPb in touch with the EUROFER structure, the corrosion rate is evaluated equal to 300-900 μm/year, with a maximum LiPb velocity of 1 m/s in the BB. The lifetime of the BB is evaluated equal to 5-6 years (Rapisarda et al., 2015).

Main issues associated to the LiPb loop

A number of safety related issues have been identified during preliminary safety assessment of the DCLL BB. They are listed below:

- Tritium will be mostly present in the LiPb and a non-negligible amount may permeate into the helium circuit (Carloni, 2014);
- Erosion/corrosion phenomena are due to high metal velocity within the modules and manifolds, in particular fouling and high contamination (Carloni, 2014);
- Activation products, as Po-210 and Hg-203 (relatively volatile and highly radiotoxic) and Fe-55 or Mn-54 may be transported in the coolant (Carloni, 2014);
- Draining of the BB in accidental scenario is not possible (Carloni, 2014);
- Extremely high LiPb mass flow rate is present in DCLL (Rapisarda et al., 2016);
- MHD (Magnetic Hydro-Dynamic) effects have to be evaluated and limited (Rapisarda et al., 2016);
- LiPb pressure is of vital importance since a sudden overpressure can cause the total damage and the PAV (Permeation Against Vacuum) with consequences for safety (Carloni, 2014);
- Exothermic reactions of LiPb with air and water may take place in accidental conditions (Carloni, 2014);
- If high LM (liquid metal) oxidation takes place, a high hydrogen production could occur (Carloni, 2014);
- Hydrogen explosion can occur (Carloni, 2014);
- The LiPb can freeze, if the minimum temperature is lower than the melting point, e.g. for an overcooling of the breeding material;
- CCFs of all circuits have to be evaluated, when the design will be mature enough (Carloni, 2014);
- Eventual reactions between activated helium and LiPb have to be investigated (if any (Rapisarda et al., 2016).

In addition, a number of technical issues have been identified during this preliminary assessment:

- Recovery of the LiPb cooling system;

- Draining pipe on the bottom of the inboard and outboard BB segments;
- Measure and control of the Li content in LiPb;
- Measure and control of the oxygen content;
- Adapt the LiPb loop according to the technical solutions chosen for the TES and the purification system.

Study will verify whether it is relevant or not to use the expansion tank to remove helium bubbles from the LiPb alloy (Rapisarda et al., 2016).

6.2.3 Postulated initiating events (PIE)

Relevant events have been recognized by the FFMEA on HTSs (Heat Transfer Systems) of the DEMO DCLL and they are listed in table 6-9.

Table 6-9 : Relevant event from FFMEA (Bertinetti et al., 2016)

PIE	Description
AOP	Loss of Off Site Power
FD1	Loss of flow in the water primary cooling loop of the divertor because pump trip
FD2	Reduction of flow in the water cooling channels of one divertor cassette because internal clogging
FF1	Loss of flow in one primary cooling loop of the FW and blanket structures because compressor trip
FF2	Reduction of flow in cooling channels of FW and blanket structure of one module because internal clogging
FM1	Loss of LiPb flow in the liquid metal circuit because electromagnetic/mechanical pump trip: the LiPb flow is lost in all blanket modules supplied by the LiPb circuit
FM2	Loss of LiPb flow in one blanket module because clogging of the outlet pipe

HB99	Loss of heat sink in all FW, BZ and divertor primary cooling circuits because trip of both HP and LP turbines due to loss of condenser vacuum
HF1	Loss of heat sink in one cooling train of the blanket module (either BZ structure or FW)
LFB1	Large loss of helium from the FW cooling circuit inside breeder blanket box: Rupture of a sealing weld
LFB2	Leak of helium from the FW cooling circuit inside breeder blanket box: Leak of a sealing weld
LMO1	LOCA Out-VV because large rupture of the liquid metal loop (performing breeding and cooling functions)
LMO2	Leak Out-VV because small rupture of the liquid metal loop
LMO3	Rupture of the SG tubes of the liquid metal loop
LDO1	LOCA Out-VV because large rupture of the divertor primary cooling loop in the water manifold feeder inside PHTS Vault
LDO2	Leak Out-VV because small rupture of the divertor primary cooling loop in the water manifold feeder inside PHTS Vault
LDO3	LOCA Out-VV from the divertor primary cooling loop (DV-PHTS) because rupture of tubes in the Heat Exchanger with the secondary loop
LDV1	LOCA in-vessel because large rupture of the divertor cassette
LDV2	Leak in-vessel because small rupture of the divertor cassette
LFO1	LOCA Out-VV because large rupture of the FW primary cooling loop in the helium manifold feeder inside PHTS Vault
LFO2	Leak Out-VV because small rupture of the FW primary cooling loop in the helium manifold feeder inside PHTS Vault

LFO3	LOCA Out-VV from the first wall primary cooling loop because rupture of tubes in a Steam Generator
LFV1	LOCA in-vessel because large rupture of the FW structure: Complete rupture of the FW
LFV2	Leak of FW cooling circuit inside VV
N/S	Not Safety Relevant

All the PIEs reported are leading to safety relevant disturbance resulting in personnel exposure and environmental releases. Each event is briefly described in the following paragraphs.

AOP: Loss of off-site power

The loss of the power supply (Bertinetti et al., 2016) to the electrical equipment of DEMO can be determined by an external event (e.g. earthquake) or by a failure on the on-site electrical network. The reference event for the PIE is the unavailability of the electrical supply to all the system of the reactor; this could induce different accident scenarios:

1. Plasma disruption and possible in-vessel break either of FW, BZ and/or divertor modules because of thermal and mechanical stresses (events as discussed below for the in-vessel LOCA PIEs);
    - VV pressurization;
    - Pressure relief to Expansion Volume (EV) / Vacuum Vessel Pressure Suppression System (VVPSS), with eventual reactions between water from the divertor and LiPb from the BZ;
    - VV radioactive products and tritium released into EV/VVPSS and VV surrounding area through containment leaks;
    - Possible loss of VV penetration leak-tightness because the high overpressure inside the vessel.

2. Trip of pumps and consequential events as it will be discussed for loss of flow PIEs (see next paragraphs).

3. Trip of pumps, isolation of valves due to failed closed valves and consequential events as discussed for the loss of heat sink PIEs.

The following mitigating measures have been identified

- VV rupture disk opening;
- Release of pressure to EV/VVPSS;
- Start of Emergency Diesel generator;
- Start of the Emergency Cooling;
- Vent of Cryostat to reduce the temperature in the VV and its surrounding structures;
- Pressure relief from primary loops towards expansion volumes;
- Pressure relief from secondary loop towards expansion volumes.

FD1: Loss of flow in the primary cooling loop of the divertor because pump trip

Several causes can determine the loss of flow in the primary cooling loop of the divertor (Bertinetti et al., 2016). The selected representative event is the pump trip. As consequences of the initiator the following chain of accidents can occur:

- Loss of flow in the divertor cooling channels;
- Over-heating and over-pressurization of divertor primary loop;
- Loss of capability to remove plasma heat from divertor;
- Divertor rupture because thermal and/or mechanical (disruption) stress;
- In-vessel LOCA;
- VV pressurization;
- Pressure relief to VVPSS/EV;
- VV radioactive products and tritium released into VVPSS/EV room surrounding area through containment leaks;
- Possible loss of VV penetration leak-tightness because the high overpressure inside the vessel;
- VV radioactive products and tritium released into the VV surrounding area through penetration leaks.

Redundant detection and measures of primary loop parameters could be able to actuate automatic actions to get safe conditions in case of anomalies. The first action is the soft or fast plasma shutdown.

FD2: Loss of flow in cooling channels of one divertor cassette

Several initiators have been grouped under this PIE because similarity of the effects (Bertinetti et al., 2016). The selected representative event is the clogging of several cooling channels inside one divertor cassette. As consequences of the initiator, the following chain of accidents can occur:

- Loss/Reduction of capability to remove plasma heat and heat produced by the neutron reaction from the divertor cassette;
- Divertor rupture because local thermal and/or mechanical (disruption) stress;
- In-vessel LOCA from divertor;
- VV pressurization;
- Pressure relief to VVPSS/EV;
- VV radioactive products and tritium released into VVPSS/EV room surrounding area through containment leaks;
- Possible loss of VV penetration leak-tightness because the high overpressure inside the vessel.

Redundant detection and measures of primary loop parameters could be able to actuate automatic actions to get safe conditions in case of anomalies. The first action is the soft or fast plasma shutdown.

FF1: Loss of flow in one primary cooling loop of the FW and blanket structures

Several causes can determine the loss of helium flow in one primary cooling loop of the FW and blanket structures (Bertinetti et al., 2016). The selected representative event is the compressor trip. As consequences of the initiator the following chain of accidents can occur:

- Loss of flow in all the FW and BZ structure cooling channels;

- Loss of capability to remove plasma heat from FW segments and BZ structure;
- Over-heating and over-pressurization of primary loop;
- FW rupture because thermal and/or mechanical stress (plasma disruption can aggravate the thermo-mechanic load on the structures);
- In-vessel LOCA from FW and BZ structure of blanket modules;
- VV pressurization;
- Pressure relief to EV/VVPSS;
- VV radioactive products and tritium released into EV/VVPSS room surrounding area through containment leaks;
- Possible loss of VV penetration leak-tightness because the high overpressure inside the vessel
- VV radioactive products and tritium released into the VV surrounding area through penetration leaks.

Redundant detection of primary loop parameters could be able to actuate automatic actions to get safe conditions in case of anomalies. The first action is the soft or fast plasma shutdown.

As the breeding material is by independent primary loops, the damage and collapse of the FW could be prevented if safe mitigations are promptly activated.

If the LiPb is cooled even when the plasma is shutdown for a period long enough, it can solidify, especially in not well-isolated components. Special attention must be deserved for the LiPb storage tank design, in order to foresee safety component to prevent the LiPb solidification.

FF2: Loss of flow in cooling channels of FW and blanket structure of one blanket module

Several initiators have been grouped under this PIE because similarity of the effects (Bertinetti et al., 2016). The selected representative event is the clogging of several cooling channels inside the FW and BZ structures of one blanket module. As consequences of the initiator the following chain of accidents can occur:

- Loss/Reduction of capability to remove plasma heat and heat produced by the neutron reaction from the FW and/or BZ structures;
- FW rupture because thermal and/or mechanical stress (plasma disruption can aggravate the thermo-mechanic load on the structures);
- In-vessel LOCA from FW of blanket module;
- VV pressurization;
- Pressure relief to EV/VVPSS;
- VV radioactive products and tritium released into EV/VVPSS room surrounding area through containment leaks;
- Possible loss of VV penetration leak-tightness because the high overpressure inside the vessel.

Redundant detection of primary loop parameters could be able to actuate automatic actions to get safe conditions in case of anomalies. The first action is the soft or fast plasma shutdown.

As the breeding material is by independent primary loops, the damage and collapse of the FW could be prevented if safe mitigations are promptly activated.

If the LiPb is cooled even when the plasma is shutdown for a period long enough, it can solidify, especially in not well-isolated components. Special attention must be deserved for the LiPb storage tank design, in order to foresee safety component to prevent the LiPb solidification.

FM1: Loss of LiPb flow in the liquid metal circuit

Several causes can determine the loss of flow in LiPb loop (Bertinetti et al., 2016). The selected representative event is the trip of the electromagnetic/mechanical pump. As consequences of the initiator the following chain of accidents can occur:

- Overheating of the breeder material in all blanket modules;
- Expansion of the LiPb volume contained inside the blanket boxes;
- Increase of the level of LiPb inside the expansion tank;
- Possible stop of natural circulation flow of the LiPb in case of solidification of the liquid metal in the external part of the loop, in particular if pipes heaters are out of operation due to a common cause failure with the pump;

- Increase of the thermo-mechanical stress on the blanket box structures;
- Collapse of one of the blanket box structure;
- Release of LiPb coolant and He from FW channels inside the VV. The suction effect of the vacuum conditions inside the plasma chamber could facilitate the emptying of the LiPb loop;
- VV pressurization;
- Pressure relief to EV/VVPSS of the overpressure induced by the ingress of He (liquid metal alone does not generate overpressure);
- VV radioactive products and tritium released into the EV/VVPSS and through containment leaks;
- Possible loss of VV penetration leak-tightness because the high overpressure inside the vessel.

Redundant detection of LiPb loop parameters could be able to actuate automatic actions to get safe conditions in case of anomalies. The first action is the soft or fast plasma shutdown.

As the cooling of the BZ material and FW continues to operate even if the LiPb loses its flow, the damage and collapse of the blanket box could be prevented if safe mitigations are promptly activated.

FM2: Loss of LiPb flow inside one blanket module

The clogging of the outlet LiPb pipe from the blanket module is the initiating event (Bertinetti et al., 2016). As consequences of the initiator the same chain of accidents described for the FM1 PIE can occur, but in this case the anomaly is challenging only one blanket module:

- Overheating of the breeder material inside the blanket module;
- Expansion of the LiPb volume contained inside the blanket box;
- LiPb Increase of the thermo-mechanical stress on the blanket box structure and FW;
- Collapse of the blanket box structure and/or FW;
- Release of LiPb coolant and He from FW/BZ structure channels inside the VV. The suction effect of the vacuum conditions inside the plasma chamber could facilitate the emptying of the LiPb from the box;

- VV pressurization;
- Pressure relief to EV/VVPSS of the overpressure induced by the ingress of He (liquid metal alone does not generate overpressure);
- VV radioactive products and tritium released into the EV/VVPSS surrounding area through containment leaks.

Redundant detection of LiPb parameters inside the blanket could be able to actuate automatic actions to get safe conditions in case of anomalies. The first action is the soft or fast plasma shutdown.

As the cooling of the BZ material and FW continues to operate even if the LiPb loses its flow, the damage and collapse of the blanket box could be prevented if safe mitigations are promptly activated.

HB99: Loss of heat sink in all FW, BZ and divertor primary cooling circuits

This PIE (Bertinetti et al., 2016) can be related to the loss of secondary flow or the loss of secondary confinement due to the blockage of a valve or piping leak/rupture or the loss of component cooling or turbine protection intervention, e.g. in case of over-speed, high vibrations or imbalance. The reference event for the PIE is the loss of condenser vacuum for rupture of the condenser or of the interfacing lines. The PIE induces the unavailability of the heat sink to all the FW, BZ and divertor primary cooling systems of the reactor. The loss of condenser leak-tightness implies:

- Ingress of air into steam loop towards low pressure turbine;
- Loss of condenser vacuum;
- Turbines trip for protection intervention (high pressure control);
- Loss of saturated steam into turbine building once equalization of pressures;
- Building pressurization;
- Release into building of tritium permeated through SG;
- Direct release of tritium contained in secondary fluid towards the environment if HVAC is not promptly isolated;
- Fast over-pressurization of primary and secondary loops if plasma is not promptly shutdown;
- Pressure relief in primary;

- Leaks/ruptures in ex-vessel and in-vessel sections of primary loops can occur (other leaks/ruptures in secondary circuit can occur too). Both He, LiPb and divertor loops can be involved;
- Plasma disruption and possible in-vessel break of FW of blanket modules and or divertor cassettes;
- VV pressurization;
- Pressure relief to EV/VVPSS;
- Possible LiPb-water reaction in case of double rupture from blanket and divertor, with H_2 production;
- VV radioactive products and tritium released into EV surrounding area through containment leaks;
- Possible loss of VV penetration leak-tightness because the high overpressure inside the vessel.

The following preventing and mitigating features/actions have been identified:

- Redundant control of operating parameters in secondary circuit
    - Condenser and vacuum line parameters,
    - Parameters of vacuum equipment dedicated to remove incondensable gases from the condenser,
    - Hot well and degasser parameters,
    - Pressure relief devices,
    - Turbine control against over-speed, over-load, vibrations, etc.,
    - Interlock plasma operation with turbine and condenser parameters,
    - Closure of the HP stop valve and opening of the turbine by-pass valve;
- Pressure relief devices in primary circuits;
- Soft/Fast Plasma shutdown;
- VV rupture disk opening
    - Release of pressure to the EV/VVPSS;
- Switch-on atmosphere DS into building;
- Start of the Emergency Cooling (e.g. VV cooling circuit);
- Vent of Cryostat to reduce the temperature in the VV and its surrounding structures.

HF1: Loss of heat sink in one cooling train of the blanket module (either BZ structure or FW)

This PIE (Bertinetti et al., 2016) can be related to the loss of secondary flow or the loss of secondary confinement due to piping leak/rupture or valve leak/rupture in the section of the circuit interesting only one SG (e.g. high pressure steam lines from SG to steam collection header or, main steam safety valves). The reference event for the PIE is the unavailability of the heat sink to the FW primary loop cooling the FW and the BZ structures of all blanket modules in one sector of the reactor. This could imply:

- Damages of the steam circuit;
- Loss of steam into the building and building pressurization;
- Release into the building of tritium permeated through the steam generator and following environmental releases due to building leaks;
- Direct release of tritium contained in secondary fluid towards the environment if HVAC is not promptly isolated;
- Reduction of the capability to remove plasma heat from FW segments;
- Fast over-pressurization of FW primary loop if plasma is not promptly shutdown;
- Pressure relief in primary loop;
- Plasma disruption and possible in-vessel break of FW modules because of thermal and mechanical stresses;
- He ingress into the VV;
- VV pressurization;
- Pressure relief to the EV/VVPSS;
- VV radioactive products and tritium released into the EV/VVPSS surrounding area through containment leaks;
- Possible loss of VV penetration leak-tightness because the high overpressure inside the vessel.

The following preventing and mitigating features/actions have been identified:

- Redundant control of operating parameters in secondary circuit
    - SG parameters,
    - Pressure relief devices.
- Isolation of SG failed loop in secondary and primary side thank to a high efficiency isolation valves system.

- Pressure relief devices in primary circuits.
- Soft/Fast Plasma shutdown.
- VV rupture disk opening
    - Release of pressure to the EV/VVPSS.
- Switch-on atmosphere DS into building.
- Start of the Emergency Cooling (e.g. VV cooling circuit).
- Vent of Cryostat to reduce the temperature in the VV and its surrounding structures.

LFB1: Large loss of helium from the FW cooling circuit inside blanket box

The reference event for this PIE is the large loss of helium from the FW cooling circuit inside BB box because of a rupture of a sealing weld (Bertinetti et al., 2016). As consequences of the initiator the following chain of accidents can occur:

- Ingress of helium coolant into breeder box;
- LiPb-activated helium interaction (if any);
- Over-pressurization of breeder box and LiPb loop;
- Collapse of the blanket structure and/or rupture of the LiPb external loop, because both of them are not designed to withstand the He pressure of 8 MPa;
- Loss of LiPb and helium coolant into VV and/or loss of LiPb out-vessel because rupture in the external circuit;
- Possible failure of the LiPb external loop could also occur as consequences of the in-VV failure because the suction forces produced by the vacuum in plasma chamber (it has to be checked if the external LiPb circuit is able to keep leak-tightness also in high vacuum conditions):
- Ingress of air inside the VV through the by-pass opened through the internal and external breaks in the LiPb circuit;
- Reaction between LiPb and air;
- Risk of H_2 explosion, due to the H_2 production for the oxidation of the liquid metal;
- Possible air-dust reaction too with risk of explosion;
- VV pressurization;
- Pressure relief to EV/VVPSS;

- VV radioactive products and tritium released into EV/VVPSS surrounding area through containment leaks;
- Possible loss of VV penetration leak-tightness because the high overpressure inside the vessel;
- Tritium and activated dust contained inside the VV mobilized towards the port cell or building through the broken VV penetration and/or through the bypass generated in the LiPb.

Redundant detection of blanket box, helium loop and LiPb loop parameters could be able to actuate automatic actions to get safe conditions in case of anomalies. The first action is the soft or fast plasma shutdown. In this case, the leak before break conditions can play an important role in preventing catastrophic failures.

LFB2: Leak of Helium from the FW cooling circuit inside blanket box

The reference event for this PIE (Bertinetti et al., 2016) is the leak of helium from the FW cooling circuit inside breeder blanket box because loss of leak-tightness of a sealing weld.The consequences of the initiator, preventing and mitigating measures can be the same of the previous PIE LBB1. Clearly the transient of the accident chain should occur in longer time.

LMO1: LOCA Out-VV because large rupture of the liquid metal loop

The reference event for this PIE (Bertinetti et al., 2016) is the large loss of LiPb from cooling circuit inside the PHTS because large rupture of a manifold feeder. As consequences of the initiator the following chain of accidents can occur:

- Tritium and radioactive products contained in LiPb released into building;
- Eventual exothermic reaction between the LiPb and the air;
- Environmental release through building leaks;
- Environmental release through HVAC if not promptly isolated;
- Decrease of LiPb inventory inside the primary loop;
- Possible LiPb solidification in components not well heated up (e.g. storage tank);

- Loss/Reduction of capability to remove plasma heat and heat produced by the neutron reaction in the breeder;
- Expansion of the LiPb volume contained inside the blanket box;
- Increase of the thermo-mechanical stress on the blanket box structures;
- Collapse of one, or more than one, of the blanket box structure if the faulted loop is not promptly isolated and the plasma is not safely shutdown;
- Release of LiPb and helium (if also the FW fails) coolant inside the VV;
- Ingress of air inside the VV through the by-pass opened through the external and internal breaks in the LiPb circuit;
- Risk of H_2 explosion, due to the H_2 production for the oxidation of the liquid metal;
- Possible air-dust reaction too with risk of explosion;
- VV pressurization;
- Pressure relief to EV/VVPSS;
- VV radioactive products and tritium released into EV/VVPSS surrounding area through containment leaks;
- Possible loss of VV penetration leak-tightness because the high overpressure inside the vessel
- Tritium and activated dust contained inside the VV mobilized towards the port cell or building through the broken VV penetration and/or through the bypass generated in the LiPb circuit.

Redundant detection of blanket box, primary loop and LiPb circuit parameters could be able to actuate automatic actions to get safe conditions in case of anomalies. The first action is the soft or fast plasma shutdown. In this case, the leak before break conditions can play an important role in preventing catastrophic failures.

As the FW is cooled by an independent primary loop the damage and collapse of the blanket box could be prevented if safe mitigations are promptly activated.

LMO2: Leak Out-VV because small rupture of the liquid metal loop

The reference event for this PIE (Bertinetti et al., 2016) is the leak of LiPb from the liquid metal circuit inside the PHTS room because a small rupture of a manifold feeder.

The consequences of the initiator, preventing and mitigating measures can be the same of the previous PIE LBO1. Clearly the transient of the accident chain should occur in so longer time that all the consequential events inside the VV can be prevented. In any case, this event has to be considered because the following events:

- Hot liquid metal released in the room;
- LiPb reaction with the air producing H_2;
- Possible H_2 explosion inside the building in case explosive H_2-air concentration is achieved;
- Release of tritium and activated corrosion products contained in the LiPb loop released into the room;
- Release of tritium to the environment through HVAC if it is not promptly isolated;
- Release of tritium and activated corrosion products to the environment through building leaks.

The assessment of this PIE should define if the LiPb loop should be enclosed in secondary containment fulfilled by inert gas.

LMO3: Rupture of the SG tubes of the liquid metal loop

The reference event for this PIE (Bertinetti et al., 2016) is the large ingress of secondary water in the LiPb loop because of rupture of tubes in a SG. As consequences of the initiator the following chain of accidents can occur:

- Ingress of secondary water in the LiPb circuit;
- LiPb-water reaction inside the loop with H_2 production;
- Over pressurization of breeder box and LiPb loop;
- Collapse of the blanket box structure and/or rupture of the out-vessel LiPb circuit;
- Loss of LiPb and water coolant into VV in case of blanket box rupture. The suction effect of the vacuum conditions inside the plasma chamber could facilitate the emptying of the LiPb from the box and the loop and facilitate the release of secondary coolant water inside the VV;
- LiPb-water reaction inside the VV with H_2 production (large amount of LiPb can react);

- Risk of H_2 explosion;
- VV pressurization;
- Pressure relief to the EV/VVPSS;
- Possible loss of leak-tightness of a VV port plug due to thermo-mechanic stress (e.g. window);
- Release of VV activated products and tritium into port cell through the VV leak (after pressure equalization);
- Tritium and radioactive products contained in primary loop released into secondary loop (contamination of secondary loop).

Redundant detection of blanket box, primary loop and LiPb circuit parameters could be able to actuate automatic actions to get safe conditions in case of anomalies. The first action is the soft or fast plasma shutdown. Furthermore, as the FW is cooled by an independent primary loop the damage and collapse of the blanket box could be prevented if safe mitigations are promptly activated.

LDO1: LOCA Out-VV because large rupture of the divertor primary cooling loop

The reference event for this PIE (Bertinetti et al., 2016) is the large loss of water from the divertor primary cooling circuit inside the PHTS because large rupture of a manifold feeder. As consequences of the initiator the following chain of accidents can occur:

- PHTS pressurization;
- Tritium and radioactive products contained in coolant released into primary building;
- Environmental release through building leaks;
- Environmental release through HVAC if not promptly isolated;
- Decrease of water pressure and inventory inside the primary loop;
- Loss/Reduction of capability to remove plasma heat and heat produced by the neutron reaction from the breeder;
- Increase of the thermo-mechanical stress on the divertor structures;
- In-vessel LOCA from divertor cassette;
- Loss of water coolant into VV;

- VV pressurization;
- Pressure relief to EV/VVPSS;
- VV radioactive products and tritium released into EV/VVPSS room surrounding area through containment leaks;
- Possible loss of VV penetration leak-tightness because the high overpressure inside the vessel.

Redundant detection of primary loop parameters could be able to actuate automatic actions to get safe conditions in case of anomalies. The first action is the soft or fast plasma shutdown. In this case, the leak before break conditions can play an important role in preventing catastrophic failures.

LDO2: Leak Out-VV because small rupture of the divertor primary cooling loop

The reference event for this PIE (Bertinetti et al., 2016) is the leak of water from the divertor primary cooling circuit inside the PHTS because a small rupture of a manifold feeder. The consequences of the initiator, preventing and mitigating measures can be the same of the previous PIE LDO1. Clearly the transient of the accident chain should occur in longer time.

LDO3: LOCA Out-VV from the HX divertor primary cooling loop

The reference event for this PIE (Bertinetti et al., 2016) is the large loss of water from the divertor primary cooling circuit inside the secondary loop because rupture of tubes in the HX with the secondary loop. As consequences of the initiator the following chain of accidents can occur:

- Release of primary water into secondary loop;
- Tritium and radioactive products contained in primary loop released into secondary loop (contamination of secondary loop);
- Release of radioactive products through secondary loop leaks;
- Equalization of pressure between the two loops;
- Decrease of water pressure and inventory inside the primary loop;

- Loss/Reduction of capability to remove plasma heat and heat produced by the neutron reaction from the divertor;
- Divertor rupture because thermal and/or mechanical (disruption) stress;
- In-vessel LOCA;
- VV pressurization;
- Pressure relief to EV/VVPSS
- VV radioactive products and tritium released into EV/VVPSS room surrounding area through containment leaks;
- Possible loss of VV penetration leak-tightness because the high overpressure inside the vessel.

Redundant detection of primary loop parameters could be able to actuate automatic actions to get safe conditions in case of anomalies. The first action is the soft or fast plasma shutdown. Even if the induced in-vessel consequences are similar to the ones identified for the LDO1 PIE, here the transient to get criticality of the divertor structure is slower.

LDV1: LOCA in-vessel because large rupture of the divertor cassette

The reference event for this PIE (Bertinetti et al., 2016) is the large loss of water from the divertor primary cooling circuit inside the VV because large rupture of a divertor cassette. As consequences of the initiator the following chain of accidents can occur:

- Loss of water coolant into VV;
- VV pressurization;
- Pressure relief to EV/VVPSS;
- VV radioactive products and tritium released into EV/VVPSS room surrounding area through containment leaks;
- Possible loss of leak-tightness of a VV port plug due to thermo-mechanic stress (e.g. window);
- Release of VV activated products and tritium into port cell through the VV leak (after pressure equalization)

LDV2: Leak in-vessel because small rupture of the divertor cassette

The reference event for this PIE (Bertinetti et al., 2016) is the leak of water from the divertor primary cooling circuit inside the VV because a small rupture of the divertor cassette. The consequences of the initiator, preventing and mitigating measures can be the same of the previous PIE LDV1. Clearly the effects of the accident chain should be milder.

LFO1: LOCA Out-VV because large rupture of the FW primary cooling loop

The reference event for this PIE (Bertinetti et al., 2016) is the large loss of helium from the FW primary cooling circuit inside the PHTS because large rupture of a manifold feeder (ex-vessel LOCA). As consequences of the initiator the following chain of accidents can occur:

- PHTS pressurization (eventual asphyxiation problems for personnel);
- Tritium and radioactive products contained in coolant released into primary building;
- Environmental release through building leaks;
- Environmental release through HVAC if not promptly isolated;
- Decrease of helium pressure and inventory inside the primary loop;
- Loss/Reduction of capability to remove plasma heat and heat produced by the neutron reaction from the FW segments;
- Over-heating and over-pressurization of primary loop;
- FW rupture because thermal and/or mechanical stress (plasma disruption can aggravate the thermo-mechanic load on the structures);
- In-vessel LOCA from FW of blanket modules;
- VV pressurization;
- He pressure relief to EV/VVPSS;
- VV radioactive products and tritium (LiPb produced in the LiPb loop and permeated in the helium loop) released into EV/VVPSS and VV surrounding area through containment leaks;
- Ingress of air inside the VV through the by-pass opened through the external and internal breaks in the He circuit;
- Possible air-dust reaction too with risk of explosion;

- Possible loss of VV penetration leak-tightness because the high overpressure inside the vessel;
- Tritium and activated dust contained inside the VV mobilized towards the cooling room through the broken VV penetration and/or through the bypass generated in the He circuit.

Redundant detection of primary loop parameters could be able to actuate automatic actions to get safe conditions in case of anomalies. The first action is the soft or fast plasma shutdown. In this case, the leak before break conditions can play an important role in preventing catastrophic failures.

As the BZ is cooled by an independent primary loop the damage and collapse of the FW could be prevented if safe mitigations are promptly activated.

If the LiPb is cooled even when the plasma is shutdown for a period long enough, some solidification issues can occur, especially in not well-isolated components. Special attention must be deserved for the LiPb storage tank design, in order to foresee safety component to prevent the LiPb solidification.

LFO2: Leak Out-VV because small rupture of the FW primary cooling loop

The reference event for this PIE (Bertinetti et al., 2016) is the leak of helium from the FW primary cooling circuit inside the PHTS room because a small rupture of a manifold feeder. The consequences of the initiator, preventing and mitigating measures can be the same of the previous PIE LFO1. Clearly, the transient of the accident chain should occur in longer time.

LFO3: LOCA Out-VV from the SG of the first wall primary cooling loop

The reference event for this PIE (Bertinetti et al., 2016) is the large loss of helium from the FW primary cooling circuit inside the secondary water loop because rupture of tubes in the SG. As consequences of the initiator the following chain of accidents can occur:

- Release of primary helium into secondary loop;

- Tritium and radioactive products contained in primary loop released into secondary loop (contamination of secondary loop);
- Release of radioactive products through secondary loop leaks;
- Equalization of pressure between the two loops;
- Decrease of helium pressure and inventory inside the primary loop;
- Loss/Reduction of capability to remove plasma heat and heat produced by the neutron reaction from the FW;
- FW rupture because thermal and/or mechanical stress (plasma disruption can aggravate the thermo-mechanic load on the structures);
- In-vessel LOCA from FW of blanket modules;
- VV pressurization;
- Pressure relief to EV/VVPSS;
- VV radioactive products and tritium released into EV/VVPSS and VV surrounding area through containment leaks;
- Possible loss of VV penetration leak-tightness because the high overpressure inside the vessel.

Redundant detection of primary loop parameters could be able to actuate automatic actions to get safe conditions in case of anomalies. The first action is the soft or fast plasma shutdown.

Even if the induced in-vessel consequences are similar to the ones identified for the LFO1 PIE, here the transient to get criticality of the FW structure is slower. Furthermore, as the BZ is cooled by an independent primary loop the damage and collapse of the FW could be prevented if safe mitigations are promptly activated.

LFV1: LOCA in-vessel because large rupture of the FW structure

The reference event for this PIE (Bertinetti et al., 2016) is the large loss of helium from the FW primary cooling circuit inside the VV because large rupture of the FW structure. As consequences of the initiator the following chain of accidents can occur:

- Loss of helium coolant into VV;
- Loss of liquid LiPb inside VV (complete rupture of the FW is postulated);
- Possible failure of the LiPb external loop because the suction forces produced by the VV and possible subsequent reaction between LiPb and air;

- Risk of H_2 explosion, due to the H_2 production for the oxidation of the liquid metal;
- VV pressurization;
- Pressure relief to the EV/VVPSS;
- VV radioactive products and tritium released into EV/VVPSS surrounding area through containment leaks;
- Possible loss of VV penetration leak-tightness because the high overpressure inside the vessel.

LFV2: Leak of FW cooling circuit inside VV

The reference event for this PIE (Bertinetti et al., 2016) is the leak of helium from the FW primary cooling circuit inside the VV because a small rupture of the FW structure. The consequences of the initiator, preventing and mitigating measures can be the same of the previous PIE LFV1. Clearly the effects of the accident chain should be milder.

6.2.4 Considerations

Twenty-four relevant events have been recognized by the FFMEA on HTSs of the DEMO DCLL (18 event related to the cooling loops of the FW/blanket circuits, 5 related to the divertor cooling loops and 1 event to the general loss of power supply) (Pinna et al., 2017). All the PIEs are leading to safety relevant disturbance resulting in personnel exposure and environmental releases. Between these events, the most serious events, which should deserve the first attention in terms of deterministic analysis, could be the following:

- FD1 Loss of flow in the primary cooling loop of the divertor because pump trip
- FF1 Loss of flow in one primary cooling loop of the FW and blanket structures because compressor trip
- FM1 Loss of LiPb flow in the liquid metal circuit because electromagnetic/mechanical pump trip: the LiPb flow is lost in all blanket modules supplied by the LiPb circuit

- HB99 Loss of heat sink in all FW, BZ and divertor primary cooling circuits because trip of both HP and LP turbines due to loss of condenser vacuum
- HF1 Loss of heat sink in one cooling train of the blanket module (either BZ structure or FW)
- LDO1 LOCA Out-VV because large rupture of the divertor primary cooling loop in the water manifold feeder inside PHTS Vault
- LDO3 LOCA Out-VV from the divertor primary cooling loop (DV-PHTS) because rupture of tubes in the Heat Exchanger with the secondary loop
- LDV1 LOCA in-vessel because large rupture of the divertor cassette
- LFO1 LOCA Out-VV because large rupture of the FW primary cooling loop in the Helium manifold feeder inside PHTS Vault
- LFO3 LOCA Out-VV from the first wall primary cooling loop because rupture of tubes in a Steam Generator
- LMO1 LOCA Out-VV because large rupture of the liquid metal loop
- LFV1 LOCA in-vessel because large rupture of the FW structure: Complete rupture of the FW
- LMO3 Rupture of the SG tubes of the liquid metal loop.

Deterministic analyses shall demonstrate capability of the plant to manage the possible accident sequence and mitigate the consequences.

Conclusions

New generation reactors challenge the traditional safety assessment methodology, metrics, tools and standards. The major objective of this work is to develop a methodology able to drive the safety demonstration of an innovative system along the design development. A risk-informed iterative approach is pursued: the reactor preliminary design evolves thanks to preliminary risk assessment results and the updated design must undergo a more specific safety demonstration. The entire process must guarantee the achievement of the predefined safety goals and satisfy the risk tolerability criteria.

New generation systems present a wide spectrum of different technologies, materials and design with respect to the standardization of the Light Water Reactors; therefore, their safety demonstration has to rely on an updated framework of risk metrics, tolerability criteria and safety objectives, always chasing the satisfaction of the fundamental safety objective.

Since the proposed methodology is specifically developed for systems at the very preliminary design stage, technology neutral risk metrics can be used (see paragraph 2.2.2). Even if they lack of specificities and indications to guarantee consistent, uniform and unique interpretation of rules, with a consequent slowdown of the entire process, their arrangement to new system is facilitated for any technology. When the design of the analyzed system will be more detailed, technology specific criteria can be developed, as it occurred for the boiling temperature criteria for SFRs (IRSN, 2015).

Moreover, a risk-informed approach (see paragraph 2.2.2) may represent a compromise between the purely deterministic and conservative approach (i.e. the traditional regulative structure) and the risk-based approach, which is based on scenarios frequency and consequences evaluations using the best estimate values, which is more realistic but not suitable for conceptual design because of its low conservatism and of the uncertainties characterizing the results of the PSA of innovative systems.

In addition, a risk-based approach has never been completely accepted in the nuclear field.

On the other hand, the deterministic approach needs to be guided in the wide spectrum of phenomena characterizing new generation installations, which are often still research topics and are possibly very different for LWRs ones. The risk-informed strategy suits particularly well to innovative systems, since it helps the identification of the major risk contributors, criticalities and needs for additional safety provisions. In fact, it considers a major number of events sequences and prioritize them on the basis of risk importance, previous/similar operating experience, experts' elicitation. Moreover, it always considers the source of uncertainties that can highlight the need of more stringent requirements or regulatory actions, even if the list of uncertainties can be incomplete for conceptual INS.

Furthermore, performance-based requirements (see paragraph 2.2.2) are flexible enough to be adequate to new technologies, concentrating all the efforts for the fulfillment of the final goal. They enhance a continuous improvement of the system, but lack of unique means to understand if the objective is achieved, slowing the safety demonstration. In particular, risk informed and performance-based requirements help the safety assessment to give feedbacks on the design and drive its development. The methodology definition is fundamental to guarantee a systematic and as complete as possible analysis, based on functional safety. This aspect has been consistently assessed in the IEC 61508 (2005), a milestone for safety driven design. Some attempts to import the key implications of the functional safety have already been experienced (e.g. through the IEC 61513), but the will to maintain the rigid traditional safety approach led to a misrepresentation of the 61508 nature and constitutes another proof that the stiff process developed for LWRs is difficult to be applied to new generation concepts.

The main objective of the proposed methodology is to guarantee that the design evolution is always guided by safety analyses, in particular, a comprehensive understanding of safety related design vulnerabilities and the resulting implications for the risk. Its application to the case studies, in particular the identification of a list of questions about components, phenomena, procedures, physical and chemical variables and the preliminary sketch of the safety architecture, demonstrates the practical nature of the proposed approach, whose results have to be continuously updated coherently with the design evolution.

For example for the MSFR, the implementation of the methodology led to the definition of a list of relevant initiating events (PIEs), which will be further analyzed through deterministic analyses. They represent the most challenging conditions for the plant and will drive the dimensioning of the protection systems and the physical barriers, in agreement with the outputs of the quantitative studies. Additionally, the implementation of the LODs tool to some PIES, judged particularly interesting for the system, helped to preliminary assess whether the foreseen safety provisions are sufficient to cope with the accidental scenario or if additional measures have to be defined.

The implementation of these tools at a very early design stage aims at plenty fulfilling the safety and reliability criteria identified by the GIF IV and is coherent with the common practice in non-nuclear field.

A major criticality of the safety demonstration of the new generation systems is the uncertainties management; both the input data and the results are not punctual and evolves continuously. The proposed and applied approach could not prescriptive/proscriptive neither technology-specific as the one of LWRs; its technology-neutral (in fact the method has been applied to very different reactors) and performance-based characteristics try to take advantage of their own flexibility to manage the constantly variable domain of analysis, especially for conceptual design. Consequently, a difficulty in the application of this method is the non-unique guidelines: for example, for the PIEs selection different approaches have been proposed: the first one purely deterministic (based only of the severity of the consequences) and the second one risk-informed (introducing a very preliminary evaluation of the frequencies).

The safety demonstration framework defined in this work has a nature at the same time risk-informed and deterministic. For example, the LOD method took advantage of the risk-informed characteristics, in fact the low frequency of the initiator can stand as a LOD itself. On the other hand, the deterministic analysis and the quantitative results are essential for the definition of the safety margins and the demonstration of their satisfaction.

Appendix A – Lessons learned: MSFR Design open points

The objective of this section is to list the design open points raised from the MSFR safety analysis, especially from the application of the FFMEA and the MLD methods.

The list is composed of questions raised during the application of the methodology as well as suggestions to enhance the safety of the concept. These open points have been classified according to their type: systems, components, procedures, physical and chemical variables and phenomena. Moreover, the link between the safety demonstration and design evolution is highlighted (Allibert et al., 2018).

All the considerations regard the design as defined in the deliverable 1.1 of SAMOFAR project (Allibert et al., 2017).

It is important to highlight that the question about the definition of physical barriers is not only linked to the design, but also to safety considerations. It is reported in Appendix B.

8.1 Phenomena

Are there any dangerous chemical reactions between the fuel salt and all the other fluids inside the core cavity?

In theory, chemical reaction will not occur between the fuel salt and the intermediate salt (both the salts should be fluorides, therefore compatible) and all the other fluids in the core cavity and in the fuel recirculation circuits; however further analyses would be performed, when the intermediate salt will be definitively chosen (different options are still taken into account for the intermediate salt). The reaction

of the fuel with the other fluids that might be in the core cavity should also be analyzed (e.g. with the lead located in the decay tank for FPs).

In many accidents/incidents, the role of the natural circulation of the fissile salt/fertile salt and intermediate salt is not clear and demonstrated.

According to the current design, the natural circulation of the fuel salt cannot be activated since a sufficient difference between the heights of hot and the cold barycenters is not sufficient; in fact, in the current design they are at the same level. Some design arrangement could be made if the natural convection in the fuel circuit is considered necessary. As well, the possibility to have natural convection in the fertile and intermediate circuits has to be determined and its efficiency should be studied once the design of these circuits will be defined. Moreover, from the neutronics point of view, the effects of the instauration of natural convection should be analyzed, since it would imply a decrease of reactivity with respect to the case of fixed fuel salt (no circulation).

8.2 Parameters and variables issues

Is the pressure of the fuel circuit higher, equal or lower than the pressure of the inert gas in the reactor vessel?

From the safety point of view, the overpressure of the reactor vessel with respect to the core cavity could be preferred because, in case of accidents, volatile FPs are kept inside the core cavity for a certain transient time (pressures equilibrium). However, in case of a breach in the upper reflector at the pump level, the overpressure in the reactor vessel could lead to an unwanted gas entrance increasing the risk of pump cavitation, therefore the stop of the fuel salt flowrate. The pressure should also be set in order to reliably detect a reactor vessel leak (to be further investigated).

8.3 Systems

Is a depressurization system for the reactor vessel needed and further defined and developed?

If the pressure of the reactor vessel in normal conditions is lower than or equal to the pressure of the core vessel, in case of accident (involving a loss of containment of the core vessel), the gaseous FPs and the gas of the fission products removal system would exit from the core cavity to the reactor vessel increasing its pressure. In that case, before adding a depressurization system for the reactor vessel, the plausible pressure levels that can be reached must first be assessed. The strategy should be to try to ensure confinement as close as possible to the source term (and avoid its spreading in the facility).

The heating systems for the intermediate salt should be defined and designed.

In case of fuel salt drain, the intermediate salt would lose its heat source and may solidify: a heating system for the intermediate salt should be designed, in order to highlight sensible areas (i.e. the areas where the intermediate salt can easily solidify). This is important to ensure the intermediate salt draining (e.g. for maintenance actions) and to properly transfer the heat when the fuel will be re-injected in the core to restart the reactor.

The fertile salt must be maintained at liquid state in order to be drained in the controlled routine draining tanks: are there any heating systems or is the intermediate salt sufficient to maintain the fertile salt at the liquid state? Is the decay heat sufficient to maintain the fertile salt at the liquid state?

In case of fuel salt drain or loss, the fertile salt would lose its main heat source and it may solidify if its decay heat is not sufficient to maintain it at the liquid state. This is important for the fertile salt draining in the routine storage tank, e.g. for maintenance actions. The decay heat of the blanket salt should be studied in order

to understand if it is sufficient to maintain the salt at the liquid state or if it is excessive and the blanket should be cooled down.

If the storage tank for the gas of the fission products removal system is different from the expansion vessel, a system to isolate the storage tank should be designed.

If the core cavity is damaged and the fuel salt is drained, the flow of the gas (He) of the FPs removal system should be interrupted and its storage should be isolated, in order to avoid the release of gas in the reactor vessel. Therefore, a system to isolate the purification gas storage tank should be foreseen, if the storage tank is not the expansion vessel, located in the upper reflector.

Is the cooling system for the structures separated from the cooling system for the fissile and fertile salt (3 independent and separated circuits)?

The question is about the number of independent circuits required to cool down the fuel salt, the fertile salt and the structures. If there are different separated circuits, the loss of one of them would not imply the loss of the cooling of the other systems. On the other hand, 3 different circuits would increase the complexity of the system (it is plausible that collectors or several heat exchangers would be necessary). If a unique circuit is chosen for the design, it would be necessary to choose between the configurations in series or in parallel (see question below): this solution could simplify the design, but the consequences of a breach in the unique circuit would be more severe. Furthermore, one single intermediate circuit cools down four recirculation sectors, therefore a total of four intermediate circuits for the fuel salt is foreseen: further design studies should be performed to define the appropriate number of cooling systems for the structures, as well as for the fertile salt.

Different options for the disposition of the heat exchangers (HX) between the fertile/fissile salt and the intermediate salt and the HX for walls cooling (In series or in parallel)

The two propositions for the disposition of the heat exchangers are shown in fig. 8-1.

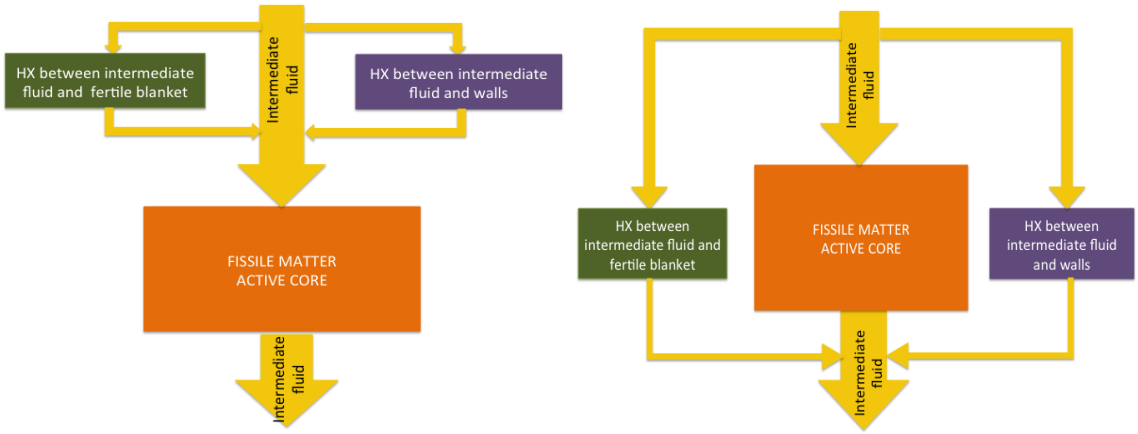

Figure 8-1 The heat exchangers are disposed in series (left), the heat exchangers are disposed in parallel (right)

The first proposition is more advantageous from the thermodynamics point of view because the outlet temperatures from the HXs with the fertile blanket and with the walls are supposed to be much lower than the outlet temperature from the active core.

The second proposition is more advantageous from the regulation point of view: the core reactivity is regulated through the temperature of the heat exchangers, and mainly through the HXs between the fissile salt and the intermediate fluid; this proposition allows a direct control of the intermediate salt temperature, without taking into account the heat exchange with the other heat sources (i.e. walls and fertile blanket).

It is also important to define the locations of the HXs and of the collectors for the intermediate fluid.

A system to evaluate the level of fuel in the expansion vessel would be useful to detect problems of the expansion vessel system.

It is important to monitor the fuel volume dilation in the expansion vessel. In case of loss of containment in the upper part of the core cavity and excessive fuel dilation, the fuel salt could exit from the expansion vessel.

The cooling system of the EDS should be defined.

The two options are listed in SAMOFAR D1.1 (Allibert et al., 2017), even if the hypothesis of a set of heat pipes is more likely than the one with water pool. In the case of a set of heat pipes, the complexity of the system would increase, but the probability of an aggressive chemical reaction of a leakage of fuel salt or intermediate salt falling down in the water pool would be zeroed, lowering the chemical hazard. Another option, with a gas (air or inert salt) as cooling fluid, is also under analysis.

Is there an in-core Decay Heat Removal System (DHRS)?

If it is possible to shut down the core and maintain the fissile salt inside the core cavity, would a DHRS exist or would a smaller part of the intermediate fluid mass flow be used to evacuate the decay heat?

8.4 Components and materials

8.4.1 Fuel circuit pump

Different options for the circulation pump: 1) mechanical or 2) magnetic driven pump.

In option 1), we consider that mechanical pumps would be used to ensure the fuel circulation in the fuel circuit. In this option, openings must be provided in the sector lid in order to let the pump shaft pass through.

In option 2), we consider that magnetic driven pumps would be used for the fuel circulation. In this option, the pump shaft rotation is magnetically driven and the openings in the sector lids (if any) are not necessary. Option 2 would be preferable from leak-tightness point of view.

8.4.2 Component of the upper closure of the core cavity

The lid and the sampling system location at the top of the expansion vessel could represent a weak point.

The lid located over the expansion vessel closes the upper reflector (and therefore the core cavity) when the sampling device is not functioning. The question is about the dimension of the lid with respect to the dimensions of the upper reflector: if the upper reflector is much thicker than the lid, it is plausible that the lid could constitute a weak point for the leak-tightness of the core cavity containing the fuel salt.

In addition, the lid as well as the sampling device will be in contact with the gaseous FPs and it could be in contact with the fuel. It could be useful to quantify the irradiation damage on these systems, whose walls can be thinner than the upper reflector ones and made of different materials.

To improve the confinement of the radioactive matter, the opening for fuel sampling should be reduced as much as possible. During the substitution of the sampling device with the lid (and vice versa), the core cavity should be isolated in order to guarantee the leak-proof containment of the fuel salt and of the FPs. Therefore, a closure (gate/lock) to isolate the core cavity and the reactor vessel should be designed, for ensuring the confinement of the radioactive matter during the substitution operations.

Finally, another option for the sampling of the fuel salt is under study where the sampling is performed through pipes entering the fuel circuit (in the same way as the normal draining pipes). This option could reduce the risks of loss of fuel circuit leak-tightness.

The design of the upper reflector could help the fuel reinjection in the core cavity, for example a slope of the walls can be foreseen in function of the volume of the expansion vessel and all the other free volumes present in the core cavity.

If the fuel salt will exit from the core cavity in its upper part (e.g. in case of breach in the upper part of the reactor and excessive fuel dilation), it could solidify outside the core cavity if it will not be helped to re-enter, for example with a slope of the walls (it could help maintenance actions).

8.4.3 Components of the fission product removal system

The components of the fission products removal system should be determined.

The fission products removal system is supposed to remove both solid and gaseous FPs online. The configuration of the system is still conceptual, for example the presence of fluids (e.g. lead) is foreseen for the salt cleaning, but specific analyses of materials compatibility are necessary. Moreover, the components of this system have not been specified.

Different options for gas circulation in fission products removal system: 1) liquid ring pump before the decay tank; 2) Compressor after the decay tank; 3) both.

In option 1), a liquid ring pump will be located between the gas separation chamber and the decay tank. This option allows the compression of the gas before entering the decay tank and a more compact decay tank dimensioning. However, this option implies a higher pressure in the decay tank than in the separation chamber.

In option 2), there will not be any pump between the gas separation chamber and the decay tank but a compressor after the decay tank. This option allows having a lower pressure in the decay tank than in the gas separation chamber that would make the gas flow passively between the two components thanks to the pressure

difference. However, as the gas is not compressed when entering the decay tank, this one has to be larger than in option 1. The compressor after the decay tank is used to control the gas pressure in the pipes between the decay tank and the bubble injector.

In option 3), we consider both a liquid ring pump between the gas separation chamber and the decay tank to limit the decay tank volume and a compressor after the decay tank to control the gas pressure in the pipes and at the bubble injectors.

Is there a purification system for the lead filter in the fission products removal system? Or will it be changed regularly?

A lead filter will be necessary to remove mainly metallic FPs. Its efficiency will be reduced with time, therefore a cleaning system has to be designed or the filter has to be substituted after a certain period of time (almost every 3 years). In the first case the system will be more complex and another fluid could be necessary, but the efficiency of the filter will be quite constant. In the second case the system will be simpler but the efficiency of the filter will decrease during the system life.

The diameter of the bubble injectors (for reactivity control and fission products removal system) should be defined.

The diameter is important because the injector could be obstructed or damaged if solid pieces would be present in the core cavity due to previous incidents/accidents or if small parts of the fuel solidify. In case of an incident where the fuel salt would go inside the injector, the probability that fuel would solidify is higher if the diameter of the pipes for gas injection is small. If the pipes have a large diameter, the fuel may contaminate a larger portion of the fission products removal system / reactivity control system before its solidification.

The location of the pipe could also be modified so that the pipes could remain inside the core vessel and limit the impact of a pipe rupture. In this case, a pipe rupture would not imply a draining of the salt anymore.

The presence/absence of a blockage valve inside the injector should be determined.

If the pipes connecting the purification gas storage tank to the injector are external to the core cavity, a breach in the pipe will be similar to a breach in the lower reflector; therefore, the fuel will be lost in the collector before, and then in the EDS. In order to avoid the fuel loss, a blockage valve could be useful to guarantee the core cavity integrity (even if a channel for the inlet of purification salt will be lost).

The existence of a valve to isolate fission products removal system has to be verified.

This is important in order to block the continuous injection of purification gas in case of accident, especially if the accident involves the loss of integrity and leak-tightness of the core cavity.

8.4.4 Components of the intermediate circuit and the cooling circuit for the structures

Valves to isolate the cooling circuit for the structures can be necessary.

In case of breach in the cooling system for the structures, a blockage valve could be very useful in order not to lose a large quantity of intermediate salt. The importance of these valves increases in the case of a unique cooling circuit for the fuel salt, for the fertile salt and for the structures. Indeed, if a single circuit is used, a loss of heat sink would imply a loss of cooling for the fuel as well as for the structures and the fertile salt.

Valves to isolate the intermediate circuit at the level of the reactor vessel walls can be necessary to limit the spreading of radioactive matter if the intermediate is contaminated by the fuel.

These valves will be important especially if the fuel salt or gaseous FPs exit from the recirculation sectors and go in the intermediate circuits (e.g. in case of a

breach in the HX). In order to contain the radioactive matter inside the reactor vessel, some valves should be foreseen to block the intermediate salt before going in the BoP area of the system, therefore before entering in the HX between the intermediate salt and the BoP fluid.

8.5 Procedures

8.5.1 Procedures related to the draining systems

Is the EDS used only for accidental situations or can be used for incidental situations or small deviation from normal operation?

In the reference MSFR design described in SAMOFAR deliverable 1.1, the EDS is supposed to be used only in case of emergency. The use of the EDS would imply that the reactor is strongly damaged. Another option is to use the EDS not only for accidental conditions but also for incidental conditions or maintenance operations. The purpose of this second option is to make the EDS behave as storage tank and the so called “storage tanks” as draining tank for start-up and shutdown.

In case of small deviations from normal operation, is it possible to use controlled routine draining tanks instead of EDS?

The question is about the procedure of management of deviations from normal operations (both small and large ones). If the EDS is used only in case of severe accidents, how can the small deviations be managed? Are the routine draining tanks used for draining the salt in order to allow maintenance? Are some small deviations monitored? Moreover, which deviations can be considered small and where is the limit between small and large deviations?

It is necessary to define when the EDS will be triggered, in function of the temperature and the pressure and if there are other methods to face incident not including the EDS triggering.

This question is linked to the previous ones and it is about the physical/chemical parameters triggering the EDS and their thresholds: for example, the maximum temperature above which the EDS is activated (the same for the pressure and for the other connected parameters, if any).

If the deviations (incident and accident) will be always faced with EDS, it could be worth to allow the recovery of the fuel salt.

If all the deviations (small and large ones) will be managed by the EDS, it may be useful to design a system to recover the fuel salt and to re-inject it in the core cavity or to send it to the storage tanks or to the reprocessing unit if necessary.

It can be useful that the routine storage tanks are in overpressure when they are not used.

In case of rupture of the valve separating the recirculation sectors from the routine draining tanks when they are not in function, the overpressure of the routine draining tank could avoid the exit of the fuel salt from the core cavity and its probable solidification in the pipe connecting the recirculation sectors and the routine draining tanks.

8.5.2 Procedures related to salt sampling

In the case that the valve separating the pressurized sampling device from the expansion vessel does not work and the failure is detected, the fuel salt should be drained in the routine storage tanks before removing the pressurized sampling device for maintenance (specific procedures).

If the valve separating the pressurized sampling device (as well as the condenser lid) from the expansion vessel fails to close during the substitution operation and if

the failure is detected, a procedure for the fuel salt drain should be activated, because the stuck open valve is equivalent to have a breach in the upper reflector and the function of ensuring the integrity and leak-tightness of the core cavity will be lost.

The procedures to move the fuel/fertile salt samples (inside the reactor building and from the reactor building to the reprocessing unit) should be defined.

The online sampling of the fuel salt and of the fertile salt is postulated, but the procedure of transferring the salts from the core cavity to the reprocessing unit is not defined yet.

8.5.3 Procedures related to reactivity control

What is the procedure in case of a small insertion of positive/negative reactivity? Is the reactor shutdown, monitored by temperature or by the bubbling system for reactivity control?

The question is about how to manage reactivity in the core cavity, especially during transients, such as the shutdown. Knowing that there are different systems to control the reactivity, which is the most efficient (therefore which one will be used) in the different unsteady situations?

Appendix B – Physical barriers definition for MSFR

Defence in depth is a safety philosophy that drives the design, construction, inspection, operation, and regulation of all nuclear facilities. Its objective is to protect the health and safety of people, to protect the environment and to ensure the availability and reliability of the facility. It is implemented through a number of measures, such as physical barriers, safety systems redundancy and diversification, strong physical security, and emergency response preparedness. In particular**, multiple, successive barriers** are designed to avoid accidental radioactive material releases.

According to IRSN definition (IRSN, 2015), "a severe accident is one in which the reactor fuel is significantly damaged due to a more or less complete core melt. This core melt is the consequence of a large temperature increase of the materials comprising the core, itself resulting from prolonged loss of core heat extraction by coolant fluid. This failure can occur only as a consequence of a large number of dysfunctions, so that its probability of occurrence is very small".

For solid-fuelled reactors (in particular LWRs), a severe accident implies:

- The loss of the first confinement barrier (the cladding);
- The loss of 2 over 3 safety functions (the heat extraction and the control of the reactivity chain);
- The third function (confinement of radioactive materials) is put on risk.

As a consequence, **a severe accident may jeopardize the integrity of many or all of the barriers to the release of radioactive material** (IAEA, 2009). Moreover, the risk of barriers degradation is one of the criteria used by the regulators to select the accidental events to be reported: "any event or abnormal condition that resulted in the condition of the nuclear installation, including its principal safety barriers, being seriously degraded" (IAEA, 2006b).

The given-above definition of a severe accident is well suited to LWRs, but difficult to be applied to other concepts. For instance, in SFRs or LFRs, the structure may in some conditions collapse before the core melting and, in VHTRs, fuel melt is considered highly improbable, or even impossible. Finally, for MSRs, the normal core state is liquid and the core melt accident has no equivalent. In 2015, for generation IV nuclear concepts, IRSN formulated a new definition of a severe accident (IRSN, 2015): “A severe accident in a nuclear reactor is an accident during which the nuclear fuel radioelement confinement function is significantly degraded, regardless whether the fuel is inside the reactor, being handled or in a storage area” (Vitkova et al., 2006). Some considerations about the application of this definition to new generation concepts can be found in paragraph 2.2.3.

Since in the case of a liquid-fuelled reactor, there is no direct equivalent of a solid-fuelled reactor accident with core melting and relative physical barriers, the aim of this chapter is to propose a definition of containment barriers useful for liquid-fuelled reactors, and for MSFR in particular.

9.1 Safety related characteristics of MSFR

The MSFR has unique features that make the standard safety definitions difficult to apply. The objective of this paragraph is to summarize the characteristics of MSFR that are related to safety.

Liquid fuel

Most MSFR peculiarities (Allibert et al., 2018) derive from the fact that it uses a liquid fuel in the form of a molten salt that plays the role of coolant as well. Some of the consequences are listed below:

- Heat is produced directly in the heat transfer fluid;
- Possibility to reconfigure passively the geometry of the fuel;
- Possibility to drain the fuel;
- Possibility to reprocess and load fuel during reactor operation.

Fuel circulation

In the MSFR, as in many MSR concepts, the fuel is circulating. Due to the relatively high speed and the turbulences in the core, the fuel is continuously mixed, therefore:

- Fuel composition is relatively homogeneous;
- Fuel irradiation is relatively uniform without need for loading plans.

Constraints on fuel circuit structure materials

The constraints on the fuel circuit structures are quite different from those of a LWR primary circuit, for instance:

- The fuel circuit is at low pressure (atmospheric pressure);
- The structures have to stand high temperatures;
- Heat exchangers, pumps and fuel circuit instrumentations are in contact with the fuel and under radiation (relatively low as they are located out of the core region);
- No structures are located in the core.

Reactivity control

The reactivity reserves in core are quite low for several reasons including:

- The daily/frequent fuel composition adjustment thanks to the fuel reprocessing and loading during reactor operation (even if it can involve incorrect fuel composition in case of mixing problems);
- The absence of absorber rods (a “geometric” control rod is still under consideration for start-up and shut-down) (IAEA, 2009).

Containment characteristics

In the MSFR, the fuel location is more dispersed than in a solid-fuelled reactor and the first confinement barrier is therefore challenging to be defined. The choice of the confinement barriers is impacted by:

- The absence of cladding;
- A significant part of fissile inventory located outside the core in the fuel recirculation sectors;
- The fuel and blanket sampling that are made during reactor operation for reprocessing, as well as the injections of reprocessed salt;
- The connections between the fuel circuit and the draining tanks and the possibility to lose a part of the salt during the transfers.

Concept under development

The safety analysis of the MSFR is limited by the available knowledge on the plant and the reactor operation. Indeed:

- The design is in development;
- Start-up and shutdown procedure are still under development;
- Inspection and maintenance procedures are not defined.

9.2 **Bibliographic survey**

The MSFR present a set of characterizing safety aspects that make difficult the definition of the physical multiple barriers and of the severe accident. Hence, this paragraph aims to find some directives in the IAEA reports (see paragraph 9.2.1) and some analogies with other NPP systems (see paragraph 9.2.2) in order to drive our analysis. Moreover, some propositions have already been done and represent the starting point for a more detailed one (see paragraph 9.2.3).

9.2.1 Rules for the definition of the containment barrier from IAEA reports

The fundamental safety objective of nuclear safety is to protect people and the environment from harmful effects of ionizing radiation (IAEA, 2006).

The primary means of preventing accidents in a nuclear power plant and mitigating the consequences of accidents is the application of the concept of DiD. A relevant aspect of the implementation of defence in depth for a nuclear power plant is the provision in the design of a series of physical barriers, as well as a combination of active, passive and inherent safety features that contribute to the effectiveness of the physical barriers in confining radioactive material at specified locations (IAEA, 2016).

The aim of this paragraph is to list the prescriptions found in the IAEA safety requirements and IAEA Safety Guides that are useful to drive the definition of the safety barriers in the MSFR.

1) Barriers shall be independent as far as is practicable (IAEA, 2016).
2) The number of barrier that will be necessary will depend upon the initial source term in terms of the amount and isotopic composition radionuclides, the effectiveness of the individual barriers, the possible internal and external hazards and the potential consequences of failures (IAEA, 2016).
3) The design shall provide for multiple physical barriers (IAEA, 2016).
4) The construction shall be of high quality so as to minimize the failures and the deviations from normal operation and to prevent that a small deviation leads to a cliff-edge effect (IAEA, 2016).
5) The design shall prevent challenges to the integrity of physical barriers, the failure of one or more barriers, the failure of a barrier as a consequence of the failure of another barrier, the accident conditions escalation (IAEA, 2016), the by-pass of a barrier (IAEA, 2016b).
6) If one level of barrier were to fail, the subsequent level would be available (IAEA, 2006b).
7) Risk assessment will determine whether barriers incorporated in the design fulfil the safety functions required of them (IAEA, 2016b).

8) Special attention has been paid for internal and external events that can challenge more than one barrier (IAEA, 2016b)

9) The selection of the main barriers should be described and justified (IAEA, 2004).

10) For each group of PIE the plant response should be assessed as well as the status of the barriers (IAEA, 2004).

11) Deterministic safety analyses are required to demonstrate that barriers to the release of radioactive material will prevent an uncontrolled release to the environment for all plant states (IAEA, 2009b).

12) The accidents where major barriers such as the containment may be ineffective should be identified, and it should be ensured that analyses are performed for these transients (IAEA Safety Standard, SSG-2, 2009). All credible failure mechanisms of the different barriers should be analysed (IAEA, 2009b).

13) Acceptance criteria should be set in terms of the variable or variables that directly govern the physical processes that challenge the integrity of a barrier (IAEA, 2009b).

14) Deterministic safety analyses are to demonstrate that, in normal operational conditions and accident conditions, a sufficient number of barriers are retained (IAEA, 2009b).

15) Probabilistic safety analyses may be used to determine the probability of damage for each barrier (IAEA, 2009b).

9.2.2 Analogy with physical barriers in other NPP

In this paragraph (Allibert et al., 2018), the physical barriers for different nuclear reactors are listed.

PWR:

- First barrier: Fuel cladding tubes/fuel matrix;
- Second barrier: Primary circuit;
- Third barrier: Reactor containment building.

CANDU (Canadian Heavy Water reactors):

- First barrier: Pellets;
- Second barrier: Fuel cladding;
- Third barrier: Heat transfer system;
- Forth barrier: Containment building (Hurst, 1997; Nuclear Power Plant Safety Systems, 2016).

SFR:

- First barrier: Cladding of the fuel;
- Second barrier: Closed primary coolant loop;
- Third barrier: Containment building (Walter et al., 2012).

VHTR:

- First barrier: Silicon carbide layer of the fuel coated particle;
- Second barrier: Primary circuit;
- Third barrier: Containment building (Bassi et al., 2005)

LFR:

- First barrier: Fuel and the fuel cladding;
- Second barrier: Lead coolant;
- Third barrier: Reactor vessel;
- Forth barrier: Containment vessel (Westinghouse Electric Company LLC, 2016)

PBMR (Pebble Bed Modular Reactor):

- First barrier: Kernel (Fahrenholtz et al., 2014);
- Second barrier: Reactor vessel;
- Third barrier: Reactor housing.

The number of needed confinement barriers can vary depending on the concept characteristics and the operational procedures. For instance, the safe storage of spent fuel is in general achieved by maintaining a minimum of two independent barriers between the fuel and the environment. For solid-fuelled reactors, the fuel cladding is considered the primary barrier. The second barrier is the confinement system, which is different for each type of storage. For wet storage, a hydraulic containment is guaranteed by the pool and effluents are managed by the ventilation system containment. Mechanical seals provide confinement boundary sealing surface for the dry storage (Vitkova et al., 2006).

9.2.3 Propositions for MSFR barrier found in other references

In this paragraph (Allibert et al., 2018), there are propositions for MSR barriers found in previous studies.

- *Marya Brovchenko PhD thesis*: the first barrier is defined as the fuel casing and is composed of a critical area (the fuel circuit) and a subcritical area (the draining system). It is important to notice that the reactor design has evolved since this definition and that the EDS is now separated from the routine draining system. Then, the reactor vessel constitutes the second barrier and includes also the reprocessing and storage units. Finally the reactor building is the third barrier (Brovchenko, 2013).

- *ORNL MSRE*: the primary containment is defined as the system of piping and vessels. “The sealed reactor and drain-tank cells are the secondary containment for the fuel salt during operation”. No containment barriers are clearly defined during maintenance. It is only mentioned “most maintenance does not entail opening the containment described above” (Haubenreich, 1968).

- In *D2.5 EVOL report* (Brovchenko et al., 2014), with a previous design of the MSFR, the confinement barriers are identified with:

    - First containment barrier: it is the fuel casing that includes critical and subcritical spaces where the fuel salt is located during normal reactor operation; in particular, we refer to all the fuel circuit devices that are in contact with the salt when the reactor is generating power.

The challenges for the first barrier are a small neutron flux, locally high temperature (up to 700°) corrosion from the salt (pink in the following fig. 9-1);

- Second containment barrier: it is the reactor vessel. In its lower part it contains a large pool partly filled with water that surrounds the subcritical part of the fuel casing. On the top of the pool there is a sealed water circuit where, via natural convection, the water flows towards air heat exchangers distributed along the vessel periphery, that ensure the passive cooling of the salt in the draining tank. Surrounding the critical part, the second barrier includes the HX walls between the intermediate circuit and the BoP (light blue in the following fig. 9-1);
- Third containment barrier: it is the reactor containment structure (maybe the reactor building) (grey in the following fig. 9-1).

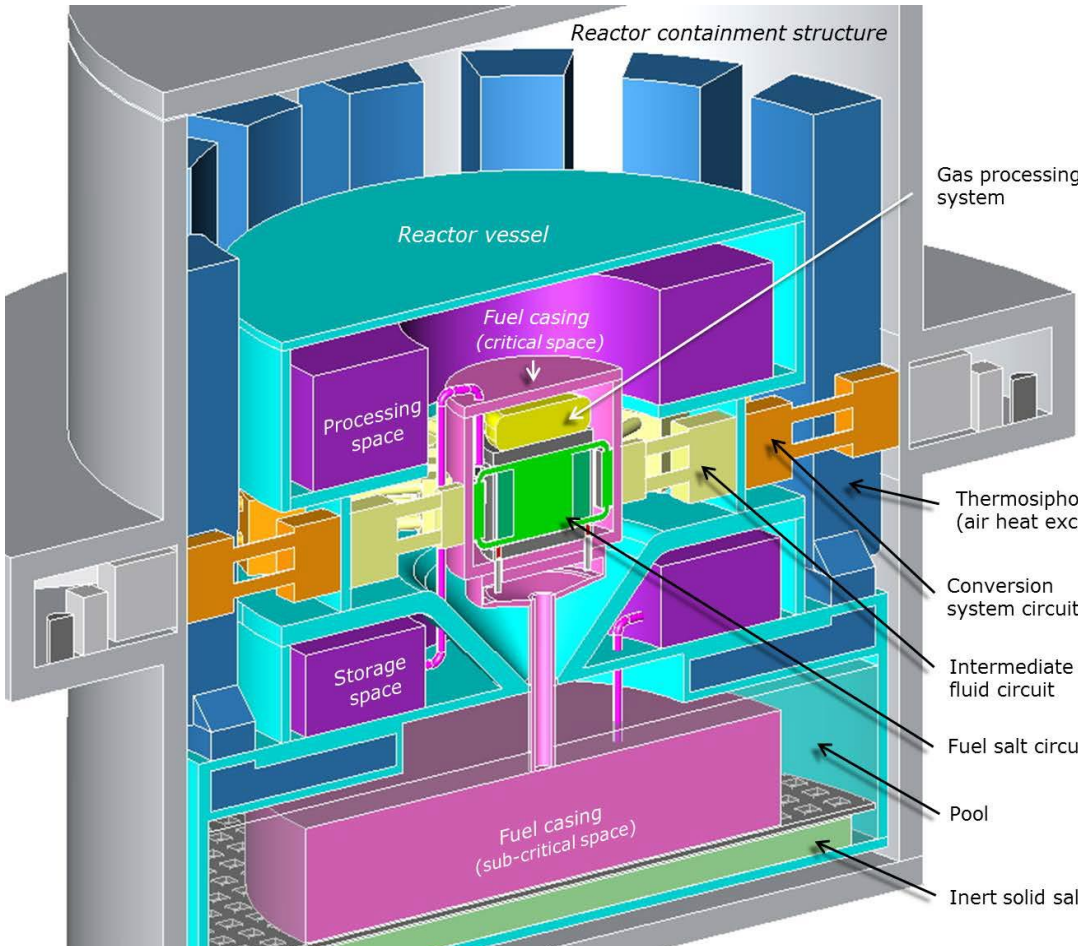

Figure 9-1 MSFR schematic representation (Brovchenko et al., 2014)

9.3 **Propositions**

The components in contacts with the fuel or holding it are different if the reactor is in different operational states. The idea of this paragraph is to define the MSFR safety barriers in function of the different normal operational states. The operational states taken in to account are:

- Power production and situations where the fuel is in the fuel circuit;
- Maintenance operations where the fuel is in the storage tanks.

Several proposals are made for the barriers based on the reference MSFR design (Allibert et al., 2017) or with minor modifications of this one. They are listed below.

9.3.1 Proposal 1

For normal operation condition (power production & maintenance / start-up /shutdown), the two proposed barriers are:

- **First barrier**: Fuel casing;
- **Second barrier:** Reactor building.

This proposal is based on the current MSFR design (Allibert et al., 2017). The two barriers must be entire and independent.

The **first barrier,** named "fuel casing", is constituted of the reactor vessel with perforations for the intermediate circuit pipes, the upper wall/lid with a removable part allowing the fuel sampling, the collector, the draining shaft and the EDS. To ensure integrity and continuity of the first barrier in case of accident (e.g. rupture of HX plate/channel), valves should be provided to isolate the part of the intermediate circuit entering the fuel casing.

The **second barrier** is constituted by the reactor building and contains the intermediate circuit, the BoP and other auxiliary systems.

The barriers are coincident in the reactor states of power production, maintenance, start-up and shutdown. The proposal 1 is illustrated in the following fig. 9.2.

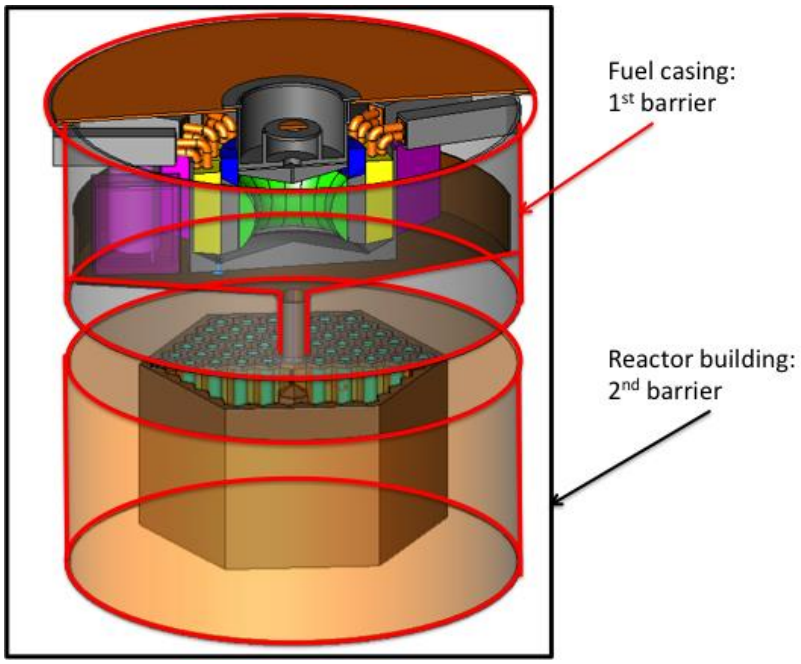

Figure 9-2 Proposal 1 of the physical barriers (Allibert et al., 2018)

The problem of this kind of barriers definition is linked to the fact that the first barrier is huge and every time that maintenance will be necessary, the first barrier needs to be opened: this involves serious issues in terms of management, procedures definition and restrictions.

If technological issues are present so that recirculation sectors cannot be closed, proposal 1 could be the final choice, while if there are not, other proposals can be more satisfactory mainly in terms of management and maintenance (see paragraph 9.3.2 and paragraph 9.3.3) (Allibert et al., 2018).

9.3.2 Proposal 2

With respect to proposal 1 (par. 9.3.1), proposal 2 foresees to seal the fuel circuit containment structures in order to confine the radioactive materials inside the fuel circuit. This barrier would be analogous to the PWR fuel rod cladding as it is the first physical component in contact with the active fuel and it holds the fuel. To limit the presence of radioactive matter in a more restricted area presents benefits for both maintenance operations and decommissioning, while in case of accident it would be more difficult for the radioactive gases to find an escaping pathway.

Moreover, proposal 2 is more similar to the PWR barriers definition. Indeed, the loss of the first barrier is, in this case, more similar to the loss of the cladding in PWR, which does not compromise the safety aspects of the reactor. On the other hand, in proposal 1, the loss of the first barrier would have a much more severe impact from both safety and process points of view than the equivalent event in PWR and other Gen IV reactors.

For normal operation condition (power production), the proposed physical barriers are:

- **First barrier**: Fuel circuit containment structures;
- **Second barrier**: Fuel casing;
- **Third barrier**: Reactor building.

This proposal is based on the current MSFR design (Allibert et al., 2017). The three barriers must be entire and independent.

The **first barrier**, named "fuel circuit containment structures", includes the core cavity, the upper and lower reflectors and the lid allowing to close the upper parts of all the sectors. In addition, the elements playing a role in the integrity and leak-tightness of this barrier have to be taken into account. Those are the intermediate circuit pipes, the HX plates/channels, the pumps shaft, the sampling device, the removable lid, etc.

The **second barrier**, named "fuel casing", is constituted of the reactor vessel, the upper wall/lid, the collector, the draining shaft and the EDS.

To ensure the independence between the first and the second barrier, a removable lid should be provided in the upper part of the fuel casing (that is a part of the second barrier) and it must be independent from the removable lid of the expansion vessel (that is a part of the first barrier).

To keep integrity of the second barrier in case of loss of the first barrier (e.g. rupture of HX plate/channel), valves should be provided to isolate the part of the intermediate circuit entering the fuel casing.

The **third barrier** is the reactor building and contains the intermediate circuit, the BoP and other auxiliary systems as in proposal 1.

For normal operation condition (maintenance / start-up /shutdown), the proposed physical barriers are:

- **First barrier**: Standard draining tank + filling/empting circuit;
- **Second barrier**: Fuel casing;
- **Third barrier**: Reactor building.

During maintenance operation, start-up or shutdown, the fuel is located in storage tanks and in the pipes connecting them to the core. This is why these structures are considered as the first barrier. The two other barriers are the same as for the case of power production.

The proposal 2 (during power production) is illustrated in the following fig. 9.3.

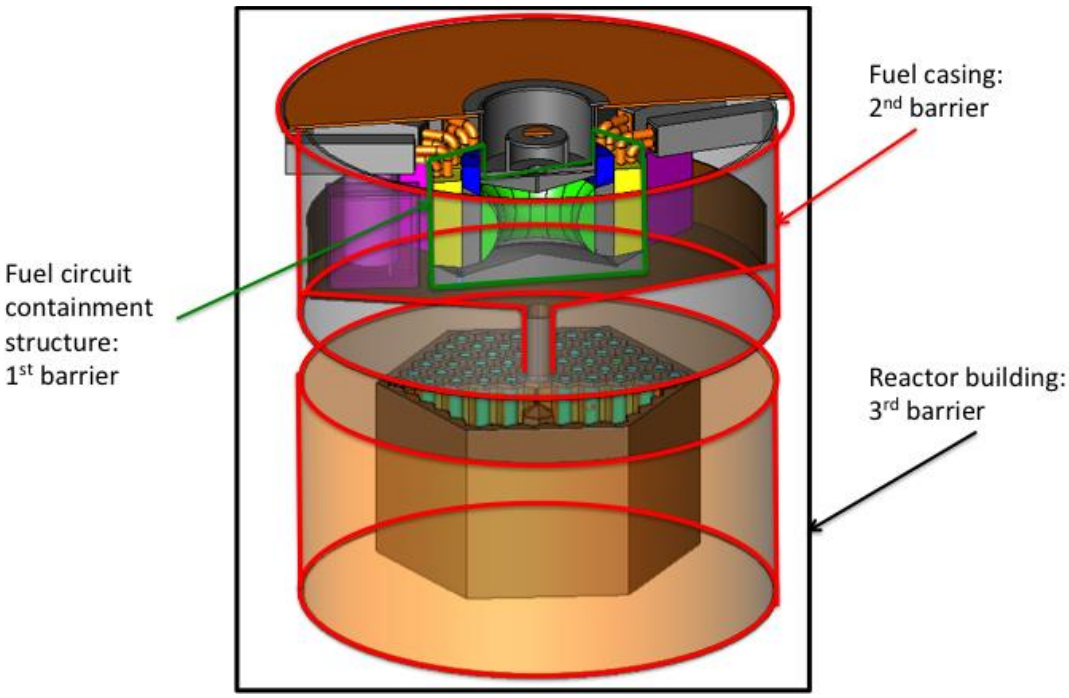

Figure 9-3 Proposal 2 of physical barriers (Allibert et al., 2018)

As a possible variation of proposal 2, it can be worth defining a unique first barrier for the power production in normal operation conditions and for the maintenance/shutdown/start-up always in normal operation conditions. This new first barrier would contain all the fuel circuit structures and the standard draining tanks with

their filling/empting circuits. This idea is useful to highlight the fact that even during maintenance the integrity and leak-tightness of the fuel circuit must be ensured; therefore, the whole zone where the active fuel is present must be entire during all the phases of normal operations (Allibert et al., 2018).

Moreover if this kind of barrier definition is accepted, the use of routine storage tanks in incidental situations (small deviations) can allow to remain inside the unique first barrier (Allibert et al., 2018).

9.3.3 Proposal 3

This proposal 3 implies an important modification of the geometry and it is proposed as a compromise between reducing the radioactive area and considering the EDS as a part of the first containment barrier. The idea is to place the collector and EDS under the fuel circuit containment structure without including the routine storage tanks. This option has the advantage of securing maintenance operation on the EDS when the fuel is in the storage tanks (no risk of leakage to the EDS).

For normal operation condition (power production), the proposed physical barriers are:

- **First barrier**: Fuel circuit containment structures + EDS
- **Second barrier**: Reactor vessel;
- **Third barrier**: Reactor building.

The three barriers must be entire and independent.

The **first barrier** includes the fuel circuit containment structures as described in proposal 2 and the EDS (including collector and draining shaft). In order to ensure the leak-tightness of this barrier, the collector should be sealed to the core vessel.

The **second barrier**, named “reactor vessel”, is constituted by a reactor vessel with an upper closure and it contains systems for thermal power generation (fuel circuit), systems for managing incident/accident situations (EDS) and systems for maintenance operation (standard draining tanks).

The **third barrier** is the reactor building and contains the intermediate circuit, the BoP and other auxiliary systems as in proposal 1 and 2.

For normal operation condition (maintenance / start-up /shutdown), the proposed physical barriers are:

- **First barrier**: Standard draining tank + filling/empting circuit;
- **Second barrier**: Reactor vessel;
- **Third barrier**: Reactor building.

During maintenance operation, start-up or shutdown the fuel is located in storage tanks and in the pipes connecting them to the core as in proposal 2 (Allibert et al., 2018). The proposal 3 is illustrated in the following fig. 9.4.

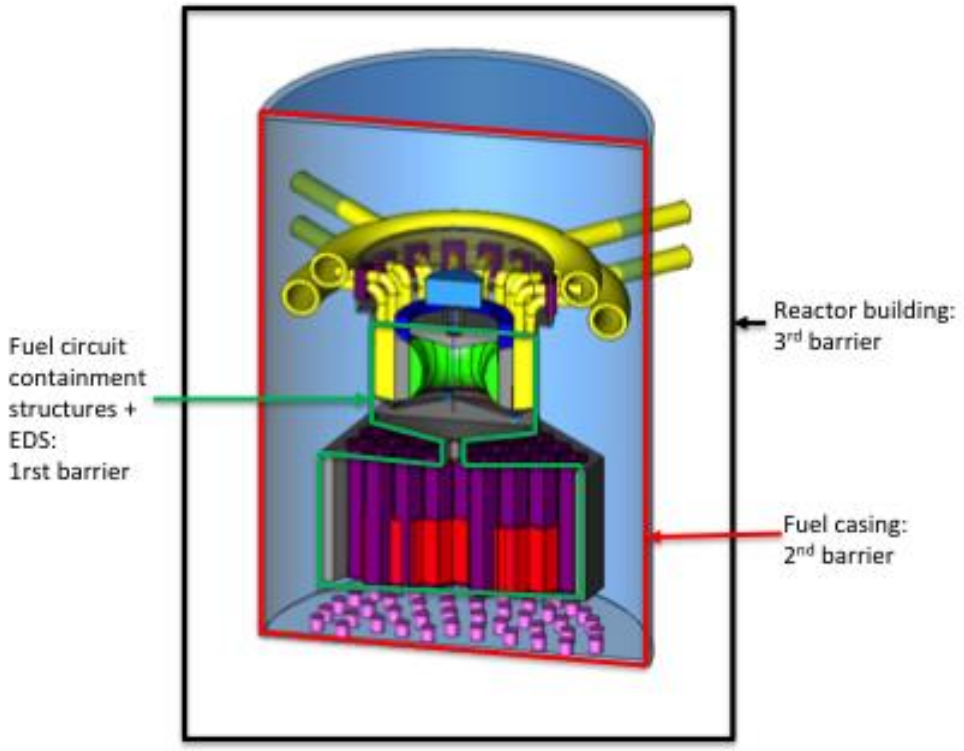

Figure 9-4 Proposal 3 of the physical barriers (Allibert et al., 2018)

Also in this case, a possible variation of proposal 3 is not to have two different barriers definitions for the power production in normal operation conditions and for the maintenance/shutdown/start-up always in normal operation conditions, for the same reasons explained for proposal 2.

Some problems could appear if the EDS is considered a part of the first barrier: in that case, the integrity and leak-tightness of the EDS must be ensured as well as the rest of first barrier; this requirement may be difficult to fulfil especially because of the dimensions and the shape of the EDS.

9.4 Other reflexions

It can be observed that the BoP is the only circuit in the reactor building with an important overpressure likely to induce a significant and sustained loading on the last confinement barrier; in fact, the salt circuits are not under high pressure and as there is no identified risk of a significant exothermic reaction between the salts and other fluids (studies are on-going). Therefore, it can be worth trying to locate the BoP out of the reactor building, or at least to consider design measures to avoid pressure related incidents/accidents impacting on several barriers. Locating the BoP outside the reactor building would notably imply a stronger focus on isolation capabilities on the intermediate loop, as well as evaluation of the intermediate salt radioactivity.

The fact that the EDS will be or not a part of the first barrier should be linked to the final role of this component: in fact, if it is intended to be used only in accidental situations it can be considered as an emergency system, therefore it may be outside the first barrier; while if it is intended to be used also during small deviations from normal operations and/or during incidental situations it is worth including it in the first barrier (Allibert et al., 2018).

References

Allibert M., Gérardin D., Heuer D., Huffer E., Laureau A., Merle E., Beils S., Cammi A., Carluec B., Delpech S., Gerber A., Girardi E., Krepel J., Lathouwers D., Lecarpentier D., Lorenzi S., Luzzi L., Poumerouly S., Ricotti M., Tiberga M., Tiberi V.; "D1.1 Description of initial reference design and identification of safety aspects" SAMOFAR report SAMOFAR_D1.1_v4_20feb2017 (2017)

Allibert M., Beils S., Carpignano A., Dulla S., Gérardin D., Heuer D., Ivaniv E., Laureau A., Merle E., Uggenti A.C., "D1.6 Identification of risks and phenomena involved, identification of accident initiators and accident scenarios" SAMOFAR report SAMOFAR_D1.6_v1.0_311018 (2018)

ARIS website, "Advanced Reactors Information System (ARIS)", available at https://www.iaea.org/resources/databases/advanced-reactors-information-system-aris

ASME/ANS, "Probabilistic Risk Assessment Standard for Advanced non-LWR Nuclear Power Plants," RA-S-1.4-2013 (2013)

Aubert J., Aiello G., Jonquères N., Li Puma A., Morin A., Rampal G., "DEMO1 WCLL blanket concept design description", Report for TA WP12-DAS-02-T03, EFDA_D_2JNFUP v1.0 (2013)

Bassi A., Bertrand F., Barbier D., Aujollet P., Anzieu P., "Massive H2 production with nuclear heating, safety approach for coupling a VHTR with a Iodine Sulfure Process cycle" (2005)

Bedford T., "Risk Acceptance Criteria, FN-curves and Multi-attribute utility theory", proceedings of 2nd ASRANET (2004)

Bertinetti A., Carpignano A., Pinna T., Savoldi L., Sobrero G., Uggenti A.C., Zanino R., "Functional Failure Mode and Effect Analysis (FFMEA) for DEMO primary cooling systems of DCLL blanket module", EuroFUSION report (2016)

Brovchenko M., “Etudes préliminaires de sûreté du réacteur à sels fondus MSFR”, PhD Thesis, Grenoble Institute of Technology, France (in French) (2013)

Brovchenko M., Heuer D., Huffer E., Merle-Lucotte E., Allibert M., Feynberg O., Ghetta V., Ignatiev V., Kloosterman J. L., Lathouwers D., Laureau A., Rineiski A., Rouch H., Rubiolo P., Rui L., Wang S., “Safety Approach of a Fast Liquid Fuel System”, EVOL report 2.5 (2014)

Bubelis E., Hering W., “Conceptual Design Definition for an Int. Cooling Loop Configuration and Coolant”, EuroFUSION report EFDA_D_2HDVN9 (2014)

Canevaro E., Cevrero D., “Elaborato Tecnico Rischio di Incidente Rilevante”, Servizio Programmazione del Territorio del Comune di Settimo Torinese (2014) (In Italian)

Carloni D., “Safety Consideration for the EU DCLL DEMO Blanket”, 2nd EU-US DCLL Workshop meeting (2014)

Carpignano A., Tuninetti S., Analisi Comparativa dei Criteri di Accettabilità del Rischio e Considerazioni sul D.M. 9 Maggio 2001”, proceedings of “Convegno Nazionale sulla Valutazione e Gestione del Rischio negli Insediamenti Civili e Industriali” (2004) (In Italian)

Carpignano A., Pinna T., Savoldi L., Sobrero G., Uggenti A. C., Zanino R., “Safety Issues related to the Intermediate Heat Storage for the EU DEMO” /. - In: FUSION ENGINEERING AND DESIGN (2016)

Carpignano, A.; Dulla, S.; Uggenti, A. C., “Safety assessment: perspectives for next generation nuclear plants”, proceedings of European Safety and Reliability Conference (ESREL2018)

Clement E., "Arbre Analyste", (2013). Available from http://www.arbre-analyste.fr/

Del Nevo A., Martelli E., Eboli M., “Summary of key parameters for the design of PHTS and related BoP for the WCLL”, EuroFUSION report EFDA_D_2APSFQ (2014)

Donatini F., Zamparelli C., Sanfiorenzo C., “Analisi termo-fluidodinamica di un sistema avanzato di accumulo termico per produzione di energia elettrica da energia solare”, proceedingd of 60° Congresso Nazionale ATI (2005) (In Italian)

Dongiovanni D., Pinna T., Carloni D., Jin X.Z., Boccaccini L.V., “Definition of DEMO safety requirements and compilation of preliminary safety design guidelines D1- FMEA for the DEMO HCPB concept”, EuroFUSION report EFDA_D_2L48QQ V3.0 (2014)

Dulla S., Krepel J., Rouch H., Aufiero M., Fiorina C., Geoffroy O., Hombourger B., Laureau A., Merle-Lucotte E., Mikityuk K., Pautz A., Ravetto P., Rubiolo P., “Sensitivity studies of the salt flux in the optimized design of the MSFR”, Deliverable D2.3, EVOL (Evaluation and Viability of Liquid fuel fast reactor system) European FP7 project, Contract number: 249696 (2014)

EUROfusion, “Programme preparing for ITER and developing DEMO”, EUROfusion website available on https://www.euro-fusion.org/programme/

Fahrenholtz W. G., Wuchina E. J., Lee W. E., Zhou Y., “Ultra-high temperature ceramics-Materials for extreme environment applications”, Wiley, The American Ceramic Society (2014)

Finan, A. E., “Enabling Nuclear Innovation: Strategies for Advanced Reactor Licensing.” DOE—NRC Advanced Non-LWR Workshop (2016)

Flauw Y., Tiberi V., Beils S., Carpignano A., Dulla S., Gérardin D., Uggenti A. C., Allibert M., Heuer D., Ivanov E., Laureau Aa., Lecarpentier D., Merle E., “D1.5 Development of an integral safety assessment methodology for MSFRs”, SAMOFAR_D1.5_v1.0_20180702 (2018)

Fleming K., “Removing a Blind Spot in Our Safety Culture”, proceedings of the International Topical Meeting on Probabilistic Safety Assessment and Analysis (PSA2017), Pittsburgh PA, USA (2017)

D. Gérardin, M. Allibert, D. Heuer, A. Laureau, J. Martinet, E. Merle "Identifiaction and study of incidental and accidental scenarios for the Molten Salt Fast Reactor", PHYTRA4 - The Fourth International Conference on Physics and Technology of Reactors and Applications, Marrakech, Morocco (2018)

Gérardin D., Uggenti A., Beils S., Carpignano A., Dulla S., Merle E., Heuer D., Laureau A., Allibert M., “A methodology for the identification of the postulated initiating events of the Molten Salt fast reactor”, Nuclear Engineering and Technology (in press), (2019)

GIF, “A Technology Roadmap for Generation IV Nuclear Energy Systems” (2002)

GIF, “Basis for the Safety Approach for Design and Assessment of Generation IV Nuclear Systems Revision 1” (2008)

GIF, “Technology Roadmap Update for Generation IV Nuclear Energy Systems” (2014)

Gil A., Medrano M., Martorell I., Làzaro A., Dolado P., Zalba B., Cabeza L. F., “State of the art on high temperature thermal energy storage for power generation. Part 1-Concepts, materials and modellization”, Renewable and Sustainable Energy Reviews 14 (2010a) 31-55

Gil A., Medrano M., Martorell I., Potau X., Cabeza L. F., “State of the art on high temperature thermal energy storage for power generation. Part 2-Case studies”, Renewable and Sustainable Energy Reviews 14 (2010b) 56-72

Haubenreich P.N., Engel J.R., Gabbard C.H., Guymon R.H., Prince B.E., "Safety analysis of operation with 233U", Rapport ORNL-TM-2111, Oak Ridge National Laboratory, Oak Ridge, Tennessee (1968)

Herrmann U., Kelly B., Price H., “Two-tank molten salt storage for parabolic trough solar power plants”, Energy 29 (2004) 883-893

Heuer D., Merle-Lucotte E., Allibert M., Brovchenko M., Ghetta V., Rubiolo P., “Towards the Thorium Fuel Cycle with Molten Salt Fast Reactors”, Annals of Nuclear Energy 64, 421–429 (2014)

Heuer D., Laureau A., Merle-Lucotte E., Allibert M., Gerardin D., "A starting procedure for the MSFR: approach to criticality and incident analysis"**,** Proceedings of the ICAPP’2017 International Conference, Kyoto, Japan (2017).

Hurst D.G., “Canada enters the nuclear age, A technical history of Atomic Energy of Canada Limited”, Atomic Energy of Canada Limited (1997)

IAEA, “Nuclear Power Reactors in the World. Reference Data Series No. 2” (2017)

IAEA, “Safety of Nuclear Power Plants: Design - Specific Safety Requirements”, Safety Standards Series No. SSR-2/1 (Rev. 1) (2016)

IAEA Safety Standard, “Safety Assessment for Facilities and Activities", General Safety Requirements No. GSR Part 4 (Rev.1) (2016b)

IAEA Safety Standard, “Severe Accident Management Programmes for Nuclear Power Plants”, Safety Guide No. NS-G-2.15 (2009)

IAEA Safety Standard, “Deterministic Safety Analysis for Nuclear Power Plant”, No. SSG-2 (2009b)

IAEA, “Guidance for the Application of an Assessment Methodology for Innovative Nuclear Energy Systems, INPRO Manual-Overview of the methodology” (2008)

IAEA, “IAEA Safety Standard for protecting people and environment, Fundamental Safety Principles, No SF-1” (2006)

IAEA Safety Standard, “A System for the Feedback of Experience from Events in Nuclear Installations”, Safety Guide No. NS-G-2.11 (2006b)

IAEA Safety Standard, “Format and Content of Safety Analysis Report for Nuclear Power Plants”, No. GS-G-4.1 (2004)

IAEA, “Basic Safety Principles for Nuclear Power Plants” 75-INSAG-3 Rev. 1 - INSAG-12, (1999)

IEC EN 61226, “Nuclear power plants - Instrumentation and control systems important for safety-Classification” (2005)

IEC EN 61508, “Functional safety of electrical/electronic/programmable electronic safety-related systems”, Parts 1÷7 (2005)

IEC EN 61513, “Nuclear Power Plants – Instrumentation and control important to safety – General requirement for systems” (2013)

INL, “Next Generation Nuclear Plant Probabilistic Risk Assessment Whit Paper, IN/EXT-11-21270” (2011)

INL, “Modernization of Technical Requirements for Licensing of Advanced Non-Light Water Reactors, Selection of Licensing Basis Events” (2017)

IRSN – “Review of Generation IV Nuclear Energy Systems” (2014)

IRSN Report, “Examen des systèmes nucléaires de 4ème génération” (2015)

Jauch U., Karcher V., Schulz B., “Thermophysical Properties in the System Li-Pb. Part I:Preparation and characterization of Li(17)Pb(83) eutectic alloy and the LiPb intermetallic compound”, KfK 4144 (1986)

Kadamabi, N. P., “Guidance for Performance-Based Regulation. NUREG/BR-0303, U.S. Nuclear Regulatory Commission” (2002)

Kasten P. R., “The MOSEL reactor concept”, in Third International Conference on Peaceful Use of Atomic Energy (1964)

Kitchen R. M., Axline M., Safety in molten salt bath operations, Kolene Corporation (2004)

Laureau A., “Développement de modèles neutroniques pour le couplage thermohydraulique du MSFR et le calcul de paramètres cinétiques effectifs”, PhD Thesis, Grenoble Alpes University, France (in French) (2015)

Lee S., “New Reactor Regulatory Activities Current Status for LLWR, SMR and non-LWRs”, USA Nuclear Regulatory Commission (2016)

Lo Pinto P., Costes L., Carluec B., Quellien P., Beils S., Bourgue L., “ASTRID Safety Design: Progress on Prevention of Severe Accident” proceedings of International Conference on Fast Reactors and Related Fuel Cycles: Next Generation Nuclear Systems for Sustainable Development (FR17), Yekaterinburg, Russia (2017)

Mathieu L., “Cycle Thorium et Réacteurs à Sel Fondu: Exploration du champ des Paramètres et des Contraintes définissant le Thorium Molten Salt Reactor”, Thèse de doctorat, Institut National Polytechnique de Grenoble, France (2005)

Mathieu L., Heuer D., Merle-Lucotte E., Brissot R., Le Brun C., Lecarpentier D., Liatard E., Loiseaux J.M., Méplan 0., Nuttin A., “Possible Configurations for

the TMSR and advantages of the Fast Non Moderated Version", Nuclear Science and Engineering 161, p. 78–89, (2009)

Merle-Lucotte E., "Le cycle Thorium en réacteurs à sels fondus peut-il être une solution au problème énergétique du XXIème siècle ? Le concept de TMSR-NM", Habilitation à Diriger les Recherches, Institut National Polytechnique de Grenoble, France (2008)

Ministero dei Lavori Pubblici, Requisiti minimi di sicurezza in materia di pianificazione urbanistica e territoriale per le zone interessate da stabilimenti a rischio di incidente rilevante, DM 9/05/01 (2001) (In Italian)

MIT Energy Initiative, "The future of Nuclear Energy in a Carbon constrained World – An interdisciplinary MIT study" (2018)

Natalizio A., Collen J., "Conceptual design of main cooling system for fusion power reactor with water cooled lithium-lead blanket", Studsvik eco&safety, TW1-TRP-PPCS1 (2014)

Government of Canada, "Nuclear Power Plant Safety Systems", available at: http://nuclearsafety.gc.ca/eng/reactors/power-plants/nuclear-power-plant-safety-systems/index.cfm (2016)

Papazoglou I.A., Aneziris O.N., "Master Logic Diagram: method for hazard and initiating event identification in process plants", Journal of Hazardous Materials A97 11–30 (2003)

Petti, D., R. Hill, J. Gehin, H. Gougar, G. Strydom, T. O'Connor, F. Heidet, et al. "A Summary of the Department of Energy's Advanced Demonstration and Test Reactor Options Study." Nuclear Technology 199, no. 2: 111–12 (2017)

Pinna T., Carpignano A., Savoldi l., Sobrero G., Uggenti A.C., Zanino R., "Functional Failure Mode and Effect Analysis (FFMEA) for the DEMO cooling systems of the WCLL blanket model", EuroFUSION report EFDA_D_2JPQSG (2015)

Pinna T., Carloni D., Carpignano A., Ciattaglia S., Johnston J., Porfiri M.T., Savoldi L., Taylor N., Sobrero G., Uggenti A.C., Vaisnoras M., Zanino R., "Identification of accident sequences for the DEMO plant", Fusion Engineering and Design 124 (2017) 1277-1280

Rapisarda D., Fernandez I., Palermo I., "2014 Design and Analysis strategy Plan (DASP2014) for DCLL BB", EuroFUSION report EFDA_D_2GDLRY v1.0 / 4.1.2-02 (2016)

Rapisarda D., Oron-Carl M., "DCLL Blanket 2014 Design Description Document", EuroFUSION report EFDA_D_2GDLRY v1.0 / 4.1.2-01 (2015)

Reungoat M., Vala L., "Conceptual design of DCLL LiPb loop with auxiliaries", EuroFUSION report EFDA_D_2MEAVA v1.0 / D-512-02a (2014)

Rouch H., Geoffroy O., Heuer D., Rubiolo P., Brovchenko M., Laureau A., Merle-Lucotte E., "Preliminary Thermalhydraulic Core Design of a Molten Salt Fast Reactor", Annals of Nuclear Energy, Vol. 64, p 449–456 (2014)

RSWG of GIF, "Guidance Document for Integrated Safety Assessment Methodology (ISAM) – (GDI)" (2014)

RSWG of GIF, "An Integrated Safety Assessment Methodology (ISAM) for Generation IV Nuclear Systems" (2011)

RSWG of the GIF, "Basis for the Safety Approach for Design & Assessment of Generation IV Nuclear Systems" (2008)

SARGEN_IV, "Proposal for a harmonization of the safety assessment practices - Deliverable 3.5" (2012)

Southern Company, "Modernization of Technical Requirements for Licensing of Advanced Non –Light Water Reactors Probabilistic Risk Assessment Approach", SC-29980-101 Rev A (2017)

Tincani A., Utili M., Granieri M., "Conceptual design od DCLL LiPb loop with auxiliaries (part b) and main components", WPB5 LiPb technologies and TES meeting (2015)

Uggenti A. C., Gérardin D., Carpignano A.; Dulla S., Merle E., Heuer D., Laureau A., Allibert M. "Preliminary Functional Safety Assessment for Molten Salt

Fast Reactors in the Framework of ohe SAMOFAR Project" proceedings of International Topical Meeting on Probabilistic Safety Assessment and Analysis (PSA 2017)

UK HSE, "Reducing Risk, Protecting People", Sudbury: HSE books (2001)

US NRC, "Feasibility Study for a Risk-Informed and Performance-Based Regulatory Structure for Future Plant Licensing", NUREG 1860 (2007)

US NRC, "An approach for determining the technical adequacy of probabilistic risk assessment results for risk informed activities", (2009) available at https://www.nrc.gov/docs/ML0904/ML090410014.pdf

US NRC "Responses to Requests for Information Senators James Inhofe and Shelley Moore Capito." ML15086A177, (2015)

US NRC, "Part 50 – Domestic Licensing of Production and Utilization facilities" (2017)

Vietti-Cook, A. "White paper on risk-informed and performance-based regulation." SECY-98-144, U.S. Nuclear Regulatory Commission (1999)

Vitkova M., Gorinov I., Dacheva D., "Safety criteria for wet and dry spent fuel storage", Nuclear Regulatory Agency (2006)

Walter A. E., Todd D. R., Tsvetkov P. V., "Fast Spectrum Reactors", Springer (2012)

Walker, J. S., and G. T. Mazuzan, "Containing the Atom: Nuclear Regulation in a Changing Environment", 1963–1971. University of California Press and U.S. Nuclear Regulatory Commission, Berkeley: University of California Press (1992)

WENRA, "Statement on Safety Objectives for New Nuclear Power Plants" (2010)

WENRA Report, "Safety of new NPP designs" (2013)

Westinghouse Electric Company LLC, "Demonstration Lead-Cooled Fast Reactor Details: Westinghouse Lead-Cooled Fast Reactor", RT-TR-15-30 Revision 1 (2016)

Wong C., “An Overview of the US DCLL ITER TBM Program”, proceedings of International Workshop on Liquid Metal Breeder Blankets (2010)