Nuclear Engineering and Technology 51 (2019) 1024–1031

Contents lists available at ScienceDirect

Nuclear Engineering and Technology

journal homepage: www.elsevier.com/locate/net

Original Article

A methodology for the identification of the postulated initiating events of the Molten Salt Fast Reactor

Delphine Gérardin [a, *], Anna Chiara Uggenti [b], Stéphane Beils [c], Andrea Carpignano [b], Sandra Dulla [b], Elsa Merle [a], Daniel Heuer [a], Axel Laureau [a], Michel Allibert [a]

[a] LPSC-IN2P3-CNRS, UJF, Grenoble INP, 53 Rue des Martyrs, 38026, Grenoble, France
[b] NEMO Group, DENERG, Politecnico di Torino, C.so Duca Degli Abruzzi 24, 10129, Torino, Italy
[c] FRAMATOME, 10 Rue Juliette Récamier, 69006, Lyon, France

ARTICLE INFO

Article history:
Received 25 April 2018
Received in revised form
3 December 2018
Accepted 15 January 2019
Available online 16 January 2019

Keywords:
Molten Salt Fast Reactor
Risk analysis
Initiating events
MLD
FFMEA

ABSTRACT

The Molten Salt Fast Reactor (MSFR) with its liquid circulating fuel and its fast neutron spectrum calls for a new safety approach including technological neutral methodologies and analysis tools adapted to early design phases. In the frame of the Horizon2020 program SAMOFAR (Safety Assessment of the Molten Salt Fast Reactor) a safety approach suitable for Molten Salt Reactors is being developed and applied to the MSFR. After a description of the MSFR reference design, this paper focuses on the identification of the Postulated Initiating Events (PIEs), which is a core part of the global assessment methodology. To fulfil this task, the Functional Failure Mode and Effect Analysis (FFMEA) and the Master Logic Diagram (MLD) are selected and employed separately in order to be as exhaustive as possible in the identification of the initiating events of the system. Finally, an extract of the list of PIEs, selected as the most representative events resulting from the implementation of both methods, is presented to illustrate the methodology and some of the outcomes of the methods are compared in order to highlight symbioses and differences between the MLD and the FFMEA.

1. Introduction

The Generation IV International Forum (GIF) has established a set of goals as research directions for future nuclear systems, which are sustainability, safety and reliability, economic competitiveness, proliferation resistance and physical protection [1]. These goals provided the basis for selecting six nuclear energy systems for further development. Among them, the Molten Salt Fast Reactor (MSFR) was retained in 2008 for its promising design and safety characteristics [2] and is currently studied in the frame of the Horizon2020 program SAMOFAR (Safety Assessment of the Molten Salt Fast Reactor). The objective of SAMOFAR is to prove the innovative safety concepts of the MSFR by advanced experimental and numerical techniques and to deliver a breakthrough in nuclear safety. Improved safety being recognized as a priority in the development and operation of nuclear systems, the development of a safety approach suitable for the MSFR and its application to the reactor is one of the main tasks of the SAMOFAR project. Indeed, because of its unique characteristics (e.g. the liquid circulating fuel playing also the role of coolant), the MSFR calls for a new safety approach based on technological neutral methodologies and relying on the fundamental safety principles [3]. In addition, the analysis tools selected have to be adapted to the MSFR early design phases. Moreover, the safety assessment should be performed in parallel to the design studies allowing to influence the direction of the concept and the design development since its 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” [4]. To fulfil these objectives, an integral safety assessment methodology for MSFRs has been proposed in the frame of the SAMOFAR project [5] and is based on the GIF Integrated Safety Assessment Methodology (ISAM) [6] and the methodology developed in the framework of the SARGENIV [7]. These methodologies are selected as conceptual methodologies by the partners of the SAMOFAR project and successively adapted to the peculiar case of the MSFR through the

* Corresponding author.
E-mail addresses: gerardin@lpsc.in2p3.fr (D. Gérardin), anna.uggenti@polito.it (A.C. Uggenti), stephane.beils@framatome.com (S. Beils), andrea.carpignano@polito.it (A. Carpignano), sandra.dulla@polito.it (S. Dulla), merle@lpsc.in2p3.fr (E. Merle), daniel.heuer@lpsc.in2p3.fr (D. Heuer), laureau@lpsc.in2p3.fr (A. Laureau), allibert@lpsc.in2p3.fr (M. Allibert).

https://doi.org/10.1016/j.net.2019.01.009

addition of suitable safety analysis tools to the methodology. A point of strength of ISAM is the direct link with the different levels of Defence-in-Depth (DiD): these levels, as well as the entire methodology, depends on the definition of the severe accident, risk metrics and physical barriers that represent still an argument of discussion for the MSFR. Therefore, the direct implementation of some of the tools of the ISAM to the MSFR resulted in being difficult, given the preliminary stage of the safety analysis and design of this concept. To overcome these difficulties, it has been chosen to rather use the ISAM as a guideline to formalize the objectives to be achieved. The first step of the ISAM, the Qualitative Safety Features Review (QSR), has been partly applied to the MSFR [8] and has pointed out the risk of fuel leak as a potential weak point of the design. This analysis has led to an evolution of the MSFR fuel circuit design in order to better cope with the risk of leak [9]. In a second step, the identification of the MSFR hazards has been undertaken. In this phase of risk assessment, it has been chosen to perform the identification of the hazards without defining the DiD levels concerned, whereas in a later stage, the completion with the DiD level identification could be of help to ensure that the safety architecture is well balanced, consistently with the Objective Provision Tree analytical tool reckoned in the ISAM.

This paper focuses on the identification of the potential hazards likely to challenge the MSFR safety and the elaboration of a list Postulated Initiating Events (PIEs), which is a core part of the global assessment methodology. To fulfil this task, the Functional Failure Mode and Effect Analysis (FFMEA) [10], which is suggested as complementary tool to fulfil this objective in the ISAM presentation, see Ref. [6], and the Master Logic Diagram (MLD) [11], which is a top-down method with a tree structure (mentioned for initiating events identification in one of the presented option in the guidance document for the application of the ISAM, see Ref. [12]), are selected and employed separately in order to be as exhaustive as possible in the identification of initiating events. Moreover, the members of the team performing the analysis have expertise in the implementation of these tools. Then, the PIEs are selected as the most representative events resulting from the implementation of both methods. The final list of PIEs will be a major input for the later steps of the global safety assessment methodology as the Deterministic Safety Analysis or the Probabilistic Safety Analysis. One main objective of the safety assessment methodology is to give feedbacks on the design, and the methods proposed in this paper also participate 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.

In section 2 the MSFR reference design used for the SAMOFAR project is presented, defining the studied system and its peculiarities; moreover some open points of the design are highlighted and the need for using technological neutral methodologies such as the ISAM is clarified. Afterwards, in section 3 the methodology chosen to compile the PIEs list of the MSFR is introduced, including the description of the FFMEA and MLD tools and the method of PIEs selection. Section 4 presents a preliminary list of the identified PIEs and the outcomes of the methods are finally compared in order to highlight symbioses and differences between the MLD and the FFMEA.

2. Description of the MSFR system

2.1. General description

The main characteristic of the MSFR is to use a fuel in the form of a molten salt. This fuel salt circulates in the fuel circuit where it is cooled down and plays therefore the role of coolant as well. The reference reactor, as defined at the beginning of the SAMOFAR project, is a 3 GW thermal power reactor with a thermodynamic efficiency of about 45%, a fast neutron spectrum and a breeding ratio of 1.1 [13]. The MSFR includes three main closed circuits for heat extraction from the fuel during power operation (the fuel circuit, the intermediate circuit and the power conversion circuit) and an open circuit acting as heat sink.

The selected fuel salt is a molten binary fluoride salt with 77.5 mol% of lithium fluoride, the remaining 22.5 mol% being a mix of heavy nuclei fluorides including the fissile and the fertile matter [13]. The fluids of the intermediate and conversion circuits have not been selected yet and constitute one of the open points of the system, however several options are proposed and will be studied in the frame of the SAMOFAR project. Other design open points will be described in paragraph 2.3.

2.2. Fuel circuit description

The fuel circuit is defined as the circuit containing the fuel salt during power operation and includes the core cavity and the cooling sectors allowing the heat extraction. Its specificities are summarized in Table 1.

The core shape is a hyperboloid resulting from previous optimization studies to improve the fuel flow in the core and limit the recirculation zones [14]. In addition, an integrated geometry of the fuel circuit (Fig. 1) was proposed in the frame of the SAMOFAR project in order to prevent the risk of fuel leakages highlighted by preliminary safety studies [15]. This solution foresees a vessel (Fig. 1 Top right) used as container for the fuel salt, vessel in which the 16 cooling sectors are disposed circumferentially (Fig. 1 Bottom right). Each sector (Fig. 1 Bottom left) comprises a heat exchanger, a circulation pump, a gas processing system, and a fertile blanket tank. A neutron shielding in B_4C is positioned between the blanket and the heat exchangers to protect the heat exchangers from the neutron flux and to increase the breeding ratio. In addition, thick reflectors made of nickel-based alloys are located at the bottom and the top of the vessel to protect the structures located outside the core [9,16].

The fuel circulation drifts the delayed neutron precursors in low importance areas, reducing the effective fraction of delayed neutrons and contributing to the reactor fast behaviour. The reactivity being mainly controlled by the neutronic feedback reactions (e.g.

Table 1
Characteristics of the MSFR fuel circuit.

Mean fuel salt temperature in fuel circuit (°C)	725
Fuel salt temperature rise in the core (°C)	100
Total fuel salt volume (m^3)	18 (half in the core and half in the cooling sectors)
Total fuel salt cycle in the fuel circuit (s)	3.9
Fuel salt dilation coefficient ($g.cm^{-3}.K^{-1}$)	$8.82.10^{-4}$
Total feedback coefficient ($pcm.K^{-1}$)	−8
Hyperboloid core dimensions (m)	Radius: 1.06 to 1.41 Height: 1.6 to 2.26
Fuel salt density ($g.cm^{-3}$)	4.1

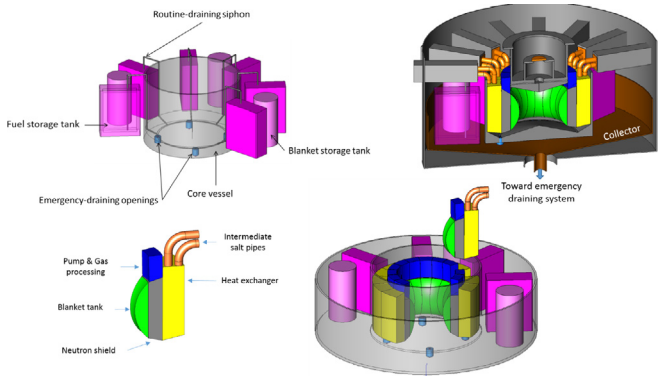

Fig. 1. Schematic representation of a cooling sector (bottom left), of the cooling sector arrangement in the core vessel (bottom right), of the storage tank arrangement around the core vessel (top left), and of the reactor vessel (top right).

no control rods are foreseen in the core), the fast response is not problematic for the reactor operation. The reactor feedback coefficients (density effect and Doppler Effect) are all negative, acting rapidly since the heat is produced directly in the coolant. The density effect comes from the fuel dilation that is possible thanks to an expansion vessel, which is a tank located at the top of the fuel circuit. Therefore, the core presents a very intrinsically stable behaviour to reactivity insertions [17].

2.3. Systems in interaction with the fuel circuit and open points on the design

Several sub-systems are connected to the fuel circuit, in particular, the fertile blanket and its cooling circuit, the fuel circuit walls cooling, the intermediate circuit, the Emergency Draining System (EDS), the fuel storage tanks, the gas bubbling system and the sampling for fuel processing. The objective of this section is to highlight their interactions and the possible impact on the subsequent safety analyses. In addition, special attention is paid on the design open points and on the possible improvements that were identified thanks to the safety analysis.

Firstly, the fertile blanket allows the breeding ratio of the reactor to increase and participates to the radial neutron shielding. The system comprises a blanket tank filled with fertile salt at liquid state, which is an integral part of the sector and is located in the circumference of the core. The fertile salt is heated up by the neutrons coming from the core losing their energy by scattering or being trapped (mainly by thorium) and by the fission of U_{233} which is produced by capture on the thorium; therefore it needs to be cooled down. Several design options are foreseen for the fertile salt cooling: an internal cooling option where the intermediate salt directly cools down the blanket tank or an external cooling option, in which the blanket tank is connected to a fertile circuit with a pump and a heat exchanger where the fertile salt is cooled down by the intermediate salt.

Then, the fuel circuit is connected to the intermediate circuit through the heat exchangers, which are designed to ensure the leak-tightness of the zones where the intermediate fluid circulates. Furthermore, the pressure of the intermediate circuit is higher than the one of the fuel circuit in order to prevent fuel leakage in case of a heat exchanger leak. The study of the intermediate circuit is to be led, keeping in mind that the reactor is mainly driven by heat extraction (e.g. there are no control rods in the core) [17]. Four intermediate circuits are considered, each of them feeding four cooling sectors in order to ensure the core cooling even if one circuit fails. The intermediate salt is also used to cool down the fertile blanket and the core walls in order to prevent their thermal degradation due to possible hot spots. However it should be determined whether this function is achieved by a unique intermediate circuit or if a dedicated cooling circuit has to be used for the walls and the fertile blanket. The application of the proposed safety analysis method and the reflection on the confinement barrier definition also highlighted the need to provide sufficient valves to isolate systems in case of malfunction or leakage.

In case of incident/accident during power production, the fuel can be drained gravitationally toward an emergency draining tank designed to passively remove the residual heat over a long period of time [9]. The residual heat associated to the fuel salt represents around 3.8% of the nominal power at the moment t = 0s where reactor shuts down; thus this value corresponds to the maximum of the residual power of the salt in time [8]. The fuel circuit is connected to this Emergency Draining System (EDS) through active and passive gates or plugs located in the bottom reflector (Fig. 1.Top left). A gas connection between the fuel circuit and the EDS allows a fast draining (around 100S). In addition to the emergency draining, a routine draining system, triggered only by active means, is used to transfer the fuel to storage areas for maintenance operations. The siphons for routine core draining and filling are placed on the sides of the core vessel. The calculations to design of the EDS are ongoing; it constitutes one of the tasks of the SAMOFAR project.

An in-core gas bubbling system is used to clean the salt from gaseous fission products and metallic particles. The gas is injected at the bottom of the core and recovered at the top to be cleaned up from a part of the fission products in the gas processing unit (Fig. 1. Bottom left) before being re-injected in the core. The gas processing unit requires a dedicated cooling system as the residual heat, at reactor shutdown, in this location represents around 1.4% of the nominal power [8]. The specific components of the bubbling system constitute one of the open points of the design to be defined.

Finally, the fuel processing is done/performed through online fuel punctures and the loading is done by fluid transfer during reactor operation. Thus, fuel salt and fertile salt samplings are regularly performed to control and adjust their chemical composition and inventory. The frequent adjustment of the fuel composition allows low reactivity reserves in core. Nevertheless, it involves a risk of reactivity insertion due to incorrect fuel composition at loading and of leak during the transfer to the processing unit. However, since the amount of daily-injected fuel is quite small (10–40 L per day), the associated consequences are limited. In the reference design of SAMOFAR, the salt puncture is done at the top of the core, through a lid over the fuel circuit expansion vessel; the safety analysis helped identifying this lid as a potential weak point and other options are currently under study.

A more complete description of the fuel circuit and the systems connected to the fuel circuit is in SAMOFAR deliverable 1.1 [16].

The peculiarities of the MSFR, summarized in this paragraph, and the preliminary stage of its design call for use of technological neutral methodologies such as the ISAM in support of the safety assessment, as reckoned by the GIF. Such methodologies should help, as they are being deployed, to catch and address the specificities of the MSFR concept. Indeed, current nuclear safety requirements and methodologies applicable to solid-fuel reactor concepts, in particular LWRs technology, may not be fully relevant in the MSFR context: for example, some LWR risk metrics (such as the Core Damage Frequency – CDF) are not significant for the MSFR. Additionally, the severe accident, traditionally coincident with the core melting, needs an updated and more general definition. Moreover, the physical barriers for the containment of radionuclides suited to the MSFRs needs, due to the liquid and circulating nature of the fuel, necessitate to be defined [18]. These examples clarify the need of a technologically neutral methodology,

applicable to the new generation concepts, especially when it comes to MSFR development. Of course, such methodology should always represent a practical declination of the IAEA Fundamental Safety Principles [3].

3. Description of the methodology

In order to be as exhaustive as possible, it is proposed for the MSFR to use two different approaches for identifying potential accident initiating events (IEs). In addition, the design of the MSFR being still in development and the operating procedures (start-up, shutdown and maintenance) under definition [19], the safety approach has to include appropriate methods, usable despite the lack of knowledge on components, systems or procedures. For this purpose, the Master Logic Diagram (top down approach) and the FFMEA (functional bottom up approach) have been selected. Both methods and their applications to the MSFR are described in the following paragraphs. These methods aim at being coherent with the ISAM. The MLD contributes to the preparation of the Objective Provision Tree (OPT), one of the tools proposed in the ISAM, whose objective is to help identifying all provisions needed to sketch the design safety architecture in order to guarantee the safety functions. In that respect, the MLD contribution is to provide a systematic identification of hazards that could affect the plant, through a top down approach with an event tree structure. The FFMEA aims at systematically investigating the hazards that could affect the MSFR functionality and allows also to recognize critical components, lack of information and/or criticalities of the design and necessity of supplementary provisions. In this optics, the outputs of the FFMEA can give insights to other ISAM tools, such as the OPT and the PIRT, the Phenomena and Identification Ranking Table, whose objective is to identify plausible phenomena significantly contributing to risk. Due to the very preliminary stage of MSFR design, the identification of the hazardous events is not arranged according to the DiD levels, which could be done in a later stage together with identification of the associated layers of provisions, as reckoned for a full deployment of the OPT tool.

The work has been performed by a team composed by design expert, safety experts and industrial experts, several of them having previous experiences in the use of FFMEA and MLD tools. Moreover, experts' judgement and experience feedback, e.g. from the ORNL MSRE [20], have been taken into account for the sake of exhaustiveness. The IEs identified here correspond to internal events that may lead to radioactive releases, due to an abnormal operating conditions of the fuel circuit. Then, from the complete list of IEs, a set of postulated initiating events (PIEs) is selected as the most representative in terms of challenging conditions for the safety of the plant. In such a way, it is possible to focus safety studies on the most relevant initiating events. In paragraph 3.3, the process of PIEs selection is described, as it was applied to the FFMEA and to the MLD.

3.1. Functional Failure Modes and Effects Analysis

The Functional Failure Mode and Effect Analysis (FFMEA) is a suitable qualitative methodology to define possible incident and accident initiators when a sufficient design detail is not available to allow more specific evaluations at component level, by investigating systematically components failures that could affect system functionality [21]. The main functions of the plant (process functions, safety functions, investment protection functions, etc.) are defined at first through the Functional Breakdown Structure (FBS) and specified in sub-functions. Moreover, the available design information and design intents (defined in the FBS) are collected and all the systems and components of the plant are listed in order to define the Plant Breakdown Structure (PBS). Then, each main function can be correlated to one or more than one of the components. Subsequently, the FFMEA table is compiled, postulating the loss of the functions rather than the specific failures of systems and components: in this way, it is possible to overcome the lack of information of systems design. Nonetheless, reference to systems/components is always highlighted, as much as possible, in order to investigate causes and safety consequences. Furthermore, possible improvements, prevention and mitigation actions are recommended. The objective of the FFMEA is to provide a complete list of potential initiating events (IEs) and give suggestions in order to improve the overall safety of the system/reactor [10].

The FFMEA allows performing MSFR safety assessment, notwithstanding its very preliminary state of design, in order to identify functional deviations able to compromise system safety, to list Postulated Initiating Events (PIEs) and to recognize critical components, lack of information and/or criticalities of the design and necessity of supplementary safety provisions.

Table 2 shows an extract of the FFMEA table compiled for the process functions of the MSFR in normal operation conditions during power production. The analysis focuses on the fuel circuit

Table 2
Extract from the FFMEA MSFR table.

Process function	PBS elements	Op. Md.	Failure mode	Cause	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 containment leak-tightness	Leak/Rupture in the core vessel	The fuel flows outside the core cavity; The amount of fissile matter in the core decreases leading to the shutdown of the chain reaction; The fuel is collected in the collector where it is subcritical; The fuel is drained in the EDS where it is in a subcritical configuration and is 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

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. A first application of the FFMEA to the MSFR is available on [22] with more details on each step of the methodology.

3.2. Master Logic Diagram

The Master Logic Diagram (MLD) is a qualitative risk analysis method whose purpose is to identify the hazards and possible initiating events of a system, through a deductive and structured approach. This "top-down" approach is particularly well suited for projects in early design phases as the analysis is based on physical phenomena and general considerations rather than specific components of the design. It also proves to be helpful to highlight the correlations between different functions/phenomena and can therefore be an asset in the study of complex systems such as nuclear power plants. It has been widely used in nuclear industry as well as in other engineering fields such as chemical plants and processes [11].

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

- Identification of the top event, which is the undesired situation to be prevented.
- Decomposition of the top-event into detailed sub-events, each sub-event being a possible cause of the considered top-event. The development continues until a sufficient level of details is reached and events directly challenging the safety functions are identified. In this step, the consideration of all physically possible phenomena is crucial for the completeness of the approach.
- Identification of the initiating events as the basic events that cannot be further divided into sub-events.

The diagram is usually presented in the form of a qualitative fault tree based on Boolean logic beginning with the top event and where the lower levels of the tree show the elementary failures.

The MLD method has been applied to the MSFR for the normal operation state of power production, similarly to the FFMEA application. In this mode, 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 [23], is presented in Fig. 2 where the top event is decomposed according to the phenomena involved (thermal, chemical, mechanical, etc.).

3.3. Identification and discussion of the PIEs

In order to identify the PIEs, all the elementary IEs are listed in a unique document and are grouped into families, depending on their potential effects on the reactor.

The grouping of IEs in a family is usually done according to criteria of similarity of the consequences associated to the single IE and of plant response.

The common practice is then to define incident and accident categories with associated occurrence frequency ranges. For a given family, PIE are then identified as envelope cases in 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 evaluation of the expected frequency for each PIE should be performed preliminary in a first time given the premature state of the current design (at least distinguishing frequent events, rare events, and very rare events), based on engineering judgement. Low probability events may also be postulated, based on the defence-in-depth principle.

For the objective of this analysis, only the most severe events of a family in terms of consequences are selected as PIEs [10], with no consideration for their occurrence frequency in a first time, which should be done in a later stage (at least with occurrence frequency ranges or expected orders of magnitude). At this stage, it is not always obvious to identify the most severe events: therefore, it has sometimes been chosen to maintain a significant number of IEs as PIEs, which could be optimized in a later stage. As final result of the work, 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

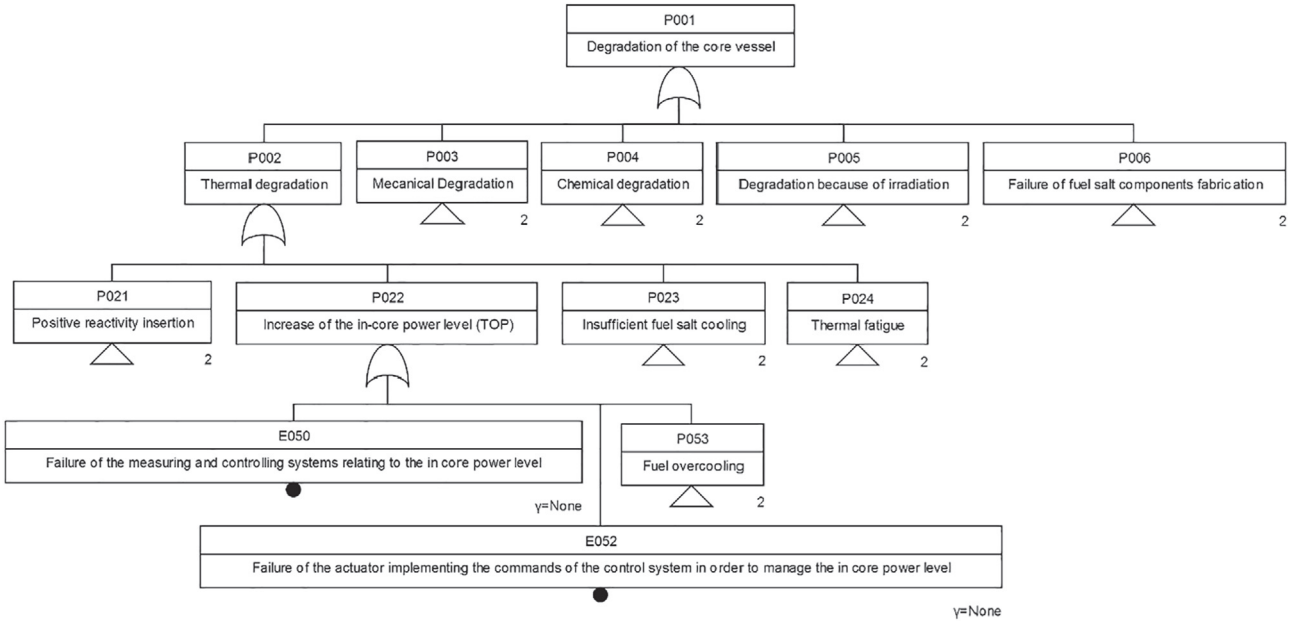

Fig. 2. Extract of the MSFR MLD.

check the compliance with safety limits and to drive the choices for the selection of the reference design [24]. It is besides reminded that the DiD principle is the fundamental principle to use for the safety analysis. In that respect, it is also underlined that some PIEs have been selected independently of their likelihood at this stage, with the goal 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 …): some of them may be later found not to be possible in the future MSFR studies and thus withdrawn from the PIEs list.

If events are estimated not to lead to any safety relevant disturbance, they can be classified as not relevant from the safety point of view (N/S). These events will not be analysed from the safety issue, nevertheless they can be important in the future when Reliability, Availability, Maintainability and Inspectability (RAMI) analysis will be performed [10].

This methodology should be iteratively applied, following the design development; similarly, the list of the PIEs evolves with the detail of the design and the investigation of the physical phenomena governing the behaviour of the system, through deterministic analyses. Therefore, this methodology aims at influencing the direction of the concept and design development from its earliest stages.

4. Results

4.1. PIEs list

As stated/explained above, PIEs are generally determined by looking at the set of elementary failures that compromise process functions and induce consequences of safety concern, grouping events that induce similar consequences in the plant into families and selecting, as representative, the most severe elementary failure of the group of events. The families of events identified for the MSFR are:

- 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

Since the conceptual phase of the design and the iterative nature of the methodology, this list will be updated following the evolution of the available information (in terms of design detail, reactor transients, experimental analyses, etc). The most severe Initiating Events of each family is selected as Postulated Initiating event. Table 3 presents an extract from the PIEs list obtained by the FFMEA and the MLD, with a selection of PIEs assumed to be representative accident initiators. These representative accident initiators are assumed to envelope all the IEs in terms of radiological consequences.

As an illustration of the plant behaviour in some events, the case of loss of liquid fuel flow family is preliminary described hereafter. In the

Table 3
Extract of assumed representative events from the list of Postulated Initiating Events obtained by the FFMEA and the MLD.

F1: Bulk precipitation of fissile matter (e.g because of an inlet of water)
F1: Accidental insertion of fuel
F1: Important deformation of the fuel circuit possibly leading to an increased core volume (e.g. the welded joints taking the recirculation sectors in the correct position collapse)
F1: Fertile blanket loading with fuel salt
F1 & F2: Fuel salt freezing scenario
F1 & F6: Rupture/obstruction of reactivity bubble injector
F2: Blockage of all sectors of fuel salt circuit
F2: Complete rupture or blockage of all the fuel circuit pumps
F3: Overworking of all the fuel circuit pumps
F3: conversion circuit pumps overworking
F3: Over-working of the pumps of the intermediate circuit
F4: Obstruction/blockage of the intermediate circuit
F4: complete loss of intermediate salt
F4: Rupture/blockage of all intermediate circuit pumps
F5: Breach in the core vessel
F5: Breach in the lower reflector (with rupture of the structure cooling system)
F5: Breach in the upper reflector with rupture of the structure cooling system and/or with damages to the expansion vessel system
F5: Breach of a heat exchanger plate/channel
F5: Rupture of blanket tank wall between fuel and fertile salt with rupture of the fuel circuit walls cooling circuit
F5: Rupture of a pipe of the reactivity control system
F5 & F11: 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
F6: Rupture of horizontal bubble injector for salt cleaning
F6: Rupture of the gas separation chamber
F6: Undetected deviation of the chemical composition
F6: Rupture of the gas processing unit (with possible leak of processing fluid)
F6: Chemical reaction between different fluids (e.g. hot part of intermediate circuit and water)
F6 & F11: Inlet of water
F7: Detachment of the wall thermal protection
F9: Complete rupture of the pressurised sampling device
F10: Prompt critical power excursion with induced shockwave
F11: Obstruction of all free levels (including the vertical inlet pipe from the core to the expansion vessel)
F12: Ejection of a conversion system component
F13: Total loss of electric power

event “complete rupture or blockage of all the fuel circuit pumps”, the loss of flow is assumed to be relatively fast as the components improving the inertia (e.g., pump flywheels) are unavailable. Moreover, in case of pump rupture, broken parts of the pump could enter the fuel flow. In the event “blockage of all sectors of fuel salt circuit”, the rapidity of the loss of flow depends on the nature of the blockage which can be caused by the presence of external elements in the fuel circuit, the presence of broken components of the fuel circuit, the precipitation or the solidification of the fuel in the heat exchanger. In the events “complete rupture or blockage of all the fuel circuit pumps” and “blockage of all sectors of fuel salt circuit”, the complete loss of fuel flow causes the increase of the temperature in the core and thus the shutdown of the chain reaction because of the negative feedback. After the shutdown of the chain reaction, the temperature of the fuel in the core and in the part of the fuel circuit that are not cooled continues to increase because of the residual heat. The major risk associated to these events is the degradation of the fuel circuit components due to the high temperature achieved. To prevent this risk, some provisions are implemented in the design, such as the emergency draining of the fuel salt. The “fuel salt freezing scenario” is characterized by the solidification of the fuel salt in a large part of the fuel circuit. No exact cause of this scenario has been identified until now. However, it has been kept in the list of events to be studied in order to test the limits of the design.

4.2. Comparison of MLD and FFMEA

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 looking for the possible causes of the loss of the functions and their consequences; while 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 MSFR components, systems or procedures. Indeed, in both methods the link with the component arrives only in a second time, making them more suitable to an application at early design phase.

The results agreed well and many events were found independently with both methods. 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. For instance, the events “Loss of Chemical Control: Chemical reaction between different fluids” or “Mechanical Degradation: Ejection of a power conversion system component in direction of the fuel circuit” only appeared through the MLD analysis. On the other hand, the FFMEA brought more details on the failure modes thanks to the effort to link the loss of each function to a component or system failure. 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.

The FFMEA has the advantage to provide additional information on the systems or procedures used for detection, prevention and mitigation, in a very preliminary approach to the defence in depth, while the MLD offers a good graphical tool to present the hazards and helps understand the logical connections 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. In addition, as a complementary result, both the methods helped to highlight the open points of the project, which could be taken into account during next steps of the design.

4.3. Critical analysis

In a solid-fuelled reactor, the accident initiators are traditionally classified in the following families (list “a minima”): LOCA (Loss of Coolant Accident), LOF (Loss of Flow), LOHS (Loss of Heat Sink), TOP (Transient OverPower), TLOP (Total Loss Of Power) and OVC (Overcooling) [25]. Moreover, in the IRSN report [26], for PWRs the term “severe accident” refers to an event causing significant damage to reactor fuel and resulting from more or less complete core meltdown”.

From the list of accident initiators, it can be noticed that a direct transposition of these categories to the MSFR is not possible and the biggest differences between the liquid-fuelled reactors and the solid-fuelled reactors are linked to peculiar characteristics of the latter: the liquid nature of the fuel makes necessary a new definition of severe accident detached from the concept of core melting and at the same time introduces new accident initiators such as the “Loss of fuel flow”, which was not conceived in the LWRs.

The safety analysis of the PIE should also take into account the particular arrangement of safety systems. The reactivity control systems deserve a special mention since the control rods are substituted by a bubbling control system for the reactivity management in normal operation conditions in the current MSFR design and the EDS for the geometrical subcritical redistribution of the core in case of emergency. The design and the operation of the EDS represent one of the major safety issues of this reactor. The concept and the dimension of the system constitute an open point of the project, as well as the Decay Heat Removal systems for long term accident management should be more precisely designed and tested. As regard radiological containment, barriers must also be defined with due account for the liquid nature of the fuel. Then, in a later stage, the safety architecture will have to be consolidated, notably ensuring proper implementation of the defence-in-depth in the design.

Along with the implementation of the tools, some open points on the design, the systems, the phenomena and procedures of the MSFR are highlighted with their advantages and drawbacks, to give inputs for the evolution of the concept in the optic of a safety-driven design.

5. Conclusion

A list of Postulated Initiating Events is produced, as reference accidents for the successive deterministic analyses that will be performed to assess the severity of the involved phenomena and transients. The list of PIEs will evolve as the design is refined step by step and the deterministic analysis on components and transients are performed. The outputs of this work represent a common starting point to be refined: it is plausible that some of the hazardous events will be removed of the list because successive analyses could show their inconsistency. On the other hand this analysis may lead the designers to provide design modifications such that some events are no longer to be considered (if they are physically impossible for example). Nevertheless, the list will likely include new events that are not highlighted yet.

Successively each accident scenario has to be classified into frequencies and consequences macro-categories (in terms of damages to the asset and environmental releases) and one or more risk matrices will be built using consistent definitions of technological inclusive risk metrics and severe accidents: based on the risk level of each accidental sequence, a number of lines of defence (e.g. provisions, protection systems, etc.) is under definition for the unprotected sequences therefore the final objective of this methodology is to help sketching the architecture of the system.

In the current study, the state of normal operation during power

production is analysed. The same analysis will be conducted for maintenance as well as start-up and shut-down procedures. Similarly, the scope of the analysis is limited to the fuel circuit and the systems directly connected and interacting with the fuel circuit. A wider study should be performed to include other systems such as the routine draining tanks and the processing units.

This first implementation of the methodology presented here is not exhaustive nonetheless it has been useful not only to highlight missing information, lack of provisions and criticalities of the system but also to define a procedure that can be applied iteratively with the evolution of the design and the knowledge of the transient behaviours.

Acknowledgments

This project has received funding from the Euratom research and training programme 2014–2018 under grant agreement No 661891. The authors also wish to thank the NEEDS (Nucléaire: Energie, Environnement, Déchets, Société) French program, the IN2P3 department of the National Center for Scientific Research (CNRS) and Grenoble Institute of Technology for their support.

The content of this article does not reflect the official opinion of the European Union. Responsibility for the information and/or views expressed therein lies entirely with the author(s).

References

[1] GIF, Technology Roadmap Update for Generation IV Nuclear Energy Systems, 2014.
[2] J. Serp, M. Allibert, O. Beneš, S. Delpech, O. Feynberg, V. Ghetta, D. Heuer, D. Holcomb, V. Ignatiev, J.L. Kloosterman, L. Luzzi, E. Merle-Lucotte, J. Uhlíř, R. Yoshioka, D. Zhimin, The molten salt reactor (MSR) in generation IV: overview and Perspectives, Prog. Nucl. Energy (2014) 1–13.
[3] IAEA, IAEA Safety Standard for Protecting People and Environment, Fundamental Safety Principles, No SF-1, 2006.
[4] GIF RSWG, Basis for the Safety Approach for Design and Assessment of Generation IV Nuclear Systems Revision 1, 2008.
[5] A. Carpignano, S. Beils, S. Dulla, Y. Flauw, D. Gérardin, D. Heuer, D. Lecarpentier, E. Merle, E. Ivanov, V. Tiberi, A. Uggenti, Development on an Integral Safety Assessment Methodology for MSFRs, 2018. Work-Package WP1, Deliverable 1.5, SAMOFAR European H2020 Project, Contract number: 661891.
[6] GIF RSWG, An Integrated Safety Assessment Methodology (ISAM) for Generation IV Nuclear Systems, 2011 version 1.1.
[7] E. Wattelle, L. Ammirabile, Proposal for a harmonized European methodology for the safety assessment of innovative reactors with fast neutron spectrum to be built in Europe, in: Work-Package WP3, Delivrable 3.5, SARGEN_IV Project, 2012. Contract number: 295446.
[8] M. Brovchenko, Etudes préliminaires de sûreté du réacteur à sels fondus MSFR, PhD Thesis, Grenoble Institute of Technology, France, 2013.
[9] D. Gérardin, M. Allibert, D. Heuer, A. Laureau, E. Merle-Lucotte, C. Seuvre, Design evolutions of the molten salt fast reactor, in: International Conference on Fast Reactors and Related Fuel Cycles: Next Generation Nuclear Systems for Sustainable Development (FR17), Yekaterinburg, Russia, 2017.
[10] T. Pinna, et al., Functional Failure Mode and Effect Analysis (FFMEA) for the DEMO Cooling Systems of the WCLL Blanket Model, EuroFUSION Report EFDA_D_2JPQSG V1.0, 2015.
[11] I.A. Papazoglou, O.N. Aneziris, Master Logic Diagram: method for hazard and initiating event identification in process plants, J. Hazard Mater. A97 (2003) 11–30.
[12] GIF RSWG, Guidance Document for Integrated Safety Assessment Methodology (ISAM) – (GDI), 2014.
[13] D. Heuer, E. Merle-Lucotte, M. Allibert, M. Brovchenko, V. Ghetta, P. Rubiolo, Towards the thorium fuel cycle with molten salt fast reactors, Ann. Nucl. Energy 64 (2014) 421–429.
[14] H. Rouch, O. Geoffroy, P. Rubiolo, A. Laureau, D. Heuer, M. Brovchenko, E. Merle-Lucotte, Preliminary thermal–hydraulic core design of the molten salt fast reactor (MSFR), Ann. Nucl. Energy 64 (2014) 449–456.
[15] M. Brovchenko, D. Heuer, E. Merle-Lucotte, M. Allibert, V. Ghetta, A. Laureau, P. Rubiolo, Design-related studies for the preliminary safety assessment of the molten salt fast reactor, Nucl. Sci. Eng. 175 (2013) 329–339.
[16] M. Allibert, D. Gérardin, D. Heuer, E. Huffer, A. Laureau, E. Merle, S. Beils, A. Cammi, B. Carluec, S. Delpech, A. Gerber, E. Girardi, J. Krepel, D. Lathouwers, D. Lecarpentier, S. Lorenzi, L. Luzzi, S. Poumerouly, M. Ricotti, V. Tiberi, Description of Initial Reference Design and Identification of Safety Aspects of the MSFR, 2017. Work-Package WP1, Delivrable 1.1, SAMOFAR European H2020 Project, Contract number: 661891.
[17] A. Laureau, D. Heuer, E. Merle-Lucotte, P. Rubiolo, M. Allibert, M. Aufiero, Transient coupled calculations of the molten salt fast reactor using the transient fission matrix approach, Nucl. Eng. Des. 316 (2017) 112–124.
[18] Southern Company, Modernization Non –Light Water Reactors Probabilistic Risk Assessment Approach, SC-29980-101 Rev A, 2017.
[19] D. Heuer, A. Laureau, E. Merle-Lucotte, M. Allibert, D. Gerardin, A starting procedure for the MSFR: approach to criticality and incident analysis, in: International Congress on Advances in Nuclear Power Plants (ICAPP'2017), Kyoto, Japan, 2017.
[20] P.N. Haubenreich, J.R. Engel, C.H. Gabbard, R.H. Guymon, B.E. Prince, Safety Analysis of Operation with ^{233}U, Rapport ORNL-TM-2111, Oak Ridge National Laboratory, Oak Ridge, Tennessee, 1968.
[21] A. Carpignano, et al., Safety issues related to the intermediate heat storage for the EU DEMO, Fusion Eng. Des. 1010–111 (part A) (2016) 135–140.
[22] A.C. Uggenti, D. Gérardin, A. Carpignano, S. Dulla, E. Merle, D. Heuer, A. Laureau, M. Allibert, Preliminary functional safety assessment for molten salt fast reactors in the framework of the SAMOFAR project, in: International Topical Meeting on Probabilistic Safety Assessment and Analysis (PSA 2017), Pittsburgh, USA, 2017.
[23] E. Clement, Arbre Analyste, 2013. Available from: http://www.arbre-analyste.fr/.
[24] T. Pinna, et al., Identification of accident sequences for the DEMO plant, Fusion Eng. Des. 124 (2017) 1277–1280.
[25] Argonne National Laboratory, Uncertainty in Unprotected Loss-of-Heat-Sink, Loss-of-Flow, and Transient-Overpower Accidents, Technical report, Advanced Fuel Cycle Initiative, 2007.
[26] IRSN, Research and Development with Regard to Severe Accidents in Pressurized Water Reactors: Summary and Outlook, 2007.