PSI - PAUL SCHERRER INSTITUT

Safety Analysis for the Licensing of Molten Salt Reactors

Master's Thesis Report

Mentor: Dr. Vinh N. Dang
Supervisor: Pr. Andreas Pautz

Dimitri D. A. Pyron

7/29/2016

Abstract

The licensing of Molten Salt Reactors (MSRs) remains an open issue; one reason is that parts of nuclear regulation are specific to Light Water Reactors (LWRs). The regulatory developments associated with the New Generation Nuclear Plant (NGNP) project provide indications on a potential path for MSR licensing. This methodology eliminates LWR-specific aspects and uses Probabilistic Safety Assessment (PSA) to define the design bases and to demonstrate the plant safety. The present study is based on this approach. The design considered in this study is the FUJI-233Um from Japan, a graphite moderated MSR, which is planned to be constructed around 2025. In the present study, Initiating Events (IEs) were identified thanks to the Master Logic Diagram (MLD) methodology. Accident scenarios, together with analyses of parameter evolutions and potential consequences, were developed in order to conduct a PSA of the design, i.e. to quantify Event trees (ETs) and Fault Trees (FTs). At the same time, an MSR-specific database was built in order to quantify the ETs developed. Once the PSA model was complete, the different scenarios were classified and verified against design targets called Top Level Regulatory Criteria (TLRC). The latter allowed identification and analyses of potential safety weaknesses. In order to improve the design in terms of safety, possible design changes were suggested. Supposing the design was improved, safety-relevant Systems, Structures and Components (SR-SSCs) and Design Basis Accidents (DBAs) were defined and identified. It points out important scenarios to consider for MSR licensing.

Contents

Table of Figures

Table of tables

Acronyms

AMSB	Accelerator Molten Salt Breeder
AOO	Anticipated Operational Occurrences
BDBE	Beyond Design Basis Event
CCDF	Complementary Cumulative Distribution Function
CCF	Common Cause Failure
DBA	Design Basis Accident
DBE	Design Basis Event
DOE	Department Of Energy
(E/S)DT(C)	(Emergency/Secondary) Drain Tank (Cooling)
EAB	Exclusion Area Boundary
ENSI	Eidgenössische Nuklear-Sicherheitsinspektorat
EPRI	Electric Power Research Institute
ET	Event tree
EVOL	Evaluation and Viability Of Liquid fuel salt reactor
FHR	Fluoride salt-cooled High-temperature Reactor
FP	Fission product
FT	Fault tree
FV	Fussell-Vesely
HTGR	High-temperature Gas cooled reactor
(HX/SG)TR	(Heat eXchanger/Steam Generator) Tube Rupture
IAEA	International Atomic Energy Agency
IE	Initiating Event
IM	Importance measure
INL	Idaho National Laboratory
JNI	Jeffreys Non-Informative (prior)

LBE	Licensing Basis Event
LWR	Light Water Reactor
MLD	Master Logic Diagram
MOSART	Molten Salt Actinide Recycler and Transmuter
MSR	Molten Salt Reactor
NGNP	New Generation Nuclear Plant
NRC	Nuclear Regulatory Commission
ORNL	Oak-ridge National Laboratory
(P/D)AC	(Primary/Derived) Acceptance Criterion
P(S/R)A	Probabilistic (Safety/Risk) Assessment
QHO	Quantitative Health Objective
RSA	Reactive Surface Area
SAMOFAR	Safety Assessment of the MOlten salt FAst Reactor
SFR	Sodium Fast Reactor
SPAR	Standardized Plant Analysis Risk
(SR-)SSC	(Safety-Related) Structures, Systems and Components
THERP	Technique for Human Error Rate Prediction
THORIMS-NES	Thorium Molten-Salt Nuclear Energy Synergetic System
TLRC	Top-level Regulatory Criteria
TTS	Thorium Tech Solution Inc.

I. Introduction

The licensing of Molten Salt Reactors (MSRs) remains an open issue; one reason is that parts of nuclear regulation are specific to Light Water Reactors (LWRs). For instance, limiting parameters for cladding failure have no sense in MSRs since there is no cladding. This remark motivated the New Generation Nuclear Plant (NGNP) project to propose regulations providing indications on a potential path for MSR licensing [1]. The NGNP project proposed a complete methodology for the licensing of generation IV reactors, consisting of a design safety analysis, where "design safety" means demonstration that the design is safe in terms of maximum radioactive release. In the present study, a complete safety assessment for the licensing of a specific Molten Salt Reactor (MSR) is performed by following the NGNP proposed approach. This analysis consists of a Probabilistic Safety Assessment (PSA) model built using the software RiskSpectrum®.

MSRs of diverse designs have been proposed and are being planned. In this study, the focus is on the 200 MWe graphite moderated molten salt reactor FUJI-233Um of Thorium Tech Solution Inc. (TTS) from Japan. This design was chosen since it seems to be one of the most mature designs with extensive literature available. Indeed, the FUJI-233Um design is largely based on the 1000 MWe Molten Salt Breeder Reactor (MSBR) of the Oak Ridge National Laboratory (ORNL), which was planned to be built in the 1970's.

No quantitative safety assessment of MSR has been published until now. Reference [2] presents some qualitative considerations about safety assessment of MSRs, but the study is incomplete and not quantitative.

Nonetheless, there is previous work relevant to the FUJI-233Um licensing. The TTS team already defined LWR-based Design Basis Accidents (DBAs) [3]. Based on this list, they identified and simulated two accidents specifically for the FUJI-233Um reactor:

- Reactivity Induced Accidents (more precisely control rods drop (graphite control rods))
- Unprotected LOCA

However, the literature about the FUJI-233Um design and other accident progressions is incomplete. Therefore, since the FUJI-233Um reactor is largely based on the MSBR design, design gaps were filled with information from the MSBR literature. For instance, the off-gas system and the unprotected loss of primary salt flow accident are based on the MSBR literature.

In order to conduct the safety assessment for the licensing of the FUJI-233Um reactor, the following tasks were performed:

- Identification of IE using the Master Logic Diagram (MLD) Method
- Development of accident scenarios, analyses of parameter evolutions and potential consequences
- Construction of an MSR-specific database for component failure rates
- Construction of Fault Trees (FTs), Event Trees (ETs) and quantification of the PSA
- Identification of safety weaknesses
- Identification of Safety-Related Structures, Systems and Components (SR-SSCs) and Design Basis Accidents (DBAS)

The present study is divided into six chapters. The links between them are represented in Figure 1. As can be seen, Chapters II and III present the two inputs of the study. Chapters IV, V and VI cover the construction of the PSA model. Chapter VII concerns the exploitation of the model, thus the results obtained thanks to the study.

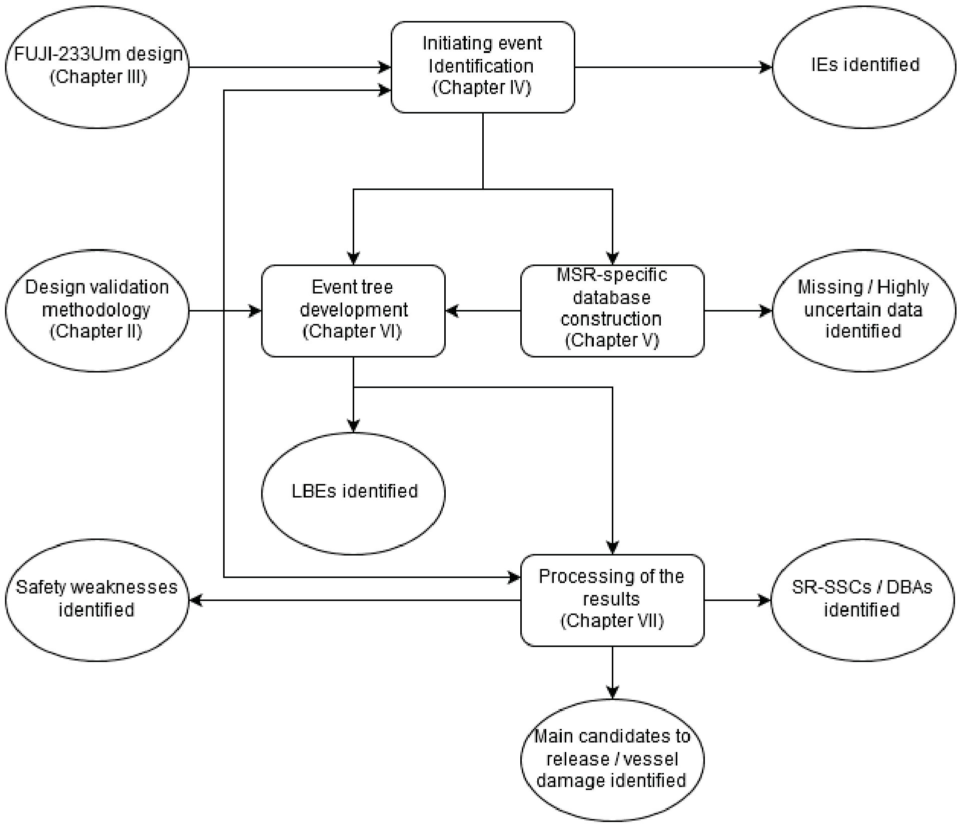


Figure 1: Flowchart of the study

More precisely, Chapter II deals with the licensing of new generation nuclear power plants (NGNP) according to the NGNP proposed approach. The NGNP methodology will be used throughout the study in order to perform a design safety analysis of the FUJI-233Um reactor. Moreover, other safety criteria have been proposed by researchers at TTS. Therefore, a comparison of the different criteria is performed. Chapter III gives an overview of the plant design and its key features. In MSRs, it may seem that the safety risk is shifted to the fission product treatment systems. This issue is addressed throughout this study by a careful examination of the off-gas system. In Chapter IV, initiating events are identified using the Master Logic Diagram methodology suggested by the NGNP project. Chapter V deals with the construction of an MSR failure rate database in order to calculate component reliabilities and initiating event frequencies. Missing and highly uncertain data are highlighted and experiments or studies are suggested to improve the database. Chapter VI gives an overview of the different accident progressions and their associated event trees. The database developed in Chapter V is used to quantify the event trees developed. Chapter VII defines NGNP-based DBAs, which will be compared with LWR-based DBAs from the literature. Main events with radioactive release or vessel damage and design safety weaknesses are identified as well. Design improvements are suggested. Finally, the licensing issues, the component failure rate database and the design improvements suggested are discussed in Chapter VIII.

II. Licensing of advanced reactors

The New Generation Nuclear Plant (NGNP) project sought to resolve key licensing issues for High Temperature Gas-Cooled Reactors (HTGRs). However, the approach that they developed tried to be as general as possible for new generation reactors. Thus this project indicates a potential path for MSR licensing.

The Energy Policy Act of 2005 directed the Department Of Energy (DOE) to establish and manage the NGNP project. This project designated the Idaho National Laboratory (INL) for the research, development, design, licensing, construction, and operation of new generation nuclear reactors. The Nuclear Regulatory Commission (NRC) has been designated as regulatory authority and DOE as manager. As required by the project, DOE and NRC, in 2008, submitted the NGNP Licensing Strategy Report to Congress [4]. In this report is presented four possible approaches for the licensing of NGNP. One of them, finally chosen by the DOE and the NRC as adequate, is a risk-informed approach combining probabilistic and deterministic engineering judgments.

The project began in 2005 and stopped promptly in 2008 due to a lack of funding. That is why the NGNP methodology has only been applied partly for a Fluoride salt-cooled High-temperature Reactor (FHR) [5] and a High Temperature Gas-cooled Reactor (HTGR) [1]. Nonetheless, the NGNP project proposed a complete methodology for the licensing of generation IV reactors, consisting of a design safety analysis, where "design safety" means demonstration that the design is safe in terms of maximal radioactive release.

II.1. The NGNP safety criteria versus the Japanese criteria

As will be seen, different safety criteria were defined. These criteria have in common that they try to demonstrate that the design is safe in terms of radioactive release. The main difference is that the NGNP-based criteria are probabilistic, whereas the LWR-based criteria from TTS are deterministic. Probabilistic means that the criteria are based on frequency + consequences calculations. Deterministic means that the criteria are limits on reactor parameters, here the fuel temperature. The link between them is explained at the end of this section.

II.1.1. The NGNP criteria: LBEs identification

NGNP-based criteria are scenario-specific. It means that the criterion depends on the frequency of the considered scenarios called Licensing Basis Events (LBEs). LBEs are defined as scenarios resulting from the particular technology and design of the plant that are considered by the licensing process. They are essential in the development of the licence application. By defining LBEs, a set of scenarios are created, which forms the basis plant analysis and represents the plant's safety performance.
Once the LBEs are identified (PSA methodology presented in the next part), a classification of them is necessary, because different probability of occurrences lead to different regulations. Obviously a

very unlikely scenario could be more harmful than a very likely scenario, which should not disturb the normal operation of the power plant and should not release radioactivity.
Therefore, the INL proposed a classification of the identified LBEs [1]. LBEs are divided in three groups according to different criteria: Anticipated Operational Occurrences (AOO), consisting of planned and anticipated events, Design Basis Events (DBE), and Beyond Design Basis Events (BDBE).

These three classes are defined by three different probabilities of occurrences per plant per year:

- AOO > 10^{-2} per plant-year
- 10^{-2} per plant year > DBE > 10^{-4} per plant-year
- 10^{-4} per plant-year > BDBE > 5.10^{-7} per plant-year

Below a probability of 5.10^{-7} per plant-year, scenarios are judged too unlikely and not considered in the licensing process.
The Advisory Committee on Reactor Safeguards (ACRS), in their paper *"Development of a Technology-Neutral Regulatory Framework"*, September 26, 2007 [6], agreed with the INL staff for the lower limit of $5*10^{-7}$/p.y. According to them, this limit allows a reduction of the risk that the licensing will divert from scenarios of real safety significance. Depending on their classes, LBEs must respect criteria defined by the NRC, called Top Level Regulatory Criteria (TLRC). The TLRC are defined in order to follow certain objectives:

- TLRC must provide direct public health and safety acceptability limits in terms of potential radiological consequences
- TLRC are independent of the reactor type
- TLRC provide easily quantifiable risk criteria

TLRC derive from different sources, which are mainly [1]:

10 CFR Part 20, Standards for Protection against Radiation (Subpart C, Occupational Dose Limits): the regulations establish standards for protection against ionizing radiation following the normal operation of the licensed NPP. The TLRC applied for AOOs derive from this regulation.

10 CFR §50.34(a)(III)(D), "Contents of Applications: Technical Information (Radiological Dose Consequences)": this section specifies dose limits to evaluate the performance of safety features mitigating releases during accidents. The TLRC applied for DBEs/DBAs derive from this regulation.

NRC Safety Goals individual fatality risks: the regulation provides Prompt and Latent Quantitative health objectives (QHOs), as well as an obligation for negligible cumulative risks from NPP during off-normal events. The TLRC applied for BDBEs derive from this regulation.

EPA Protective Action Guides offsite doses: Recommendations for emergency planning and protection during off-normal events. The TLRC applied for DBEs/DBAs/BDBE derive from this regulation (represented on Figure 2 with a dashed line).

Quantitatively, the TLRC become:

- AOO < 100 mrem total effective dose equivalent realistically calculated at the Exclusion Area Boundary (EAB)
- DBE < 25 rem total effective dose equivalent realistically calculated at the EAB
- BDBE < NRC safety goal Quantitative Health Objectives (QHOs) calculated at 1.6 km and 16 km from the plant

The EAB is the "area surrounding the reactor, in which the reactor licensee has the authority to determine all activities including exclusion or removal of personnel and property" (NRC: 10 CFR 50.2). The radius of the EAB depends on the plant design, but it is often at least 500m.

The two QHOs are a prompt fatality QHO and a latent cancer fatality QHO defined in SECY-13-0029 [7]. The classification can be illustrated by a frequency-consequence curve proposed first in NUREG-1860 [8]:

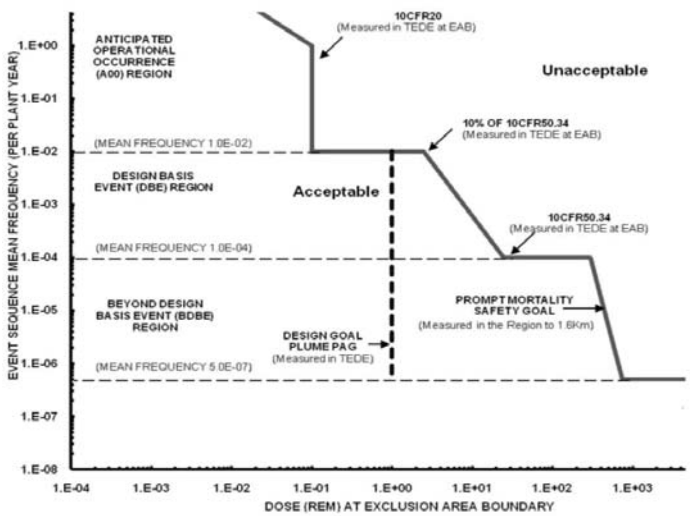


Figure 2: Frequency-consequence graph showing acceptable LBEs and their classification. Figure from the INL White Paper on Licensing Basis Event Selection [1].

As can be seen on the y-axis, the F-C curve is sequence-specific. The ACRS, in their paper *"Development of a Technology-Neutral Regulatory Framework"*, September 26, 2007 [9], agreed with the NRC staff for the use of such curve as regulatory requirement to limit radiation exposure to public. However, they pointed out that the use of a Complementary Cumulative Distribution Function (CCDF) F-C curve aggregating the contribution to risk of the different sequences would impose better limits on risk compared to the sequence-specific F-C curve. An alternative candidate CCDF F-C curve is discussed in EPRI TR-1013582, "Technical Elements of a Risk-Informed, Technology-Neutral Design and Licensing Framework for New Nuclear Plants" [10].

However, instead of complementing the sequence-specific F-C curve with a CCDF F-C curve integrating the overall risk of all event sequences, the INL decided to impose sequence-specific limits on the sequence specific F-C curve, so that if these limits are met, the overall risk of all event sequences will meet the reactor safety goals by order of magnitude [11]. Therefore the final safety criteria to meet are sequence-specific. This allows an easier verification of the conformity of scenarios towards safety criteria, as well as an easier identification of the critical SSCs in case of non-conformity. Thanks to these criteria, the designer will be able to verify the adequate margins of the LBEs, as well as to identify an area where it would be beneficial to increase the safety margins. If so, the LBEs would have to be updated in order to take into account the corresponding modification of the design.

II.1.2. The Japanese criteria

The NGNP project defined their criteria based on criteria that establish limits on the risk or consequences of potential radiological releases from nuclear power plants in the United States. However, the Japanese, trying to show the inherent safety of MSRs, derived Light Water Reactor (LWR) performance-based DBA-criteria. If, during an event, these criteria are met, there is no release and the system is safe. If not, the fuel salts must be quickly drained to the drain tank. Their objective is to keep re-startup capability. One may note that, according to them, no DBA can cause a large radioactive release. This assumption is verified throughout this study.

The 4 objectives to keep re-startup capability for a LWR are:

- Limits for minimum Departure from Nucleate Boiling Ratio or Minimum Critical Power Ratio
- Fuel cladding shall not mechanically fail
- Maximum fuel enthalpy
- Maximum reactor system pressure

However, for an MSR, fuel is molten salts. Thus, there is no criterion for fuel failure. Moreover, the molten salts having a very high melting point and a low vapour pressure, the first, third and fourth criteria cannot be applied. The second criterion cannot be applied neither, since there is no cladding in an MSR. However, for long term operation, this limit applied to reactor vessel and piping seems reasonable [12]. Two criteria derive from this consideration.

The first one tries to determine the limiting fuel temperature to maintain tensile strength of the Hastelloy-N. Based on existing data, and even if there is no data above 704°C, it is extrapolated that 1000°C could be the maximum allowable temperature (see Figure 3).

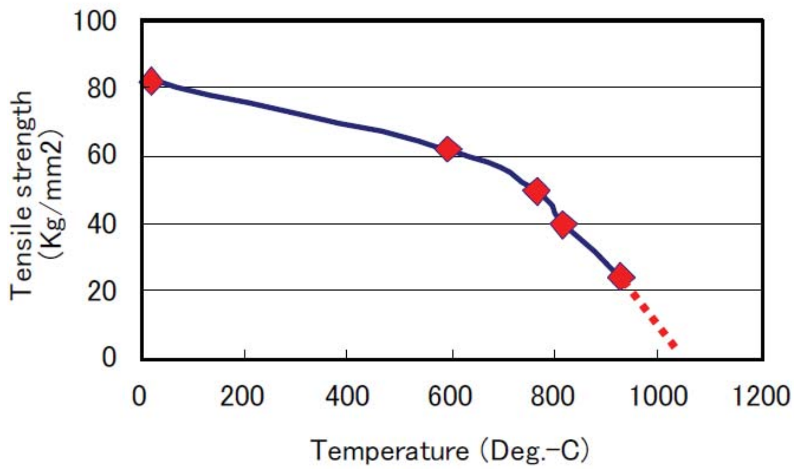


Figure 3: tensile strength against temperature for Hastelloy-N [12]

The second criterion derives from the consideration that the allowable fuel temperature should be less than the temperature which causes plastic strain of 1% during 1 hour under the design load. As can be understood, this criterion is design specific. For the FUJI reactor, a maximum inlet temperature of 1050K and a maximum outlet temperature of 1200K were determined using the Larson-Miller plot. Concerning the FUJI-233Um design, if the second criterion is met, then the first one is met too.

II.1.3. Comparison of the two criteria

At first glance, the two criteria seem totally different. One derives from criteria that establish limits on the risk or consequences of potential radiological releases from nuclear power plants in the United States. The other derives LWR performance based DBA criteria. The question is: which one is the most restrictive? And how are they related?

The answer to the first question is quite obvious. The Japanese criteria are more restrictive than the NGNP criteria. Indeed, if the former is met, then the re-startup capability of the MSR is preserved. It means that there is no external release. Thus the NGNP safety limits are met. It comes from the fact that the NGNP project sought criteria for the licensing of NGNP, whereas the Japanese sought to demonstrate the inherent safety of the FUJI reactor.

The NGNP criteria define authorised limits in terms of radioprotection; they can hereinafter be defined as "Primary Acceptance Criteria" (PAC). However, the use of these PAC implies one major problem for safety assessments. The compliance proof would require a computational chain up to radiological loads. This requires an immense program of inspections/monitoring/testing combined with validation of highly precise tools able to predict the evolution of these materials during operation. Similarly, highly advanced and reliable tools should be available to predict the response of the different materials during a dynamical event.

That is why surrogate criteria could be established, which if fulfilled, would with certitude imply that the PAC limits are met. Such surrogate criteria are often referred as Derived Acceptance Criteria (DAC). The Japanese criteria are DAC. Moreover, three categories of DAC are usually defined: the safety, operation and design criteria. Safety criteria refer to numerical limit imposed on the calculated physical variables and on the plant conditions during and after an event. Operational criteria refer to operational limits imposed on various physical parameters during normal operation as to ensure that in case of an event, the physical critical variables will not reach the DAC. These criteria bound the allowed conditions of the plant state before an event. Design criteria are imposed by vendors for the design of the different reactor elements regarding the intended performance requirements before, during and after an event. In the present case, the Japanese criteria are obviously design criteria, since it represents the limit beyond which failure of the barrier is assumed to occur.

Since the PAC imposed by the NGNP project are uneasy to verify, the second Japanese criterion will be used throughout this study. If the latter is verified, the TLRC are met with certainty.

II.2. Design validation for new generation nuclear power plant

LBEs were previously defined. In order to quantify the probability of such scenarios, a risk-informed approach using both deterministic and probabilistic methods is appropriate. In such a study, "deterministic" refers to a method evaluating fixed scenarios based on physical principles. Uncertainties are taken into account by imposing bounding criteria often following regulations. "Probabilistic" refers to an evaluation of the likelihood of a particular scenario [1]. This risk-informed approach is developed from the Probabilistic Safety Assessment (PSA), and is essential to develop a design optimized according to safety objectives. The PSA method consisting in the identification of initiating events among a full set of plant operating state and the identification of different event sequences allows an exhaustive search for Licensing Basis Events (LBEs).

Moreover, the LBEs identification and classification is useful for the safety classification of SSCs. In other words, it allows the establishment of the necessary capability and reliability of the different SSCs in order to meet the requirements of the Top Level Regulatory criteria (TLRC).

II.2.1. Overall concept

In the INL white paper "*Next Generation Nuclear Plant Licensing Basis Event Selection"*, September 16, 2010 [1], the staff defined a process for licensing basis event selection considering a combination of deterministic and probabilistic analyses. The method consists in establishing a preliminary list of initiating events and then calculating the frequency and the consequences of each of the event sequences developed from IEs.

The NGNP methodology is an iterative process. First a deterministic engineering judgement allows the determination of an initial IE list. This first list leads to a certain design that can withstand them.

Then a PSA based on the design allows a quantification of the frequencies of the different scenarios, leading to a possible classification of them. Source terms are then calculated, allowing a quantification of the consequences of the different scenarios. After that, a new cycle is done until the final design is set and the development is complete. As can be understood, the PSA is used to establish and refine the LBEs, demonstrating that the design places the LBEs in the acceptable part of the frequency-consequence curve. The flowchart representing this process is shown on Figure 4.

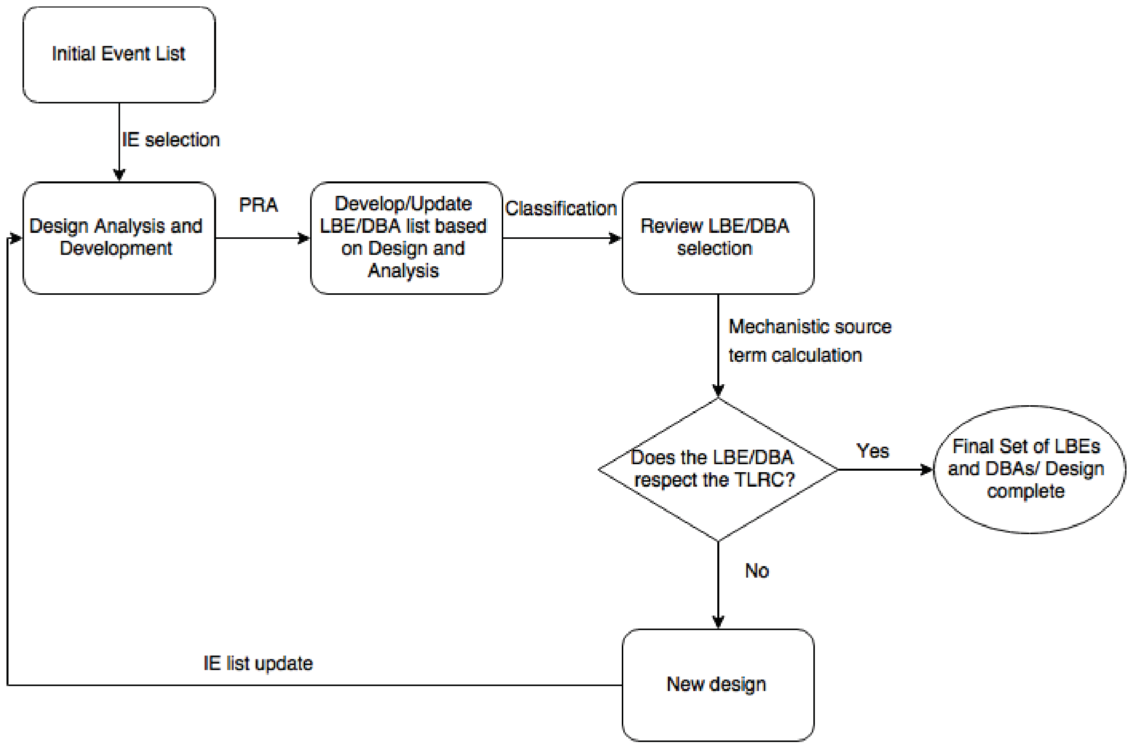


Figure 4: Flow chart for the LBE selection process
Figure updated from [1]

As can be seen on Figure 4, design safety analysis means design validation. That is why both terms will be used in this report.

In the end, frequencies of occurrence of event sequences have to be calculated, as well as their consequences. Consequences are evaluated according to mechanistic source terms and transport calculations. Frequencies are evaluated using PSA. Initiating events are identified using the Master Logic Diagram.

II.2.2. Initiating event identification

IEs are identified thanks to the Master Logic Diagram (MLD) methodology. This process consists in a hierarchical depiction of ways in which perturbations can occur. At first, the diagram begins with a top event representing an end state. Then, the lower levels show possible subsystem and component failures. The diagram ends when levels below the stopping level have the same consequences as the latter. The beginning of a general nuclear power plant MLD is given as an example:

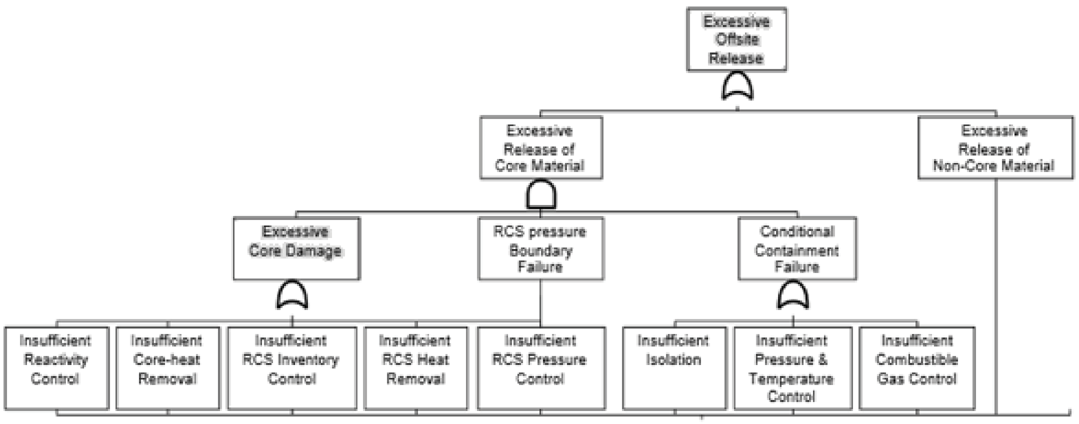


Figure 5: General nuclear power plant MLD [13]

Once IEs are identified, a grouping and a screening of the latter are performed. The grouped IEs are then used for scenario development. The quantification of IE frequencies is based on models or from experience. The figure below explains the further treatment of IEs:

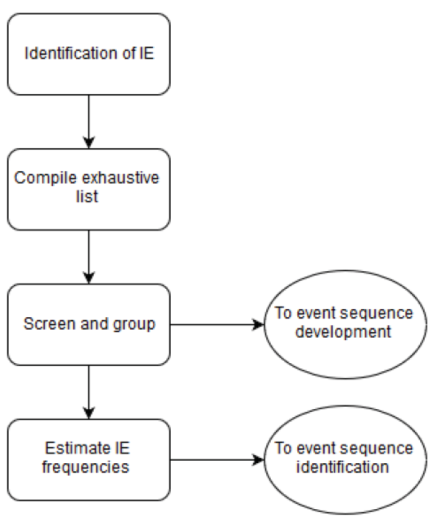


Figure 6: Grouping and screening process of the identified IEs
Figure updated from [1]

One may note that the use of old MLD, like LWR MLD for example, is possible and recommended. In the present case, a previous study of YOSHIOKA and MITACHI will be used [14], as well as a report from a workshop on FHR licensing [5]. Once an exhaustive list of IEs is established, LBEs are identified by studying the response of the SSCs according to the corresponding IE. A PSA is then used to evaluate the probability of occurrences of LBEs. Having identified the LBEs together with their frequencies allows us to classify them and to define Design Basis Accidents (DBAs).

II.2.3. Identification of SR-SSCs and DBAs

A DBA is defined as "postulated accident that a nuclear facility must be designed and built to withstand without loss of the systems, structures, and components necessary to assure public health and safety" (NRC).

However, as already explained, DBAs are currently defined only for LWR. Therefore, a methodology has to be developed in order to identify them for NGNP. In the Idaho National Laboratory (INL) white paper "*Next Generation Nuclear Plant Licensing Basis Event Selection*", September 16, 2010 [1], DBAs are identified as DBEs where only the safety-related Systems, Structures and Components (SR-SSCs) are considered available. But before anything, how to define safety-related SSCs? What is the classification of the different SSCs?

SSCs are classified based on criteria derived from the prevention and mitigation of LBEs [15]. SSCs are categorized in three classes [16] according to the following figure:

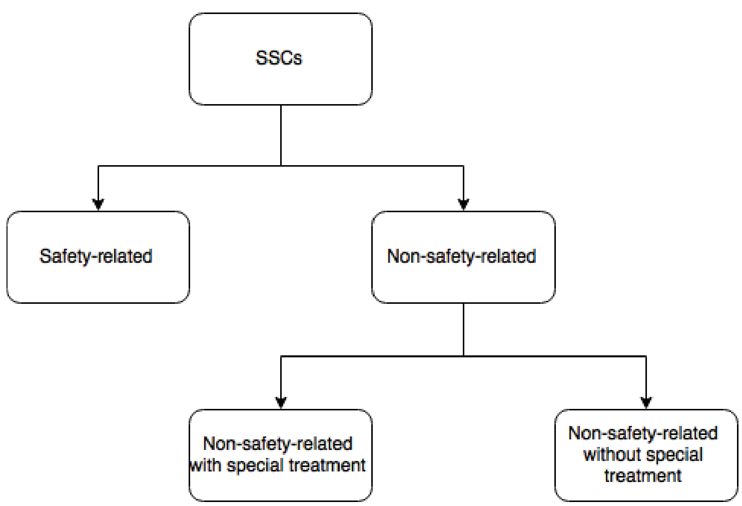


Figure 7: Classification of SSCs

In this study, the focus is set on safety-related SSCs, since their definition is part of the definition of DBAs. Safety-related SSCs includes:

- SSCs performing safety functions to prevent or mitigate the consequences of DBEs, in order to meet the TLRC criteria

- SSCs performing safety functions to prevent the frequency of BDBEs with consequences above the 10 CFR 50.34 dose limits from going into the DBE region

The first step for safety-related SCCs classification is to determine the required safety functions for DBEs, where 'required' refers to functions that have to be successful during DBEs to meet the TLRC. The next step for each necessary safety function is to review the DBEs to identify which SSCs are available and have sufficient capability and reliability to meet the safety function. This set of SSCs determined is classified as safety-related for a required safety function.
Moreover, BDBE are re-analysed with all the SSCs considered deterministically. Since BDBE may have consequences above the DBE limit, guarantee should be provided that the frequency does not increase above the DBE limit. Any BDBE with consequences above the DBE limits are revised to determine which safety function is needed to prevent a frequency increase into the DBE region.

These two considerations are illustrated below:

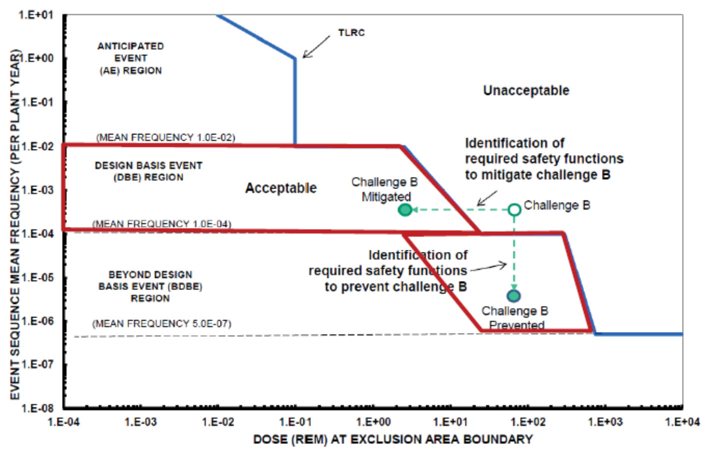


Figure 8: Classification of SSCs as safety related. Figure updated from [1].
The area inside the red blocks represents the events being considered in order to define SR-SSCs

A special treatment is applied for Safety-Related SSCs. It consists in both reliability requirements resulting from accident prevention considerations and capability requirements resulting from accident mitigation considerations. More information can be found in reference [16].

Moreover, special treatment not only ensures the reliability and the capability of each safety-related SSC, but it increases the confidence that the safety-related SSC will perform its safety function despite its uncertainty. The purpose of the special treatment is to increase the certainty that the SSC will perform its safety function under expected scenarios, together with its uncertainties. Hence, the special treatment is an important part of defence-in-depth [17].

II.3. Implementation steps of the NGNP methodology as basis for a design safety analysis

All in all, the design validation according to the NGNP methodology is a nine step process:

1. The approach begins with a deterministically selected list of Initiating Events. The Master Logic Diagram Method has to be followed in order to establish an exhaustive list. Incorporation of results from other studies is recommended.

2. Event sequence families are identified based on the list of IEs. It corresponds to IE grouping.

3. PSA is then used to define the relevant event sequence families, called LBEs, and their associated probabilities.

4. A classification of the licensing basis events is done according to the standards defined by the INL in his paper "*Next Generation Nuclear Plant Licensing Basis Event Selection*", September 16, 2010.

   Three classes are defined by three different probabilities of occurrences per plant per year:

   - AOO < 10^{-2} per plant-year
   - 10^{-2} per plant year < DBE < 10^{-4} per plant-year
   - 10^{-4} per plant-year < BDBE < 5.10^{-7} per plant-year

   Below a probability of 5.10^{-7} per plant-year, scenarios are judged too unlikely and not considered in the licensing process.

5. Safety-related SSCs are identified by analysing every DBEs and BDBEs exceeding the DBE TLRC limit. Analyses consist in determining which SSCs are available and have sufficient capability and reliability to meet a specific safety function.

6. DBAs are identified from the DBEs, considering only the safety-related SSCs as available.

7. A Mechanistic source term has to be calculated using transport codes, thermodynamic codes and structural mechanics codes. This source term allows the estimation of the consequences of the different event sequences.

8. The different LBEs, together with their uncertainties, are displayed on the frequency-consequence curve. They (mean and upper bound) have to meet the TLRC according to the first classification:

   - AOO < 100 mrem total effective dose equivalent realistically calculated at the EAB

- DBE < 25 rem total effective dose equivalent realistically calculated at the EAB
- BDBE < NRC Safety Goal Quantitative Health Objectives calculated at 1.6 km and at 16 km from the plant

9. If the criteria are verified, the specific design is validated. If not, a new design has to be developed and the LBEs/DBAs list has to be updated.

The nine-step process is summarized in the following flowchart. Attention should be paid about the identification of DBAs, since a previous identification of safety-related SSCs is needed. The starting point is represented by a black dot. As can be seen, the LBE selection method is an iterative process until the design is validated.

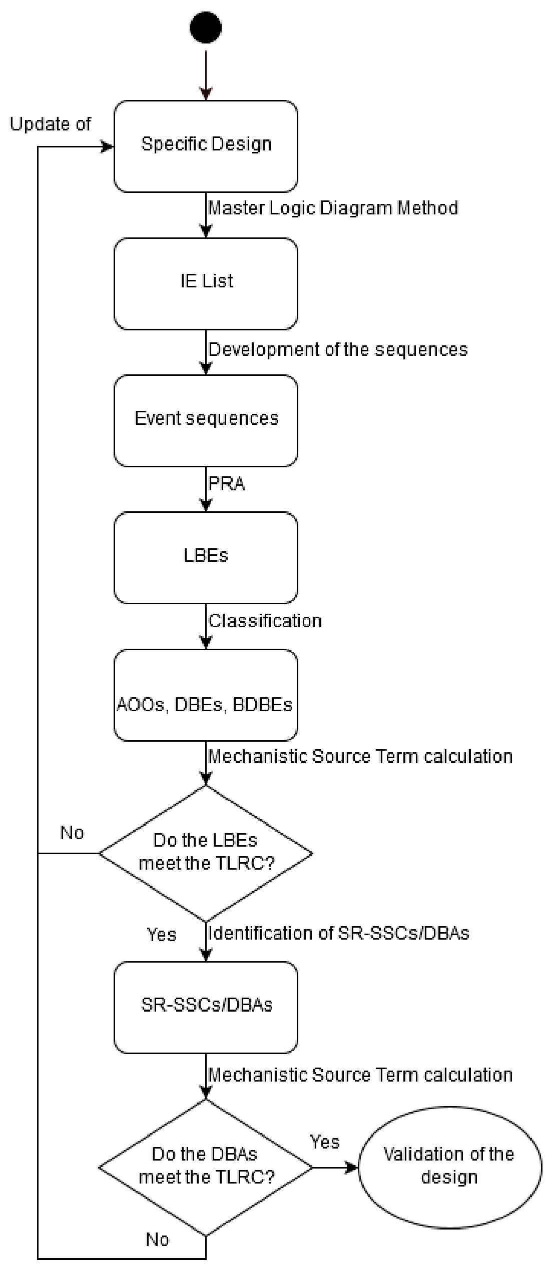


Figure 9: Summary of the nine-step process for the validation of the design

The NRC validated this procedure proposed by the Idaho National Laboratory for an HTGR. In this report, the NGNP methodology is used as basis for the FUJI-233Um design safety analysis. The FUJI-233Um reactor corresponds to a preliminary design; it means that the analysis concerns only the first cycle and the beginning of the second cycle of the NGNP methodology. The flowchart representing the major steps of the study is given in Figure 10. The different chapters treating the different steps are indicated as well.

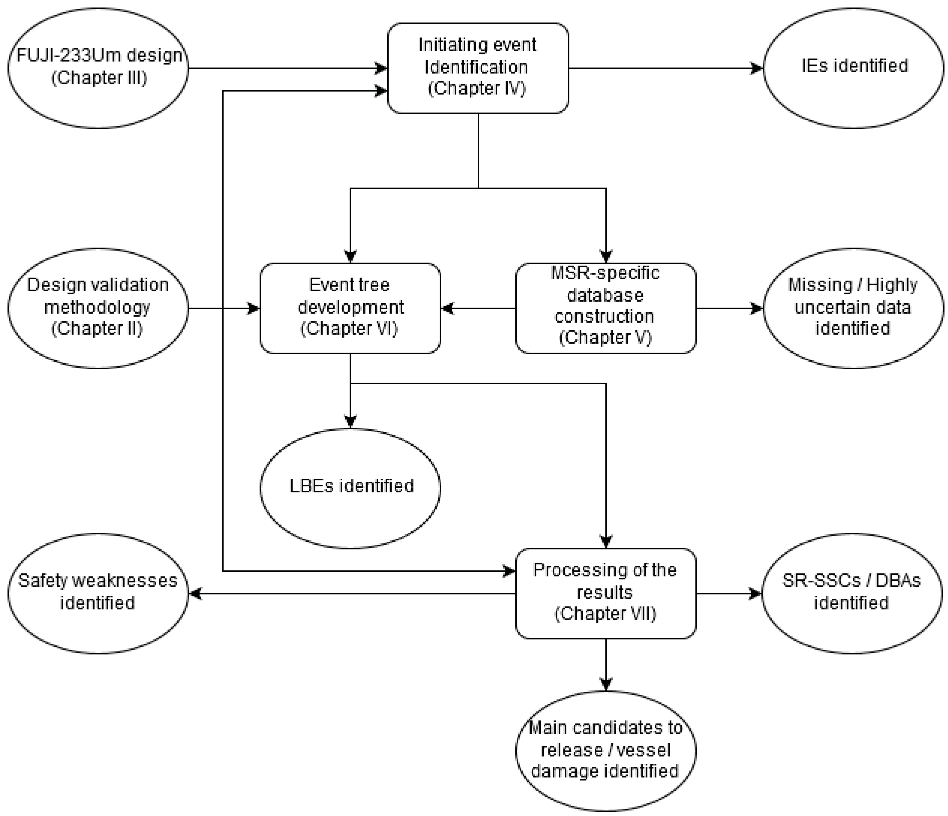


Figure 10: Flowchart of the study

The circles represent inputs or outputs. The squares represent processing of the inputs. The four main outputs of this study are:

- Identification of missing or highly uncertain data and suggestions to improve the database
- Identification of SR-SSCs and DBAs and comparison with the literature
- Identification of main scenarios with radioactive release/ vessel damage
- Identification of safety weaknesses and suggestions to improve the design

As can be seen, Chapter II and III deal with the inputs necessary for the study. Chapter IV, V and VI correspond to the implementation of the PSA model. Chapter VII presents the different results obtained thanks to the study.

The description of the methodology followed throughout this study has been developed in Chapter II. Thus, the next part deals with the second input of the study: the plant design and its main characteristics.

III. Plant design and key features

In this part is presented the second input of the study, i.e. the plant design and its main characteristics.

III.1. Reactor design and procedures

III.1.1. The reactor design

MSRs have been chosen as new generation reactors by the Generation IV International Forum (GIF). The main properties making MSRs attractive are:

- Inherent safety
- Excellent neutron economy
- Liquid fuel (no fabrication, online refuelling, gaseous fission product removal…)

The present study is based on the FUJI-233Um design for reasons explained in my semester project report [18]. The FUJI reactor operates in a closed thorium-uranium fuel cycle (Th^{232} as fertile material and U^{233} as fissile material). Its design is largely based on the 1000 MWe MSBR from ORNL, which was planned to be built in the 70's. The main differences are no continuous chemical processing and no periodic core graphite replacement compared to the MSBR.

The FUJI reactors are designed to generate electricity, as well as to produce hydrogen and/or desalinate seawater.

The scheme of the FUJI-233Um reactor core is given in Figure 11. The general scheme of the FUJI-233Um reactor is depicted on Figure 12. The general design of the FUJI-233Um power station is showed on Figure 13. The design of the reactor is very close to the MSBR from the ORNL. One may add that the first step of the THORIMS-NES program (complete fuel cycle concept, in which electricity is generated by MSRs and in which reprocessing, as well as breeding, is done remotely by Accelerator Molten Salt Breeders (AMSB)) is the construction and operation of a mini-FUJI reactor. This reactor should provide a first proof of the feasibility of such reactors, as well as education and training of project staffs. The geometry of the mini-FUJI is the same as the FUJI-233Um but at a different scale.

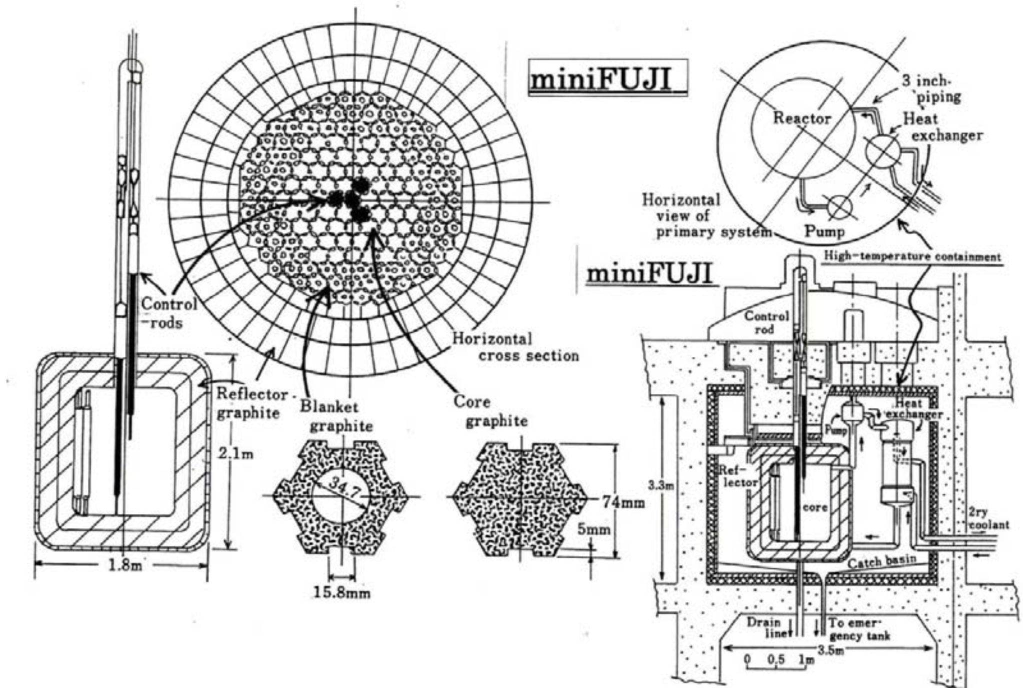


Figure 11: Core design of the FUJI-233Um
Figure from TTS website

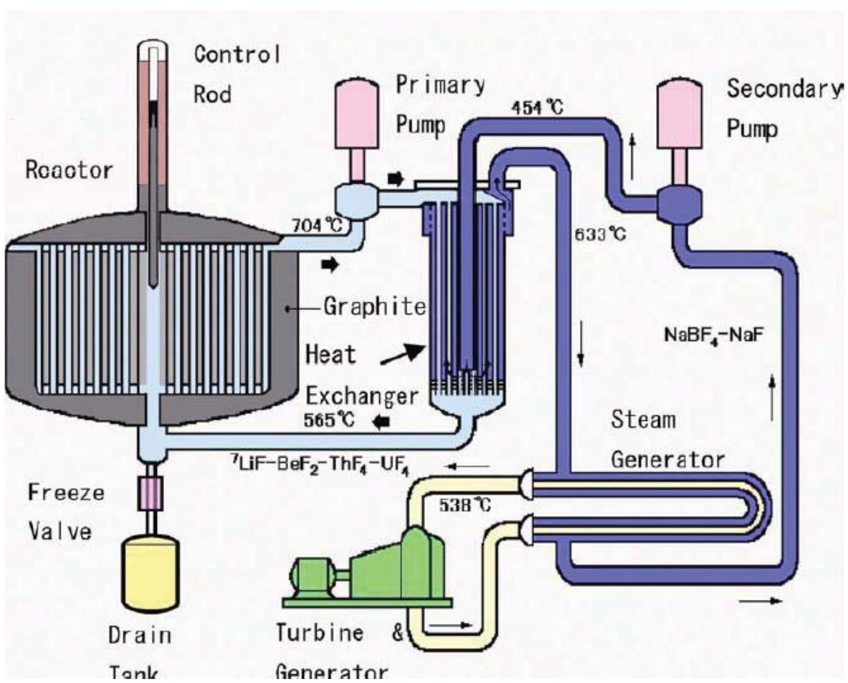


Figure 12: Reactor design of the FUJI-233Um
Figure from TTS website

As can be seen on Figure 12, the FUJI-233Um reactor consists in a single fluid pumped-loop design. The fuel salt is $LiFBeF_2$-ThF_4-UF_4 (flibe). The reactor is moderated via graphite installed into the core. A supercritical steam Rankine cycle is used to extract energy from the heat generated with an efficiency of 44.4%. The construction cost is estimated to be 1584 Million US$ for a 1 GWe plant.

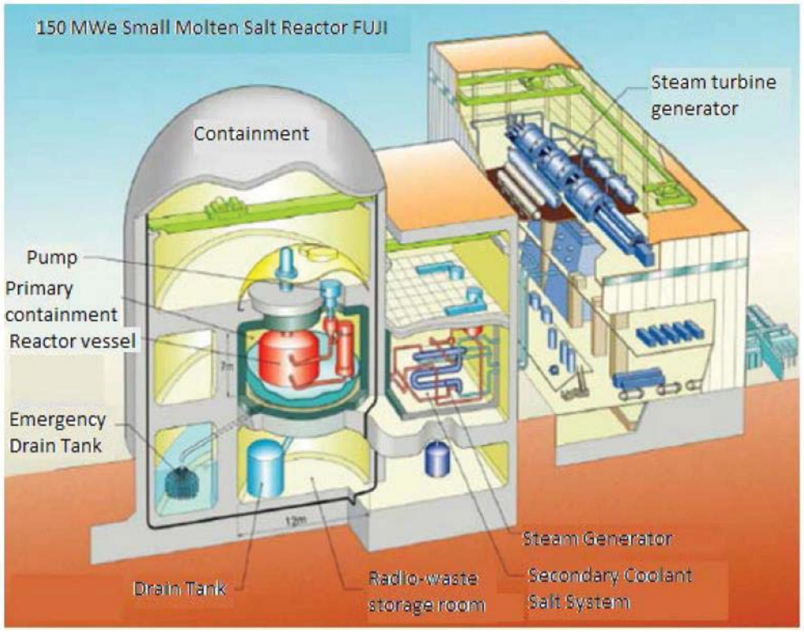


Figure 13: Plant design of the FUJI-233Um
Figure from TTS website

The design of the reactor is such that there are three SSCs for the shutdown of the reactor, and only one for the heat removal from the core. These are given below.

Table 1: SSCs for reactor shutdown [3]

Reactor Shutdown systems			
High speed shutdown system (SCRAM)	CRs	Active	Small number of rods sufficient
Second shutdown system	Fuel salt drain system	Passive	No return to criticality in a drain tank
Third shutdown system	Fuel salt density adjustment system	Active	Used also as Th make-up system

Table 2: SSCs for heat removal [3]

Heat removal systems			
ECCS - Cooling water make-up system	Unnecessary	-	Drain system could be used as back-up
Decay heat removal system	Decay heat removal system	Passive	If drain system used, decay heat removal system may become unnecessary

The drain tank, located below the reactor cell, will be used only in case of a:

- Leak in the primary circuit
- Loss of heat removal
- Loss of coolant or circulation in the secondary loop
- Loss of power or mechanical failure in the primary loop
- Inadvertent thawing of the freeze valve

The drain tank is the main safety component of a MSR. It has many purposes; the drain tank is used as decay container for the off-gas system, it also serves as container for volume accommodation in the primary circuit and it is an intermediate for the fertile and fissile fuel salt injection. But the main role of the drain tank is to keep the fuel salt at a reasonable temperature (passive drain tank cooling system) and to prevent a criticality accident (criticality impossible without graphite) when the freeze valve opens.

Moreover, the volume of the drain tank should be enough to accommodate the volume of the fuel salt as well as the volume of the cooling salt in case of a heat exchanger tube rupture (due to the pressure difference, the cooling salt will go into the primary circuit). All in all, the failure probability of the drain tank should be very small, in the order of magnitude of the failure probability of a Reactor Pressure Vessel in a LWR.

The secondary heat transfer loop was judged necessary for 6 reasons:

- Additional barrier for the containment of fission products in the fuel salts in case of an HXTR
- Barrier to tritium migration
- Reduces the possibility of freezing the fuel salt
- Less likely that the primary system will be subjected to high pressure in case of a SGTR
- Reduces the probability of oxygen ingress
- Additional degree of freedom to control the system by varying the secondary salt flow

Concerning the use of U-233 as fuel, one problem arising from it is the necessary remote handling of the fresh fuel. Indeed, direct handling of U-233 is impossible due to the small quantity of U-232 always mixed with U-233, U-232 being a strong gamma emitter. An example is given in "Nuclear Fuel Cycle Science and Engineering" [19]; the authors explain that a sphere of 10 kg of U-233 with a very low U-232 content of about 5 ppm (minimum that can be reached) would impose a dose rate of 0.11mSv/h at 1m after 1 month, and 1.1 mSv/h at 1m after one year (build-up of fission products).

In order to identify possible accidents during transients, the startup, shutdown, and flow reduction procedures have to be studied. The development of these procedures will also help us to build the event trees.

III.1.2. Startup, standby and shutdown procedures

These procedures correspond to procedures written for the MSBR by ORNL [20]. Since the FUJI-233Um design is largely based on the MSBR, it is estimated that the considerations developed from them are still valid for the Japanese reactor.
The procedure for the startup of the MSBR is as follow:

- Primary and secondary cell electric heaters are started
- Primary and secondary circulation pumps are turned on to circulate helium in the salt systems
- When the secondary system reaches 454°C, the loop is filled with coolant salt from the heated drain tank (salt circulation starts since the pumps are working)

- When the primary system reaches 538°C, the loop is filled from the fuel salt drain tank (and obviously salt circulation starts)
- The reactor is made critical at zero power; it means removal of safety rods and insertion of graphite control rods
- When the wanted power is reached, an automatic neutron flux level controller is used
- At the same time, the steam system is warmed and brought to operating conditions by using an oil or gas-fired auxiliary boiler (3600 psia and 538°C).

The procedure for a normal shutdown is as follow:

- Power reduced until 8% by gradually decreasing the flow to the main turbine to zero and relocating the generated steam to the hot standby system

If the hot standby condition is aimed:

- Steam from the SGs is used to drive the boiler feed pump turbine and to continue the circulation
- The auxiliary boiler feedwater system is turned on

If no hot standby condition is aimed:

- Feedwater is still provided to one or two SGs
- After ten days of heat removal, the fuel salt is sent to the drain tank
- Cell electric heaters (electric space heaters = resistance heating) in the secondary coolant salt cell are used to keep the secondary salt warm

The procedure following a flow reduction depends on where the flow reduction happens:

- If a primary salt flow reduction happens, the secondary salt and cooling circuit have to be stopped, in order to prevent the salt from freezing (at SGs and/or HXs) (load reduction by reducing the water cooling flow is not acting quickly enough).
- If a secondary salt flow reduction happens, the water cooling circuit has to be stopped, in order to prevent freezing of the secondary fuel salt at the SG, but the primary salt flow need not to be stopped
- If a flow reduction in the cooling circuit happens, an auxiliary feedwater system may be implemented and used. Otherwise, no specific procedure has to be followed concerning possible freezing

Now that the reactor design is well understood, the off-gas system has to be studied as well. This system is specific to MSRs and is often recognized as the major threat for radioactive release. This affirmation will be infirmed or not thanks to this study.

III.2. Off-gas system

III.2.1. The off-gas system design

At first glance, MSRs seem to be inherently safe, essentially because the source term is reduced by continuous removal of the fission gases (FGs). However, by creating an inherently safe reactor, it is often stated that the safety problem has been shifted to the fission product treatment systems, which are the off-gas system and the processing system. Since the reprocessing is done by Accelerator Molten Salt Breeders (AMSBs), one has to justify this affirmation by studying the off-gas system.

There is no documentation available for the off-gas system of the FUJI-reactor, and since the design of the FUJI-reactor is largely based on the MSBR design, the off-gas system of the MSBR is considered, supposing that the FUJI-233Um off-gas system design would be similar. The flow diagram of the MSBR, incorporating the off-gas system, is presented below:

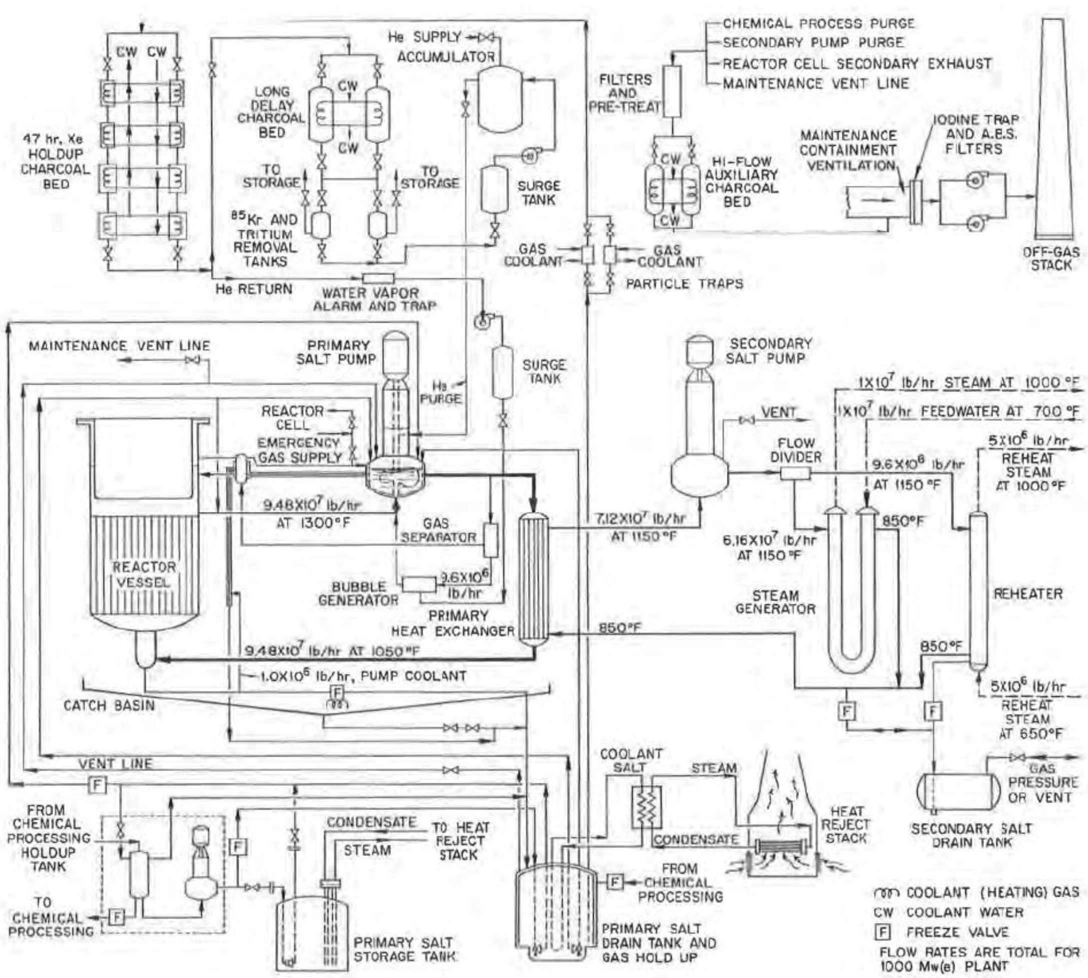


Figure 14: MSBR off-gas system [20]

This heavy diagram can be simplified into a simpler but not simplified scheme:

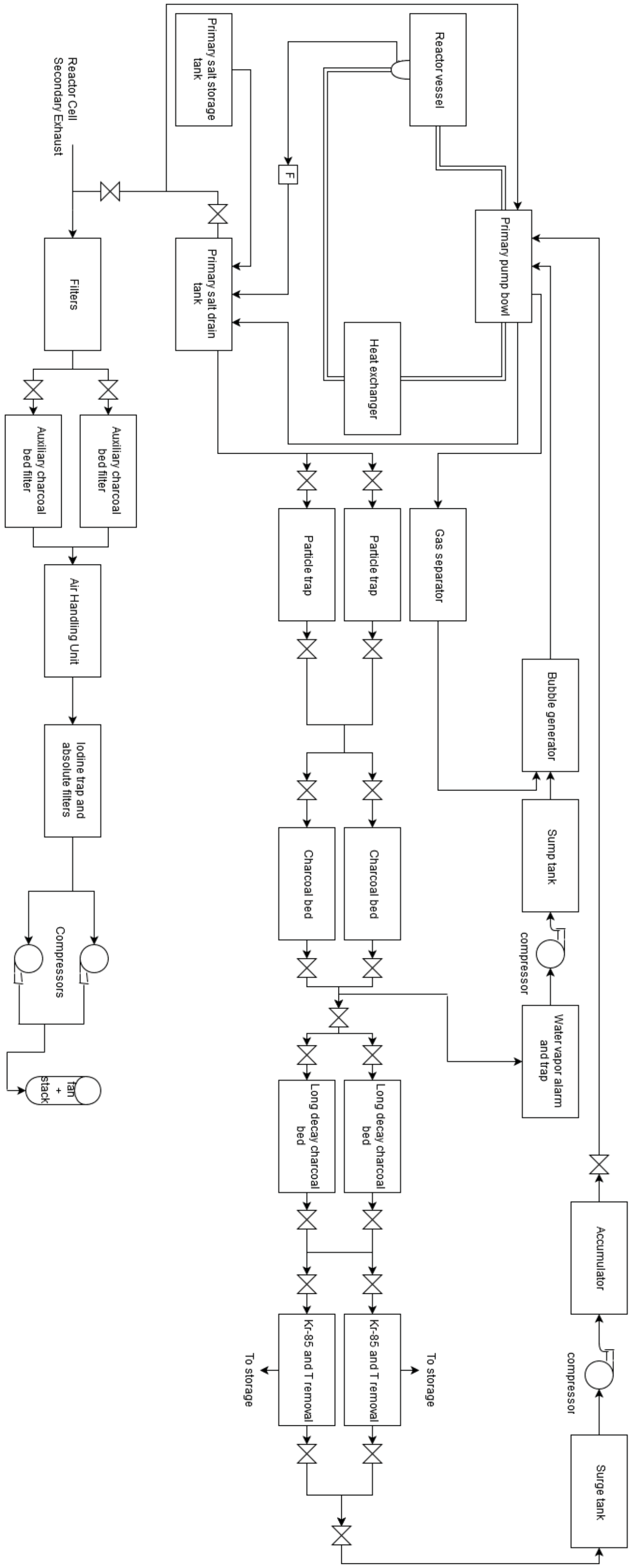


Figure 15: Flowchart of the MSBR off-gas system

As can be seen on Figure 15, fission gases go first to the drain tank, which has the function of decay tank. An average of two hours is spent by fission gases in the tank. Then the FGs go to the first delay beds. They are charcoal beds. They retain Xenon for 47 hours, so that 97% of the Xenon decays in this filter. Then most of the gases leaving the charcoal beds are compressed for reintroduction into the salt-circulation system at the bubble generator. The other part enters the long decay charcoal beds, retaining Xenon for about 90 days. Then everything goes to the Krypton and Tritium traps before entering a gas storage tank. The cleaned gas from this tank is reintroduced into the circulation system as purge gas for the circulation pumps. The accumulated Krypton and Tritium, together with the stable noble gases, are stored in tanks in the waste cell facility. The latter is located below the reactor cell.

The fission gases removed from the off-gas system are compressed and stored temporarily until they have decayed to ground levels. This is a well-known technology for non-radioactive gases. In the MSBR case, according to their decay constants, Krypton-85 and Tritium should be kept for 100 years before being released to the atmosphere. Such engineered storage is easily feasible [20].

As can be seen on Figure 14, the off-gas system uses particular filters: charcoal beds. This system needs a further study.

III.2.2. Charcoal bed

Charcoal beds are described briefly in this section. The function of a charcoal bed is to retard the fission gases, so that the heat load and the radiation level are reduced. The MSBR project sought to use as much charcoal beds as possible since its construction and operation are very simple compared to the rest of the off-gas system. The retardation is based on a dynamic adsorption of the fission gases. "Dynamic" means that the adsorption is reversible. Dynamic adsorption could be represented as a probabilistic process where FGs jump from one adsorption site to another. The adsorbent is activated charcoal. The heat load is transferred to boiling water, as can be seen on Figure 16. One may note that the efficiency decreases with time due to the accumulation of solid Fission Products (FPs). During the operation of the MSRE, the holdup time at 100 cm^3/min helium flow was estimated. The holdup time for Xenon was 30 days compared to 2.5 days for Krypton. That is why, by analogy, the holdup time for Xenon is supposedly 12 times higher in every charcoal beds.

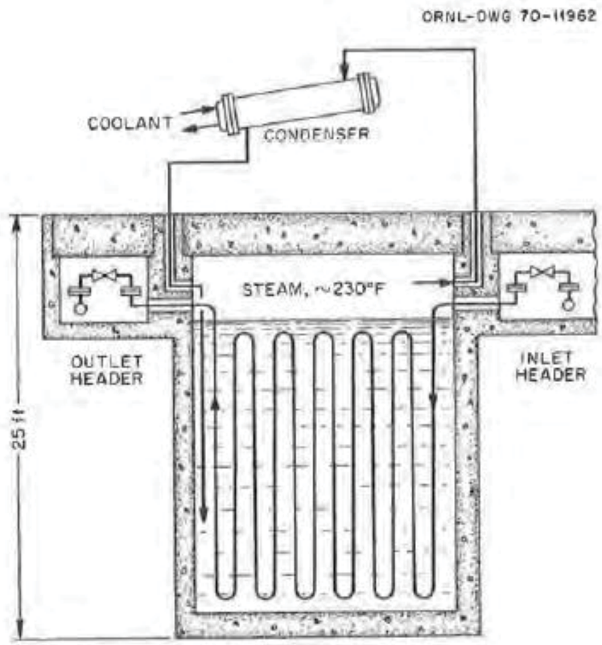


Figure 16: Charcoal bed used in the off-gas system of the MSBR [20]

The self-sustaining burning of the charcoal bed needs fuel, oxygen, heat and a chemical reaction. The oxygen supply could come from a pipe leak. That is why the failure mode "filter leakage" is considered in the PSA model.

III.2.3. Waste storage cell and containers

The fission gases removed from the off-gas system are compressed and stored temporarily until they have decayed to ground levels. This is a well-known technology for non-radioactive gases. According to its decay constant, Krypton-85 and Tritium should be kept for 100 years before being released to the atmosphere. According to [20], such engineered storage is easily feasible.

In the upper level of the reactor building, a cell is provided for storage and dismantling of radioactive materials. After a certain decay time, the equipment is cut as required and moved out to the waste storage below the reactor cell. Due to decay heat, double walls and an inert gas cooling system are used to cool the equipment. A work area is provided adjacent to the upper and waste cells, in order to handle remotely the radioactive materials.

The waste storage cell is designed to permanently store waste from the plant over its full lifetime. Due to the decay heat, a closed-circuit inert gas cooling system, similar to the one for the upper cell cooling, is used.

A general scheme of the different MSBR cells is given below:

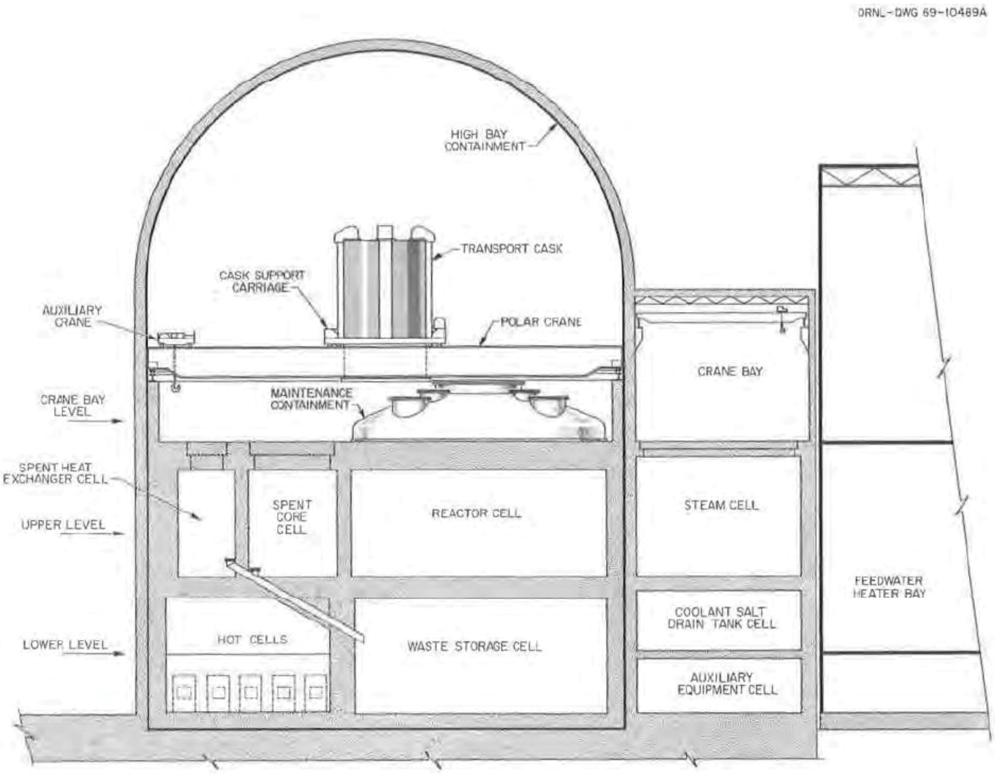


Figure 17: Sectional view of the reactor building [20]

Below the core, the catch pan of the emergency drain tank is made of stainless steel. Stainless steel has a melting point of 1363˚C and is corrosion resistant to molten fluoride salt [21].There are two valves in series from the containment to the drain tank: the upper one is a passively actuated valve by thermal switch, the other one is an actively actuated valve, normally held open. This system allows a quicker cleanup of a salt spill. The latter can be used to isolate the emergency drain tank from the containment during maintenance or failure of the first valve.

It is important to notice that two systems are still not designed: robots for salts handling and the High Temperature Containment (HTC) [22]. The first ones are not a problem for the PSA construction, but the second one may be. A MATLAB script simulating the heat transfer to the reactor vessel in case of a loss of heat supply to the HTC has been written. It showed that more than 29 hours are necessary for the vessel temperature to be at the fuel salt melting point. Therefore, this system is not relevant for the PSA construction since it has almost no consequence. For more details on this simulation, please refer to Appendix 6.

III.3. Key features

In this section is presented the main operating characteristics of the FUJI-233Um reactor, as well as its fission product inventory after 30 years of operation. At the end of the section, this FP inventory is compared to the one of a Boiling Water Reactor (BWR), in order to point out one of the advantages of the FUJI-233Um.

III.3.1. Main operating characteristics

The major design characteristics of the FUJI, as well as its neutronic, thermal-hydraulic and other operating parameters are given below:

Table 3: Design and operating characteristics of the FUJI-233Um [3]

Major design characteristics	
Installed capacity (thermal)	450 MW
Installed capacity (electric)	200 MW
Availability	90%
Type of fuel/coolant	LiF-BeF2-ThF4-UF4
Fuel enrichment	71.75 - 16 - 12 - 0.25 mol% with 2.0 wt% of fissile material in heavy metal
Type of moderator/reflector	Graphite
Type of structural material	Modified Hastelloy-N (Ni based with 11-13 wt% Mo, 6-8wt% Cr, 1-2wt% Nb, 0-1wt% Si)
Core Characteristic dimensions	
Core-I	radius of 2.2 m, graphite fraction of 64 vol%
Core-III	outer radius of 2.8 m, graphite fraction of 71 vol%
Core -IV	outer radius of 3.0 m, graphite fraction of 76 vol%
Core height	2.1 m
Power density in the core	7.3 kW/L
Vessel type	closed, tank type.
Vessel Characteristic dimensions	
Inner diameter	6.84 m
Height	2.94 m
Wall thickness	5.0 cm
Number of circuit	3, including an intermediate molten salt heat transport system
Neutron physical characteristics	
Temperature reactivity coefficient	-3*10-5 dK/K at BOC
Void reactivity coefficient	0.07 %dK/%void at BOC (boiling does not occur)

Burn-up reactivity swing	0.001 dK/30EPFD (Effective Full Power Days) applicable during the whole operation since continuous refuelling
Peaking factors	
Max axial peaking factor	1.3
Max lateral peaking factor	1.2
Reactivity control mechanism	
Control Rod (CR), type 1	Graphite regulating rods
Control Rod (CR), type 2	B4C based shutdown rods
Other mechanisms	Fuel salt drain system
Number of independent active reactor control and protection (RCP) systems	3
Cumulative worth of each RCP	
2 Graphite CR	0.12% dK
4 Emergency shutdown rods	3.6 % dK
Fuel salt drain system	well below critical
Thermal-hydraulic characteristics	
Cycle type	Supercritical steam Rankine Cycle (at turbine inlet: P=24 Mpa, T=810K)
Thermodynamic efficiency	44.40%
Circulation type	Forced
Core inlet coolant T	840 K
Core outlet coolant T	980 K
Core flow rate	0.711 m3/s
Fuel salt volume in the vessel	21.1 m3
Total fuel salt volume	26.4 m3
Pressure in the primary circuit	0.5 Mpa
T limit for fuel	1800 K (boiling T)
T limits for structurals	3000 K for graphite and 1400 K for Hastelloy
Maximum T of fuel	985 K
Average T of fuel	910 K
Max T in normal operation for structurals	1000 K for graphite and 980 K for Hastelloy
Average T in normal operation for structurals	920 K for graphite and 910 K for Hastelloy
Operating cycle parameters	
Average discharge burn-up	100 GWd/ton
Fuel lifetime	longer than plant lifetime
Period between refuelling in EPFD	
Fissile feeding	2 kg of U-233 into the core in the form of LiF-UF4 (73-27 mol%) every 30 EFPD
Fertile feeding	67 kg of Th into the core in the form of LiF-BeF2-ThF4-UF4 (72-16-12 mol%0 every 150 EFPD
Mass balances	
U-233 Inventory	800 kg
U-233 feed in 30 years (capacity factor 90%)	755 kg
U-233 + U-235 inventory after 30 years	1107 kg (with carrier salt), can be used in the next MSRs
Natural Th consumption in THORIM-NES	1000 kg/Gwe/EFPY
Design and operating characteristics of systems for non-electric applications	

Hydrogen production	120 tons H2/day at 450 MWth
Seawater desalination	28000 m3/day from multi-effect distillation at 450 MWth

These parameters will be used throughout the report.

III.3.2. Fission product inventory after 30 years of operation

As already explained, there is no onsite reprocessing in the FUJI-233Um reactor during its lifetime. The reprocessing is achieved by the Accelerator Molten Salt Breeders (AMSBs). The salt is processed in a batch mode to remove the ^{233}U and some fission products (^{233}U removed by fluorination) every 7.5 years [23]. Then, the decontaminated diluent salt will be used to produce make-up fuel for the FUJI-233Um reactor.

The estimated concentration of FPs after 30 years of operation (15 years of full power operation) is given below:

Table 4: Fission product inventory after 30 years of operation [3]

FP group		Production from 233-U [a/o] (atomic percentage)	Amount dissolved in the fuel salt [kg]	Amount separated to gas phase [kg]
Group I	Xe	27.6		312.0
	Kr	6.5		45.9
	T			0.1
Group II	I	2.6	27.6	
	Br	0.4	2.8	
	Te	4.1	43.5	
	Cs	17.8	56.0	144.0
	Rb	7.2	0.5	51.0
	Sr	11.8	28.1	60.5
	Ba	6.3	0.3	72.0
	Ce	14.1	166.0	
	Nd	16.4	199.0	
	Y	5.9	1.5-7.5	42.0-37.0
	Zr	30.0	232.0	2.0-10.0
Group III	Mo	21.6	175.9	2.0-10.0
	Se	0.9	6.1	
	Sn	0.3	3.0	

Table 4 represents the basis for source term calculations. Indeed, in order to be conservative, the source term is calculated at the worst case scenario, i.e. when the fission product concentration is the highest, i.e. after 30 years or operation.

Group I elements are removed during the operation of the MSR. Elements of the Group II are soluble in low quantities in the fuel salt. It is expected that their impact is negligible. Group III elements will float or be segregated at the pump bowl. Their total amount is not large, but their behaviours have to be confirmed by experiments. As can be seen, the total amount of FP created during the reactor operation is very low. In order to illustrate the last remark, a table comparing the U/Pu/MA production in a BWR and in the FUJI-U3 reactor [23] is given below.

Table 5: Comparison of U/Pu/MA production in a BWR and the FUJI-U3 reactor [23]

	FUJI-U3	BWR
Output power (GWe)	1	1
Reactor operation time (year)	30	25.9
Load factor	0.75	0.87
Initial inventory of U-fissile (t)	5.7	3.9
Net feed of U-fissile (t)	2.1	20.7
U-fissile total demand (t)	7.8	24.6
Final remaining U-fissile (t)	7.9	6.6
Net production in reactor life		
U-fissile (t)	0.1	-18
Pu-total (kg)	3.5	5080
Minor actinides (kg)	23	543

As can be seen, in the FUJI-U3 case, fissile uranium is created. Moreover, there are about 24 times less minor actinides produced in the FUJI-U3 case. It points out one of the main advantages of MSRs.

Now that the two inputs for the study are well described, the NGNP methodology can be applied to perform the design analysis of the FUJI-233Um. The first step is the IE identification thanks to the Master Logic Diagram (MLD) method.

IV. Safety analysis part 1: Initiating Events identification

The Initiating Events (IEs) identification has two purposes. The first one is the identification of possible challenges to the plant. The second one concerns the identification of scenarios by studying the response of SSCs to the IE.

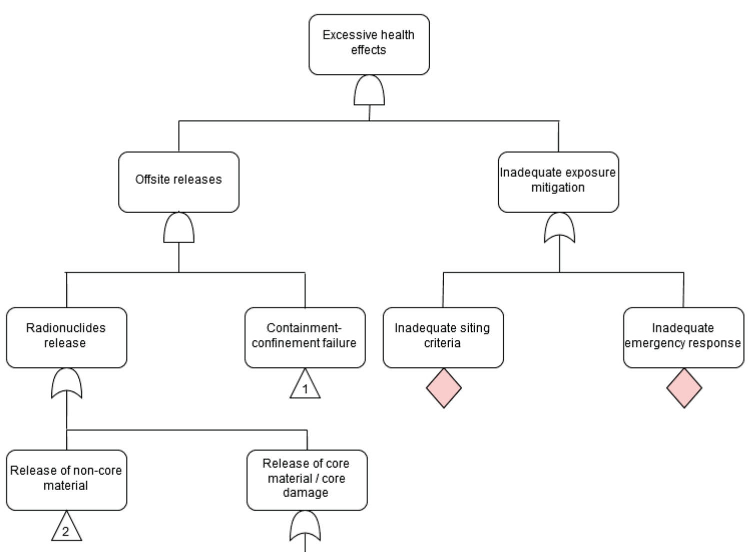
For New Generation Nuclear Plant, the IE list usually derives from comparable existing reactors PSA and based on generic references. In the present case, a previous study of Yoshioka and Mitachi [14], a report from a workshop on FHR [5], and LWR MLDs are used. This list has to be combined with specific analysis to consider exclusive characteristics of the new design.

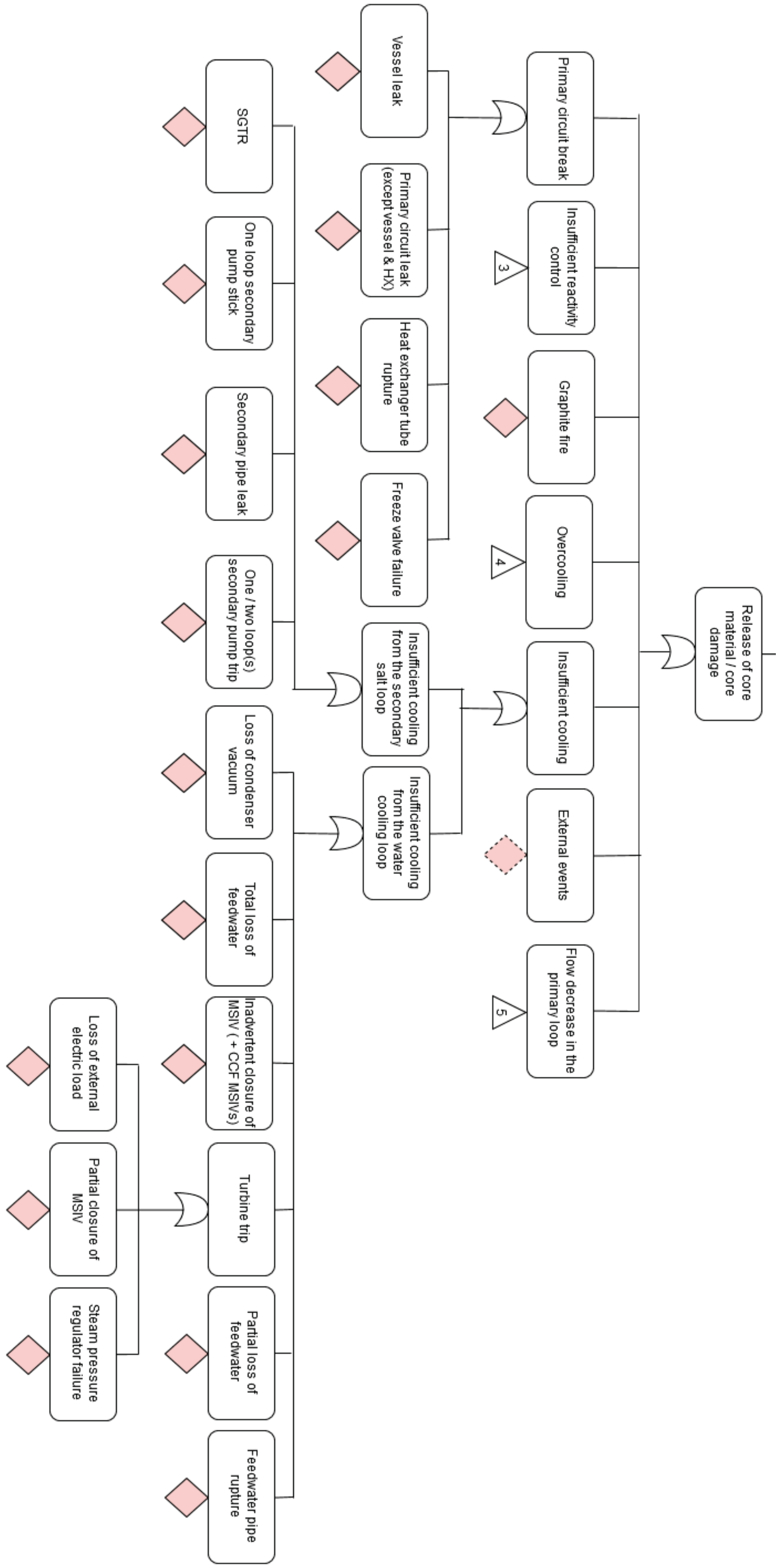
IV.1. Master Logic diagram method

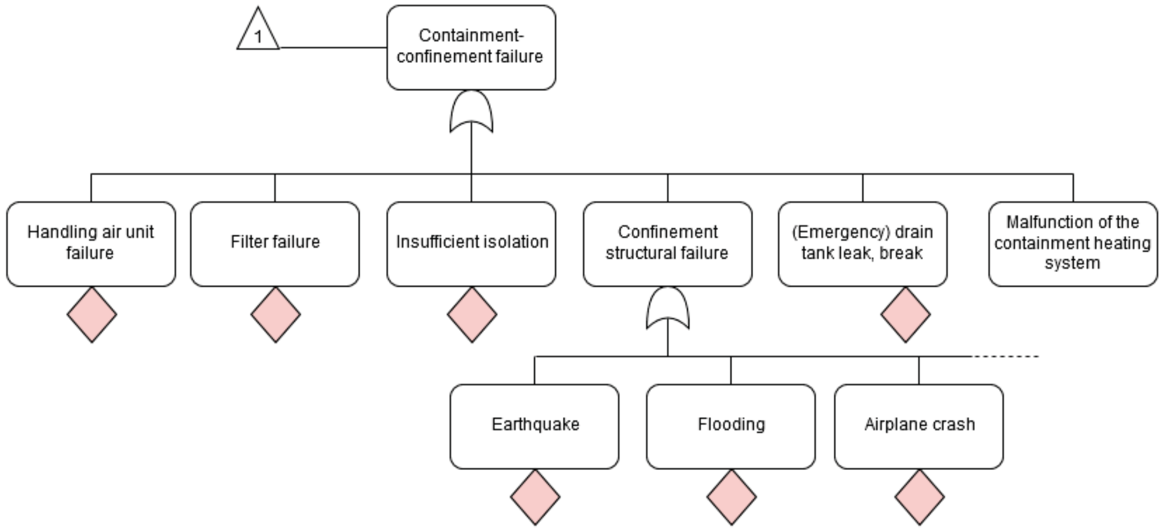
The MLD methodology is a well matured analysis. It has been used, for instance, in the Ringhals, Oskarshamn, Forsmark, Seabrook and Midland PSAs, in order to establish an exhaustive list of IEs. This process consists in a hierarchical depiction of ways in which perturbations can occur. At first, the diagram begins with a top event representing an end state. Then, the lower levels show possible subsystem and component failures. The diagram ends when levels below the stopping level have the same consequences as the latter.

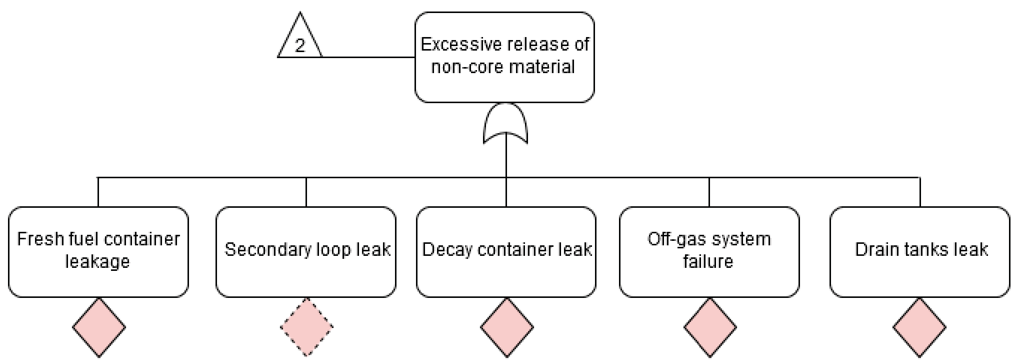
IV.1.1. Reactor MLD

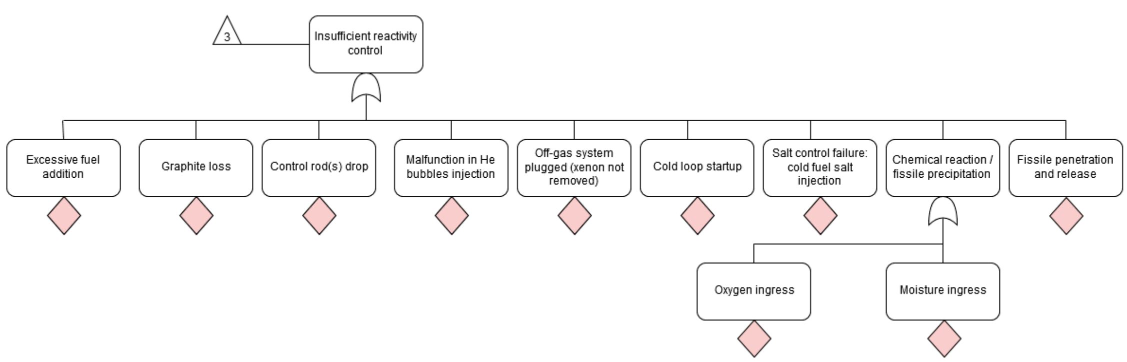
The IE list is found below the block "radionuclides release". The other blocks like "containment-confinement failure" and "inadequate exposure mitigation" are capability requirements derived from accident mitigation considerations. Top events (found in page 38) are generic blocks found in old LWR MLD for instance [24]. The reactor MLD is given below, together with its key:




Release of core material / core damage
Primary circuit break
Insufficient reactivity control
3
Graphite fire
Overcooling
4
Insufficient cooling
External events
Flow decrease in the primary loop
5
Vessel leak
Primary circuit leak (except vessel & HX)
Heat exchanger tube rupture
Freeze valve failure
Insufficient cooling from the secondary salt loop
Insufficient cooling from the water cooling loop
SGTR
One loop secondary pump stick
Secondary pipe leak
One / two loop(s) secondary pump trip
Loss of condenser vacuum
Total loss of feedwater
Inadvertent closure of MSIV (+ CCF MSIVs)
Turbine trip
Partial loss of feedwater
Feedwater pipe rupture
Loss of external electric load
Partial closure of MSIV
Steam pressure regulator failure


1
Containment-confinement failure
Handling air unit failure
Filter failure
Insufficient isolation
Confinement structural failure
(Emergency) drain tank leak, break
Malfunction of the containment heating system
Earthquake
Flooding
Airplane crash


2
Excessive release of non-core material
Fresh fuel container leakage
Secondary loop leak
Decay container leak
Off-gas system failure
Drain tanks leak


3
Insufficient reactivity control
Excessive fuel addition
Graphite loss
Control rod(s) drop
Malfunction in He bubbles injection
Off-gas system plugged (xenon not removed)
Cold loop startup
Salt control failure: cold fuel salt injection
Chemical reaction / fissile precipitation
Fissile penetration and release
Oxygen ingress
Moisture ingress

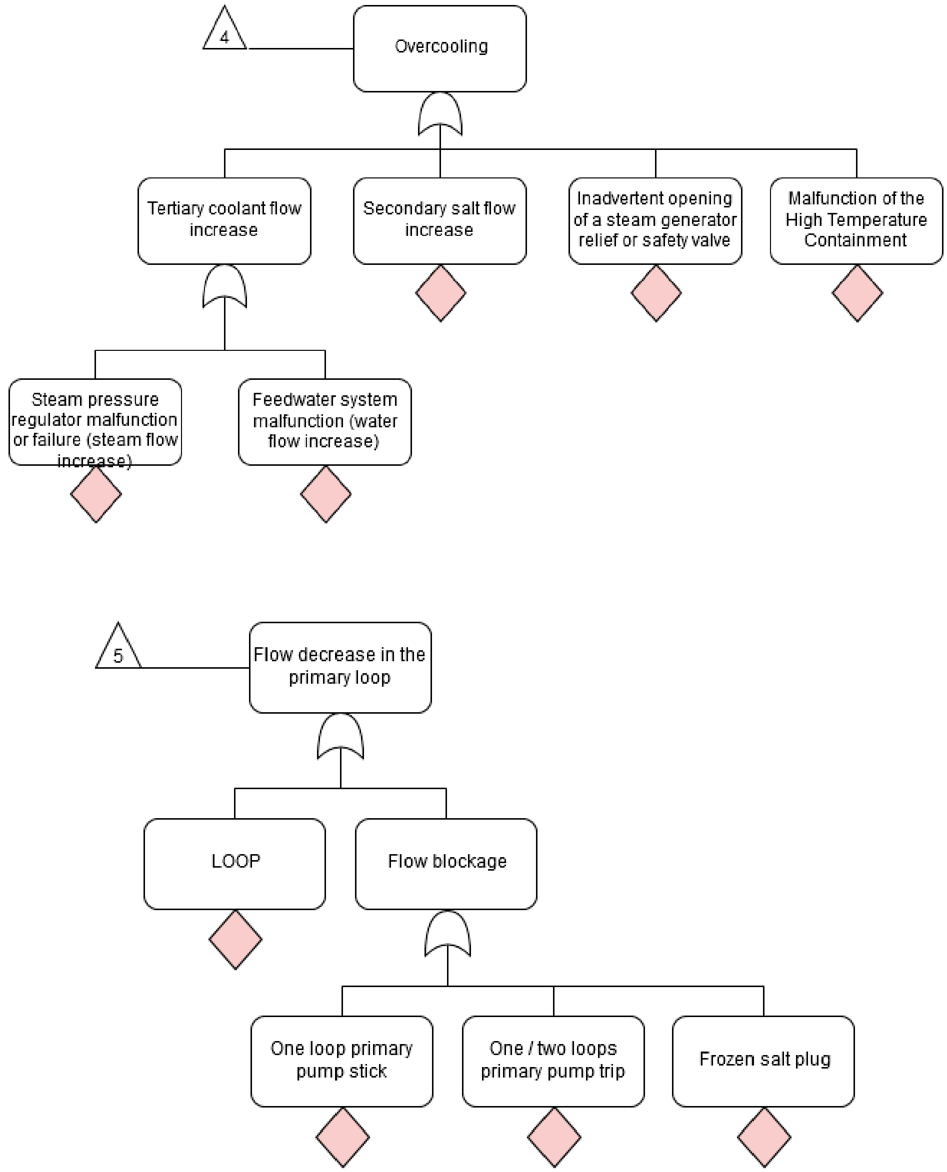
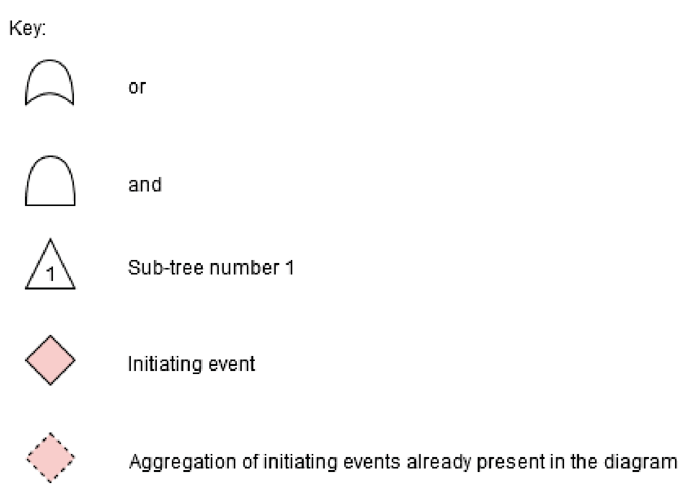


Figure 18: Reactor MLD



Remark: In the MLD developed, core cooling is arbitrarily chosen to begin at the secondary side of the heat exchanger. Thus, it means that a loss of primary salt flow is not considered as an insufficient core cooling. This choice was made in order to be consistent with the list developed in the next section. It does not change the PSA model.

A Loss Of Offsite Power (LOOP) will cause a loss of flow in the primary, secondary and water cooling loop. It means that a loss of flow will be conjugated with a loss of heat sink. Thus this basic event can be put at different places in the diagram. In order to alleviate the diagram, it is placed only under the loss of primary salt flow block.

The reactor MLD is complete and leads to a first list of initiating events. This list is presented in part IV.2., when IE grouping is performed. However, the initiating event "off-gas system leakage" needs a special treatment explained in the next section.

IV.1.2. The off-gas system specific case: NGNP methodology limitations

According to the NGNP methodology, scenarios with a frequency below $5 * 10^{-7}$/r.y. are screened out and scenario specific safety targets are set [1]. The last two remarks are problematic. Indeed, it means that if a system is decomposed into very small subsystems, the probabilities of these scenarios could be screened out even if the total system failure probability is relevant. For example, if there are 100 totally independent valves in series with a leakage probability of 10^{-7}, the total leakage probability would be 10^{-5}. However, if 100 branches for the failure of one valve are drawn on the event tree, there would be 100 scenarios with a failure probability of 10^{-7}. Supposing an initiating event frequency of 1/r.y., every scenario in the second case would be screened out, even if the first case shows that they should not.

The problem was discovered when studying the off-gas system. Indeed, a small decomposition was necessary because a leak after or before a specific filter would change the dose at EAB. The minimal cut-sets resulting from this decomposition resulted in every scenario frequency lower than the consideration limit of $5 * 10^{-7}$/r.y.

This issue has already been highlighted by the ACRS, in their paper *"Development of a Technology - Neutral Regulatory Framework"*, September 26, 2007 [6]. They pointed out that the use of a Complementary Cumulative Distribution Function (CCDF) F-C curve aggregating the contribution to risk of the different sequences would impose better limits on risk compared to the sequence-specific F-C curve. An alternative candidate CCDF F-C curve is discussed in EPRI TR-1013582, "Technical Elements of a Risk-Informed, Technology-Neutral Design and Licensing Framework for New Nuclear Plants" [25].

The first conclusion is that the NGNP methodology is not adequate for the off-gas system of a MSR. This remark will be further developed in the last section of this report. The second conclusion is that a conservative NGNP methodology could be used for the study of the off-gas system. This modified methodology would consist of calculating the total leakage frequency of the off-gas system independently of the size of the break and its position. Then, the auxiliary off-gas system reliability would be calculated and multiplied with the leakage frequency. It would give an upper bound for the frequency of having an off-gas leakage possibly exceeding the TLRC. The methodology is developed in the next section.

IV.1.3. Another approach for the off-gas system

The aim of this methodology is to prove that a release beyond the TLRC due to an off-gas leakage is unlikely to happen; it means that it is at maximum a BDBE. For this purpose, a leakage probability of the off-gas system is calculated. This probability aggregates every leakage probability, being large or small leakages, in order to be conservative. Then the reliability of the auxiliary off-gas system is calculated. The multiplication of the two values gives an upper limit for a release frequency possibly exceeding the TLRC. The calculation is developed in this section.

IV.1.3.i. Off-gas system study

The fault trees for the total leakage frequency of the off-gas system and the total leakage probability of the auxiliary off-gas system are given below:

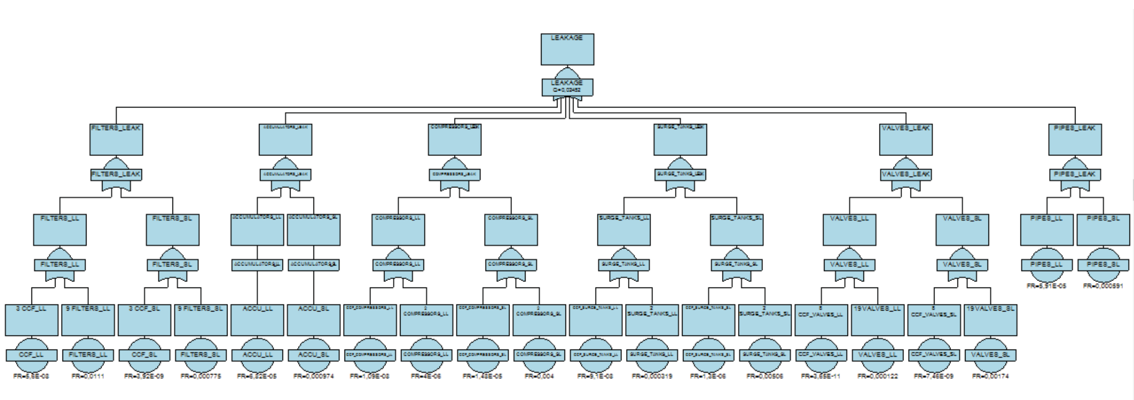


Figure 19: Fault tree for off-gas system leakage

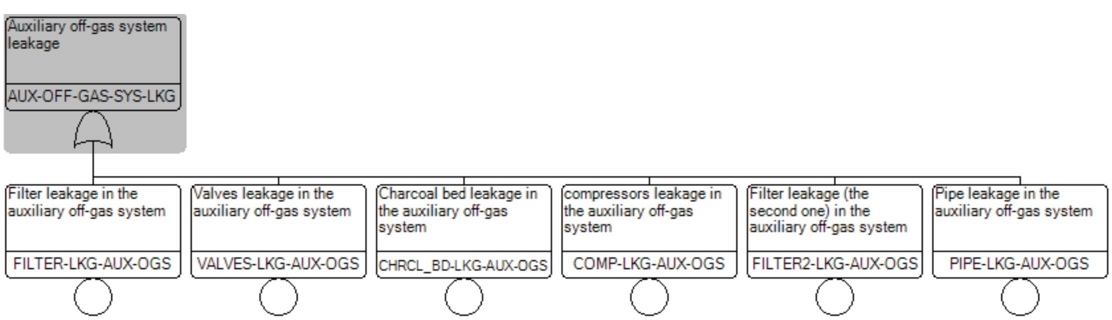


Figure 20: Fault tree for auxiliary off-gas system leakage

After determining the values associated to the fault trees, the event tree is developed:

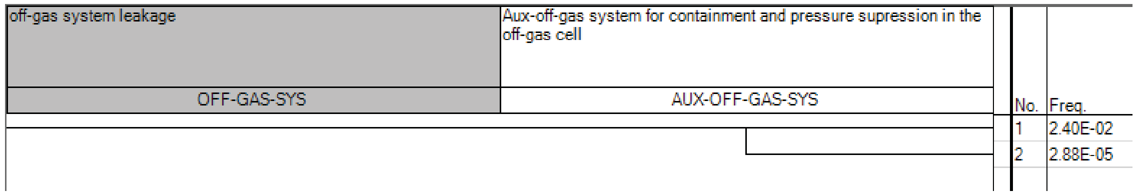


Figure 21: Off-gas system event tree for an off-gas leakage possibly exceeding the TLRC

As can be seen, the frequency of an off-gas system leakage possibly exceeding the TLRC is at maximum in the BDBE category. It means that an off-gas system leakage possibly exceeding the TLRC is very unlikely to happen. Now, the dose at the EAB has to be calculated (since the Japanese criterion cannot be applied for the off-gas system), knowing that the dose should be lower than the limit of 3000 mSv. The radionuclide inventory is given in a previous section. According to the NGNP methodology, TEDE has to be calculated. TEDE is a term of the NRC combining the effects of both internal and external exposures. Mathematically, it is the sum of the deep dose equivalent (dose to the skin to a depth of 1 cm from external gamma radiation) and the committed effective dose equivalent (total internal dose to the body in 50 years after inhalation or ingestion of the radionuclides). The noble gases exclude the possibility of internal exposure. Only tritium can be ingested (or inhaled since it is the same factor). The fission products transport will have to be evaluated in a future study.

One may notice that if a release from the worst possible location (at the off-gas system inlet) calculated at EAB is below the BDBE limit, then the off-gas system is safe according to the NGNP project.

IV.1.3.III. Suggestion for a better off-gas system study

After the different remarks from the previous parts, it is suggested to study the off-gas system as another system apart from the reactor. Explicit links would then be made between the two systems. Indeed, the off-gas system possesses its own source term (fission gases flowrate at the entrance of the off-gas system at steady-state) and its own safety system (the auxiliary off-gas system).

The off-gas system of MSRs is similar to other off-gas system from reprocessing plants. The first idea would be to develop a separate study for the off-gas system and to apply the methodology developed for reprocessing plants. One example of a PSA developed for a reprocessing plant was performed for the TOKAI reprocessing plant [26]. More generally, different safety assessments of fuel cycle facilities in the world are presented in reference [27]. One may note that the studies differ a lot according to the country.

IV.2. Initiating event grouping

Back to the reactor study, once IEs are identified, a grouping and a screening of the latter are performed. The grouping is performed in 8 categories. The 7 first categories derive from NUREG-0800 applied for LWR [28]. In the present study, another category includes MSR-specific IEs. The idea under this grouping is to show that the MSR incorporates the LWR regulations. Besides, the grouping will be of help when building the event trees. Indeed, IEs are grouped according to their effects on the system. Thus IEs from the same group should have a similar accident progression, only differing by the intensity of their effect. The IEs list was found using the MLD methodology, and then verified with the FHR IEs list [5], together with the NUREG-0800 [28] and ENSI-a05 recommendations [29]. The grouped IE list is given below:

Table 6: Grouped IE list

Increase in heat removal by the secondary system
Secondary salt flow increase
Cooling flow increase (feedwater system malfunction and steam pressure regulator system failure)
Inadvertent opening of a steam generator relief or safety valve
Decrease in heat removal by the secondary system
One / Two loop9s0 secondary pump trip
Turbine trip
Inadvertent closure of Main Steam Isolation Valve (MSIV) (+CCF MSIVs)
Loss of condenser vacuum
Total loss of feedwater
Partial loss of feedwater
Feedwater pipe rupture
Secondary pipe leak
Steam generator tube rupture
Decrease in primary loop system flowrate
One / Two loop(s) primary pump trip
Loss Of Offsite Power (LOOP)
Reactivity and power distribution anomalies
Graphite loss (**)
Control rod(s) drop
Malfunction in He bubbles injection (**)
Cold loop startup (*)
Salt control failure: excessive fuel addition (*)
Salt control failure: cold fuel salt injection (**)
Oxygen / Moisture ingress: fissile precipitation (**)
Off-gas system plugged (loss of removal of poisons (Xenon)) (**)

Fissile penetration to graphite and release (**)

Increase in primary salt inventory

Salt control failure (*)

Heat eXchanger Tube Rupture (HXTR)

Decrease in primary salt inventory

Freeze valve failure

Leak from reactor vessel

Leak from the primary circuit

Radioactive release from a subsystem or component

Off-gas system failure

Decay container leakage (***)

Fresh fuel container leakage (***)

Drain tank leakage

MSR-specific category

Graphite fire (**)

Malfunction of the containment heating system (**)

(*) = IE explained in the next section and considered in the PSA model
(**) = IE explained in the next section and not considered in the PSA model
(***) = IE not considered in the PSA model because they are not part of the reactor study
The other IEs are similar to IEs considered for LWR licensing. Thus, they are not explained. They are all considered in the PSA model.

Concerning the turbine trip, it groups the loss of external electric load, the partial closure of MSIV and steam pressure regulator failure. The cooling flow increase groups the feedwater system malfunction and the steam pressure regulator failure. Due to lack of data, the probability of a secondary circuit flow increase is set equal to the probability of a water cooling flow increase.

Many IEs, for example total loss of feedwater, can be understood in general terms due to their analogy with LWR IEs. In the next section, MSR-specific IEs, together with their accident progressions, are presented.

IV.3. Explanation of MSR-specific IEs

Some IEs are MSR-specific and thus it is not always easy to understand their effects and their corresponding accident progression. That is why MSR-specific accidents are developed in the next section. At the same time, a screening is performed for IEs with too low frequency or no consequence for the plant operation.

IV.3.1. Cold fuel salt injection

The present calculations try to show that a malfunction in the fuel salt injection, leading to an injection of cold fuel salt (heaters malfunction), is harmless to the system. The temperature of the fuel salt injected is chosen to be at its melting point, i.e. 500°C. The density of the fuel salt is found to follow the relation: $d = 3.752 - 0.00068 * (T - 273)$ [30] with T in Kelvin and d in g.cm^{-3}. Besides, it is supposed that the two fertile and fissile fuel salt tanks are emptied together at once. The temperature of the core fuel salt is equal to its average $T_{core} = 637.0$°C.

The total mass added is 69 kg (67 kg of fertile fuel and 2 kg of fissile fuel). It corresponds to a volume of:

$$V_{add} = \frac{m_{add}}{d} = 20.22\ dm^3$$

Moreover, one has:

$$V_{core} = 21.1\ m^3$$

If complete mixing in the core is supposed:

$$T_{moy} = \frac{T_{add} * V_{add} + T_{core} * V_{core}}{V_{add} + V_{core}} = 636.9°\text{C}$$

The hypothesis of complete mixing is reasonable since the fuel salt is injected in the pump bowl, thus the salt is mixed before being injected in the core. One Has:

$$\Delta T = -0.1°\text{C}$$
$$\Delta\rho = -3 * 10^{-5} * \Delta T = 3 * 10^{-4}\ \% \frac{dK}{K} \ll 0.1\% \frac{dK}{K} = \beta$$

The result shows a considerable margin. Even if complete mixing in the core is not achieved, and knowing that a conservative assumption concerning the injection temperature was made, one can reasonably assume that the cold fuel salt injection accident has no consequence on the operation of the plant.
However, the temperature of the fuel salt is not the main problem when fuel salt is injected. Thus the second accident considered here is the fissile fuel salt injection accident.

IV.3.2. Fuel salt injection accident

The maximum amount of fissile fuel salt injected at once is 2 kg [3]. Compared to 800 kg of ^{233}U in the core, it corresponds to an increase in fissile inventory of 0.25%. Supposing perfect mixing (injected at the pump bowl) one has:

$$k' = \frac{P'}{L} \sim 1.0025 * \frac{P}{L} = 1.0025 * k$$
$$\rho \sim 0.25\,\% \frac{dK}{K}$$

According to N. SUZUKI and Y. SHIMAZU [31], such a reactivity addition could be a threat to the reactor. Thus this accident will be considered when building the event trees.

IV.3.3. Cold loop startup

When the flow restarts from stand-by conditions, cold fuel salt may be injected into the core. Due to the negative temperature reactivity coefficient, it inserts a positive reactivity. If the fuel salt in the core is considered at its average temperature, i.e. $T_{core} = 637.0$°C [3], and the cold fuel salt injected at its minimal temperature, i.e. the temperature of the containment $T_{cont} = 497$°C, then:

$$k_T = -3 * 10^{-5} * \Delta T = 0.42\% \ \frac{dK}{K}$$

According to N. SUZUKI and Y. SHIMAZU [31], this insertion of reactivity would lead to a damage of the reactor. Thus, this accident has to be considered. A normal startup from cold zero power should proceed as follow [20]: The primary and secondary cell electric heaters are turned on, and the primary and secondary pumps are started to circulate helium instead of the salt in the systems. When the temperature of the secondary salt reaches 454°C, the secondary circuit is filled with the salt from the heated secondary drain tank. Similarly, when the primary salt reaches 538°C, the primary loop is filled with the heated salt from the drain tank. The salts will continue circulating isothermally until the power escalation starts. Concurrently with the salt systems being heated, the cooling system is warmed and brought to operating conditions in order to prevent the steam generator from excessive thermal gradients.

The reactor is made critical by fully removing the safety rods and inserting adequately the graphite control rods. The final approach to criticality is achieved by slow insertions of fissile fuel salts.

IV.3.4. Graphite loss accident

This accident corresponds to the loss of a part of the graphite block. In this accident, two effects concur: reactivity is removed due to the loss of graphite, and reactivity is added due to the fissile fuel salt replacing the graphite lost. In order to compare these effects, their reactivity added per volume is calculated.

The corresponding data for the mini-FUJI are used:

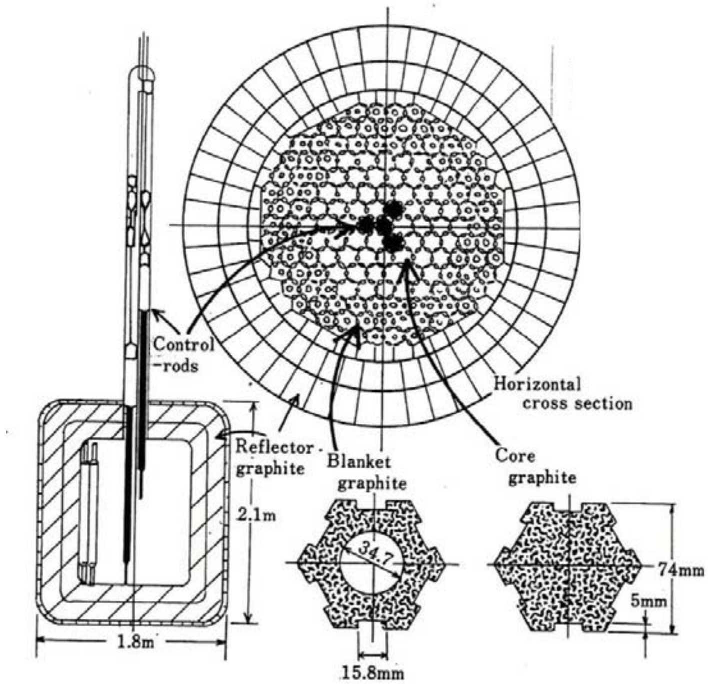


Figure 22: Control rod geometry in the FUJI design
Figure updated from TTS website

Therefore the volume of a control rod is approximately:

$$V_{rod} = S_{rod} * H = \frac{3 * \sqrt{3} * \left(\frac{37}{\cos(36°)}\right)^2}{2} * 2.1 = 1.14 * 10^{-5}\ m^3$$

The reactivity of a control rod is equal to $0.06\ \% \frac{dK}{K}$. Therefore the reactivity added per volume due to the graphite loss is equal to (CR in graphite):

$$\rho_V^G = \frac{-\rho_{CR}}{V_{rod}} = -5 * 10^3 \% \frac{dK}{K} / m^3$$

N.B.: It was considered that the differential reactivity worth of the CR was constant, meaning that the integral CR worth is linear (see Figure 23). Therefore, the reactivity added per volume is underestimated in the centre of the core and overestimated at the corners.

The reactivity inserted due to the fissile replacement is equal to:

$$\rho_V^F = \frac{\rho_{fuel}}{V_{fuel}} = \frac{0.25}{\frac{m_{fuel}}{d_{fuel}}} = \frac{0.25 * 11}{2} * 10^3 = 1 * 10^3\ \% \frac{dK}{K} / m^3$$

N.B.: Remember that for 2 kg of fissile fuel added in the core, a reactivity of $0.25\ \% \frac{dK}{K}$ was added. d_{fuel} is calculated using the relation given in the cold fuel salt injection accident for a temperature of 637°C. The same approximation for the differential reactivity worth of the fissile salt is done.

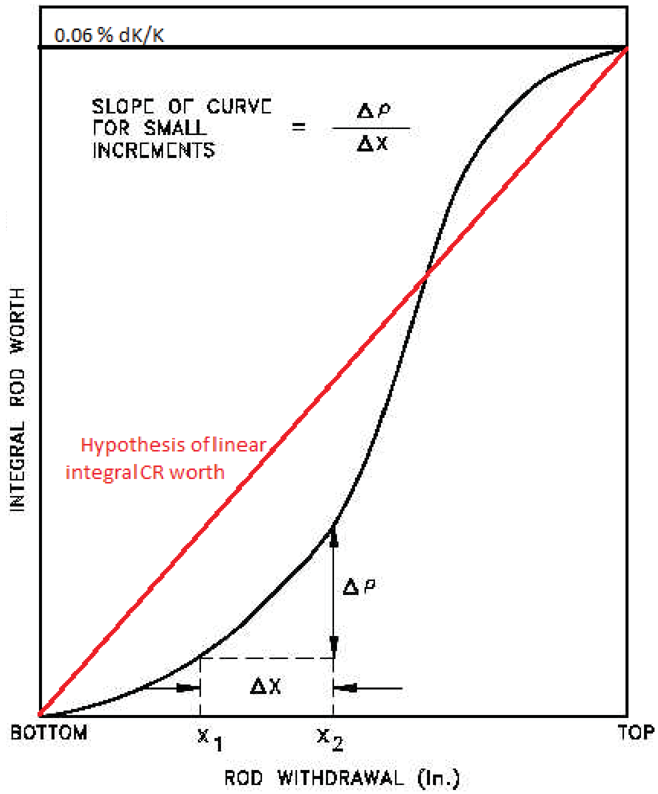


Figure 23: Illustration of the hypothesis of linear control rod worth
Figure updated from DOE-HDBK-1019/2-93

The first result is that the absolute reactivity added per volume for the graphite and for the fuel salt have the same order of magnitude. Thus one can expect a negligible overall effect, one effect compensating the other.

The second result comes from the fact that $|\rho_V^G| > |\rho_V^F|$, meaning that the overall reactivity added would be negative. Since the hypothesis of constant differential reactivity worth is done for both calculation (meaning that the place of the graphite loss in the core has no importance), the results are still valid.

This result is consistent with a safety analysis report on MSRE [32].

IV.3.5. Malfunction in He bubbles injection

An accident where the injector increases the amount of helium injected in the primary loop is studied in this section. The normal operating condition for helium is 0.2% volume [31]. By increasing the amount of helium in the system, the void fraction increases, leading to a reactivity insertion since there is a positive void reactivity coefficient. According to N. SUZUKI and Y. SHIMAZU [31], the maximum reactivity insertion should be less than $0.1\,\%\frac{dK}{K} = \beta$. The void reactivity coefficient for the FUJI reactor is equal to $0.07\,\%\frac{dK}{K}/\%void$. Thus, in order to reach the maximum reactivity insertion limit, the volume of helium needed is:

$$V_{He} = \frac{\rho_{max}}{\rho_{\%void}} + 0.2 = 1.63\ \%void$$

This value is extremely high; it corresponds to an increase in the injection rate of 815%. An injector cannot have such capability, thus this accident is harmless to the reactor. Moreover, this effect would not have to be taken into account when depressurization occurs, for example when a break in the primary loop happens [33]. Indeed, with a decrease in pressure, the volume of the helium bubbles will grow, leading to a positive reactivity addition due to the positive void reactivity coefficient. According to the author of [31], this effect is negligible compared to the loss of fuel and flow.

IV.3.6. Fissile precipitation

When oxygen enters the primary loop (air or moisture ingress for example), it reacts with the fuel salt to create UO_2 [14]. UO_2 is not soluble in the salts, and its melting temperature is well above the salt temperature in the reactor. Therefore it will precipitate and deposit on the surface of the primary loop. If this precipitate is suddenly injected into the core, it corresponds to a reactivity insertion.
The volume in the primary circuit is approximately $V_{loop} = 5\ m^3$. Considering a tube radius of r = 10 cm, the contacting surface of the primary circuit is:

$$S_{loop} = 2 *\ \pi * r_{tube} * z = \frac{\pi * {r_{tube}}^2 * z}{\frac{r_{tube}}{2}} = \frac{V_{loop}}{\frac{r_{tube}}{2}} = \frac{5}{\frac{10}{2} * 10^{-2}} = 10^2\ m^2$$

Using the density of UO_2 and a deposited layer of 0.1 mm, one obtain a mass:

$$m_{loop} = S_{loop} * x_{layer} * d * P_{fissile} = 10^{-1} * 11 * 10^2 * 0.02 = 2.2\ kg$$

This amount is a threat for the operation of the reactor, thus safety systems have to be implemented in order to limit oxygen ingress.

In the FUJI-233Um design, the high temperature containment is filled with inert gas (depleted air would work), so that the probability of oxygen ingress is largely reduced. In order for the oxygen to be in contact with the fuel salt, it has to go through two barriers: the high temperature containment and the structure of the primary circuit. There are only few possible bypasses:

- one through the seal of the pump bowl
- two through the seals for the inlet and the outlet of the secondary circuit
- two through the emergency drain tank and the drain tank lines
- one through the control rod drive

Industrial seal with low leakage probability are available.

The precipitate can come from the salt injection system too. However, the salt injection system can be designed so that the oxide precipitate particles, having a high inertia, will hit the walls of a sinusoidal pipe, thus will be retained from going into the primary circuit. A particle filter can also be implemented at the fresh fuel tank outlet.

Another possibility comes from the precipitation of fuel salt due to its saturation (concentration higher than the solubility limit). The consequence of the latter is small, since the precipitate volume would be small.

In the end, the initiating event corresponding to graphite precipitation seems to be very unlikely.

Besides, in order to evaluate the consequences of such IE, a transient analysis for this scenario has been performed [34]. One may note that this accident belongs to a broader category of transients concerning periodic perturbations. Periodic perturbations may represent a slug of fissile precipitate, a void concentration or a cold portion of fuel flowing through the primary circuit. These periodic precipitations have been studied for startup and operation cases. The authors used a Multiphysics model to simulate this accident. It is a 2-D simulation using COMSOL Multiphysics. The neutronic part is treated by the two-group diffusion theory and the thermo-hydraulic part is treated by the RANS/k-e model, together with empirical correlation for the heat transfer between fuel and graphite. The startup case is given below. A fissile precipitate producing a total reactivity insertion of 25 pcm was simulated. As can be seen, the dynamics is characterized by an asymptotic linear evolution of the power, thus limiting the reaction time. This accident is important during startup.

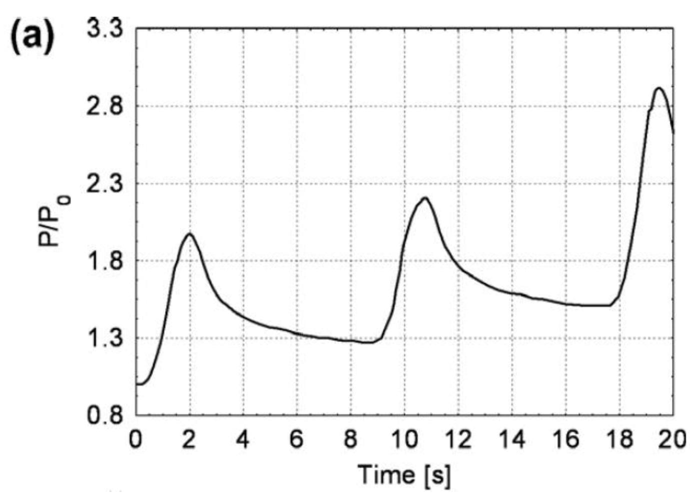


Figure 24: Power excursion in case of a periodic reactivity insertion during startup [34]

Concerning the nominal power case, the results for the temperature and the power are given below. The perturbation, this time, concerns a slug corresponding to a reactivity insertion of 500 pcm, thus corresponding to a reactivity insertion of 5$. It is understood that this insertion corresponds to an upper limit (4 kg of ^{233}U).

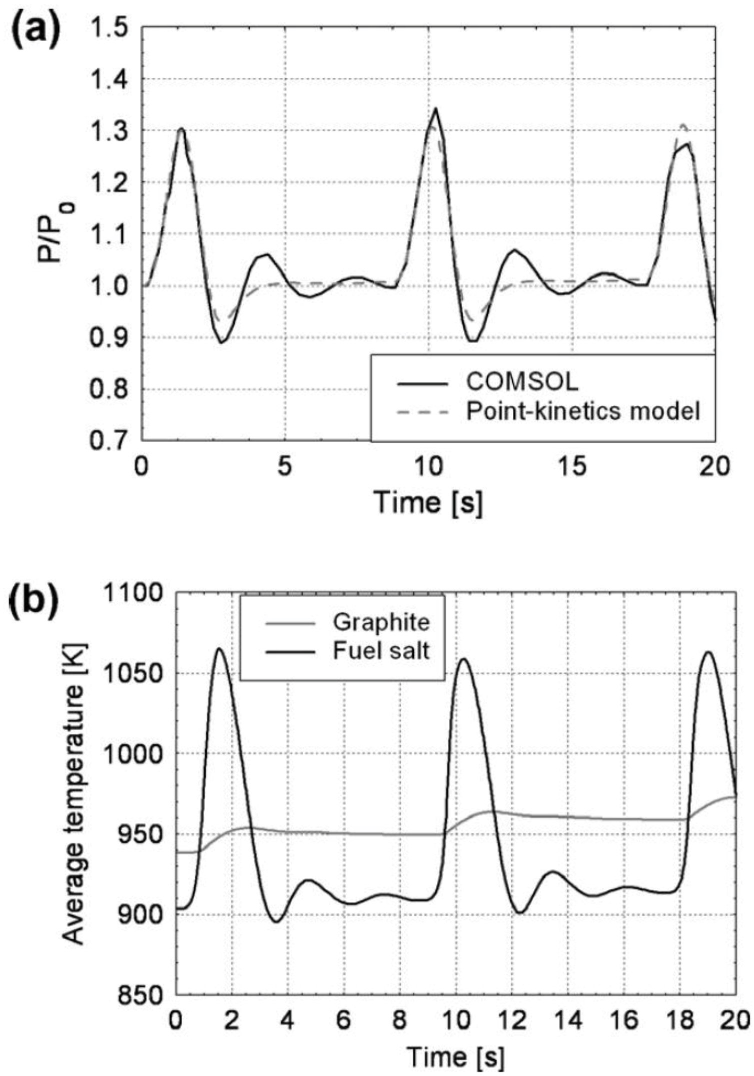


Figure 25: Power and temperature changes during operation after a periodic addition of reactivity [34]

As can be seen, the power dynamics is characterized by a constant power. The average temperature of the fuel salt is well below the safety limit of 1130K. Concerning the graphite temperature, it increases by ten degrees every ten seconds approximately. The temperature limit for graphite is 3000K. However, by taking the Hastelloy temperature limit (1200K), one finds a reaction time of 4 minutes and 20 seconds for equipment or operators to react to this transient. In the end, according to these simulations, a periodic perturbation has few consequences, except during startup. Therefore, only the initiating event "cold loop startup" will be developed in the event trees.

IV.3.7. Fissile penetration to graphite

Efforts have been made to obtain low permeability graphite, i.e. graphite with very small pore entrances [35]. Indeed, the salt penetration to graphite comes from low surface tension of the molten salts, so that they wet graphite. The porosity of such graphite can be held small (less than 1 µm). Following the Washburn relation verified for fluoride salt systems [35]:

$$\Delta p = -\frac{4 * \gamma * cos\theta}{\delta}$$

With γ the surface tension, δ the entrance diameter of the pores penetrated, θ the contact angle and Δp the pressure difference between the pores filled with helium and the fuel salt. Molten salts at 700°C have surface tensions about 230 dynes/cm, a contact angle of 150˚.

Supposing $\delta = 1\ \mu m$, one has:

$$\Delta p = 120\ psia = 8.2\ atm$$

Thus the graphite will not wet. Moreover, tests at 165 psia have shown that radiation does not alter the non-wetting characteristic of the fuel salt to the graphite [35]. The effect of the fuel salt composition does not change the results. The penetration was limited to cracks and to small penetrations of the surface.

Techniques were developed to reduce even more fissile penetration:

- Pore volume sealing technique
- Surface coatings and seals

For more information about these techniques, please refer to [35].

Therefore, graphite has requirements concerning its non-wetting characteristic. If these are respected, such accident is incredible to occur, so that the fissile penetration to graphite accident is not considered when developing the event trees.

IV.3.8. Graphite fire

There can be two causes of graphite fire. One is due to the Wigner effect and the other is due to oxygen ingress into the primary loop.

IV.3.8.i. Wigner effect

The Wigner effect corresponds to the displacement of atoms in a solid caused by neutron irradiation, in other words, it is a measure of the energy stored by deformations in a lattice. The problem comes when this energy is released following a temperature increase. Graphite irradiated

at ~30 °C, for instance, and then heated to 70 °C can rise rapidly in temperature to ~400 °C, which is approximately that required for thermal oxidation in the presence of oxygen.
In an MSR, the neutron irradiation induces deformations of the lattice. However the high operation temperature has an annealing effect on these deformations. Thus, one needs to consider the result of these competing effects.

Very few measurements were done at high irradiation temperature. Some experiments were done at 350 and 390˚C [36]. The results suggested a shift of the release peak towards high temperature and a damping of the peak. For a HTGR, 600 ˚C was found to be the critical temperature where the deformations created by irradiation and annealing are equivalent [37].

Other experiments showed that the total stored energy is a function of the fast neutron dose, but it tends to saturation and reduces in magnitude with increased irradiation temperature. However, even with a prolonged annealing at 1000 ˚C, all the stored energy is not released. This suggests that there is another release peak. Other studies suggested this peak to be around 1200 ˚C [36]. This peak is expected to be insignificant due to the saturation effect.

Thus, what can be supposed, but not verified, is that the high operating temperature of the MSR leads to more annealing than neutron induced deformation. However, this suggestion would have to be confirmed with experiments simulating the operating conditions of MSRs.

IV.3.8.III. Graphite burning

The four conditions for self-sustained oxidation (fuel, oxygen, heat and chemical reaction), as defined by the National Fire Protection Association (NFPA), are introduced to define the parameters required for self-sustained burning [38].

- Fuel

In the present case, the fuel is the carbon atoms. At atomic scale, every carbon atoms may be fuel for the reaction. However, the carbon atoms are arranged in graphene planes, and only atoms at RSA (Reactive Surface Area) can be considered as fuel. Thus it limits the fuel available for graphite-oxygen reaction.

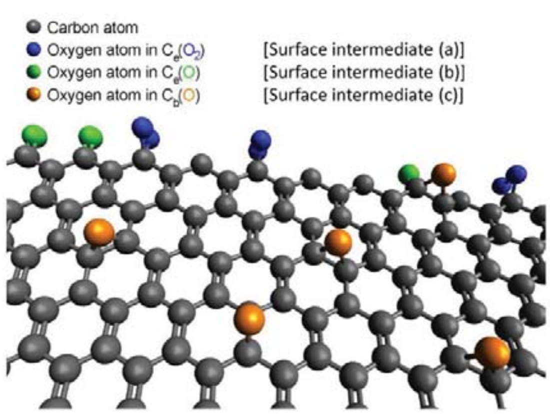


Figure 26: RSA on a graphene [38]

The blue and green atoms are located at RSA, whereas orange atoms in the bulk are stable surface intermediates. The atoms at RSA can easily desorb to create CO or CO_2. The other atoms are stable and will not desorb from the interior to form CO or CO_2.

- Oxygen

The probability of oxygen ingress is reduced by the containment being filled with inert gas. Moreover, as explained in the previous part, diffusion of the oxygen through the graphite pore structures is drastically reduced by reducing the porosity of the graphite. Thus there is practically no penetration of graphite by the oxygen.

- Heat

The graphite-oxygen reaction is exothermic. It means that heat will be produced by the reaction. It could lead to a raise of the local temperature, allowing further oxidation to occur. However, graphite has a very high thermal conductivity, thus heat is expected to be conducted away from the RSA. All in all, even if the reaction produces heat, the large thermal conductivity and the large mass of graphite is expected to remove the heat from the local regions (see Figure 27). This affirmation is proved by experiments [38].

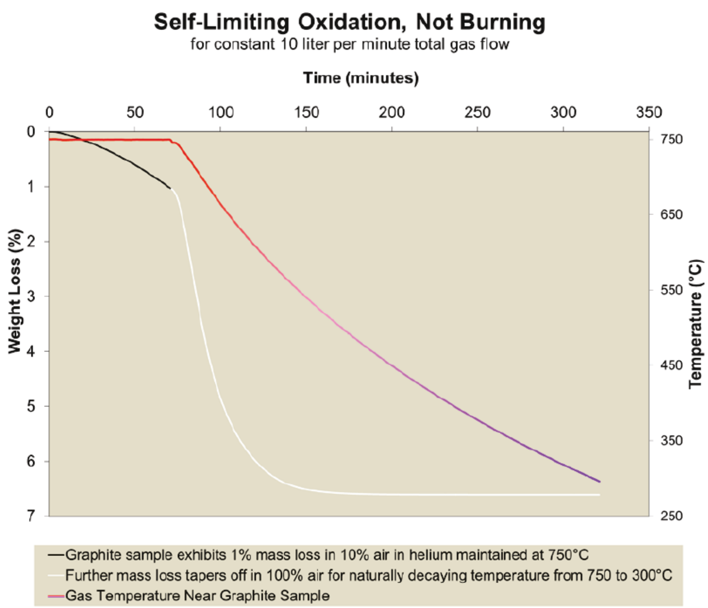


Figure 27: Self-limiting oxidation of nuclear grade graphite [38]

- Chemical reaction

The chemical chain reaction, necessary for self-sustained oxidation, needs continuous supply of available carbon atoms, a certain amount of oxygen, and a high temperature for a high reaction rate. Since the carbon atoms are only available at RSA, and the unlikely oxygen supply is restricted to the graphite surface, even if the temperatures reached in a MSR are high enough, a chain reaction is not expected to occur.

However another study [39] showed that the penetration of salt in graphite increases the release of flammable CO and CO_2 during thermal decomposition of graphite-oxide, leading to a poor thermal stability, and thus a higher fire hazard. Thus the conclusion holds only if the graphite has non-wetting characteristics, as explained previously.

IEs have been identified, explained and sometimes screened out. Therefore, qualitative event trees can be built if the accident progression is well understood. In order to quantify them, a database for IE frequencies and safety system reliabilities has to be established. It is important to note that parts V and VI, i.e. the construction of qualitative ETs and their quantifications, are performed at the same time when building PSA models. In the present study, since MSRs have very few known SSCs responding to the IEs identified, the quantification of their reliability can be performed before the qualitative construction of the ETs. That is why the next part presents the MSR-specific database construction.

V. Safety analysis part 2: MSR-specific database construction

As already explained, Chapters V and VI, i.e. the construction of qualitative ETs and their quantifications, are performed at the same time when building PSA models. In the present study, since MSRs have very few known SSCs responding to the IEs identified, the quantification of their reliability can be performed before the qualitative construction of the ETs.
Two lists have to be established: A first one corresponding to IE frequencies and a second one for component reliabilities. The estimation of component failure rates is explained first. It applies to frequency estimations as well as safety system component reliabilities. It allows the construction of the MSR-specific database. However, some data are highly uncertain and, in some cases, missing. These cases are discussed at the end of the section.

V.1. Probabilistic tool for the component failure rate estimation

Different probabilistic tools have been used in order to develop the MSR-specific database. Jeffreys non-informative priors are used for Bayesian estimations of component failure rates. The alpha factor is used to quantify common cause failures. Human Reliability Analysis (HRA) is used to quantify human errors.

V.1.1. The Jeffreys non-informative prior

Most of the available data for new generation reactors are either raw data from experiments or plant specific operating experience (MSRE or other LMFBR). In both cases, a probability distribution has to be used. The Jeffreys non-informative prior distribution can be seen as the distribution corresponding to a maximum entropy distribution, where the unidentified parameter is approximately a location parameter [40]. The Jeffreys non-informative prior is often used since its distribution represents the fact that we know nothing about the location parameter, which is here the mean.

For the distributions considered in this study, the Jeffreys non-informative prior is either a Poisson random count (when the raw data is the number of failure in a time interval) or a binomial law (when the raw data is the number of failure on demand).

When the distribution is binomial(n,p), the posterior distribution is a beta(f+1/2, s+1/2), with f the number of failures and s the number of successes on demand. Its mean is equal to (f+1/2)/(f+s+1). When the distribution is a Poisson random count, the posterior distribution is an improper distribution with the particularity that it is a limit of a gamma function. If n is the number of failure during time t, the posterior distribution would be a gamma(n+1/2, t). Its mean is equal to (n+1/2)/t. A MATLAB program or a spreadsheet can easily compute the failure rates according to raw data.

However, one has to notice that a non-informative prior can be not realistic enough, in the sense that the posterior mean is pulled toward the prior mean, and the prior mean can be quite unrealistic. For example, if the failure probability of a system is estimated from a number of failures on demand, a binomial law would be used as prior. Its implicit mean is ½. Thus the posterior mean deduced from the raw data would be strongly pulled toward ½, leading to an overestimated value.

Remark: Although the uniform distribution is frequently considered as a non-informative prior, it is in fact more biased than Jeffreys non-informative priors. For more information, please refer to [41].

V.1.2. Alpha factor for Common Cause Failures (CCFs)

Different model exists in order to quantify common cause failures. The CCFs in the Standardized Plant Analysis Risk (SPAR) models (plant specific PSA models of the US NPP) are calculated by using the Alpha-factor method. Hence, a database containing alphas calculated by Bayesian and frequentist approach was constructed by the NRC [42]. Since the database seemed adequate for MSR components, this Alpha-factor method was used in the PSA model.

This Method is explained in NUREG/CR-5485, Section 5.3 [43]. The sought probability $Q_k^{(m)}$is the probability of k specific components failing in a group of m components.

For a two trains (A/B) system, the cut-sets are {A,B} and {CCF(A,B)}. Hence, the failure probability for the system is (use of a staggered testing formula [43]):

$$P(failure) = P(A * B) + P\big(CCF(A,B)\big) = Q_1Q_1 + Q_2 = (\alpha_1 Q_T)^2 + \alpha_2 Q_T$$

α_1 and α_2 are given in reference [42].

Example: The compressors present in the auxiliary off-gas system. The two failure modes are "Fail to start" (FTS) and "Fail to run" for 24 hours (FTR). The Fault-tree is given below:

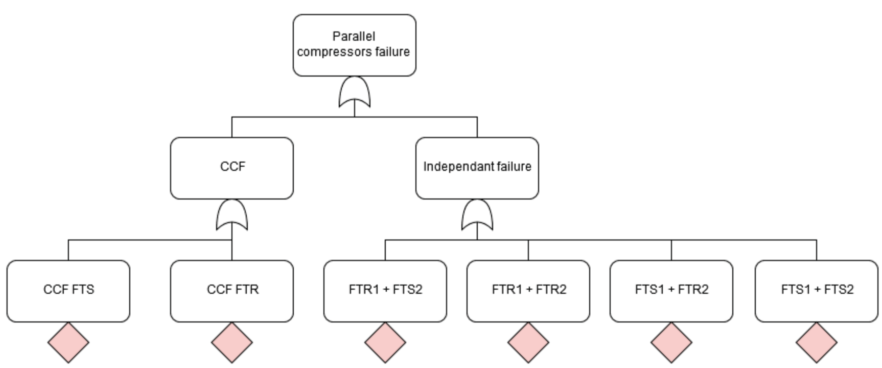


Figure 28: Example of a FT with CCF

According to the formulation given previously (FTR1 & FTR2 case contained in the CCF(FTR) case), the failure probability of the two compressors in parallel is equal to:

$$P(failure) = P(CCF_{FTS}) + P(CCF_{FTR}) + P(FTR_1 \,\&\, FTS_2) + P(FTS_1 \,\&\, FTR_2)$$

V.1.3. SPAR-H and THERP for the Human Reliability Analysis

Human reliability is an integral part of the LBEs of the MSR. For instance, THERP and SPAR-H are two techniques for the assessment of human errors in nuclear power plants that affect the availability of systems. A secondary goal of such analysis is the identification of error-prone equipment designs, poor safety culture, imperfect written procedures and other similar problems so that improvement can be considered.

V.1.3.i. THERP method

The Technique for Human Error Rate Prediction (THERP) methodology provides a mean to identify and quantify the potential for human errors in NPP tasks. This methodology consists of four phases [44]:

- Familiarisation (Plant visit, Review information from system analysts)
- Qualitative analysis (task analysis, development of HRA event trees)
- Quantitative analysis (Assignment of nominal HEPs, estimation of the relative effects of PSFs, Assessment of dependence, determination of success and failure probabilities, determination of the effects of recovery factors)
- Assimilation (Sensitivity analysis if needed, information supply to system analysts)

All the necessary data are summarized in the 20th chapter of NUREG/CR-1278. The different tables are given from table 20-1 to table 20-27. In order to find the data needed, flowcharts are given in Appendix 1.

In the end, this method is relatively simple since one has only to follow the diagram and the indications. The hardest part in such study is the qualitative characterisation of the tasks.

However, THERP was judged not adequate for the PSA model developed. The major problem of this technique is that PSFs are not well defined (see the PSF flowchart in Appendix 1). The PSFs considered in this method are stress (external or internal), trainings, adequate equipment, long working hours, good ergonomic practices, personnel characterisation, and heavy task load. Moreover, the stress factor is mixed with the fitness for duty factor, the latter being impossible to evaluate correctly for the analysis of a preliminary design, where the safety culture is not yet established. That is why another method had to be used for the PSA model developed.

.

V.1.3.III. SPAR-H method

In the 1990s, the NRC decided to develop an improved and easy-to-use HRA method. This method requires to complete a worksheet designed to easily quantify the PSFs and HEP of interest. A SPAR-H analysis is complete after 9 steps, which is easier than the 5 flowcharts of the THERP method [45]:

1) Fill the headers
2) Does the basic event involves diagnosis, action, or both diagnosis and action?
3) If diagnosis is involved, then rate the eight PSFs. Justify if a non-nominal value is selected and documents the reasons for this choice
4) Report the selected multipliers on the second page, where HEP are calculated
5) Calculate the HEP without dependency. If three or more PSFs are negative (superior to 1), then apply the adjustment factor provided
6) If action involved, repeat steps 3 to 5 in the action section
7) Calculate the total HEP, be it the diagnosis HEP, the action HEP, or the joint HEP
8) Determine the appropriate level of dependency. If there is no dependency, explain the reason and apply the total HEP from step 7
9) If a level of dependency has been assigned, then evaluate the task failure probability with dependence

The worksheets are given in Appendix 2. However, as every simplified method, SPAR-H has modelling and analysis limitations. The PSFs seem exhaustive. However it may be difficult to assign a specific influence into a specific category. This categorisation is left to the analyst and should be justified. The main goal of this method being simplicity, it is impossible, in the SPAR-H method, to determine the contribution of aleatory versus epistemic sources of uncertainty on the HEP as a function of PSF influences. The last problem comes from the assignation of nominal PSFs when not enough knowledge on the safety culture is available. This may lead to underestimation of HEPs.

However, the advantage of the SPAR-H method is that the PSFs related to the task are well separated from the PSFs related to the safety culture. It is the reason why this method was chosen in comparison to the THERP method. The 3 PSFs related to the task are: the available time, the stress and the complexity. In Appendix 3 are presented the results and the documentation for the calculation of the different HEP involved in the PSA.

In order to compare these two methods, a table comparing the different PSFs, together with their values, is given in the next part.

V.1.3.IV. Comparison of the two methods and choice of one method

One may compare the multipliers given by the different PSFs in both methods:

Table 7: Comparison of the PSFs for the two methods THERP and SPAR-H Updated from NUREG/CR-6883 [45]

SPAR-H PSFs	SPAR-H PSF levels	SPAR-H multipliers	THERP multipliers
Available time	Inadequate time	P(failure) = 1	P(failure) = 1
	Time available = time required	10	10
	Nominal time	1	1
	Time available > 5*time required	0.1	
	Time available > 50*time required	0.01	0.01
Stress / Stressors	Extreme	5	5.25
	High	2	2.5
	Nominal	1	1 for optimal, 2 for low stress
Complexity	Highly complex	5	5*
	Moderately complex	2	2**
	Nominal	1	1
Experience / Trainings	Low	3	2
	Nominal	1	1
	High	0.5	
Procedures	Not available	50	50
	Incomplete	20	10
	Available, but poor	5	10
	Nominal	1	
Ergonomics / HMI	Missing / Misleading	50	100, 1000
	Poor	10	6, 10
	Nominal	1	
	Good	0.5	
Fitness for duty	Unfit	P(failure) = 1	
	Degraded Fitness	5	
	Nominal	1	
Work process	Poor	2	
	Nominal	1	
	Good	0.8	

* Heavy task load for dynamic tasks, requiring considerable interaction between operator and system identification

** Heavy task load for step by step, rule-based tasks

As can be seen, apart from some exception, the PSFs are sensibly the same. That is why, when the nominal HEPs are similar, consistent result between the two methods are obtained.

V.2. IE frequency and component reliability database

A database quantifying the safety system component reliabilities and the IE frequencies has to be established in order to quantify the event trees. Then, the failure rate of a system is calculated using Fault Trees (FTs). The methodology, together with some examples, is briefly explained at the end of the section.

V.2.1. Safety system component reliability table

The failure rates for the different components present in the FTs are given in Table 8. The SPAR (Standardized Plant Analysis Risk) reference is an update of NUREG/CR-6928 [46]. When possible, data from other Liquid Metal Cooled Reactor are taken. It is really important to use data from LMFBR for the primary and secondary circuits since the physical parameters (temperature, pressure, heat transfer loop, etc.) are comparatively the same for such reactors. However, they are very different from the LWR parameters. Concerning the water cooling circuit, data from PWRs can be taken since this circuit is similar to the secondary circuit of the latter. The last version of the report was updated in 2010.

The different failure modes present in the table are:

- FTR: Failure To Run
- FTS: Failure To Start
- FTO: Failure To Open
- FTC: Failure To Close
- FTOP: Failure To Operate
- FTI: Failure To Insert

The symbols /h and /d mean per hour and per demand respectively.

Table 8: Reliability table for components used in the FTs

Component	Failure mode	Failure rate		Source
Secondary pump	FTR	5.00E-05	/h	[47]
	FTS	5.00E-03	/d	[47]
Water cooling pump	FTR	1.00E-04	/h	SPAR
	FTS	5.00E-03	/d	SPAR
Unpressurized tank	Leakage	7.62E-07	/h	SPAR
Battery charger	FTOP	2.43E-06	/h	SPAR
Battery	FTOP	5.86E-07	/h	SPAR
DC bus	FTOP	2.35E-07	/h	SPAR
Freeze valve	FTO	4.95E-03	/d	[48]
Engine drive pump	FTR	1.10E-03	/h	SPAR
	FTS	3.30E-03	/h	SPAR
Explosive valve (Emergency DT)	FTO	2.60E-03	/d	SPAR

Fan	FTS	7.09E-04	/d	SPAR
	FTR	4.71E-06	/h	SPAR
Flow sensor	FTOP	8.15E-04	/d	SPAR
	FTR	1.02E-07	/h	SPAR
Pressure sensor	FTOP	1.17E-04	/d	SPAR
	FTR	8.22E-07	/h	SPAR
Positive displacement pump	FTS	2.50E-03	/d	SPAR
	FTR	7.09E-04	/d	SPAR
Shutdown rods	FTI	3.00E-05	/d	EGG-SSRE-8875
Secondary valve (Drain Tank)	FTC	3.00E-03	/d	SPAR
	FTR	3.00E-07	/h	SPAR
Temperature sensor	FTOP	4.32E-04	/d	SPAR
	FTR	8.40E-07	/h	SPAR
Transistor	FTOP	1.00E-08	/h	[47]
Auxiliary feedwater system	FTOP	3.41E-04	/d	[48]
Pipe (DTC)	Leakage	9.96E-08	/h	[51]
DHX1 (DTC)	FTOP	3.00E-05	/h	[51]
DHX2 (DTC)	FTOP	8.30E-07	/h	[51]
HEP nominal time (DT + FSI)	FTOP	2.00E-03	/d	[45]
HEP extra time (DT + FSI)	FTOP	2.00E-05	/d	[45]
HEP barely no time (DT + FSI)	FTOP	2.00E-02	/d	[45]
HEP secondary valve	FTOP	1.10E-02	/d	[45]
Trip signal generation	FTOP	2.00E-07	/d	[49]

The final values (after implementation of the mission times, test intervals...) are present in the RiskSpectrum® PSA model. The auxiliary feedwater system reliability is calculated by averaging the plant-specific estimates of AFW unreliability (based on the IPE failure rates) of 72 nuclear plants in the US [48].

Most of the components in this list are not present in the primary or secondary circuit (electronic systems or pumps from the water cooling circuit). Thus generic component reliability data for LWR can be used as their estimates (SPAR estimates).

V.2.2. IE frequency table

The different initiating event frequencies are given below. Sometimes, two values for the same frequency are present. The second values are LMFBR-specific from reference [50]. They have an error factor of 10. Thus, they are given only to show that the first values are inside the uncertainty bound of the second ones. The second values are not implemented in the PSA model.

The parameters are presented together with their source (last column). The value for the one loop pump trip may seem high. However, in NUREG/CR-6928, the pump failure rate is 0.04/r.y for a LWR. The viscosity of the salt being higher than the water viscosity, this frequency seems reasonable.

Table 9: IE frequency list for the FUJI-233Um reactor

Component failure and failure mode	IE (/r.y.)	Source
Freeze valve spurious operation (analogy with solenoid operated valve) (generic data)	4.38E-03	WSRC-TR-93-262
Freeze valve spurious operation (analogy with solenoid operated valve) (LMFBR data)	2.63E-03	[47]
One loop pump trip in the secondary circuit (analogy SFR)	1.00E-01	[51]
One loop pump fail to run in the secondary circuit (analogy LMFBR)	4.40E-01	[47]
Two loops pump trip in the secondary circuit (analogy SFR)	2.00E-02	[51]
One loop pump stick in the secondary circuit (analogy one pump stick PHTS SFR)	3.00E-03	[51]
One loop pump external rupture in the secondary circuit (analogy LMFBR)	4.38E-03	[47]
Heat exchanger tube rupture (analogy SFR)	7.40E-04	[51]
Heat exchanger tube rupture (analogy LMFBR) (tube bank leak)	8.77E-03	[47]
Vessel leak (analogy SFR)	8.00E-05	[51]
Turbine trip (analogy SFR)	1.00E-01	[51]
CR drop (analogy SFR)	1.00E-02	[51]
One loop pump trip in the primary circuit (analogy SFR)	1.00E-01	[51]
One loop pump fail to run in the primary circuit (analogy LMFBR)	4.40E-01	[47]
Two loops pump trip in the primary circuit (analogy SFR)	2.00E-03	[51]
One loop pump stick in the primary circuit (analogy SFR)	3.00E-03	[51]
One loop pump external rupture in the primary circuit (analogy LMFBR)	4.38E-03	[47]
Leak from the primary loop except reactor vessel & HX (analogy SFR)	2.00E-03	[51]
Loss of offsite power (analogy SFR)	1.50E-02	[51]
Main feedwater pipe rupture (Kozloduy power plant)	5.00E-03	IAEA-TECDOC-719
Total loss of Feedwater flow (Kozloduy power plant)	1.00E-02	IAEA-TECDOC-719
Partial loss of feedwater flow (Kozloduy power plant)	1.00E-01	IAEA-TECDOC-719
Closing of MSIV (analogy PWR)	2.40E-01	IAEA-TECDOC-719
Closing of 2 MSIVs (analogy PWR)	6.14E-02	[43]
Loss of condenser vacuum (analogy PWR)	4.10E-01	IAEA-TECDOC-719
Coolant flow increase (analogy PWR)	3.10E-01	IAEA-TECDOC-719
Inadvertent opening of a steam generator relief or safety valve (analogy PWR Grand Gulf)	1.40E-01	IAEA-TECDOC-719
Secondary salt flow increase (analogy cooling flow PWR)	3.10E-01	IAEA-TECDOC-719
Secondary circuit leak (analogy primary circuit without vessel)	2.00E-03	[51]
Cold loop startup (analogy PWR)	< 1.00E-2	IAEA-TECDOC-719
Salt control failure = salt injection failure	< 12	(12 injections/EFPY)
Steam generator tube rupture (tube bank small, medium, large leak) (analogy LMFBR)	5.52E-02	[47]

The salt control failure frequency is difficult to estimate. The failure comes mainly from calibration or testing error (leading to wrong fissile concentration for example). It is very unlikely that the operator would inject twice the concentration. Moreover, the fuel salt system injection design is unknown. That is why an arbitrary value x for the initiating event frequency is set. And after developing the scenarios, a condition on x is obtained according to the frequency goal set. The same methodology will be applied to the cold loop startup. This consideration is developed in a further section.

Now that component failure rates have been estimated, system failure rates can be calculated by using the Fault Tree (FT) methodology. A brief explanation of the method and special calculations of certain system failure rates are presented in the next section.

V.2.3. Fault trees for system reliabilities

The fault tree method is a top-down analysis. Starting from the top event, lower level events are identified by depicting the ways the system can fail. When data are present for the event (failure rate for example), the event is called basic event and is the last event of the branch (it is often a component). A fault tree develops the logical paths leading to the failure of the top event. The special calculations of certain system reliabilities are explained below.

The Shutdown Rods insertion reliability has to be evaluated. This system activates from a reactor trip. In order to justify the fact that the trip signal and logic units are considered highly reliable, one may refer to [49]. The study is based on a typical reactor trip system from a generation III+ reactor. It means that the reactor trip system is digitized. The basic software failure probability was chosen to be 1E-7. The application software probability was chosen to be 1E-6. The final result of this study shows that the failure probability of an automatic trip on demand and the failure probability of generating automatic trip signal are around $2 * 10^{-7}$ and $1 * 10^{-7}$respectively. Thus, in their own words, they state: "The most important contributor to the unavailability of RPS is the failure probability of control rods to insert into the core" [49].

The value for the insertion failure is taken from EGG-SSRE-8875, i.e. coming from the Seabrook PSA. Since Seabrook is a PWR, this value should be conservative for an MSR (non-pressurized). The value is $3 * 10^{-5}$ [52]. In another study by S.A. Eide et al., the failure rate to insert is equal to 1.5E-5 (1999) [53]. In order to be even more conservative, the highest value in the PSA model developed is credited.

Another system, whose reliability has to be evaluated, is the drain tank cooling. The design of the drain tank cooling for the FUJI reactor is given below [54]:

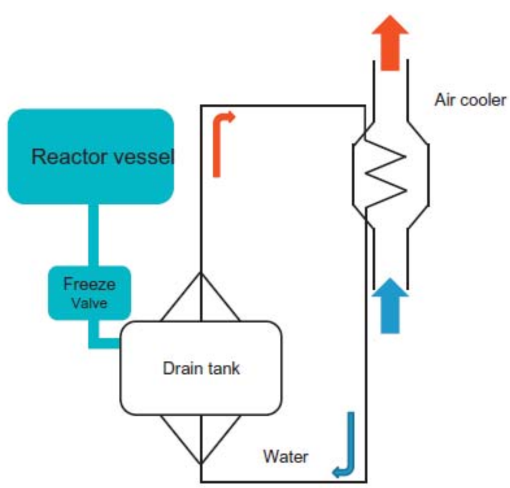


Figure 29: Drain tank cooling of the FUJI-233Um reactor [54]

It is a passive system actuated when the freeze valve opens. The failure rate of passive systems is always hard to quantify since it depends strongly on the scenario. However, a study for an HTGR cooling system has already been done. This system is very similar to the FUJI-233Um cooling system, except that the secondary loop is filled with water. Moreover, the working temperatures are quite different (around 200°C difference). However, these data are credited for the analysis. The results are given below [55]:

Table 10: Failure rate of the different Drain Tank Cooling components

Drain tank cooling	Failure mode	Failure rate	Comment	Source
Pipe rupture	Rupture	9.96E-8/h	3E-9/hm + 60 tubes + 33.2 m	[51]
DHX1	Failure to operate	3E-5/h	/	[51]
DHX2	Failure to operate	8.3E-7/h	/	[51]
Tank	Leakage	7.62E-7/h	/	SPAR
Total	Fail to cool	2.28E-03	72 h of cooling	

The mission time was chosen to be 72 hours. The final failure probability of the drain tank cooling system is then 2.28E-03.

The technique used consists of modelling the components unreliabilities of the system. It is achieved by identifying the failures that degrade the natural mechanisms of the passive system and by associating the relative unreliabilities of the components designed to assure the function. Other analyses were done, leading to very different results [56]. A first one by Mackay et al. resulted in a failure rate of 0.305 per demand for a GFR cooling system. Mathews et al. found a failure probability of $2.5 * 10^{-3}$ for a FHR cooling system, Bassi and Marques gave an upper bound of $5 * 10^{-6}$ using linear regression techniques for a GFR cooling system. Despite the fact that the systems are similar, the uncertainty of such passive system is huge, and very sensitive to the technique used. Hence the value calculated here is subject to a big uncertainty. This is a recurrent problem of passive systems [56].

The last example of FT analysis is a generic FT for valves and pumps. The general scheme for valves/pumps activation is presented as follow:

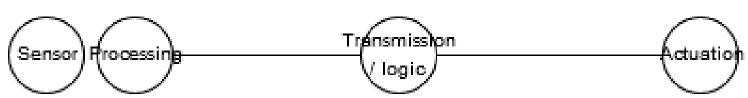


Figure 30: Generic failure modes of a component activation

All in all, valves/pumps activation failure can arise from the sensor(s) failure, the processing failure, the transmission failure or the actuation failure. The related fault trees are given in Appendix 5 – part 1. Now that the methods for the failure rate estimation have been established, the different results are presented in the next parts.

V.3. Discussion on the missing or highly uncertain data

V.3.1. Highly uncertain data

As already explained in the introduction, the inaccuracy of some data comes primarily from three sources:

- The necessity to address a large number of systems and phenomena
- The lack of reliability and experimental data
- The lack of knowledge of new phenomena

The main uncertainty is on the freeze valve, which is the main MSR-specific component. The second biggest uncertainty is on the drain tank cooling but this uncertainty is inherent to every passive system.

Concerning the freeze valve, no data are present in the literature, except an experimental report summarizing the physical performances of different types of freeze valves [57]. Data from this report are used, but the uncertainty is very large: from $6.89 * 10^{-7}$ to $3.28 * 10^{-2}$ with a mean frequency of $4.95 * 10^{-3}$ for the 90% confidence interval. More tests are necessary in order to remove the uncertainty. Nonetheless, by analogy with a solenoid operated valve, be it generic or LMFBR specific data, the values are approximately the same as the one calculated from experience (3.01E-4 and 2.63E-3 respectively). Thus, one can suggest that the mean value calculated is not absurd (error factor of 20). It is expected that a better evaluation of the freeze valve reliability would result in a lower value.

For the cooling of the passive drain tank, an analogy with an HTGR passive cooling is done. An HTGR passive cooling reliability has been estimated in reference [55].

For the emergency drain tank cooling, since the tank is placed in borated water, the failure of the Emergency Drain Tank (EDT) cooling is the probability of an unpressurized tank leakage.

V.3.2. Missing data

Data are missing primarily for two reasons:

- The system/component is still not designed
- The system/component is not major concern for the conceptual design

The two systems still not designed are the High Temperature Containment and the robots for salts handling (please refer to part III.2.3.). The components, which are not major concern for the conceptual design, are the valves/pumps, and the electronics. First, we had to determine which kinds of valves/pumps were present in the design. A table summarizing the advantages and disadvantages of the different valves is given below:

Table 11: Advantages and disadvantages of the different types of valve
Table based on various manufacturers and design studies

Type of valve	Advantages	Disadvantages
Air operated valve	High reliability Flow control	Possible air ingress Fully open of fully closed
Hydraulic operated valve	High reliability Automatic Flow control No use of external pressure or external power	Possible air or oil ingress No flow change
Motor operated valve	Broad operating conditions Flow control	Average reliability
Solenoid operated valve	No oxygen ingress	Fully open or fully closed
Manual valve	Easy to manufacture and use	Low reliability Environment should allow direct operation
Explosive valve	High reliability Fast actuation	Single use
Check valve	Prevent backflow	No flow control No flow stop

In the off-gas system, since we do not want backflow, we decided to credit check valves. When valves are in contact with molten salts, solenoid operated valve were chosen because the impossibility of air ingress is primordial. For the secondary drain tank valve and the emergency drain tank valve, explosive valves were credited since these valves are used only in case of an accident, thus a fast response and a high reliability are important. The isolation valve is also an explosive valve for the same reasons.

In the same way, there is no data available concerning the processing of the different activation signals, especially the processing of the signals activating one loop and two loops load reduction. Thus, we had to construct the signal processing by ourselves (it has to be automatic since freezing occurs some seconds after SCRAM). The processing has to be resistant to spurious signal and must have a high reliability. Thus we used two flow detectors per loop per circuit, giving 12 detectors in total. The system was made redundant in order to increase its reliability. The non-redundant system is given below:

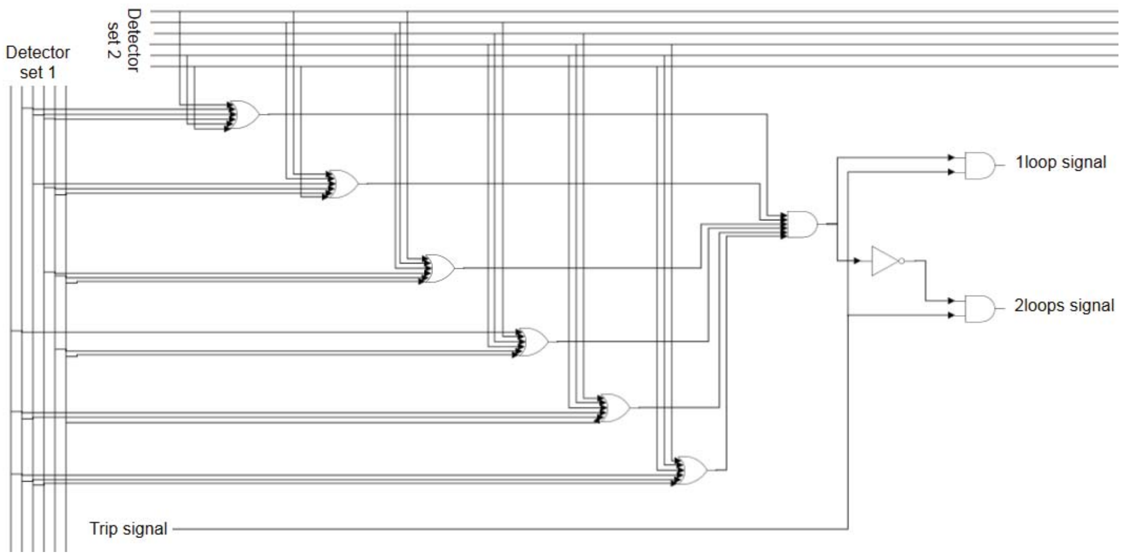


Figure 31: Signal processing for 1loop and 2loops signals

The fault tree corresponding to this system reliability is given in Appendix 5 – part 1.

Concerning the off-gas system, no data were available for the charcoal beds failure rates. The failure rate for the leakage of a generic filter in a BWR off-gas system was used. This value will have to be updated when more experience will be available.

Last but not least, information about the Secondary Drain Tank Cooling (SDTC) was missing. The SDT is cooled by air, but is it forced or natural air cooling? In this study, the conservative assumption (less reliable) of a forced SDTC with two fans in parallel is assumed (see Appendix 5 – part 1 for the SDTC FT). If it is not the case, the SDTC reliability would increase by far.

Now that an MSR-specific database has been built, the event tree can be developed and quantified. This is the subject of the next part.

VI. Safety analysis part 3: Event tree development

In order to develop qualitative event trees, knowledge of the different accident progressions is necessary. First, a literary review on some accident progressions is performed. These accidents are Reactivity Induced Accidents (RIAs), Loss Of Flow (LOF) accidents, and Loss Of Coolant Accidents (LOCA).
Then, accident progression diagrams are developed for every IE, leading to a qualitative construction of ETs, together with a LBE identification. Some accidents have not been yet studied for the FUJI reactor, like the combination of Loss Of Heat Sink (LOHS) and Loss Of Flow (LOF) in case of a LOOP.

VI.1. Literature review on accident progressions

VI.1.1. Reactivity induced accident

One advantage of the MSR is that it can operate with a small excess reactivity due to the continuous removal of fission gases (krypton, Xenon) and Tritium. However, due to the fuel salt circulating in the loop, the delayed neutron fraction is reduced. Moreover, U-233 has a lower beta effective than U-235. It renders the reactor less controllable; the reactor is more likely to have a prompt jump in criticality when inserting reactivity. Therefore, the evaluation of reactivity insertion in the FUJI reactor has to be evaluated.

In the paper of SUZUKI and SHIMAZU, transients without SCRAM were analysed [31]. The results showed an inherent safety of the FUJI-reactor thanks to the temperature reactivity feedback, despite having a very low beta effective. In the accident scenario simulated, the reactivity was added as a step, no SCRAM was performed and the heat sink is supposed to be kept constant. In order to estimate if there is an accident or not, the Japanese criterion is used. According to this criterion, the maximum inlet and outlet temperatures allowable are 1050 K and 1200 K respectively. The result of the simulation is shown below:

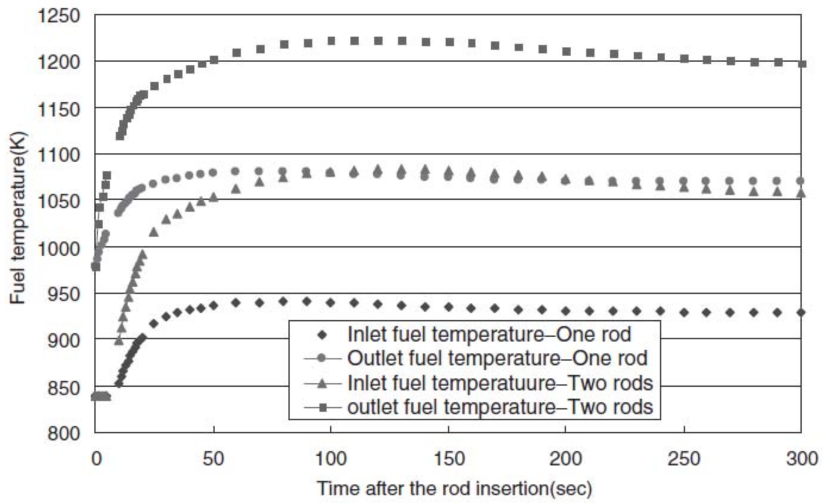


Figure 32: Temperature increase in case of a RIA accident in the FUJI reactor [31]

As can be seen in Figure 32, one rod insertion is harmless to the reactor operation. In their study, the FUJI design was non-optimized. In this design, one rod had a reactivity worth of 0.172%dK/K. In the current FUJI design, the maximum reactivity inserted due to control rods drop is 0.12%dK/K. Therefore, the control rods drop accident is impossible to occur in the current FUJI-233Um design.

It is also important to notice that a reactivity insertion of 0.344%dK/K slightly violates the safety criterion. It means that there is a certain safety margin for the control rods drop.

VI.1.2. Loss of flow

A locked rotor of the salt circulating pump interrupts the flow. Moreover, in a locked rotor accident, a positive reactivity is inserted because of the decrease of the loss of delayed neutron out of the core due to the flow circulation. This accident will also result in a loss of heat transfer. The simulation of this progression reported in [58] was performed for the MSBR, which has four loops. In the FUJI reactor, there are only 2 loops. Thus the result for the loss of two pumps corresponds to one pump lost with the FUJI design and four pumps lost correspond to two pumps lost with the FUJI design. (Indeed, the flowrate is reduced by N/4 in the model, with N the number of blocked pump.)
The variation of the heat transfer coefficient with the primary salt flow rate is taken into account as follow:

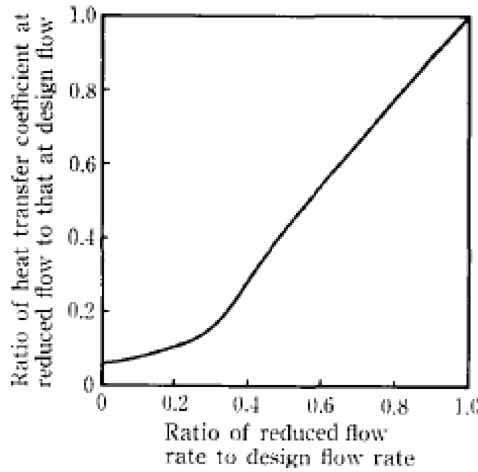
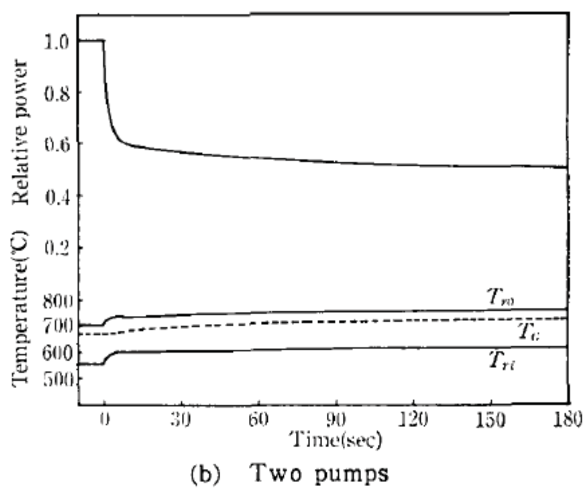


Figure 33: Heat transfer coefficient according to the primary salt flow rate [58]

And the final results with the heat transfer coefficient varying are given below:



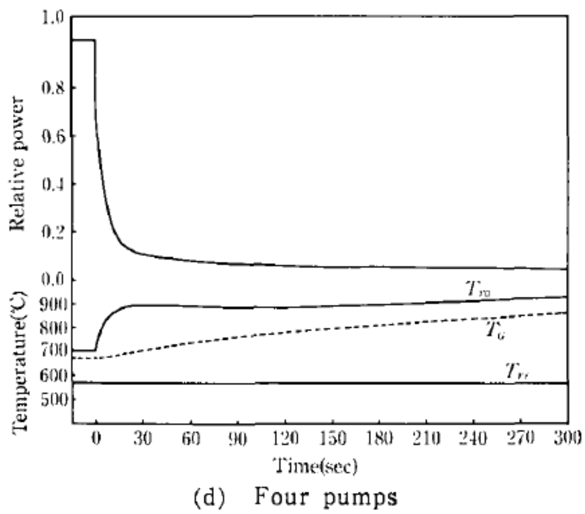


Figure 34: Temperature increase for the MSBR in case of a two or four loops pump trip [58]

As can be seen, after 300s, the outlet temperature is below 900˚C even for the complete loss of flow. It is estimated that the freeze valve will be automatically actuated around 300s, or that an operator would drop the SD rods. Therefore, a loss of flow accident is not harmful if managed in time.

VI.1.3. Loss of primary fuel salt

During a Loss Of Coolant Accident (LOCA), in addition to the fuel salt leakage, a positive reactivity is added. Indeed, the depressurization leads to expansion of the Helium bubbles. The reactor having a positive void reactivity coefficient, a positive reactivity is inserted. The system pressure transients depend primarily on the position of the break. Thus, three different break positions are identified [33].

Break 1: Break between the fuel salt pump and the heat exchanger.

The salt pressure at the break is the highest in the primary circuit. The fuel salt flows out of the core due to the pressure difference. The model assumes that the loop is isolated; it means that the salt flow in this loop is lost. Thus, the model simulates a loss of flow at half the rated value. This loss of fuel salt flow inserts reactivity by the decrease of the loss of the delayed neutrons.

Break 2: Break near the reactor inlet

In this case, the fuel will flow out of the core due to pressure difference but also due to gravity. The fuel salt flows downward and the helium bubbles flow upward due to buoyancy. The bubbles are segregated from the fuel salt and the top of the core becomes voided. Therefore, fuel salt is absent in this region and the primary pump loses suction. In this case, the flow is totally lost. One may also add that negative reactivity is added since neutron leakage increases due to a smaller fuel volume.

Break 3: Break at the exit of the reactor

In this case the fuel salt will flow out of the core due to the pressure difference, until the primary circuit pressure falls to atmospheric pressure. The fuel salt flow could be preserved, however an isolation of the loop is preferable and assumed in the model.

The result for the first case is given below:

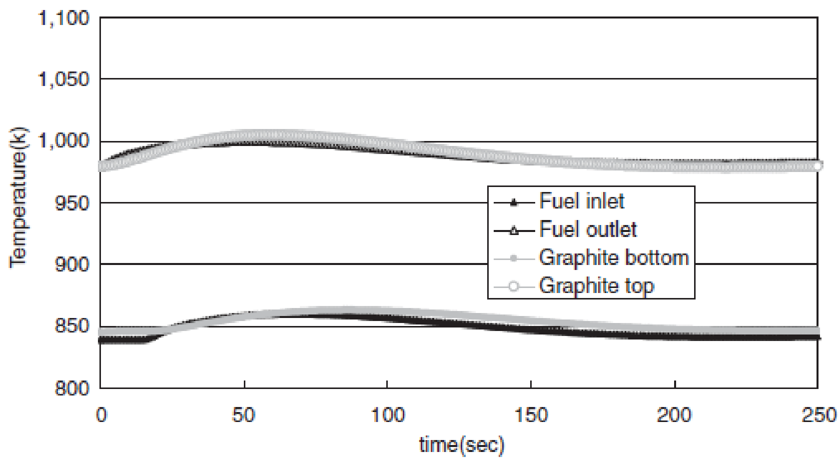


Figure 35: Temperature increase in case of a break of type 1 [33]

The safety criterion is met. The result for the second case is given below:

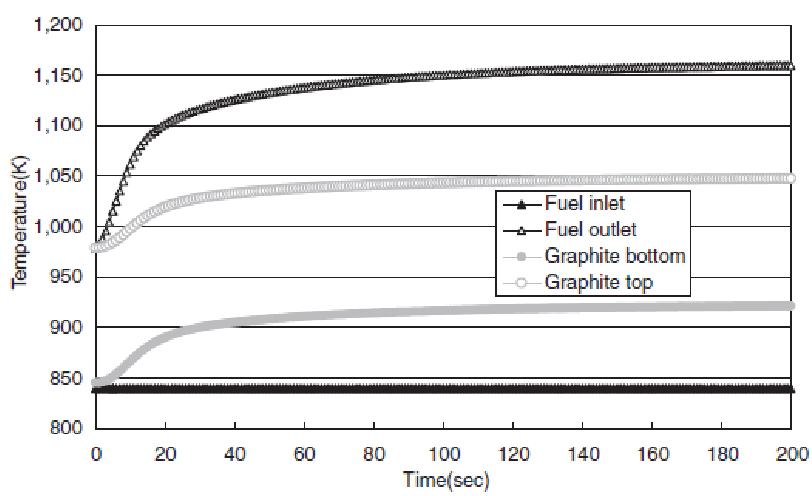


Figure 36: Temperature increase in case of a break of type 2 [33]

The safety criterion is met. The result for the last case is shown below:

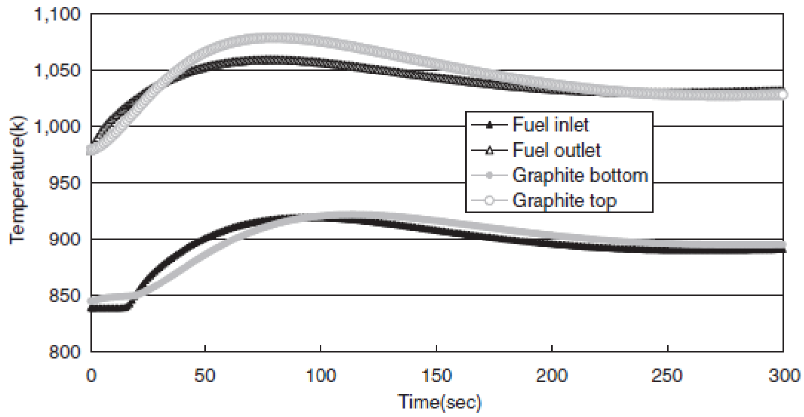


Figure 37: Temperature increase in case of a break of type 3 [33]

The safety criterion is met. Therefore, the only problem in a depressurization accident is the management of the leaked fuel salt. The spilled salt is collected in a catch pan, and then redirected to an emergency drain tank surrounded by borated water. One may add that the worst case scenario is a break near the reactor inlet.

VI.1.4. Specific phenomena: salt with water and salt freezing

VI.1.4.i. Reaction between coolant salt and water

The reaction between hot molten salt and water is still a current research topic. When the hot material is not soluble, like lava with water for example, an interface between the hot lava and water is created. According to the lava viscosity, a larger interface would be created, thus leading to a steam explosion. The only parameter affecting the production of a steam explosion is the viscosity of the lava. The limit is estimated to be around 1.37E2 poises, well above the viscosity of the molten salts [59]. However, for MSRs, the salt is soluble with water. Thus, one can suppose that interface creation and mixing of salt with water are competing effects in the present case.
An experiment destined to test this phenomenon was performed in 1955 [60]. 230 kg of molten salts at 815℃ were injected into a water bath under the water level. No steam explosion occurred. However, the temperature and the pressure conditions did not correspond to the operating conditions of the FUJI-233Um reactor. Moreover, in the case of a SGTR, water is injected into hot salt and not the inverse. Therefore, further experiments are needed. However, in this study, it is supposed that no steam explosion can occur.

VI.1.4.III. Freezing

This phenomenon has to be studied in order to understand when it could happen or not. There are two places where it could happen, at the heat exchanger between the primary and secondary salt circuit, and at the steam generator between the cooling circuit and the secondary salt circuit. Indeed, the melting point of the primary fuel salt is about 500˚C, and the temperature of the secondary salt at the inlet of the heat exchanger is about 454˚C. Thus, a flow reduction in the primary loop causes an overcooling, and possibly a freezing, of the fuel salt in the heat exchanger. The same holds at the steam generator. The melting point of the secondary salt is about 380˚C. A flow reduction in the secondary salt causes an overcooling of the secondary salt, possibly leading to a freezing in the steam generator.

A freezing corresponds to a volume shrinking. Thus, a pipe break due to freezing is impossible to occur. However re-melt accidents may happen, for example at the freezing valve. The freezing plug begins to melt, starting from the centre and like a needle; it means that the melt still cannot circulate through the valve. The expansion of the salt due to the melting will create a radial stress on the pipe where the valve is, possibly leading to a break of the pipe and a failure of the valve. However, the ORNL explained that they froze and melt it 100 times without problem [57].

When the reactor is scrammed, the power decreases quickly to the decay heat level. If the different cooling flows are not reduced, then a freezing at the heat exchangers could occur. When freezing occurs, a plug is created and the flow stops. It leads to core overheating and vessel damage if no action is taken. In order to estimate the time necessary for the freezing to occur, a MATLAB script simulating the different exchanges of heat was written. The heat transfer model used was the Newton's law of cooling with the heat transfer coefficients given in reference [20]. The result is that freezing occurs after some seconds. This result is validated by another study on MSFR [61]. That is why, in the event trees, an automatic reduction of the load after a scram is considered. A human action is not credited because of the short time window. More details can be found in Appendix 7.

VI.2. Accident progression

These considerations help to build accident progression diagrams. The diagrams try to be as general as possible, representing the categories defined in part IV.2. One example for a SGTR is given below. The other diagrams are presented in Appendix 4.

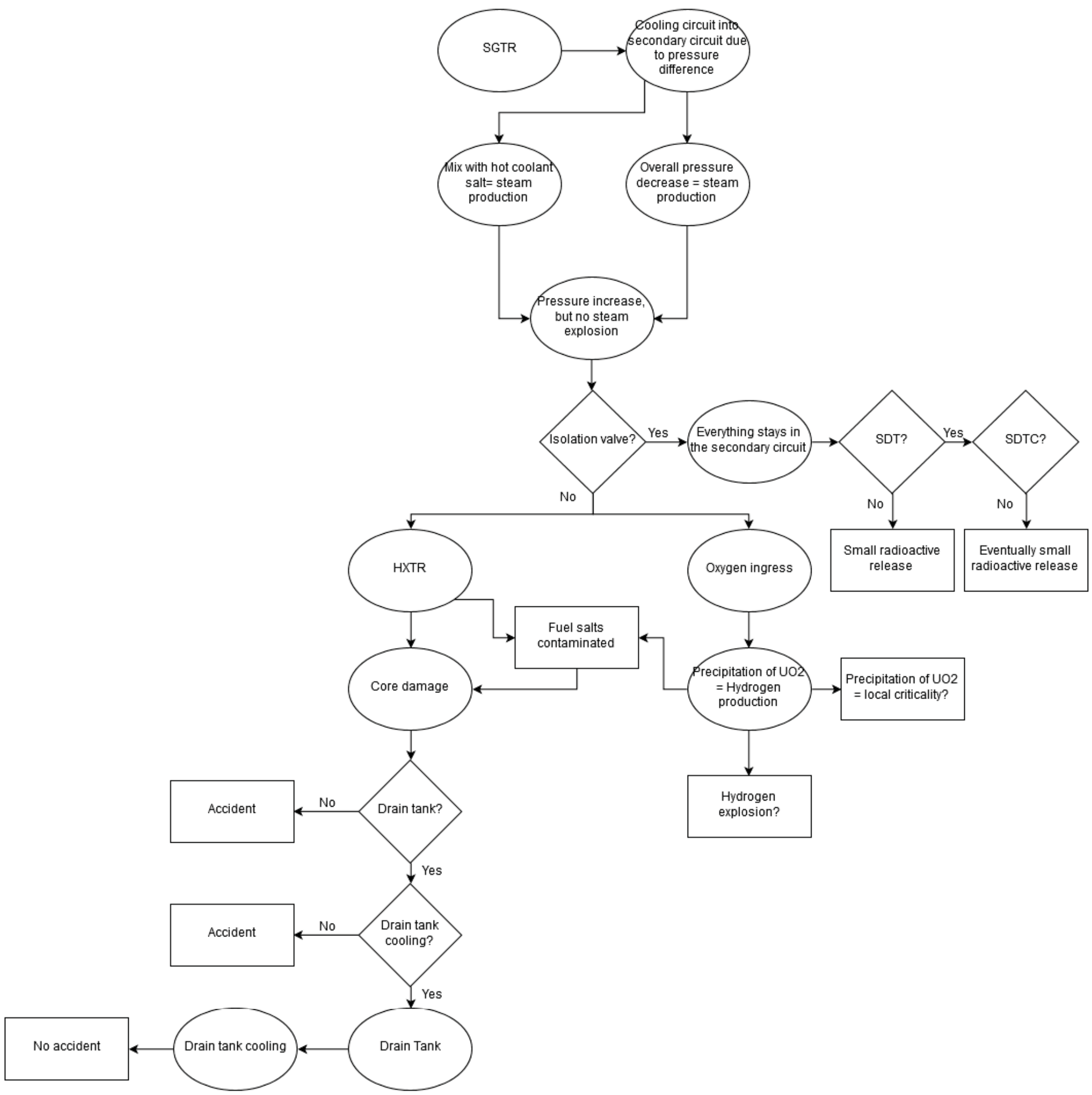


Figure 38: Flowchart of the accident progression during a Steam Generator Tube Rupture

The particular case of a SGTR needs attention. Indeed, in a previous section, it was suggested that further experiments are needed in order to evaluate if a steam explosion occurs when water enters the secondary circuit. But aside from this consideration, when rupture disks or isolation valves (i.e. relief valves isolating the secondary circuit from the primary circuit in case of a pressure increase) fail to act, the pressure increase in the secondary circuit could lead to a HXTR. Moreover, it would result in oxygen ingress into the primary circuit, thus a fissile precipitation with hydrogen production (hydrogen production can be reduced by using purified water in the tertiary circuit). In the end, the fuel salts would be contaminated so that shutdown would be mandatory and re-startup capability of the reactor would be lost. The particular consequences of this scenario will have to be evaluated in a future work (hydrogen explosion? Local criticality due to the UO_2 stack?). Eventually, this accident is very unlikely to happen, and safety improvements are suggested in the last sections in order to prevent such accident to occur.

Now that accident progressions are well understood, event trees can be built and quantified thanks to the failure rates estimated in Chapter V.

VI.3. Event trees

Event trees are built by studying the response of SSCs to the corresponding IEs defined in part IV.2. The event trees are developed using the software RiskSpectrum®. They can be found in Appendix 5 – part 2.

It is important to notice that only one train is implemented for every safety systems. The aim of this choice is to add redundancy only if needed. Indeed, the problem arising from the current practice (Single Failure Criterion) is the necessary redundancy to withstand a single failure in plant's response to particular events. Using reliability criteria, more redundancy and diversity are added for frequent events, whereas less redundancy and diversity are necessary for non-likely events (thus decreasing cost and complexity).

When ETs are built, LBEs are identified at the same time. And once LBEs are identified, they can be classified according to their frequency. At the end of this section, particular cases are presented, where "particular" means that their IE frequency could not be evaluated. Therefore, reliability criteria are determined for their maximal frequency.

VI.3.1. Identification and classification of LBEs

The ET development corresponds to the LBE identification. Indeed, by building ETs, scenarios are created and quantified. Then, this quantification allows a classification of the LBEs identified. An example is given in Figure 39 where AOOs, DBEs, and BDBEs are identified. Scenario with a frequency higher than 1E-8 are considered, in case the upper bound of their uncertainty is higher than the BDBE limit. However, in this study, since the uncertainty is not considered, they are just classified as CSDRD (considered) without further treatment.

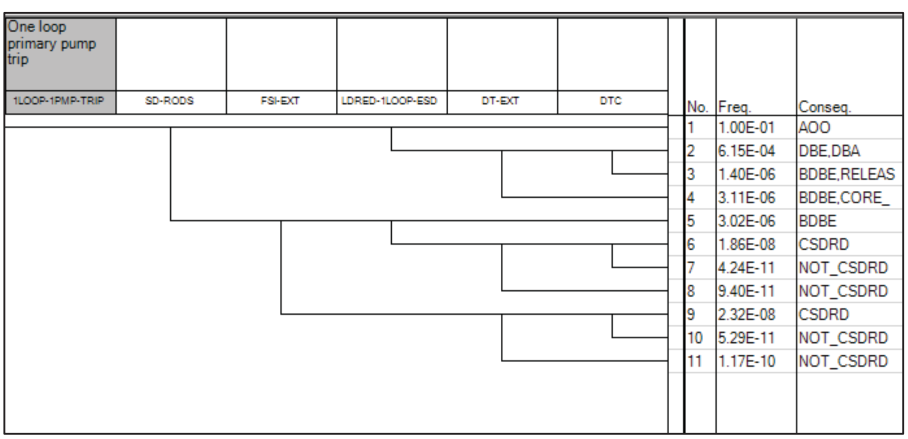


Figure 39: Example of event tree with AOO, DBE, and BDBEs identified

The LBE classification is in the column consequences since it comes from their frequency value. The most important LBEs for this study are the DBEs and the BDBEs since they are used to identify safety-related SSCs. Once the latter are defined, DBAs are identified as DBEs where only the safety-related SSCs are available. Moreover, a special treatment is applied to SSCs identified as safety-related in order for them to meet certain reliability objectives (see further section). Thus a particular attention should be paid to these systems.

VI.3.2. Particular cases

From the section V.3., one missing and one highly uncertain IE failure rate were identified: the cold loop startup and the failure of the fuel salt injection. For these two particular cases, safety criteria are defined in terms of maximal frequency, so that no release or no vessel damage could happen.

VI.3.2.i. Cold loop startup

The only data available was from IAEA-TECDOC-719 [62]. First this value is uncertain by itself (only a maximal frequency), and second this value was calculated for PWRs. When building the event tree, the upper bound value for the initiating event is assigned, as can be seen on Figure 40.

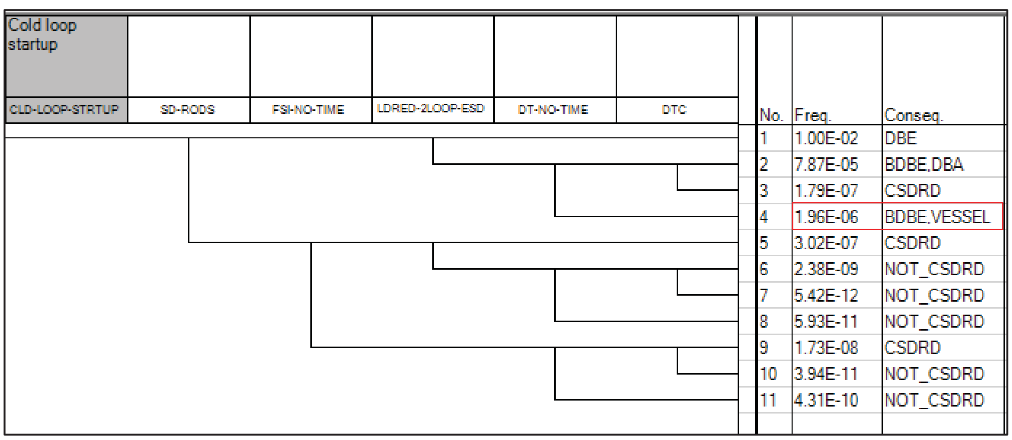


Figure 40: Cold loop startup event tree

According to the event tree, there is no possible release after a cold loop startup. However, vessel damage (more than 1% plastic deformation of the reactor vessel) may happen. The accident progression is as follow:

- No flow reduction means Loss Of Flow (LOF) either at the tertiary circuit or secondary circuit
- Loss of flow implies overheating (LOHS)
- Since the drain tank does not actuate (freeze valve FTO), the hot salt stays in the primary circuit
- After some time, the thermal stress (together with the gravity) would imply plastic deformation of the reactor vessel, thus vessel damage.

As explained in the section IV.3.6., this event happens very quickly (some minutes) that is why the case "barely no time available" is considered for the Human Reliability Analysis. In the end, this initiating event does not lead to vessel damage if the initiating event frequency is below 2.55E-3, what is presumably true since 1E-2 is an upper bound. Otherwise, the reliability of the drain tank has to be increased or another cooling system has to be implemented.

VI.3.2.III. Failure of the fuel salt injection system

The same approach is used for the failure of the fuel salt injection system. However, its frequency is missing and not highly uncertain, that is why an arbitrary value of 1 per reactor-year is assigned. One may notice that the maximum initiating event frequency of this IE is 12 per reactor-year since fresh fissile fuel is injected once every month.

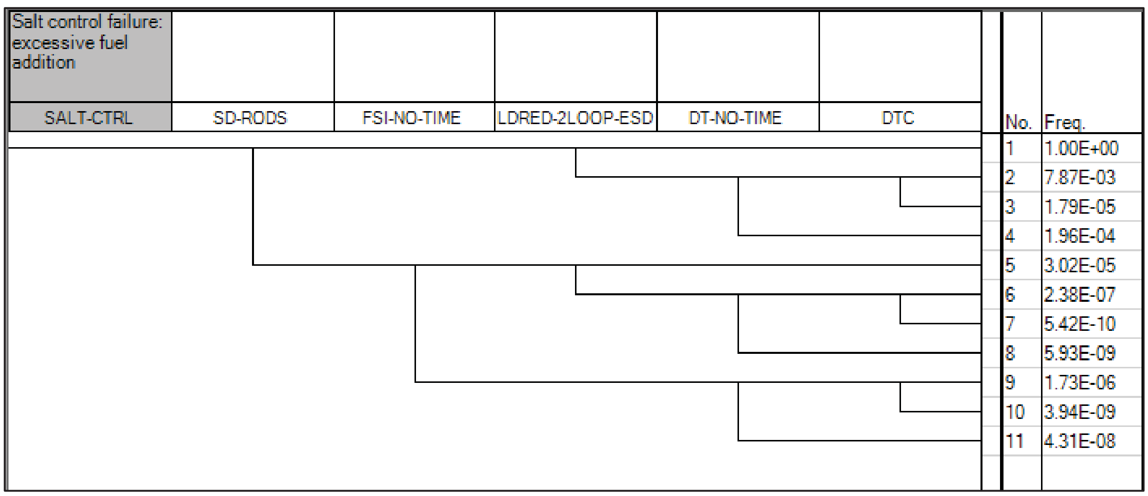


Figure 41: Fuel salt injection failure event tree

According to the event tree, there is possible release after salt control failure. Indeed, if no cooling is performed when salts enter the DT, then the latter will melt, leading to radioactive release. In order to remove this possibility, the IE frequency should be lower than 2.79E-2/r.y., (corresponding to a failure frequency of 0.34 per injection). Moreover, vessel damage may happen the same way as previously. In order to remove this possibility, the IE frequency should be lower than 2.55E-3. It means the failure frequency should be lower than 3E-2 per injection. Another way of screening the vessel damage out would be to increase the reliability of the drain tank or to add another cooling system. In the last section of this report is proposed another possible cooling system in case of emergency.

VII. The PSA model: design safety analysis

In order to build the PSA model, IEs were identified and grouped in Chapter IV. Then, accident scenarios, analyses of parameter evolutions and potential consequences were performed to develop ETs in Chapter VI. Consequently, the ETs were quantified using inputs developed from the MSR-specific database built in Chapter V. LBEs were identified when building the ETs. Then, LBEs were classified according to their frequency in the last section. The main result of the study is that, even if we could not affirm it (no transport calculation), it seems that **every LBE comply with the TLRC**. Indeed, there is noticeable release only if the drain tank cooling fails, which would only lead to the release of a rather small amount of radioactive material since the radionuclides are imprisoned in the liquid salts, themselves contained in the drain tank cell. The only uncertain release concerns an off-gas system leakage, which will have to be evaluated in a near future. Supposing LBEs comply with the TLRC, SR-SSCs classification can be performed and DBAs can be defined.

In order to prove the safety of the FUJI-233Um, the author proposes to define two more restrictive DBE criteria, which would replace the DBE TLRC, and which could be verified more easily by avoiding the need for transport calculation. They are radioactive release and vessel damage. In this part, we will see that very simple design changes would reduce the release and vessel damage frequencies by far, as well as the amount of radioactive material released. These changes eliminate all DBEs with vessel damage or radioactive release. One might need to remember that DBEs are scenarios, whose frequencies are between 1E-2/r.y. and 1E-4/r.y. Please refer to section II.1.1. for more details.

At the end of this Chapter, SR-SSCs and DBAs are defined. Two different identifications are performed by considering the two different criteria (TLRC and vessel damage + TLRC). Indeed, we will see that DBAs definition only considering the TLRC as safety criteria does not meet the Defence-in-Depth (DiD) principles.

In the two next sections are presented the main initiating events leading to radioactive release or vessel damage. This "or" is exclusive. Indeed, vessel damage may cause a fuel leak in the High Temperature Containment (HTC). However, every leak will be caught by the catch pan leading to the emergency drain tank. The emergency drain tank, together with its cooling, is a safety-related system with high reliability. Thus, if the EDT is assumed to fail, then this scenario would be classified as non-considered, i.e. its frequency would be below the consideration limit. Therefore, no release is considered in case of vessel damage due to this probabilistic cut-off. On the other hand, the results show that a release implies the failure of an auxiliary component of the reactor: the SDT or the DT. Thus, no vessel damage is involved during release. The study of these scenarios can therefore be performed separately.

VII.1. Identification of components involved in radioactive release

Safety weaknesses are easy to identify thanks to the NGNP methodology. Since the criteria are scenario-specific, specific scenarios not respecting the criteria can be identified. Once the exhaustive list of non-acceptable scenarios is established, components involved in scenarios that violate the criteria can be identified. The identification is done through the use of importance measures. These systems are defined as critical.

VII.1.1. Use of importance measures

Risk importance measures are dependent on the unwanted event to be studied. In the present case, the IMs will be developed according to release or vessel damage. According to the reference [63], "the Fussell-Vesely importance measure alone is able to identify potential components for safety improvements". That is why the Fussell-Vesely IM is chosen as being adequate to identify safety weaknesses of the FUJI-U233m reactor. The risk equation relative to a specific unwanted event can be written as follow:

$$R = R_{s,x_i} + R_{s,\bar{x}_i}$$

Where R_{s,x_i} corresponds to the cutsets containing the basic event X_i, which represents here the unavailability of component i, and where $R_{s,\bar{x}_i}$ corresponds to the cutsets not containing X_i. If the basic event is independent from the other basic events of the risk equation, one has:

$$R_{s,x_i} \sim X_i$$

Hence:

$$R(X_i) \sim a * X_i + b$$

The Fussell-Vesely IM is then defined as follow:

$$FV = \frac{R_{s,x_i}}{R} = \frac{aX_i}{aX_i+b} \sim \frac{a}{b} X_i \text{ when } aX_i \ll b \qquad [63]$$

As can be seen, the FV IM is approximately proportional to the unavailability of the component risk significance considered. That is why the FV IM directly shows the component unavailability effect on the unwanted event.

In the next parts, the FV IM will be used to identify components involved in radioactive release or vessel damage. In order to identify the components involved, a preliminary identification of scenarios with vessel damage or release is necessary.

VII.1.2. Main initiating events leading to radioactive release

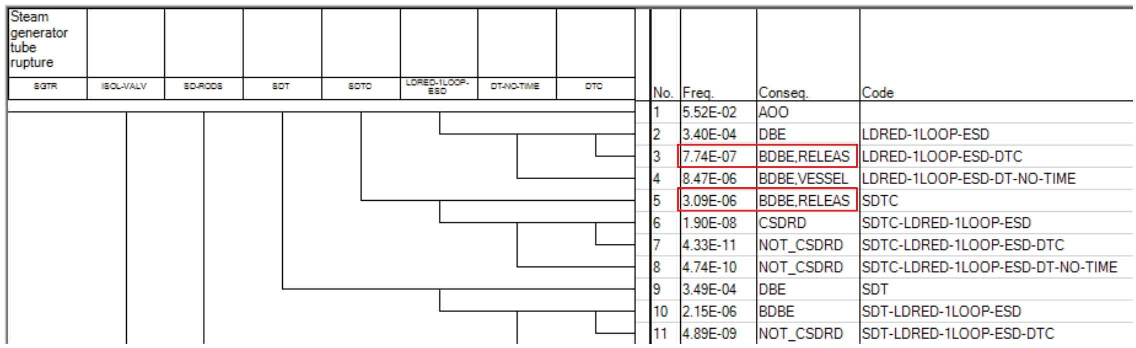
The aggregated release frequency is equal to 1.23E-3/r.y, whereby the amount and type of radioactive material may vary widely among the scenarios. In order to reduce this value, design improvements will be suggested (see section VII.4.). Scenarios with release are identified if:

- the DT cooling fails, given the freeze valve successfully opened (possibly large release)

- the SDT cooling fails, given the SDT valve successfully opened (small release)

Indeed, if no cooling is performed when salts enter the DT or SDT, then the latter will melt, leading to radioactive release.

For example, in Figure 42, the scenarios identified by a red frame lead to release. One is due to the failure of the DTC given the freeze valve opened. The other is due to the failure of the SDTC given the secondary freeze valve opened.



No.	Freq.	Conseq.	Code
1	5.52E-02	AOO	
2	3.40E-04	DBE	LDRED-1LOOP-ESD
3	7.74E-07	BDBE,RELEAS	LDRED-1LOOP-ESD-DTC
4	8.47E-06	BDBE,VESSEL	LDRED-1LOOP-ESD-DT-NO-TIME
5	3.09E-06	BDBE,RELEAS	SDTC
6	1.90E-08	CSDRD	SDTC-LDRED-1LOOP-ESD
7	4.33E-11	NOT_CSDRD	SDTC-LDRED-1LOOP-ESD-DTC
8	4.74E-10	NOT_CSDRD	SDTC-LDRED-1LOOP-ESD-DT-NO-TIME
9	3.49E-04	DBE	SDT
10	2.15E-06	BDBE	SDT-LDRED-1LOOP-ESD
11	4.89E-09	NOT_CSDRD	SDT-LDRED-1LOOP-ESD-DTC

Figure 42: Identification of scenarios with release

Once scenarios with release are identified, a diagram representing the main IEs leading to release can be established in Figure 43 (IE absent if it contributes less than 3% to release).

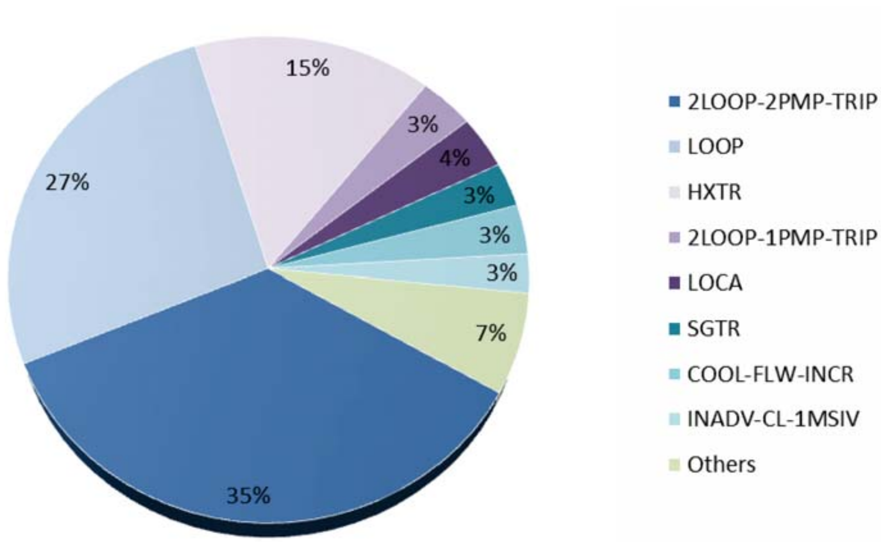


Figure 43: Main IEs leading to radioactive release (Total = 1.23E-3/r.y.)

One may add that the amount of radioactive material released is not taken into account in the last diagram. For the SDTC failure, the release is very small; only a small amount of tritium, which was not removed from the secondary loop by the off-gas system. Concerning the DTC failure, the amount released can be consequent, thus an improvement of it has to be done. Improvements are suggested in the last section of the report.

It is important to notice that the IE "off-gas system leakage" is not taken into account in this section because its study has been done separately in a previous part. Off-gas system leakage necessarily leads to release. Moreover, it has been demonstrated that the maximum off-gas system release frequency is equal to 2.88E-5/r.y. It represents around 22% of the total release frequency from the core.

VII.1.3. Systems involved in radioactive release

The FV IMs of the different critical systems involved in radioactive release are given below:

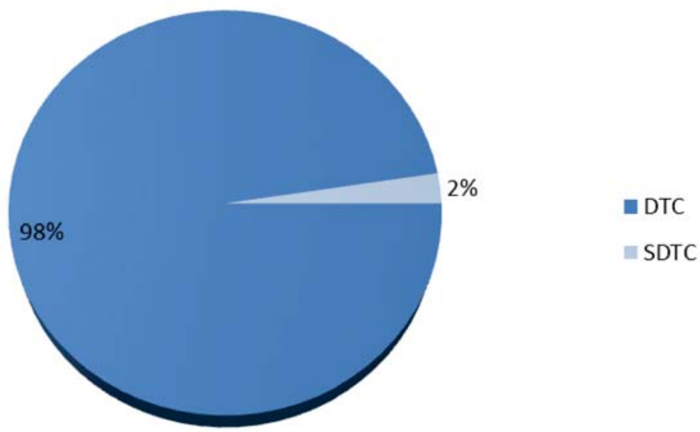


Figure 44: Components causing release (Total = 1.23E-3/r.y.)

The critical systems are "drain tank cooling" and "secondary drain tank cooling". One has to notice that SDTC failure never means large release. Indeed, the source term would only consist of tritium that migrated from the primary circuit to the secondary, and that was not removed by the off-gas system. Moreover, it has to go outside of the coolant salt cell. Basically, the only critical system leading to a non-negligible release is the DTC. Suggestions for improvements are given in section VII.3.

One may also notice that only one component is involved in non-negligible radioactive release (without considering the off-gas system leakage). Therefore, if the DTC reliability is increased, one could affirm that there is no significant release for the FUJI-233Um design according to the NGNP methodology (except for the off-gas system).

Strictly speaking, there are other scenarios involving other systems leading to release. However, scenarios with failure of these systems have a frequency below the consideration limit. Therefore, they are not considered in the licensing process. It can be noticed that the aggregated frequency of the non-considered scenarios is equal to 6.54E-6/r.y. Knowing that the total release frequency is equal to 1.23E-3/r.y., the other systems together contribute to maximum 0.5% of the total release, which is negligible.

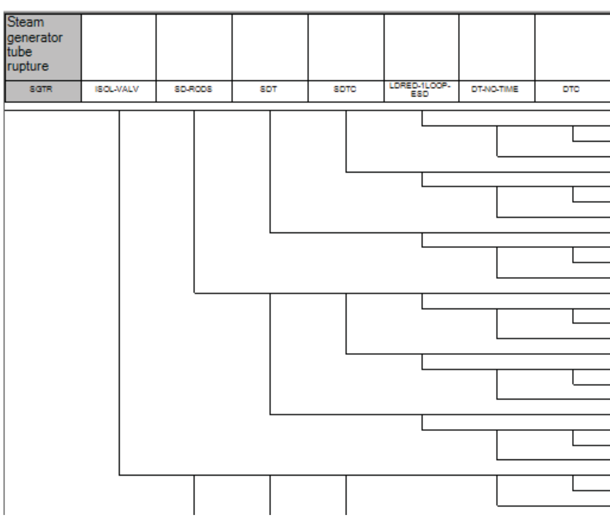
VII.2. Identification of components involved in vessel damage

The same analysis can be performed concerning vessel damage. Vessel damage means loss of integrity of the reactor vessel. In the present case, vessel damage never means release since everything leaking from the reactor vessel will be drained to the emergency drain tank, which has a very high reliability (according to the NGNP methodology, if the EDT fails, such scenario would be screened out).

VII.2.1. Main initiating events leading to vessel damage

The aggregated vessel damage frequency is equal to 3.12E-3/r.y. This value is quite high compared to the core damage frequency for LWR licensing. Therefore, improvements in the design will have to be suggested (see last section). A scenario with vessel damage is identified in case of prolonged LOHS, together with drain tank unavailability, or in case of an SGTR with failure of the isolation valve.

For example, in Figure 45, the two scenarios identified by a red frame lead to vessel damage; one due to the absence of core cooling when the DT is unavailable and one due to the isolation valve failure.



No.	Freq.	Conseq.	Code
1	5.52E-02	AOO	
2	3.40E-04	DBE	LDRED-1LOOP-ESD
3	7.74E-07	BDBE,RELEAS	LDRED-1LOOP-ESD-DTC
4	8.47E-06	BDBE,VESSEL	LDRED-1LOOP-ESD-DT-NO-TIME
5	3.09E-06	BDBE,RELEAS	SDTC
6	1.90E-08	CSDRD	SDTC-LDRED-1LOOP-ESD
7	4.33E-11	NOT_CSDRD	SDTC-LDRED-1LOOP-ESD-DTC
8	4.74E-10	NOT_CSDRD	SDTC-LDRED-1LOOP-ESD-DT-NO-TIME
9	3.49E-04	DBE	SDT
10	2.15E-06	BDBE	SDT-LDRED-1LOOP-ESD
11	4.89E-09	NOT_CSDRD	SDT-LDRED-1LOOP-ESD-DTC
12	5.36E-08	CSDRD	SDT-LDRED-1LOOP-ESD-DT-NO-TIME
13	1.67E-06	BDBE	SD-RODS
14	1.03E-08	CSDRD	SD-RODS-LDRED-1LOOP-ESD
15	2.34E-11	NOT_CSDRD	SD-RODS-LDRED-1LOOP-ESD-DTC
16	2.56E-10	NOT_CSDRD	SD-RODS-LDRED-1LOOP-ESD-DT-NO-TIME
17	9.33E-11	NOT_CSDRD	SD-RODS-SDTC
18	5.74E-13	NOT_CSDRD	SD-RODS-SDTC-LDRED-1LOOP-ESD
19	1.31E-15	NOT_CSDRD	SD-RODS-SDTC-LDRED-1LOOP-ESD-DTC
20	1.43E-14	NOT_CSDRD	SD-RODS-SDTC-LDRED-1LOOP-ESD-DT-NO-TIME
21	1.05E-08	CSDRD	SD-RODS-SDT
22	6.49E-11	NOT_CSDRD	SD-RODS-SDT-LDRED-1LOOP-ESD
23	1.48E-13	NOT_CSDRD	SD-RODS-SDT-LDRED-1LOOP-ESD-DTC
24	1.62E-12	NOT_CSDRD	SD-RODS-SDT-LDRED-1LOOP-ESD-DT-NO-TIME
25	2.01E-04	DBE,VESSEL_D	ISOL-VALV
26	4.58E-07	CSDRD	ISOL-VALV-DTC
27	5.01E-06	BDBE,VESSEL_	ISOL-VALV-DT-NO-TIME

Figure 45: Identification of scenarios with vessel damage

Once scenarios with vessel damage are identified, a diagram representing the main IEs leading to vessel damage can be established in Figure 46 (IE absent if it contributes less than 2% to vessel damage).

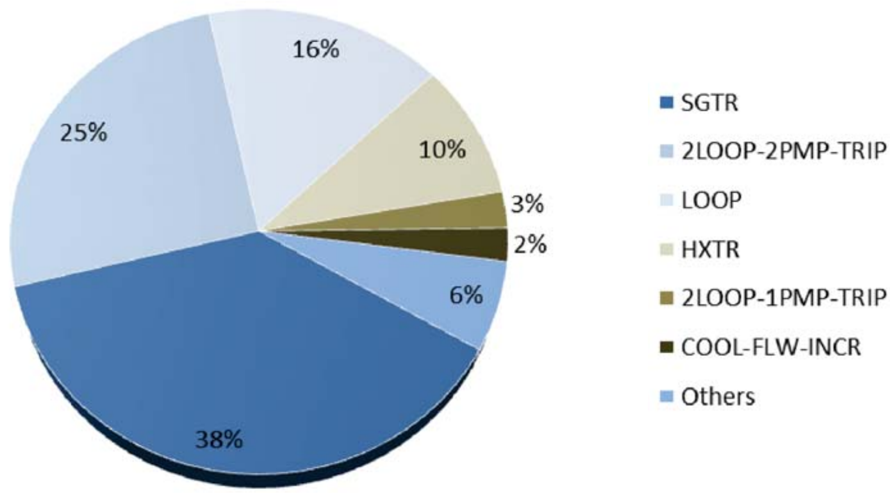


Figure 46: Main IEs leading to vessel damage (Total = 3.12E-3/r.y.)

As can be seen, the SGTR is the main contributor to vessel damage, because, in addition to possible prolonged LOHS without DT, the isolation valve may fail, leading to vessel damage too. The second most important IE is a scenario not identified as by the Japanese analysis from reference [3]. That is why the design has to be modified in order to remove possible vessel damage during this scenario.

If we consider that vessel damage is as unwanted as release, then we can aggregate the total unwanted event frequencies by adding the result from the two pie charts (remember the two events are exclusive). The main results are presented in Table 12.

Table 12: Ranking of the different IEs according to their unwanted event frequencies

Initiating events	Aggregated frequency (/r.y.)
2LOOP-2PUMP-TRIP	1.40E-03
LOOP	1.04E-03
HXTR	5.91E-04
SGTR	5.61E-04
2LOOP-1PUMP-TRIP	1.31E-04
LOCA	1.25E-04
COOL-FLW-INCR	1.18E-04
INADV-CL-1MSIV	9.36E-05

All in all, the four IEs requiring particular attention are:

- Steam Generator Tube Rupture
- Total loss of secondary salt flow in the two loops
- Loss of offsite Power
- Heat eXchanger Tube Rupture

One may remark that LOCA and RIA, which are DBAs in the LWR licensing, are not critical in terms of safety according to the NGNP methodology.
Indeed, a LOCA is not particularly safety relevant since the catch pan and the EDT will collect the spilled salt (if failure, the scenario is screened out), without possible release or vessel damage (except the break obviously). An RIA is not safety relevant since MSRs have a very negative temperature reactivity coefficient and a small excess reactivity. One may refer to section VI.1. for quantitative justifications.

VII.2.2. Systems involved in vessel damage

The FV IMs of the different critical safety functions involved are given below:

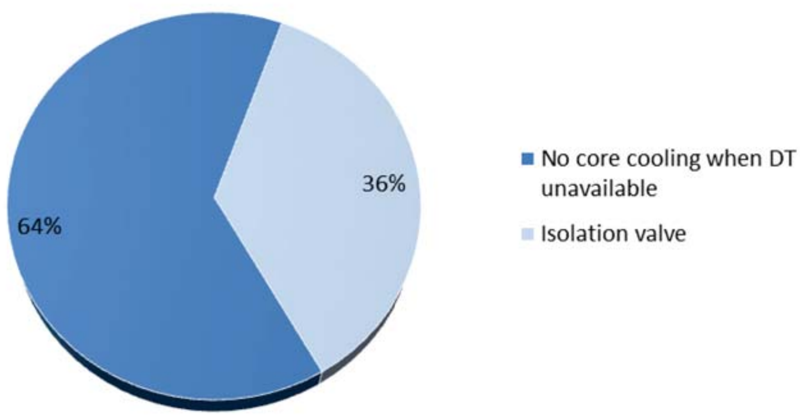


Figure 47: Components causing vessel damage (Total = 3.12E-3)

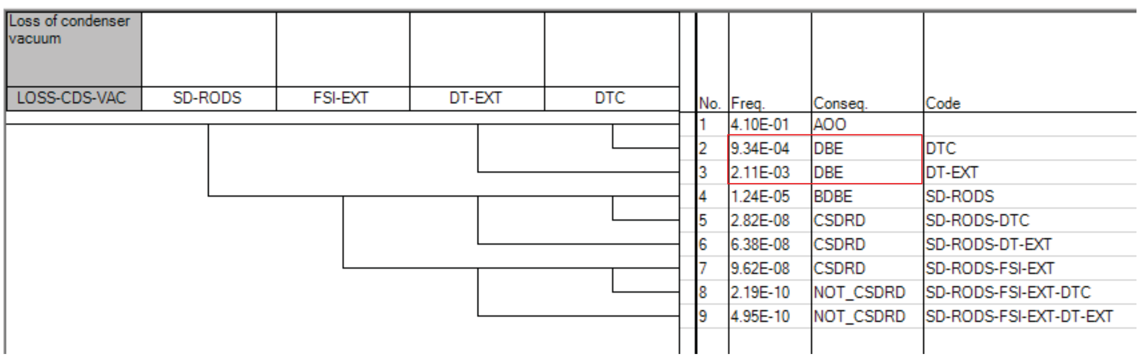
The critical systems are "DT & core cooling failures" and "Isolation valve failure". One has to notice that there are really few systems involved in vessel damage scenarios. It means that if the reliability of such systems is improved, scenarios with vessel damage could be screened out, so that no vessel damage would happen according to the NGNP methodology.

Strictly speaking, there are other scenarios involving other systems leading to vessel damage. However, scenarios with failure of these systems have a frequency below the consideration limit. Therefore, they are not considered in the licensing process. It can be noticed that the aggregated frequency of the non-considered scenarios is equal to 6.54E-6/r.y. Knowing that the total vessel damage frequency is equal to 3.12E-3/r.y., the other systems together contribute to maximum 0.2% of the total release, which is negligible.

VII.3. Suggestions for safety improvements

The two critical safety systems identified are the DTC and the isolation valve. Suggestions to improve their reliabilities are presented in this section. Moreover, the most important safety weakness identified is the absence of core cooling in case of a LOHS without DT (freeze valve did not open). Suggestions to overcome this weakness are also presented in this section.

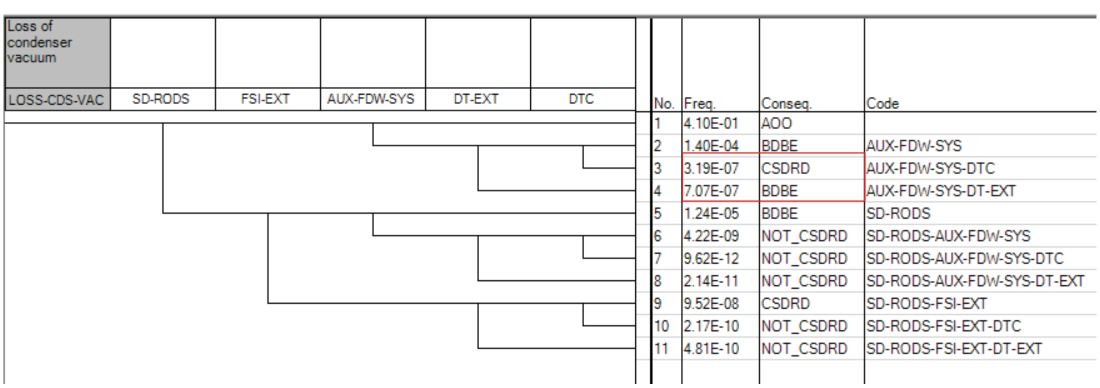
The first improvement suggested concerns core cooling without DT when the IE affects the water cooling loop. An auxiliary feedwater system has never been mentioned in a paper related to the FUJI-233Um reactor. Thus, it was not considered in a preliminary design. However, when looking at the event tree in Figure 48, it can be noticed that a cooling system is necessary when the freeze valve does not open, since a loss of condenser vacuum leads to a LOHS, and since no load reduction is possible. Moreover, this scenario is a DBE (likely to happen). Therefore, improvements have to be made in order to reduce the probability or mitigate the consequences of such scenario.



No.	Freq.	Conseq.	Code
1	4.10E-01	AOO	
2	9.34E-04	DBE	DTC
3	2.11E-03	DBE	DT-EXT
4	1.24E-05	BDBE	SD-RODS
5	2.82E-08	CSDRD	SD-RODS-DTC
6	6.38E-08	CSDRD	SD-RODS-DT-EXT
7	9.62E-08	CSDRD	SD-RODS-FSI-EXT
8	2.19E-10	NOT_CSDRD	SD-RODS-FSI-EXT-DTC
9	4.95E-10	NOT_CSDRD	SD-RODS-FSI-EXT-DT-EXT

Figure 48: Loss of condenser vacuum before adding an auxiliary feedwater system

The author decided to implement an auxiliary feedwater system in order to reduce the risk of a LOHS due to a tertiary circuit failure when the drain tank is unavailable. The result is given below:



No.	Freq.	Conseq.	Code
1	4.10E-01	AOO	
2	1.40E-04	BDBE	AUX-FDW-SYS
3	3.19E-07	CSDRD	AUX-FDW-SYS-DTC
4	7.07E-07	BDBE	AUX-FDW-SYS-DT-EXT
5	1.24E-05	BDBE	SD-RODS
6	4.22E-09	NOT_CSDRD	SD-RODS-AUX-FDW-SYS
7	9.62E-12	NOT_CSDRD	SD-RODS-AUX-FDW-SYS-DTC
8	2.14E-11	NOT_CSDRD	SD-RODS-AUX-FDW-SYS-DT-EXT
9	9.52E-08	CSDRD	SD-RODS-FSI-EXT
10	2.17E-10	NOT_CSDRD	SD-RODS-FSI-EXT-DTC
11	4.81E-10	NOT_CSDRD	SD-RODS-FSI-EXT-DT-EXT

Figure 49: Loss of condenser vacuum after adding an auxiliary feedwater system

As can be seen by comparing Figure 48 and 49, scenarios with vessel damage and release have now a lower frequency (near the exemption limit). It is also the case for the other similar event trees (see Appendix 5 – part 2). In the end, the implementation of an auxiliary feedwater system is recommended for the FUJI design. The AFWS would be used for the following IEs:

- Loss of condenser vacuum
- Inadvertent closing of the MSIVs
- Total loss of feedwater

However, LOHS can also result from a loss of secondary salt flow (see Figure 50). In this particular case, the auxiliary feedwater system cannot be used to cool the core, so that the scenario numbered 3 leads to vessel damage. Moreover, it is a DBE, so this scenario is likely to happen.

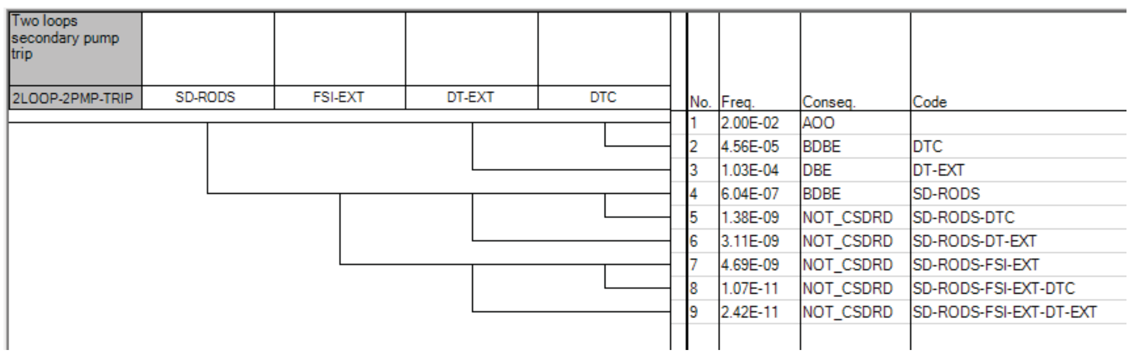


Figure 50: Event tree for the initiating event "2 secondary pump trips"

In this case, the improvement proposed would be to use the accommodation line in order to transfer the hot salt from the core to the drain tank, where it will be cooled, and to use the fuel salt injection line to re-inject the cooled salt into the core. The procedure would be as follow:

- Fertile salt is injected in order to increase the salt volume in the primary circuit
- Hot fuel salt is lighter than cold fuel salt, so it will be withdrawn at the pump bowl by the accommodation line
- Cold fuel salt is heavier than hot fuel salt, so after being injected at the pump bowl, it will go down to cool the core

The main advantage of this suggestion is that no system is added. However, thermodynamic studies have to be performed in order to verify that this solution effectively cools the core.

Another solution consists of having an auxiliary loop in the secondary circuit. But this solution adds another system in the design, thus increasing costs and complexity.

The second system identified as critical is the drain tank cooling. Moreover, if its reliability is increased, it would mean that there is practically no release during the operation of the FUJI-233Um reactor (only small traces of tritium confined in the secondary circuit cell). It would be a strong advantage over the other reactors. In order to increase its reliability, two solutions are proposed.

The first one, and the simplest one, would be to add another cooling loop in parallel of the first one. However, since the design and operating parameters would be sensibly the same, the overall reliability would not be increased by much. Indeed, a passive system often fails because of the operating conditions, which are out of its operating range. Two systems in parallele see the same operating conditions. Thus, if one fails because of the operating conditions, the other would fail too. Moreover, since the systems are identical, the CCF parameter would be high.

The second solution is to add a borated water tank in a separate cell and above the drain tank cell, together with a temperature sensor and explosive valves in parallel. When the temperature of the fuel salts in the drain tank is too high, the temperature sensor sends a signal to open the explosive valves, thus flooding the drain tank cell. The reliability was calculated for one temperature sensor and two explosive valves in parallel. The failure probability of the DTC function is reduced from 5.96E-3 to 6.95E-5. With such reliability, every scenario with a drain tank cooling failure would be under the exemption limit. Therefore, according to the NGNP methodology, there would be no release due to DTC failure (and only traces of Tritium when the SDT fails, as well as fission gases when the off-gas system fails).

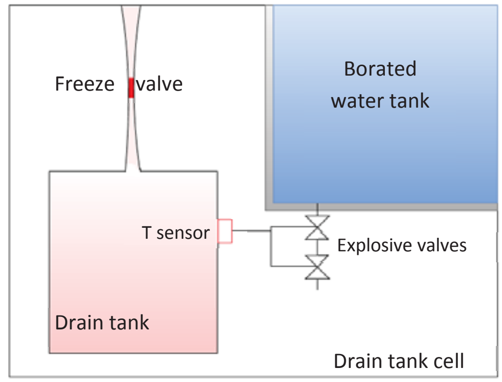


Figure 51: Suggestion to improve the DTC reliability

The last critical safety system identified is the isolation valve in case of a SGTR. This DBE does not lead to a release, but to vessel damage, which could be easily avoided by implementing rupture disks in addition to the isolation valve (or another isolation valve in parallel). One may note that an explosive valve was credited instead of a rupture disk in the PSA model. The generic failure rate for rupture disk is equal to 2E-6/h [64]. If the rupture disk is tested every 4 months, then an explosive isolation valve has approximately the same reliability as a rupture disk.

Once these improvements are made, the aggregated release frequency is reduced from 1.23E-3 to 2.62E-6 per reactor-year (every scenario with release due to DTC failure is below the consideration limit). But first of all, the source term during leakage becomes very small (thus the TLRC are met by orders of magnitude). Supposing the last solution proposed for core cooling is effective, the aggregated vessel damage frequency goes from 3.12E-3 to 8.94E-5 per reactor-year (every scenario with vessel damage is below the exemption limit except during a LOOP (injection not available)). It can be said that the system is now very safe in terms of release and vessel damage.
In the next sections, an improved design is sometimes considered. The following table summarizes what improvements have been done to the preliminary design:

Table 13: Summary of the improvements considered in the improved design

	Preliminary design	Improved design
AFWS	Absent	Present
DTC	One train	Diversity added: borated water tank in the DT cell
Isolation valve	One train	Diversity added: Rupture disk added
Core cooling given freeze valve failure	Absent	Use of the injection and accommodation lines + DTC to cool the core

A table summarizing the consequences in terms of frequency of the improvements suggested is given below:

Table 14: Summary of the improved systems suggested and their consequences in terms of safety

	Preliminary design	Improved design
Release (/r.y.)	1.23E-03	2.62E-06
DTC (failure probability)	5.96E-03	6.95E-05
Vessel damage (/r.y.)	3.12E-03	8.94E-05
Isolation valve[1] (failure probability)	3.63E-03	1.06E-05
Auxiliary feedwater system (failure probability)	absent	3.41E-04

It is important to notice that the SDT is supposed to be cooled by forced air cooling (see section V.3.2.). In this study, the SDT cooling consists of 2 fans in parallel. If one wants to decrease the release frequency to zero (even if it is not really necessary), one could think of putting more fans. All in all, the release frequency could be easily reduced to zero due to the probabilistic cut-off (without taking into account off-gas system releases).

VII.4. Identification of DBAs

DBAs are defined as DBE where only the SR-SSCs are considered available. Thus, a preliminary identification of SR-SSCs is necessary. Their identification is also useful to determine important systems, whose reliabilities have to be high. These systems have to meet certain reliability criteria to fulfil their mission: it is the aim of the "special treatment". The "special treatment" is used for the systems identified as SR to meet their reliability criterion. It consists of design considerations, qualification, control of changes, documentation, reporting, maintenance, testing, surveillance and quality assurance [16].

As mentioned, two different DBA identifications are performed by considering two different criteria (TLRC and vessel damage + TLRC). As mentioned, it will be shown in the next section that DBAs definition only considering the TLRC as safety criteria does not meet the DiD principles.

VII.4.1. Identification of TLRC-based SR-SSCs and DBAs

The only safety criteria considered in this section are the TLRC. Since the preliminary design from Chapter III, without improvements, seems to meet the TLRC, this design is considered in this section.

The first step for safety-related SSC classification is to determine the required safety functions for DBEs, where 'required' refers to functions that have to be successful during DBEs to meet the TLRC.

In order to meet the TLRC, the only required functions are "containment of large liquid radioactive release" and "mitigation of large gaseous radioactive release".

[1] Relief valve in case of secondary pressure increase

The next step for each required safety function is to examine the DBEs to determine which SSCs are available and have sufficient capability and reliability to meet the safety function. That is why a list of unavailable system together with their associated DBE is established in Table 15.

Table 15: List of unavailable systems during DBEs

DBEs	System unavailable
1LOOP-1PUMP-TRIP + SD_RODS[2] + DT + DTC	LDRED
1LOOP-2PUMP-TRIP + SD_RODS + DT + DTC	LDRED
2LOOP-1PUMP-TRIP + SD_RODS + DT + DTC	Nothing
2LOOP-2PUMP-TRIP + SD_RODS	DT + DTC
CLD-LOOP-STRTUP + SD_RODS + LDRED	Nothing
COOL-FLW-INCR + SD_RODS + DT + DTC	LDRED
FDW-TUBE-RUPT + SD_RODS + LDRED[3]	Nothing
FV-FAIL + SDRY_VALVE + SD_RODS + LDRED	Nothing
HXTR + SD_RODS + DT + DTC	Nothing
INADV-CL-1MSIV + SD_RODS + DT + DTC	LDRED
INADV-CL-2MSIV + SD_RODS + DT + DTC	LDRED
INADV-OP-SGRV + SD_RODS + DT + DTC	LDRED
LOCA + SD_RODS + DT + DTC + EDT + EDTC	Nothing
LOSS-CDS-VAC + SD_RODS + DT + DTC	LDRED
PART-LOSS-FDW + SD_RODS + DT + DTC	LDRED
SEC-LEAK + SD_RODS + SDT + SDTC + LDRED	Nothing
SEC-SALT-FLW-INCR + SD_RODS + DT + DTC	LDRED
SGTR + SD_RODS + DT + DTC + ISOL_VALVE[4] + SDT + SDTC	LDRED
SGTR + SD_RODS + ISOL_VALVE + LDRED	SDT + SDTC
SGTR + SD_RODS + DT + DTC + SDT + SDTC	ISOL-VALVE
TURB-TRIP + SD_RODS + DT + DTC	LDRED

The SSCs that have sufficient capability and reliability to perform these required safety functions are:

For the containment of large liquid radioactive release:

- The High Temperature Containment (HTC)
- The Emergency Drain Tank (EDT)
- The EDT Cooling (EDTC)

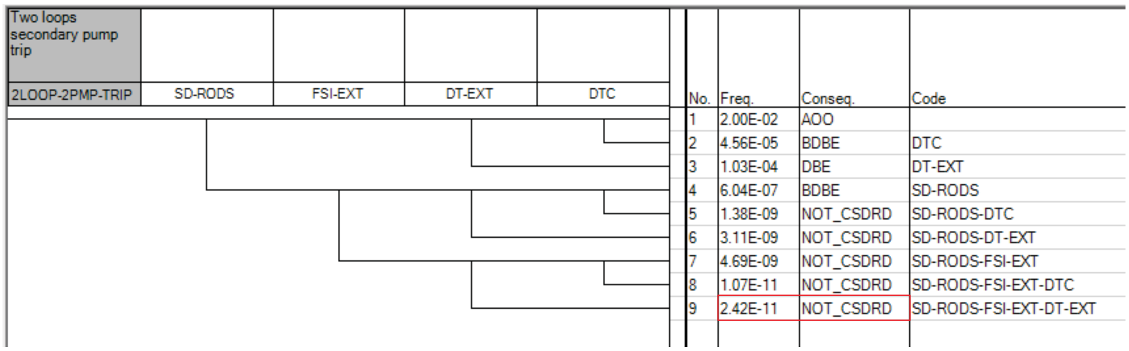
For the containment of large gaseous radioactive release:

- The auxiliary off-gas system
- The off-gas cell

The non-safety related systems are the load reduction system, the drain tank and its cooling, the secondary drain tank and its cooling, the fuel salt injection system, the isolation valve, the shutdown rods and the remaining structures.

[2] Insertion of shutdown rods
[3] Load reduction after emergency shutdown
[4] Relief valve in case of secondary pressure increase

DBAs are defined as DBEs where only the safety-related SSCs are considered available. According to the SR-SSCs identified, it means that in almost every ET, a DBA consists of vessel damage and eventually LOCA, but everything leaking from the primary circuit will be caught by the catch pan and redirected to the emergency drain tank (see Figure 52). In the end, the TLRC are met.



No.	Freq.	Conseq.	Code
1	2.00E-02	AOO	
2	4.56E-05	BDBE	DTC
3	1.03E-04	DBE	DT-EXT
4	6.04E-07	BDBE	SD-RODS
5	1.38E-09	NOT_CSDRD	SD-RODS-DTC
6	3.11E-09	NOT_CSDRD	SD-RODS-DT-EXT
7	4.69E-09	NOT_CSDRD	SD-RODS-FSI-EXT
8	1.07E-11	NOT_CSDRD	SD-RODS-FSI-EXT-DTC
9	2.42E-11	NOT_CSDRD	SD-RODS-FSI-EXT-DT-EXT

Figure 52: Example of DBA with vessel damage

However, is it appropriate to say that the DBAs are safe, even if the vessel is totally destroyed? That is why more restrictive criteria are defined in order to remove the possibility of vessel damage during DBAs. This consideration is an integral part of DiD (addition of one barrier: the reactor vessel) and is developed in the next section.

VII.4.2. Identification of SR-SSCs/DBAs related to vessel damage and release

The safety criteria considered in this study are the TLRC and vessel damage. Since the first design without improvements does not meet the criteria (more particularly vessel damage, see previous section), the improved design is considered in this section.

The two TLRC-based safety functions were identified in the last section. The safety functions related to vessel damage are found to be "Heat removal" and "Control of the core heat generation".

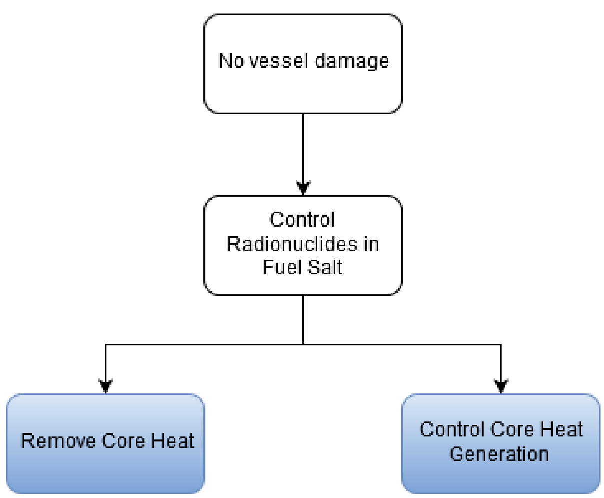


Figure 53: Diagram for the identification of Safety-Related functions

All in all, four safety functions are identified. The two first concern accident prevention and the two last concern accident mitigation:

- Control of the core heat generation
- Heat removal
- Containment of large liquid radioactive leakage
- Containment of large gaseous radioactive leakage

The next step for each required safety function is to examine the DBEs to determine which SSCs are available and have sufficient capability and reliability to meet the safety function. That is why a list of unavailable system together with their associated DBE is established in table 16. Please refer to Table 15 for the key.

Table 16: List of unavailable systems during DBEs

DBEs	System unavailable
1LOOP-1PUMP-TRIP + SD_RODS + DT + DTC	LDRED
1LOOP-2PUMP-TRIP + SD_RODS + DT + DTC	LDRED
2LOOP-1PUMP-TRIP + SD_RODS + DT + DTC	Nothing
2LOOP-2PUMP-TRIP + SD_RODS + DT + DTC	IMP-CORE-COOL
CLD-LOOP-STRTUP + SD_RODS + LDRED	Nothing
COOL-FLW-INCR + SD_RODS + DT + DTC	LDRED
FDW-TUBE-RUPT + SD_RODS + LDRED	Nothing
FV-FAIL + SCDRY_VALVE + SD_RODS + LDRED	Nothing
HXTR + SD_RODS + DT + DTC	Nothing
INADV-CL-1MSIV + SD_RODS + DT + DTC	LDRED
INADV-OP-SGRV + SD_RODS + DT + DTC	LDRED
LOCA + SD_RODS + DT + DTC + EDT + EDTC	Nothing
PART-LOSS-FDW + SD_RODS + DT + DTC	LDRED
SEC-LEAK + SD_RODS + DT + DTC + SDT + SDTC	Nothing
SEC-SALT-FLW-INCR + SD_RODS + DT + DTC	LDRED
SGTR + SD_RODS + DT + DTC + SDT + SDTC + ISOL_VALVE	LDRED
SGTR + SD_RODS + LDRED + ISOL_VALVE	SDT + SDTC
TURB-TRIP + SD_RODS + DT + DTC	LDRED

Therefore, the safety-related SSCs to control the core heat generation are:

- The drain tank (no graphite = no moderation = no power generation)
- The isolation valve (if secondary salt ingress, then no control of core heat generation)

The SR-SSC to remove heat is:

- The drain tank cooling

The SR-SSCs to contain large liquid radioactive leakage are:

- The emergency drain tank
- The emergency drain tank cooling

- The HTC

The SR-SSCs to contain large gaseous radioactive leakage are:

- The auxiliary off-gas system
- The off-gas cell

The non-safety related systems would be the load reduction system, the secondary drain tank and its cooling, the fuel salt injection system, the shutdown rods and the remaining structures.

Three SSCs are added to the initial list. It means that "special treatment" has to be applied to these systems, thus increasing cost and complexity. However, one more barrier (the reactor vessel) is implemented to prevent release, thus increasing the DiD. In the end, a safety margin is added to meet the TLRC.

The two lists of DBAs identified are presented in Table 17. Even if they have the same header (it is the IE), their scenarios are totally different. For example, in Figure 52, the scenario numbered 9 is a TLRC-based DBA, whereas the scenario numbered 7 is a DBA related to vessel damage and release. Fewer DBAs are present in the second list since the improved design is considered.

Table 17: Comparison of TLRC-based DBAs and DBAs related to vessel damage and release

TLRC-based DBAs	DBAs related to vessel damage and release
1LOOP-1PUMP-TRIP	1LOOP-1PUMP-TRIP
1LOOP-2PUMP-TRIP	1LOOP-2PUMP-TRIP
2LOOP-1PUMP-TRIP	2LOOP-1PUMP-TRIP
2LOOP-2PUMP-TRIP	2LOOP-2PUMP-TRIP
CLD-LOOP-STRTUP	CLD-LOOP-STRTUP
COOL-FLW-INCR	COOL-FLW-INCR
FDW-TUBE-RUPT	
FV-FAIL	FV-FAIL
HXTR	HXTR
INADV-CL-1MSIV	INADV-CL-1MSIV
INADV-CL-2MSIV	
INADV-OP-SGRV	INADV-OP-SGRV
LOCA	LOCA
LOSS-CDS-VAC	
PART-LOSS-FDW	PART-LOSS-FDW
SEC-LEAK	SEC-LEAK
SEC-SALT-FLW-INCR	SEC-SALT-FLW-INCR
SGTR	SGTR
TURB-TRIP	TURB-TRIP

VII.4.3. Comparison of DBAS related to vessel damage and release with the literature

The aggregated DBA frequency for the improved design is equal to 6.82E-5/r.y. However, it is irrelevant to compare this value with the LWR limit since the LWR DBA definition is different from the NGNP DBA definition. Indeed, the NGNP DBA list includes scenarios without any possible challenge to the plant. These scenarios are often very likely, thus increasing the MSR aggregated DBA frequency. In the present case, there is no vessel damage during DBAs.
In the next table, a comparison is done between the DBAs identified by the NGNP approach and the LWR-based DBAs identified by R. YOSHIOKA [3]:

Table 18: Comparison of DBAs identified using two different methods

LWR-base DBAs [3]	NGNP-based DBAs (Use of DT and DTC)	Release (system involved)
Fuel salt flow decrease	Fuel salt flow decrease	No
Reactivity insertion (cold loop startup)	Reactivity insertion (cold loop startup)	No
Fuel salt loss by pipe rupture	Fuel salt loss by pipe rupture	No
Heat exchanger pipe rupture	Heat exchanger pipe rupture	No
Steam generator pipe rupture	Steam generator pipe rupture	No
Destructive accident in off-gas system	Destructive accident in off-gas system	Yes (filters)
Malfunction of fuel salt adjustment equipment	Malfunction of fuel salt adjustment equipment	No
	Primary flow reduction	No
	Secondary flow reduction	No
	Loss of secondary flow	No
	Water cooling flow increase	No
	Feedwater tube rupture	No
	Freeze valve failure	No
	Inadvertent closure of a MSIV	No
	Inadvertent opening of a SGRV	No
	Partial loss of feedwater	No
	Leak in the secondary circuit	Yes (SDT)
	Secondary salt flow increase	No
	Turbine trip	No

As can be seen, every DBAs identified by the Japanese analysis are present in the DBA list established thanks to the NGNP methodology. However, the NGNP method defines a lot more DBAs.

The DBAs must meet the DBE TLRC. Since the DT, the DTC, the EDT and the EDTC are classified as Safety-Related, there is only small release during DBAs (see Table 18). Therefore, **the improved design is validated** according to the NGNP methodology.

The analysis of the PSA model built is now finished. Since it is the first time the NGNP methodology has been applied (or at least published), advantages and disadvantages of the method can be highlighted. This is the subject of the last section of this report.

VII.5. Discussion about the NGNP methodology

This thesis report documents one of the first "full" applications of the NGNP methodology. However, one may notice that part of the method has already been applied for an FHR [5] and some examples have been developed for an HTGR by the INL, in order to illustrate their methodology [1]. Since it is the first time the whole NGNP method is applied, methodological issues have been noticed throughout the study. They are presented in this section.

In a previous part, the screening process and the scenario-specific TLRC proposed by the NGNP methodology seemed to be an issue, especially for the off-gas system where component decomposition is necessary. In order to overcome this first problem, the ACRS suggested imposing a limit on an aggregated frequency-consequence. This limit considers screened out scenarios so that scenarios with large release are considered in the licensing process, even if they have low frequencies [6]. Another solution proposed by the author would be to impose a maximum cumulative frequency on the aggregated screened out scenarios, so that scenarios not considered in the licensing process will almost never occur during the plant lifetime. In this study, the cumulative frequency for non-considered scenarios (safe and unsafe scenarios) is equal to 6.54E-6/r.y. Therefore, the screening process is justified for this study.

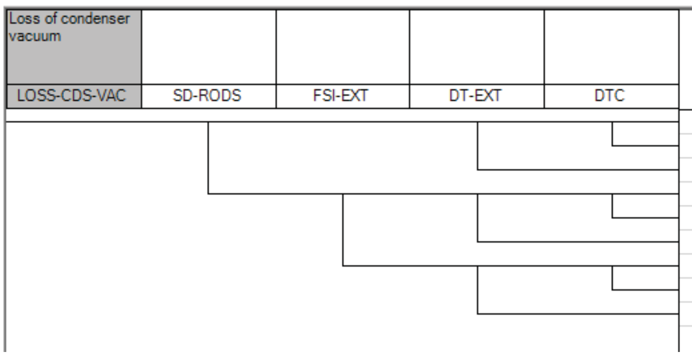
Another problem noticed by the author during the study is that the NGNP methodology tends the analyst to push the scenarios in the lower categories. In other words, it is more likely that the analyst will try to implement redundancy instead of adding diversity, even if the DiD principles state the inverse. It is also worth noticing that accident prevention is preferred against accident mitigation.

Nonetheless, the NGNP methodology has many advantages. The TLRC applied to sequence-specific scenario helps the analyst to identify critical component, and thus it becomes easier to improve a reactor design. The inflexible Single Failure Criterion is replaced by a Reliability Criterion. Indeed, the problem arising from the current practice (Single Failure Criterion) is the necessary redundancy to withstand a single failure in plant's response to particular events, without regard for their likelihood. Using a reliability criterion, more redundancy and diversity are added for frequent events, whereas less redundancy and diversity are necessary for non-likely events. Last but not least, the NGNP methodology tries to be as close as possible to the LWR methodology. For example, it tries to use the same vocabulary (BDBE, BDBA, DBE, DBA …). Moreover, LWR requirements are met if the NGNP methodology is applied. In the end, it would be easier for analysts to go from LWR licensing towards NGNP licensing.

Eventually, the present study has two limitations:

- The NGNP approach does require that external IEs (e.g. earthquake) be addressed. These have not been treated in this analysis. Their study does not change the result of the present safety analysis about internal IEs. It is also important to notice that external IEs are site-specific. That is why external IEs have not been taken into account in this study.
- No uncertainty has been taken into account in the present study. Thus, the same safety analysis with uncertainties on failure rates could be performed, in order to validate more accurately the design for its licensing. Uncertainties were not taken into account in the PSA

model built since some key MSR components have highly uncertain failure rates, and since the LBE classification is not robust to high uncertainties. For instance, in Figure 54, if the uncertainty on the freeze valve is taken into account (upper bound of 3.28E-2), then the event would be classified as AOO instead of DBE. Therefore, the results of the study become totally different since they are totally dependent on the LBE classification.



No.	Freq.	Conseq.	Code
1	4.10E-01	AOO	
2	9.34E-04	DBE	DTC
3	2.11E-03	DBE	DT-EXT
4	1.24E-05	BDBE	SD-RODS
5	2.82E-08	CSDRD	SD-RODS-DTC
6	6.38E-08	CSDRD	SD-RODS-DT-EXT
7	9.62E-08	CSDRD	SD-RODS-FSI-EXT
8	2.19E-10	NOT_CSDRD	SD-RODS-FSI-EXT-DTC
9	4.95E-10	NOT_CSDRD	SD-RODS-FSI-EXT-DT-EXT

Figure 54: Example of scenario not robust against high uncertainties

However, it seems that the PSA model is rather robust. Therefore, the take-home messages will not change despite the limitations.

VIII. Conclusion

In the present study, a complete safety assessment of the FUJI-233Um reactor is performed by building a PSA model using RiskSpectrum®. The TTS team from Japan already studied two accident progressions specifically for the FUJI-233Um reactor. However, the literature about the FUJI-233Um design and other accident progressions is still incomplete. Therefore, since the FUJI-233Um reactor is largely based on the MSBR design, the gaps were filled with information from the MSBR literature. Besides, the lack of data was overcome by taking data from LMFBRs and PWRs justified by analogies.

Thanks to the NGNP methodology, a complete safety analysis of the FUJI-233Um reactor has been performed. One safety weakness and two critical systems in terms of radioactive release and vessel damage respectively were identified:

- No core cooling during LOHS when the DT is unavailable
- Drain tank cooling
- Isolation valve

Possible safety improvements have thus been suggested. The SR-SSCs, which represent the main safety systems of the FUJI-233Um reactor, were defined twice. The first identification defines TLRC-based SR-SSCs. However, every DBA based on this identification satisfied the TLRC but led to vessel damage. It is opposite to the Defence-in-Depth principles. Thus another more restrictive criterion was taken into account: vessel damage. This added criterion allows an easier verification of the TLRC by avoiding the need for transport calculation.

The first list of TLRC-based SR-SSCs is:

- The auxiliary off-gas system
- The off-gas cell
- The High Temperature Containment
- The emergency drain tank (containment of liquid leakage from the primary circuit)
- The emergency drain tank cooling

The second list of SR-SSCs related to vessel damage and release adds three other systems to the first list:

- The drain tank (drainage of fuel salt from the primary circuit)
- The drain tank cooling
- The isolation valve

"Special treatments" is applied in order for them to meet their reliability objectives. Thanks to the second list of SR-SSCs identified, DBAs were defined and compared with the literature. Every DBAs present in the literature were identified using the NGNP approach. Moreover, only very small releases were identified during DBAs. Therefore, **the improved FUJI-233Um design is validated** according to the NGNP methodology for the licensing of generation IV reactors.

This thesis report documents one of the first "full" applications of the NGNP methodology. Therefore, methodological issues have been highlighted. The main issue comes from the facts that TLRC are sequence-specific and that scenarios with frequency lower than $5 * 10^{-7}$/r.y. are screened out. The off-gas system needs a decomposition at the component level since a break before or after a specific filter does not lead to the same consequences. Thus, the NGNP methodology cannot be applied to the off-gas system of an MSR. In order to overcome this limitation, suggestions have been proposed by the ACRS and the author:

- Impose a limit on an aggregated frequency-consequence curve in addition to the TLRC
- Impose a maximal cumulative frequency for the aggregated screened out scenarios

This way, it is assured that there is no important scenario not considered in the licensing process due to component decomposition. Besides, a modified NGNP methodology has been applied for the off-gas system. From this study, it can be said that the off-gas system seems safer than what could be stated, i.e. that the risk from the reactor is shifted to the off-gas system in an MSR. Thanks to this study, it can be said that the risk is not only shifted to the off-gas system, but also effectively reduced.

Even if containing some methodological issue, the NGNP licensing process is an interesting and easy-to-use licensing method. The sequence-specific TLRC allow a rapid estimation of the critical components, the too stringent Single Failure criterion is replaced by a reliability criterion focusing on the critical components, and the NGNP methodology uses a vocabulary similar to the LWR licensing, so that it will be easier for analyst to go from LWR licensing toward NGNP licensing.

All in all, the analysis performed in this work support the safety claims of the FUJI-233Um. If the improvements suggested are taken into account, vessel damage will be unlikely to happen and radioactive releases are substantially reduced to small traces of tritium from the secondary circuit.

Moreover, the present report opens up paths for new studies. Five different studies could be performed. The last two represent limitations of the present work:

- The first one would focus on component reliability estimation, in order to reduce the uncertainty on key-MSR components
- The second one would focus on verifying the phenomena hypothesized in this study (for example steam explosion)
- The third one would consist of a computational model simulating transients and the transport of radionuclides at EAB if release
- The fourth one would consist of integrating external events into the PSA model built
- The last one would consists of integrating uncertainty on failure rates, since they have not been considered in the present study

Finally, the take-home messages from this study are:

- There is still a lot of highly uncertain data and phenomena concerning the FUJI-233Um reactor
- The limiting IEs to consider regarding vessel damage and release are:
    - Total Loss of secondary Salt flow
    - Loss of Offsite Power
    - Heat exchanger tube rupture
    - Steam generator tube rupture
- Very few systems are involved in release and vessel damage, straightforward improvements can be identified
- The FUJI-233Um reactor can be easily licensed with safety margins if the improvements suggested are taken into account
- The NGNP methodology, even if containing some issues, is an adequate methodology for the licensing of generation IV reactors

Acknowledgements

I would like to express my gratitude to my mentor Vinh N. Dang for the valuable observations, remarks and engagement through the learning process of this master thesis. Besides, I would like to thank all the Risk and Human Reliability Group for the warm welcoming and the nice coffee breaks in the mornings. Also, I would like to thank the participants of the Journal Club, who have willingly shared their precious time to listen and to suggest improvements for my Master's Thesis.

References

[1] "Next Generation Nuclear Power Plant - Licensing Basis Event Selection White Paper," INL/EXT-10-19521, Idaho National Laboratory, Idaho Falls, September 2010.

[2] B. M. Elsheikh, "Safety assessment of molten salt reactors in comparison with light water reactors," *Journal of Radiation Research and Applied Sciences,* vol. 6, pp. 63-70, 2013.

[3] "Status of Small Reactor Designs Without On-Site Refuelling," International Atomic Energy Agency, Vienna, Austria, IAEA-TECDOC-1536, January 2007.

[4] "Next Generation Nuclear Plant Licensing Strategy - A Report to Congress," ML082290017, Department of Energy, Nuclear Regulatory Commission, August 2008.

[5] "FHR Functionnal Requirements and LBE Identification White Paper," Department Of Energy, Berkeley, August 2013.

[6] D. E. Klein, "Development of a Technology-neutral Regulatory Framework," ACRSR-2267, Nuclear Regulatory Commission, September 26, 2007.

[7] W. D. Travers, "Plan for resolving policy issues related to licensing non-light water reactor designs," SECY-02-0139, Nuclear Regulatory Commission, July 22, 2002.

[8] "An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis," Regulatory guide 1.174, November 2002. [Online]. Available: http://www.nrc.gov/reading-rm/doc-collections/reg-guides/power-reactors/rg/01-174/.

[9] A. L. Vietti-Cook, "Policy issues related to licensing non-light-water reactor designs," SECY-03-0047, Nuclear Regulatory Commision, March 28, 2003.

[10] "Use and development of Probabilistic Safety Assessment," NEA/CSNI/R(2007)12, Nuclear Energy Agency, November 14, 2007.

[11] "Ordonnance sur la radioprotection," SR 814.501, Conseil fédéral suisse, June 22, 1994.

[12] S. Yoichiro and Y. Ritsuo, "Proposal of Safety Criteria for MSRs (In comparison with LWRs)," in *Thorium Energy Conference 2010*, London, 2010.

[13] G. E. Apostolakis, "Engineering Risk Benefit Analysis," in *Lectures*, Massachusetts Institute of Technology, 2007.

[14] R. Yoshioka and K. Mitachi, Safety criteria and guidelines for MSR accident analyses, 2014.

[15] "Next Generation Nuclear Plant Probabilistic Risk Assessment White Paper," INL/EXT-11-21270, Idaho National Laboratory, Idaho Falls, September 2011.

[16] "Next Generation Nuclear Plant Structures, Systems, and Components Safety Classification White Paper," INL/EXT-10-19509, Idaho National Laboratory, Idaho Falls, September 2010.

[17] "Next Generation Nuclear Plant Defense-in-Depth Approach," INL/EXT-09-17139, Idaho National Laboratory, Idaho Falls, December 2009.

[18] D. Pyron, "Licensing Basis Event Selection for MSR (internal report)," Villigen, December 2015.

[19] I. Crossland, Nuclear Fuel Cycle Science and Engineering, Oxford: Woodhead Publishing, 2012.

[20] R. C. Robertson, "Conceptual Design Study of a Single-Fluid Molten-Salt Breeder Reactor," ORNL, ORNL-4541, June 17, 1971.

[21] J. R. Keiser, J. H. DeVan and D. L. Manning, "The corrosion Resistance of Type 316 Stainless Steel to Li2BeF4," ORNL, Oak Ridge, tennessee, ORNL/TM-5782, April 1977.

[22] K. Furukawa, Revolution in Nuclear Power Plants, Thorium Molten-Salt Reactor System, Originally in Japanese, August, 2001.

[23] K. Mitachi, T. Yamamoto and R. Yoshioka, "Self-sustaining Core Design for 200 MWe Molten-Salt Reactor with Thorium-Uranium Fuel: FUJI-U3-(0)," in *TU2007, International Workshop on Thorium Utilization for Sustainable Development of Nuclear Energy*, Tsinghua University, Beijing, China, 4-6 December 2007.

[24] R. Simard, "Licensing needs for future plants," in *ACRS workshop on Regulatory Challenges for Future Nuclear Power Plants*, Washington, DC, June 5, 2001.

[25] "Technical Elements of a Risk-informed, Technology-Neutral Design and Licensing Framework for New Nuclear Plants," EPRI-1013582, 2006.

[26] M. ISHIDA, T. NAKANO, K. MORIMOTO and I. NOJIRI, "PSA Application on the Tokai Reprocessing Plant," in *Probabilistic Safety Assessment and Management*, London, Springer-Verlag, 2004, pp. 543-548.

[27] "Safety Assessment of Fuel Cycle Facilities - Regulatory Approaches and Industry Perspectives," in *OECD/NEA Workshop*, Toronto, Canada, NEA/CSNI/R(2012)4, 27-29 September 2011.

[28] "Standard Review Plan," Nuclear Regulatory Commission, NUREG-0800, March 3, 2007.

[29] "Probabilistic Safety Analysis (PSA): Quality and Scope," Eidgenossisches Nuklearsicherheitsinspektorat, ENSI-A05/e, March 2009.

[30] S. Cantor, J. W. Cooke, A. S. Dworkin, G. D. Robbins, R. E. Thoms and G. M. Watson, "Physical Properties of Molten-Salt Reactor Fuel, Coolant, and Flush Salts," ORNL, ORNL-TM-2316, August 27, 1968.

[31] N. SUZUKI and Y. SHIMAZU, "Reactivity-Initiated-Accident Analysis without Scram of a Molten Salt Reactor," *Journal of Nuclear Science and Technology,* vol. 45, no. 6, pp. 575-581, 2008.

[32] P. Haubenreich and J. Engel, "Safety Calculations for MSRE," ORNL, ORNL-TM-251, May 15, 1962.

[33] S. Nobuhide and S. Yoichiro, "Preliminary Safety Analysis on Depressurization Accident without Scram of a Molten Salt Reactor," *Journal of Nuclear Science and Technology,* vol. 43, no. 7, pp. 720-730, 2006.

[34] A. Cammi, V. D. Marcello, L. Luzzi, V. Memoli and M. E. Ricotti, "A multi-physics modelling approach to the dynamics of Molten Salt Reactors," *Annals of Nuclear Energy,* no. 38, pp. 1356-1372, 2011.

[35] E. S. Bettis, W. H. Cook, W. P. Eatherly, D. K. Holmes, R. J. Kedl, C. R. Kennedy, S. S. Kirslis, H. E. McCoy, A. M. Perry, R. C. Robertson, D. Scott and R. A. Strehlow, "Graphite behavior and its effects on MSBR performance," ORNL, Oak Ridge, Tennessee, ORNL-TM-2136, February 1969.

[36] N. C. Gallego and T. D. Burchell, "A review of Stored Energy Release of Irradiated Graphite," ORNL, Oak Ridge, Tennessee, ORNL/TM-2011/378, September 2011.

[37] S.-C. Tsai, E.-W. Huang, J.-J. Kai and F.-R. Chen, "Microstructural evolution of nuclear grade graphite induced by ion irradiation at high temperature environment," *Journal of Nuclear Materials,* no. 434, pp. 17-23, 2013.

[38] W. Windes, G. Strydom, R. Smith and J. Kane, "Role of Nuclear Grade Graphite in Controlling Oxidation in Modular HTGRs," Idaho National Laboratory, Idaho falls, INL/EXT-14-31720, November 2014.

[39] B. Yuan, L. Song, K. M. Liew and Y. Hu, "Mechanism for increased thermal instability and fire risk of graphite oxide containing metal salts," *Materials Letters,* no. 167, pp. 197-200, 2016.

[40] L. A. Corwin, "Constrained Noninformative Priors," Idaho National Engineering Laboratory, Idaho falls, October 1994.

[41] A. Y. L. Mu Zhu, "The counter-intuitive Non-informative Prior for the Bernoulli Family," *Journal of Statistics Education,* vol. 12, no. 2, 2004.

[42] Nuclear Regulatory Commission, "CCF Parameters Estimations," 2012. [Online]. Available: http://nrcoe.inl.gov/resultsdb/ParamEstSpar/. [Accessed 14 June 2016].

[43] A. Mosleh, D. M. Rasmuson and F. Marshall, "Guidelines on Modelling Common-Cause Failures in Probabilistic Risk Assessment," Nuclear Regulatory Commission, Washington, DC, NUREG/CR-5485, INEEL/EXT-97-01327, November 1998.

[44] A. D. Swain and H. E. Guttmann, "Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications," Nuclear Regulatory Commission, Washington, DC, NUREG/CR-1278, August 1983.

[45] D. Gertman, H. Blackman, J. Marble, J. Byers and C. Smith, "The SPAR-H Human Reliability Analysis Method," Nuclear Regulatory Commission, Washington, DC, NUREG/CR-6883, INL/EXT-05-00509, August 2005.

[46] Nuclear Regulatory Commission, "Industry Average Parameter Estimates," 2010. [Online]. Available: http://nrcoe.inl.gov/resultsdb/AvgPerf/. [Accessed 14 June 2016].

[47] T.-M. Bajenescu and M. I. Bazu, Reliability of Electric Components: A practical Guide to Electronic Systems Manufaturing, Berlin: Springer, DOI: 10.1007/978-3-642-58505-0, 1999.

[48] J. Poloski, G. Grant, C. Gentillon, W. Galyean and J. Knudsen, "Auxiliary/Emergency Feedwater System Reliability, 1987 - 1995," Nuclear Regulatory Commission, Idaho Falls, NUREG/CR-5500, INEEL/EXT-97-00740, May 1998.

[49] S. Kamyab, M. Nematollahi and G. Shafiee, "Sensitivity analysis on the effect of software-induced common cause failure probability in the computer-based reactor trip system unavailability," *Annals of Nuclear Energy,* no. 57, pp. 294-303, 2013.

[50] L. Cadwallader, *Reliability and Maintainability Data for Liquid Metal Cooling Systems,* Idaho Falls: Idaho National Laboratory, 2015.

[51] K. Kurisaka, T. Sakai, H. Yamano, S. Fujita, K. Minagawa, A. Yamaguchi and T. Takata, "Development of a level-1 PSA method applicable to Japan Sodium-cooled Fast Reactor," *Nuclear Engineering and Design,* no. 269, pp. 268-280, 2014.

[52] A. Blanchard, "Savannah River Site Generic Data Base Development," Westinghouse Safety Management Solution, Aiken, SC, WSRC-TR-93-262, May 1998.

[53] S. A. Eide, M. B. Calley, C. D. Gentillon, T. Wierman, D. Rasmuson and D. Marksberry, "Westinghouse Reactor Protection System Unavailability, 1984 - 1995," in *Idaho National Engineering & Environmental Laboratory*, Washington, DC, INEEL/CON-99-00374, August 22-25, 1999.

[54] T. Ishiguro, W. V. Rooijen, Y. Shimazu and H. Mochizuki, "Design of a passive residual heat removal system for the FUJI-233Um," *Annals of Nuclear Energy,* no. 64, pp. 398-407, 2013.

[55] B. Luciano, "Reliability study of a special decay heat removal system of a gas-cooled fast reactor demonstrator," *Nuclear Engineering and Design,* no. 280, pp. 473-480, 2014.

[56] E. Zio and N. Pedroni, "Estimation of the functionnal failure probability of a thermal-hydraulic passive system by Subset Simulation," *Nuclear Engineering and Design,* no. 239, pp. 580-599, 2009.

[57] M. Richardson, "Development of Freeze Valve for Use in the MSRE," ORNL, Oak Ridge, Tennessee, ORNL-TM-128, February 28, 1962.

[58] Y. SHIMAZU, "Locked Rotor Accident Analysis in a Molten Salt Bredder Reactor," *Journal of Nuclear Science and Technology,* no. 15, pp. 935-940, December 1978.

[59] B. Zimanowski, G. Frohlich and V. Lorenz, "Experiments on steam explosion by interaction of water with silicate melts," *Nuclear Engineering and Design,* no. 155, pp. 335-343, 1995.

[60] C. W. Forsberg, "Reactors with Molten Salts: Options and Missions," in *Frederic Joliot & Otto Han Summer School on Nuclear Reactors*, Cadarache, France, August 25 - September 3, 2004.

[61] M. Aufiero, A. Cammi, O. Geoffroy, M. Losa, L. Luzzi, M. E. Ricotti and H. Rouch, "Development of an OpenFOAM model for the Molten Salt Fast Reactor transient analysis," *Chemical Engineering Science,* no. 111, pp. 390-401, 2014.

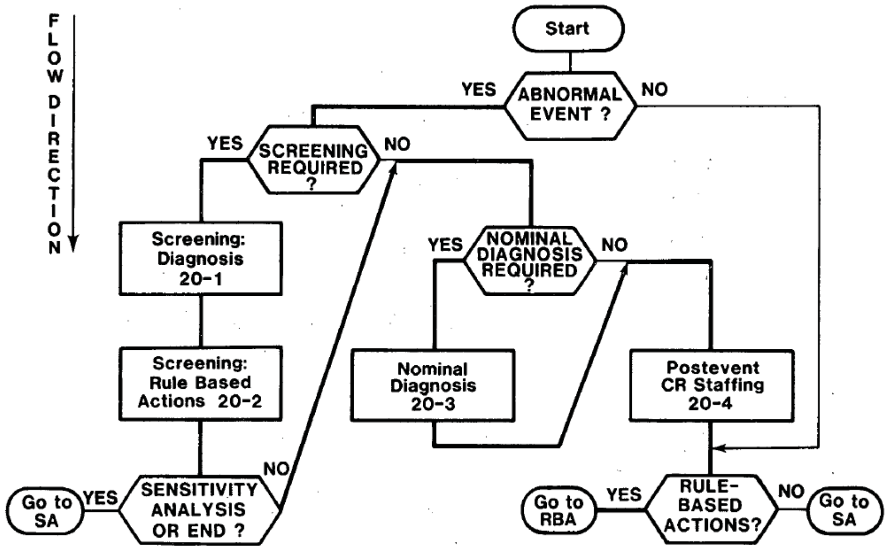
[62] "Defining initiating events for purposes of probabilistic safety assessment," International Atomic Energy Agency, Vienna, Austria, IAEA-TECDOC-719, September 1993.

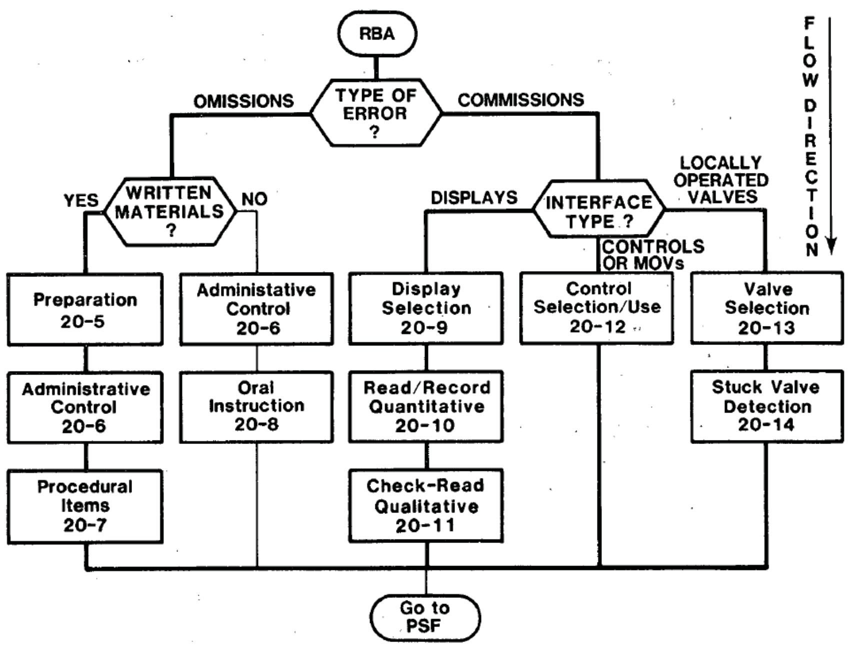
[63] M. V. d. Borst and H. Schoonakker, "An overview of PSA importance measures," *Reliability Engineering and System Safety,* no. 72, pp. 241-245, 2001.

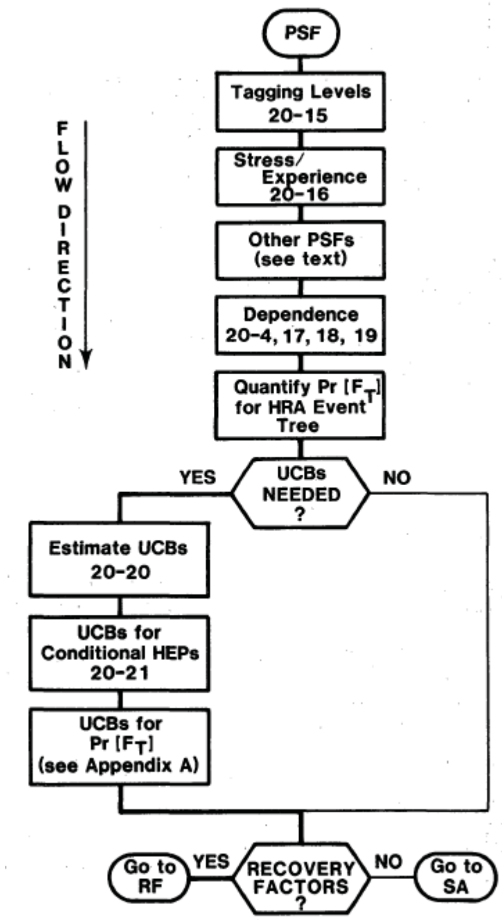
[64] L. Cadwallader, "Selected component failure rate values from fusion safety assessment tasks," Idaho National Engineering and Environmental Laboratory, Idaho falls, INEEL/EXT-98-00892, September 1998.

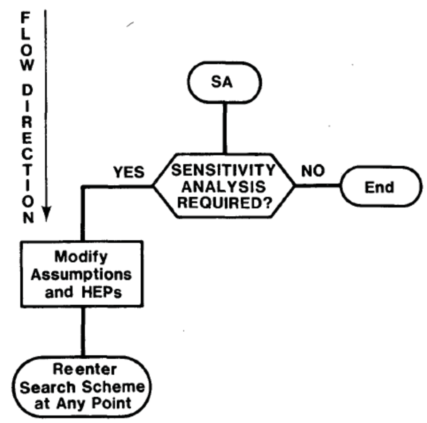
Appendix 1: THERP flowcharts

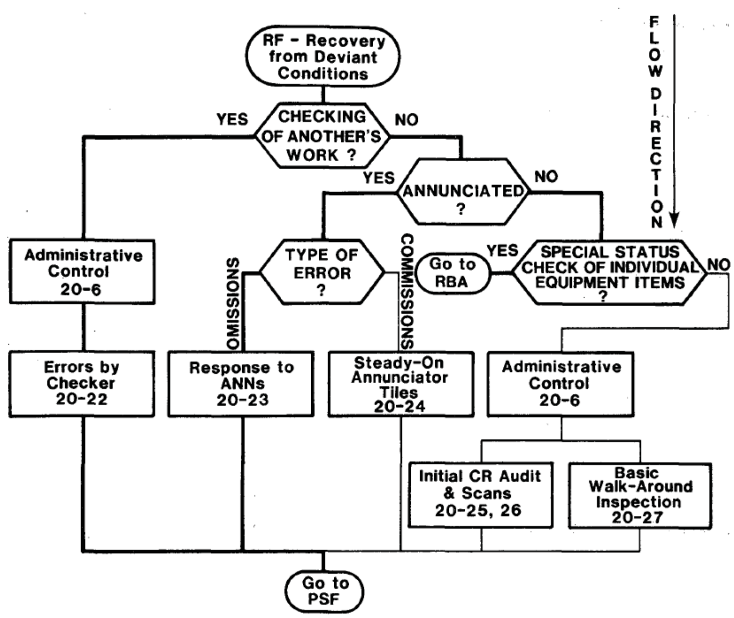
All the necessary data are present in the 20th section of NUREG/CR-1278. The different tables are given from table 20-1 to table 20-27. Flowcharts are used to find the necessary data.






PSF
Tagging Levels 20-15
Stress/ Experience 20-16
Other PSFs (see text)
Dependence 20-4, 17, 18, 19
Quantify Pr [F_T] for HRA Event Tree
UCBs NEEDED ?
YES
NO
Estimate UCBs 20-20
UCBs for Conditional HEPs 20-21
UCBs for Pr [F_T] (see Appendix A)
RECOVERY FACTORS ?
Go to RF
Go to SA
FLOW DIRECTION


SA
SENSITIVITY ANALYSIS REQUIRED?
YES
NO
End
Modify Assumptions and HEPs
Reenter Search Scheme at Any Point
FLOW DIRECTION


RF - Recovery from Deviant Conditions
CHECKING OF ANOTHER'S WORK ?
YES
NO
ANNUNCIATED ?
Administrative Control 20-6
TYPE OF ERROR ?
OMISSIONS
COMMISSIONS
Go to RBA
SPECIAL STATUS CHECK OF INDIVIDUAL EQUIPMENT ITEMS ?
Errors by Checker 20-22
Response to ANNs 20-23
Steady-On Annunciator Tiles 20-24
Administrative Control 20-6
Initial CR Audit & Scans 20-25, 26
Basic Walk-Around Inspection 20-27
Go to PSF
FLOW DIRECTION

Appendix 2: SPAR-H Worksheets

In order to perform a SPAR-H analysis, the following pages have to be filled. The final result is calculated in the last case at the end.

HRA Worksheets for At-Power

SPAR HUMAN ERROR WORKSHEET

Plant:__________ Initiating Event:________ Basic Event :____________ Event Coder:___________

Basic Event Context:____

Basic Event Description:____

Does this task contain a significant amount of diagnosis activity? YES ☐ (start with Part I–Diagnosis) NO ☐ (skip Part I – Diagnosis; start with Part II – Action) Why?______________________

PART I. EVALUATE EACH PSF FOR DIAGNOSIS

A. Evaluate PSFs for the Diagnosis Portion of the Task, If Any.

PSFs	PSF Levels	Multiplier for Diagnosis	Please note specific reasons for PSF level selection in this column.
Available Time	Inadequate time	P(failure) = 1.0 ☐	
	Barely adequate time (≈2/3 x nominal)	10 ☐	
	Nominal time	1 ☐	
	Extra time (between 1 and 2 x nominal and > than 30 min)	0.1 ☐	
	Expansive time (> 2 x nominal and > 30 min)	0.01 ☐	
	Insufficient information	1 ☐	
Stress/ Stressors	Extreme	5 ☐	
	High	2 ☐	
	Nominal	1 ☐	
	Insufficient Information	1 ☐	
Complexity	Highly complex	5 ☐	
	Moderately complex	2 ☐	
	Nominal	1 ☐	
	Obvious diagnosis	0.1 ☐	
	Insufficient Information	1 ☐	
Experience/ Training	Low	10 ☐	
	Nominal	1 ☐	
	High	0.5 ☐	
	Insufficient Information	1 ☐	
Procedures	Not available	50 ☐	
	Incomplete	20 ☐	
	Available, but poor	5 ☐	
	Nominal	1 ☐	
	Diagnostic/symptom oriented	0.5 ☐	
	Insufficient Information	1 ☐	
Ergonomics/ HMI	Missing/Misleading	50 ☐	
	Poor	10 ☐	
	Nominal	1 ☐	
	Good	0.5 ☐	
	Insufficient Information	1 ☐	
Fitness for Duty	Unfit	P(failure) = 1.0 ☐	
	Degraded Fitness	5 ☐	
	Nominal	1 ☐	
	Insufficient Information	1 ☐	
Work Processes	Poor	2 ☐	
	Nominal	1 ☐	
	Good	0.8 ☐	
	Insufficient Information	1 ☐	

Rev 1 (1/20/04)

Reviewer: ___________

Plant:__________**Initiating Event:**________**Basic Event :**_____________ **Event Coder:**___________

Basic Event Context:____

Basic Event Description:____

B. Calculate the Diagnosis Failure Probability.

(1) If all PSF ratings are nominal, then the Diagnosis Failure Probability = 1.0E-2
(2) Otherwise, the Diagnosis Failure Probability is: 1.0E-2 x Time x Stress or Stressors x Complexity x Experience or Training x Procedures x Ergonomics or HMI x Fitness for Duty x Processes

Diagnosis: 1.0E-2x ____ x ____ x ____ x ____ x ____ x ____ x ____ x ____ = $\boxed{}$

C. Calculate the Adjustment Factor IF Negative Multiple (≥3) PSFs are Present.

When 3 or more negative PSF influences are present, in lieu of the equation above, you must compute a composite PSF score used in conjunction with the adjustment factor. Negative PSFs are present anytime a multiplier greater than 1 is selected. The Nominal HEP (NHEP) is 1.0E-2 for Diagnosis. The composite PSF score is computed by multiplying all the assigned PSF values. Then the adjustment factor below is applied to compute the HEP:

$$HEP = \frac{NHEP \cdot PSF_{composite}}{NHEP \cdot (PSF_{composite} - 1) + 1}$$

Diagnosis HEP with Adjustment Factor = $\boxed{}$

D. Record Final Diagnosis HEP.

If no adjustment factor was applied, record the value from Part B as your final diagnosis HEP. If an adjustment factor was applied, record the value from Part C.

Final Diagnosis HEP = $\boxed{}$

Reviewer: ___________

Plant:__________ **Initiating Event:**________ **Basic Event :**____________ **Event Coder:**__________

Basic Event Context:____

Basic Event Description:____

PART III. CALCULATE TASK FAILURE PROBABILITY WITHOUT FORMAL DEPENDENCE ($P_{w/od}$)

Calculate the Task Failure Probability Without Formal Dependence ($P_{w/od}$) by adding the Diagnosis Failure Probability from Part I and the Action Failure Probability from Part II. In instances where an action is required without a diagnosis and there is no dependency, then this step is omitted.

$P_{w/od}$ = Diagnosis HEP ________ + Action HEP ________ = [ ]

Part IV. DEPENDENCY

For all tasks, except the first task in the sequence, use the table and formulae below to calculate the Task Failure Probability With Formal Dependence ($P_{w/d}$).

If there is a reason why failure on previous tasks should not be considered, such as it is impossible to take the current action unless the previous action has been properly performed, explain here: ____________________

Dependency Condition Table

Condition Number	Crew (same or different)	Time (close in time or not close in time)	Location (same or different)	Cues (additional or no additional)	Dependency	Number of Human Action Failures Rule ☐ - Not Applicable. Why?______________
1	s	c	s	na	complete	When considering recovery in a series e.g., 2nd, 3rd, or 4th checker If this error is the **3rd error in the sequence**, then the dependency is at least **moderate**. If this error is the **4th error in the sequence**, then the dependency is at least **high**.
2				a	complete	
3			d	na	high	
4				a	high	
5		nc	s	na	high	
6				a	moderate	
7			d	na	moderate	
8				a	low	
9	d	c	s	na	moderate	
10				a	moderate	
11			d	na	moderate	
12				a	moderate	
13		nc	s	na	low	
14				a	low	
15			d	na	low	
16				a	low	
17					zero	

Using $P_{w/od}$ = Probability of Task Failure Without Formal Dependence (calculated in Part III):

For Complete Dependence the probability of failure is 1.
For High Dependence the probability of failure is $(1+ P_{w/od})/2$
For Moderate Dependence the probability of failure is $(1+6 \times P_{w/od})/7$
For Low Dependence the probability of failure is $(1+19 \times P_{w/od})/20$
For Zero Dependence the probability of failure is $P_{w/od}$

Calculate $P_{w/d}$ using the appropriate values:

$P_{w/d}$ = (1 + (______ * ______))/ ______ = [ ]

Reviewer: __________

Appendix 3: HEP justification

In this Appendix, the HEP values are given and justified. NO-TIME means "barely adequate time" in the SPAR-H vocabulary. N means "nominal time" and EXT means "extensive time available". The diagnosis complexity for DT/FSI activation is set on "obvious diagnosis" since it is easy to know if the reactor has been tripped or not. These procedures are present in a lot of scenarios, thus one can expect the operator(s) to be well trained for these cases. That is why stress and complexity for the actuation is set on "nominal". For the secondary valve closure after a freeze valve thawing, the time available is around 5 minutes, thus "nominal time" is credited. The diagnosis is less obvious than in the other cases since the reactor is still normally operating during thawing of the freeze valve. The analysis assumes that only one indicator (a sound and/or a light) indicates the freeze valve failure. HEPn stands for nominal Human Error Probability.

DT/FSI-NO-TIME			
Analysis		Actuation	
Available time	10	Available time	10
Stress	1	Stress	1
Complexity	0.1	Complexity	1
HEPn	1.0E-02	HEPn	1.0E-03
Total	2.00E-02		

DT/FSI-N			
Analysis		Actuation	
Available time	1	Available time	1
Stress	1	Stress	1
Complexity	0.1	Complexity	1
HEPn	1.0E-02	HEPn	1.0E-03
Total	2.00E-03		

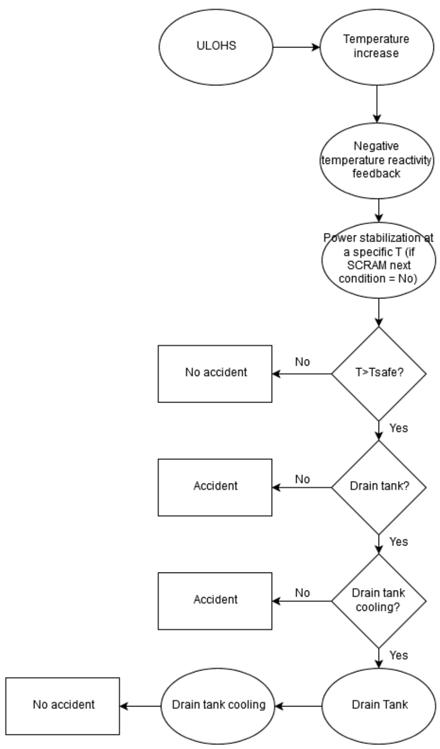
SCRDY_VALVE-N			
Analysis		Actuation	
Available time	1	Available time	1
Stress	1	Stress	1
Complexity	1	Complexity	1
HEPn	1.0E-02	HEPn	1.0E-03
Total	1.10E-02		

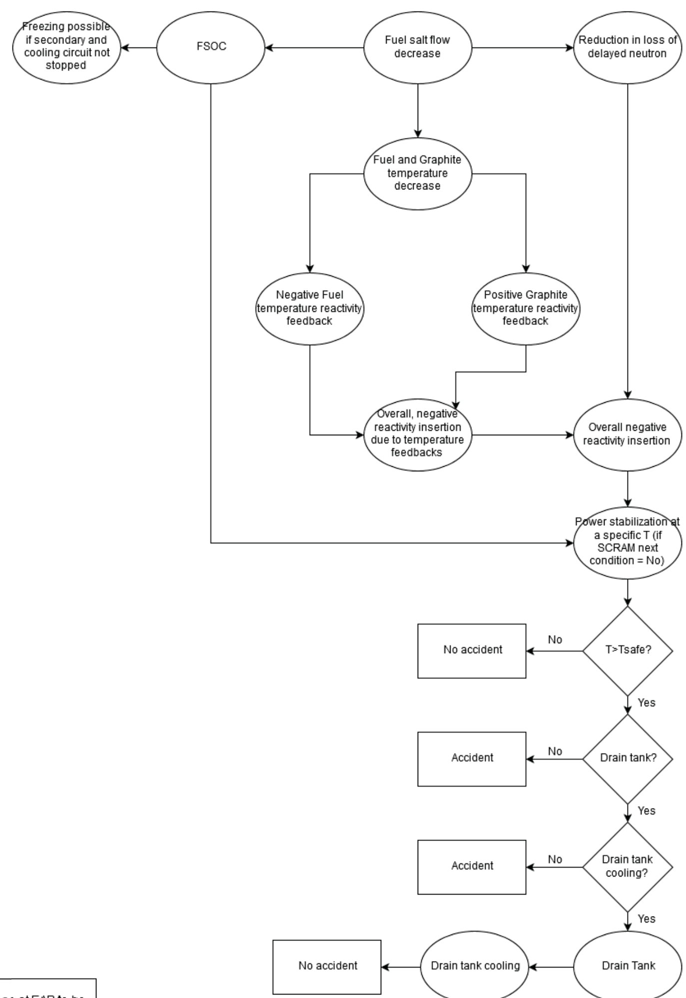
DT/FSI-EXT			
Analysis		Actuation	
Available time	0.01	Available time	0.01
Stress	1	Stress	1
Complexity	0.1	Complexity	1
HEPn	1.0E-02	HEPn	1.0E-03
Total	2.00E-05		

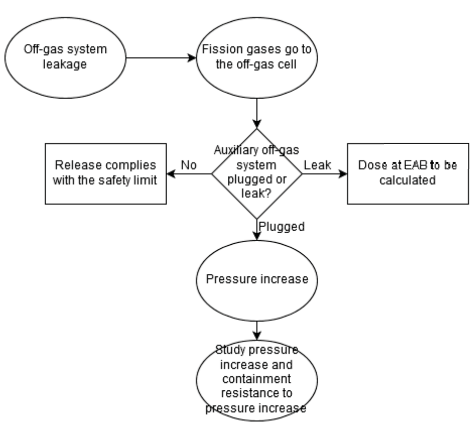
Appendix 4: Accident progression flowcharts

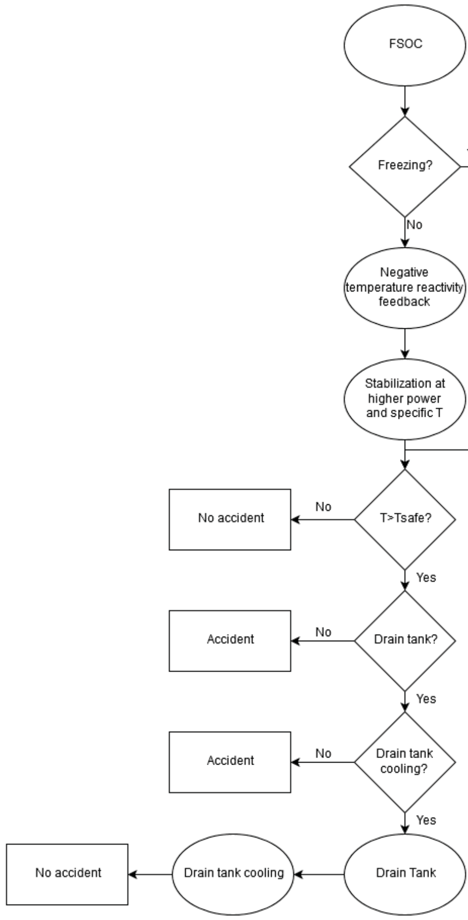
The different accident progression trees are developed below. One may add two remarks. The first one concerns the LOOP case. If the freeze valve fails, a LOHS combined with a LOF are combined. However, the probability of freeze valve failure in this case is very small since a LOOP implies a loss of electricity supply for the cooling of the freeze valve and thus an opening of the latter.

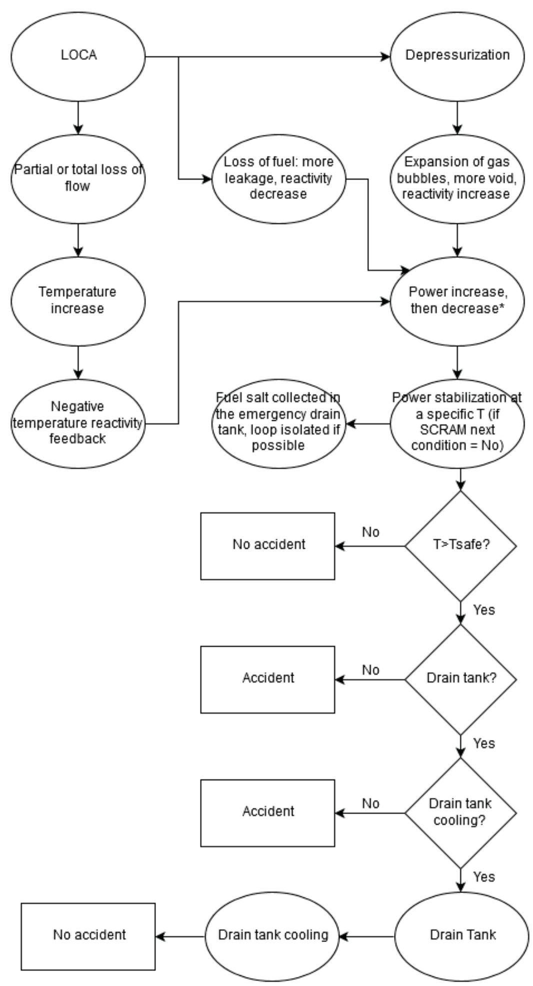
As already mentioned in the report, there are still uncertainties concerning the accident progression in case of a SGTR. That is why an open question in a circle does not have a successor.

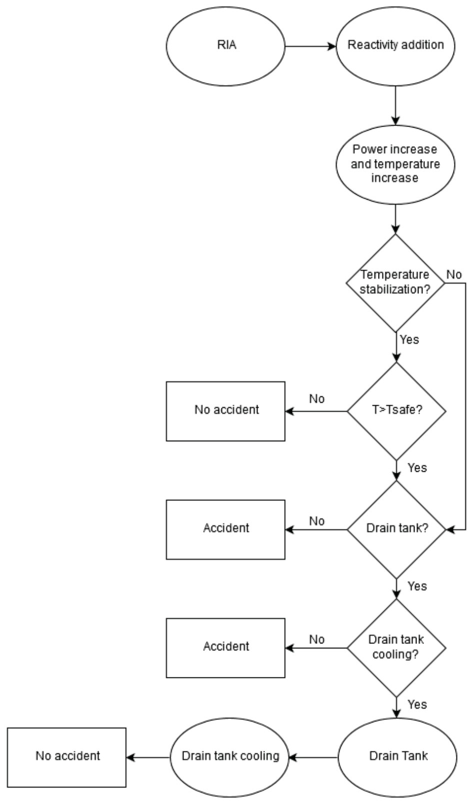


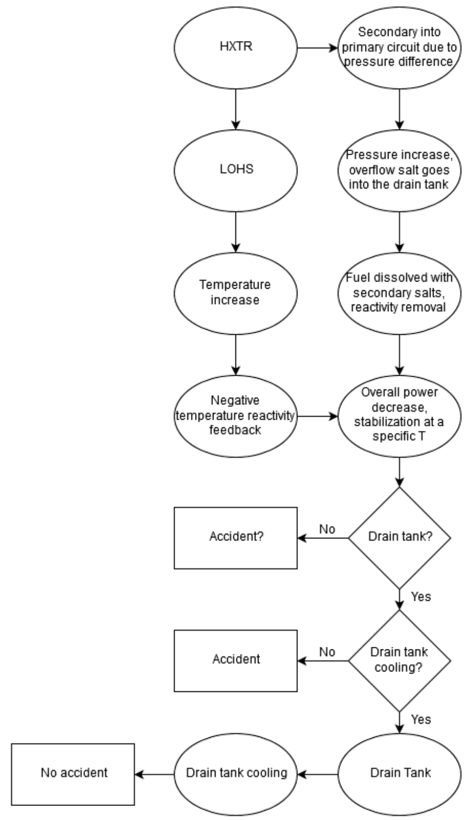


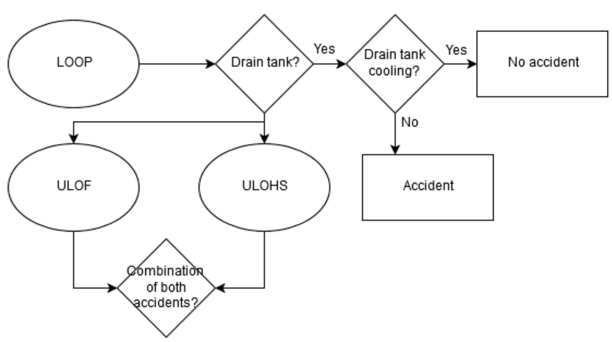


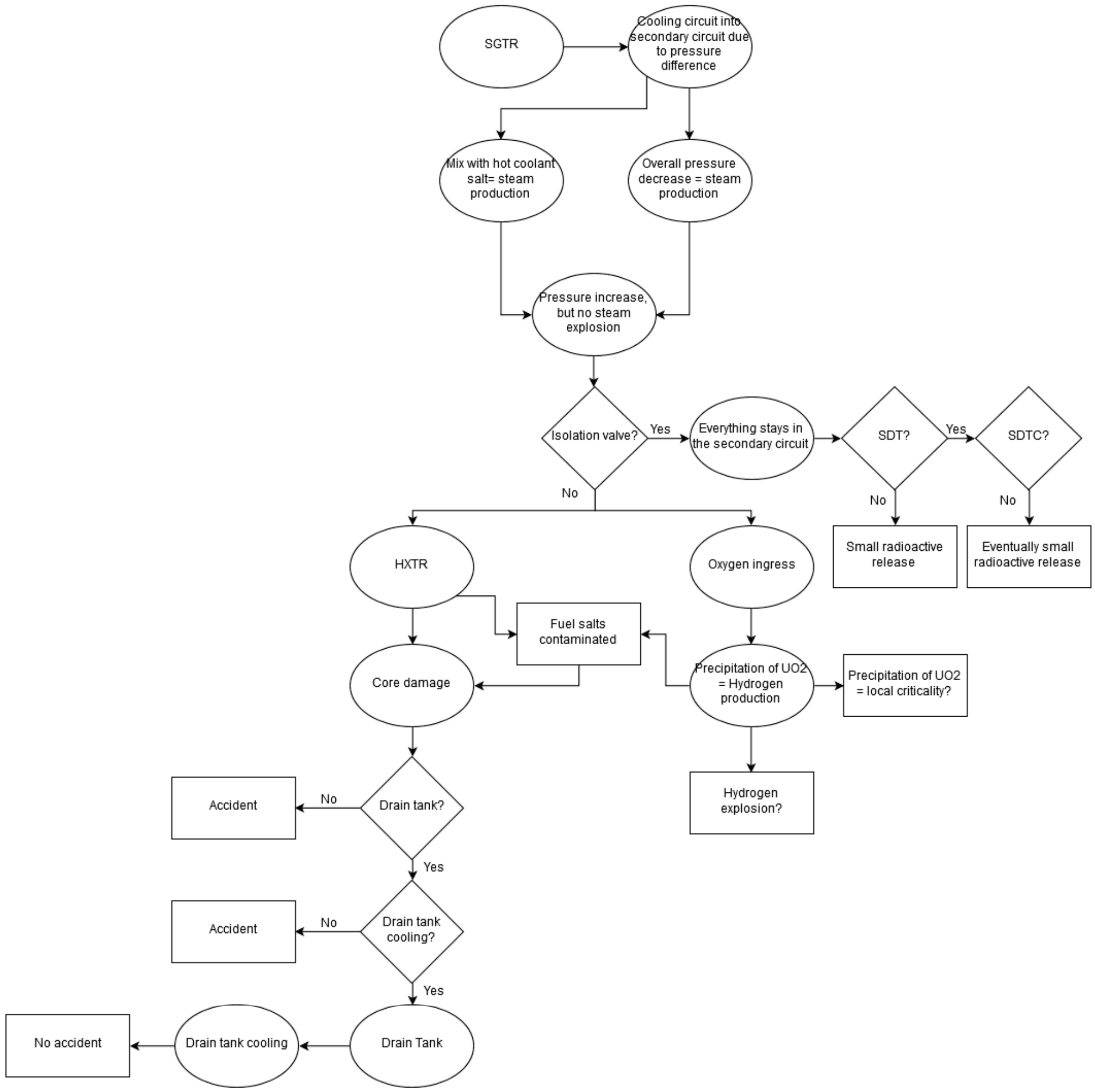

FSOC
Freezing?
Yes
Flow reduction
No
Negative temperature reactivity feedback
Core temperature increases
Stabilization at higher power and specific T
No accident
No
T>Tsafe?
Yes
Accident
No
Drain tank?
Yes
Accident
No
Drain tank cooling?
Yes
No accident
Drain tank cooling
Drain Tank


LOCA
Depressurization
Partial or total loss of flow
Loss of fuel: more leakage, reactivity decrease
Expansion of gas bubbles, more void, reactivity increase
Temperature increase
Power increase, then decrease*
Negative temperature reactivity feedback
Fuel salt collected in the emergency drain tank, loop isolated if possible
Power stabilization at a specific T (if SCRAM next condition = No)
No accident
No
T>Tsafe?
Yes
Accident
No
Drain tank?
Yes
Accident
No
Drain tank cooling?
Yes
No accident
Drain tank cooling
Drain Tank


RIA
Reactivity addition
Power increase and temperature increase
Temperature stabilization?
No
Yes
No accident
No
T>Tsafe?
Yes
Accident
No
Drain tank?
Yes
Accident
No
Drain tank cooling?
Yes
No accident
Drain tank cooling
Drain Tank

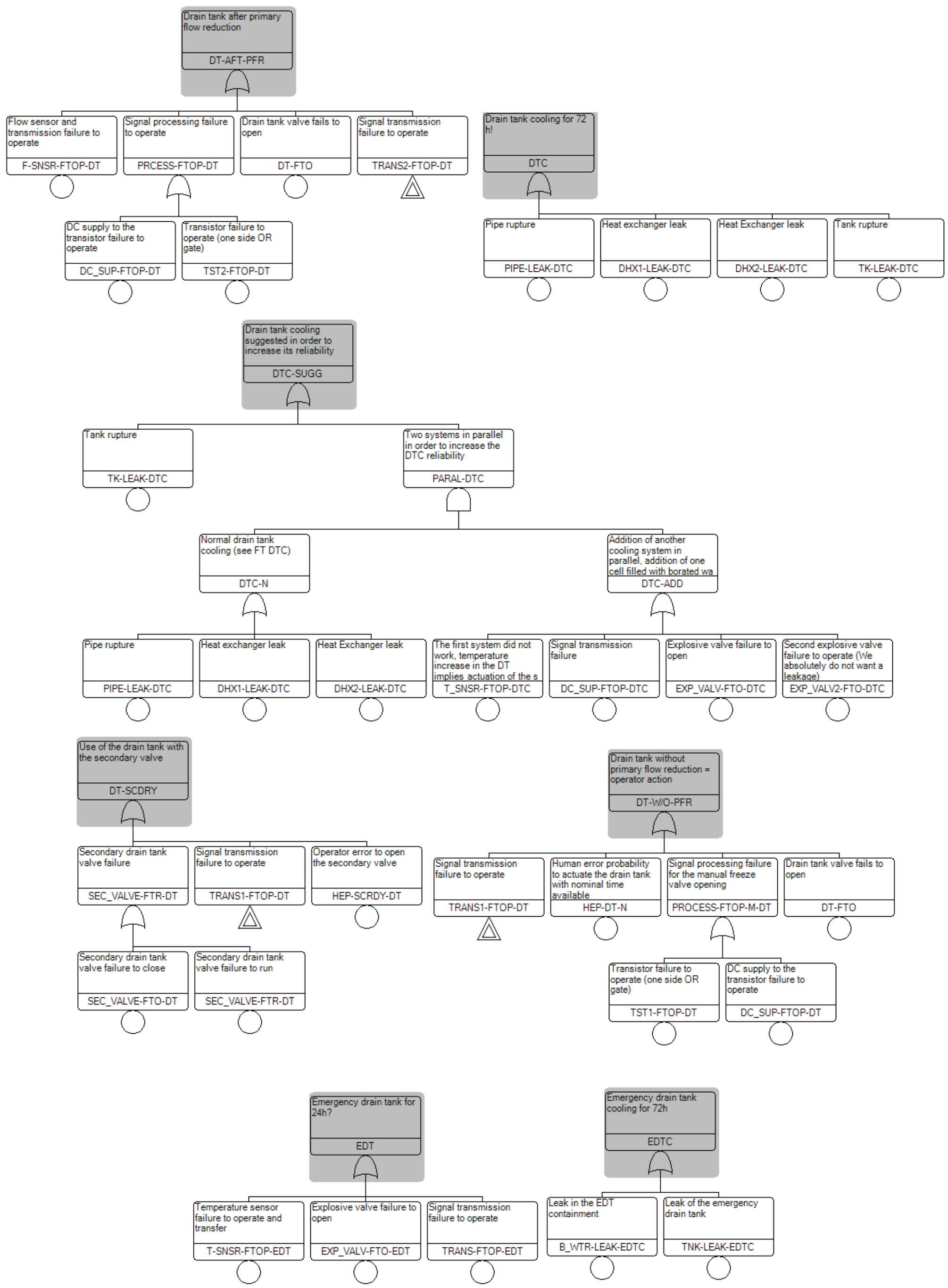

HXTR
Secondary into primary circuit due to pressure difference
LOHS
Pressure increase, overflow salt goes into the drain tank
Temperature increase
Fuel dissolved with secondary salts, reactivity removal
Negative temperature reactivity feedback
Overall power decrease, stabilization at a specific T
Accident?
No
Drain tank?
Yes
Accident
No
Drain tank cooling?
Yes
No accident
Drain tank cooling
Drain Tank

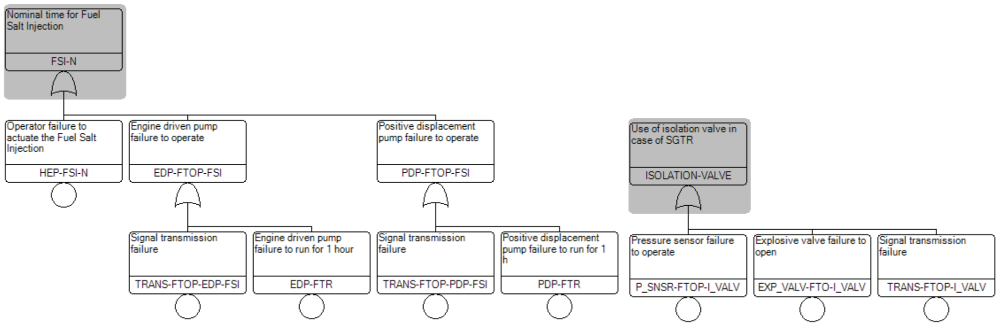

LOOP
Drain tank?
Yes
Drain tank cooling?
Yes
No accident
No
Accident
ULOF
ULOHS
Combination of both accidents?

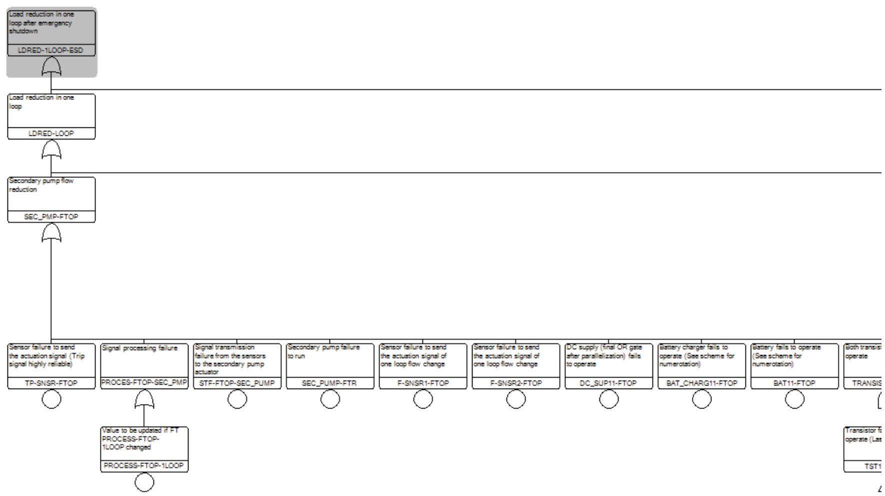

SGTR
Cooling circuit into secondary circuit due to pressure difference
Mix with hot coolant salt= steam production
Overall pressure decrease = steam production
Pressure increase, but no steam explosion
Isolation valve?
Yes
Everything stays in the secondary circuit
SDT?
Yes
SDTC?
No
No
Small radioactive release
Eventually small radioactive release
No
HXTR
Oxygen ingress
Fuel salts contaminated
Core damage
Precipitation of UO2 = Hydrogen production
Precipitation of UO2 = local criticality?
Hydrogen explosion?
Accident
No
Drain tank?
Yes
Accident
No
Drain tank cooling?
Yes
No accident
Drain tank cooling
Drain Tank

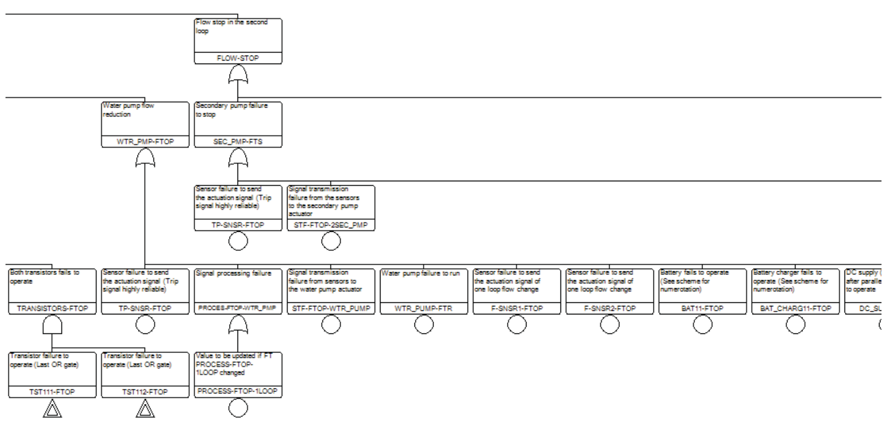
Appendix 5 – Part 1: Fault trees

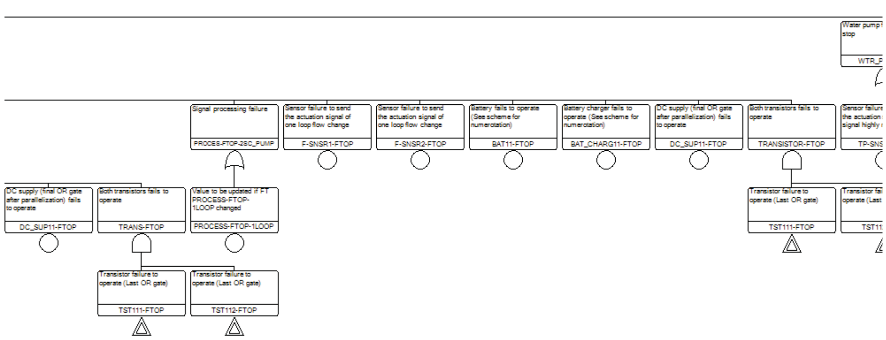
In this part is presented the different FTs developed in the PSA model. 23 FTs have been built. In this Appendix, only the most important FTs are present. 161 Basic events and 78 gates were created in order to build the FTs. 12 CCFs events were created. The key for FTs and ETs top events is given at the end of Appendix 5.

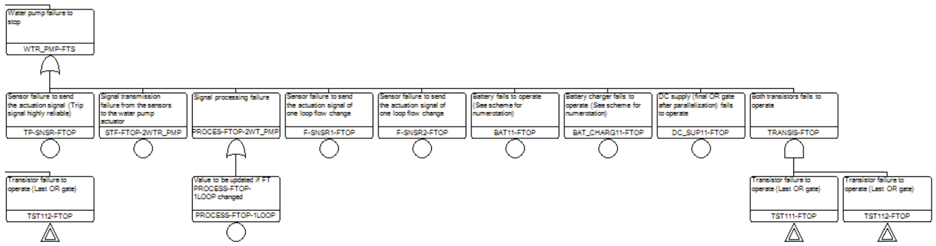


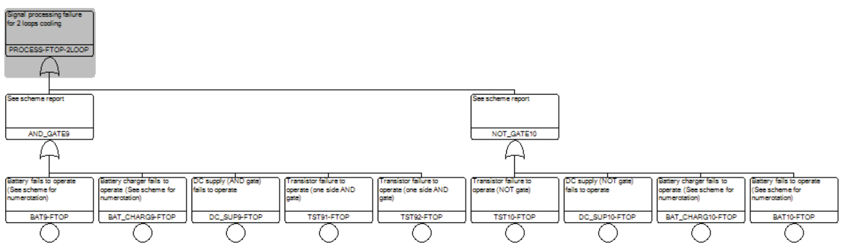

Nominal time for Fuel Salt Injection
FSI-N
Operator failure to actuate the Fuel Salt Injection
HEP-FSI-N
Engine driven pump failure to operate
EDP-FTOP-FSI
Positive displacement pump failure to operate
PDP-FTOP-FSI
Use of isolation valve in case of SGTR
ISOLATION-VALVE
Signal transmission failure
TRANS-FTOP-EDP-FSI
Engine driven pump failure to run for 1 hour
EDP-FTR
Signal transmission failure
TRANS-FTOP-PDP-FSI
Positive displacement pump failure to run for 1 h
PDP-FTR
Pressure sensor failure to operate
P_SNSR-FTOP-I_VALV
Explosive valve failure to open
EXP_VALV-FTO-I_VALV
Signal transmission failure
TRANS-FTOP-I_VALV

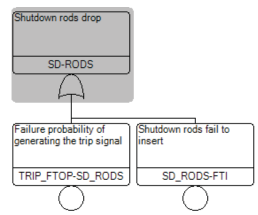


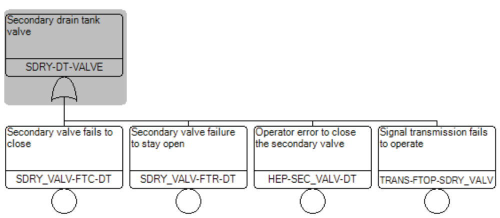


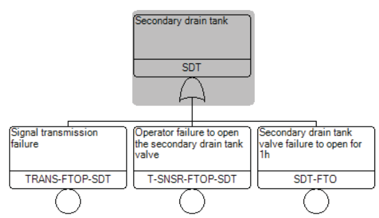


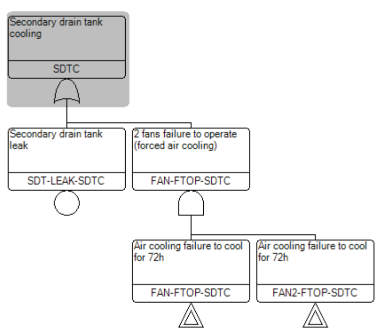

Water pump failure to stop
WTR_PMP-FTS
Sensor failure to send the actuation signal (Trip signal highly reliable)
TP-SNSR-FTOP
Signal transmission failure from the sensors to the water pump actuator
STF-FTOP-2WTR_PMP
Signal processing failure
PROCES-FTOP-2WT_PMP
Sensor failure to send the actuation signal of one loop flow change
F-SNSR1-FTOP
Sensor failure to send the actuation signal of one loop flow change
F-SNSR2-FTOP
Battery fails to operate (See scheme for numerotation)
BAT11-FTOP
Battery charger fails to operate (See scheme for numerotation)
BAT_CHARG11-FTOP
DC supply (final OR gate after parallelization) fails to operate
DC_SUP11-FTOP
Both transistors fails to operate
TRANSIS-FTOP
Transistor failure to operate (Last OR gate)
TST112-FTOP
Value to be updated if FT PROCESS-FTOP-1LOOP changed
PROCESS-FTOP-1LOOP
Transistor failure to operate (Last OR gate)
TST111-FTOP
Transistor failure to operate (Last OR gate)
TST112-FTOP


Signal processing failure for 2 loops cooling
PROCESS-FTOP-2LOOP
See scheme report
AND_GATE9
See scheme report
NOT_GATE10
Battery fails to operate (See scheme for numerotation)
BAT9-FTOP
Battery charger fails to operate (See scheme for numerotation)
BAT_CHARG9-FTOP
DC supply (AND gate) fails to operate
DC_SUP9-FTOP
Transistor failure to operate (one side AND gate)
TST91-FTOP
Transistor failure to operate (one side AND gate)
TST92-FTOP
Transistor failure to operate (NOT gate)
TST10-FTOP
DC supply (NOT gate) fails to operate
DC_SUP10-FTOP
Battery charger fails to operate (See scheme for numerotation)
BAT_CHARG10-FTOP
Battery fails to operate (See scheme for numerotation)
BAT10-FTOP


Shutdown rods drop
SD-RODS
Failure probability of generating the trip signal
TRIP_FTOP-SD_RODS
Shutdown rods fail to insert
SD_RODS-FTI

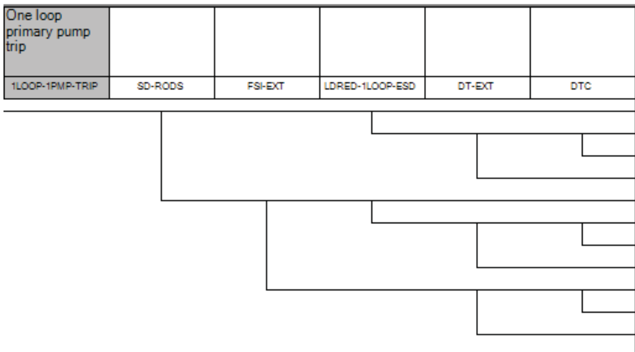

Secondary drain tank valve
SDRY-DT-VALVE
Secondary valve fails to close
SDRY_VALV-FTC-DT
Secondary valve failure to stay open
SDRY_VALV-FTR-DT
Operator error to close the secondary valve
HEP-SEC_VALV-DT
Signal transmission fails to operate
TRANS-FTOP-SDRY_VALV


Secondary drain tank
SDT
Signal transmission failure
TRANS-FTOP-SDT
Operator failure to open the secondary drain tank valve
T-SNSR-FTOP-SDT
Secondary drain tank valve failure to open for 1h
SDT-FTO

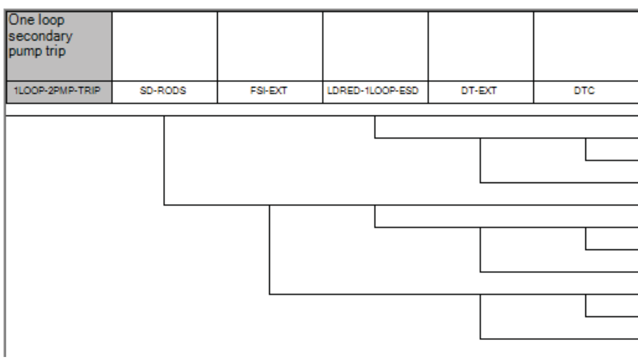

Secondary drain tank cooling
SDTC
Secondary drain tank leak
SDT-LEAK-SDTC
2 fans failure to operate (forced air cooling)
FAN-FTOP-SDTC
Air cooling failure to cool for 72h
FAN-FTOP-SDTC
Air cooling failure to cool for 72h
FAN2-FTOP-SDTC

Appendix 5 – Part 2: Event trees

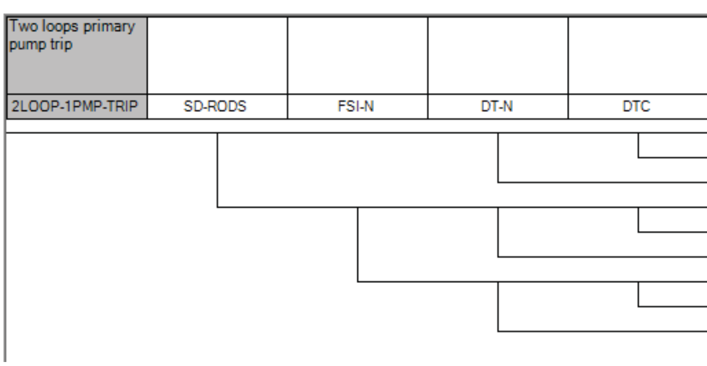
In the second part of this Appendix are presented the main event trees developed. The second column contains the scenario frequencies. The third column correponds to the classification of the scenarios according to their frequencies. Together in this column are represented radioactive release and vessel damage. The last column is the code of the scenario. All in all, 325 scenarios are evaluated, based on 25 event trees. The key for the FTs and ETs top events is given at the end of Appendix 5.



No.	Freq.	Conseq.	Code
1	1.00E-01	AOO	
2	6.15E-04	DBE	LDRED-1LOOP-ESD
3	1.40E-06	BDBE,RELEAS	LDRED-1LOOP-ESD-DTC
4	3.11E-06	BDBE,VESSEL	LDRED-1LOOP-ESD-DT-EXT
5	3.02E-06	BDBE	SD-RODS
6	1.86E-08	CSDRD	SD-RODS-LDRED-1LOOP-ESD
7	4.24E-11	NOT_CSDRD	SD-RODS-LDRED-1LOOP-ESD-DTC
8	9.40E-11	NOT_CSDRD	SD-RODS-LDRED-1LOOP-ESD-DT-EXT
9	2.32E-08	CSDRD,DBA	SD-RODS-FSI-EXT
10	5.29E-11	NOT_CSDRD	SD-RODS-FSI-EXT-DTC
11	1.17E-10	NOT_CSDRD	SD-RODS-FSI-EXT-DT-EXT

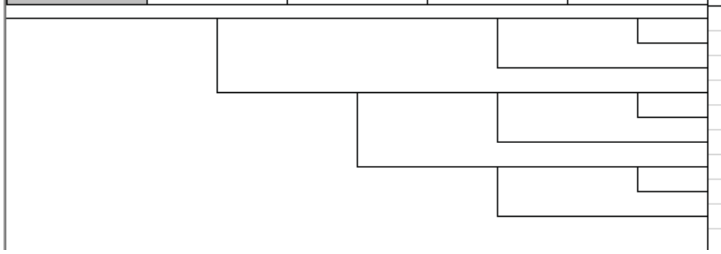


No.	Freq.	Conseq.	Code
1	1.00E-01	AOO	
2	6.15E-04	DBE	LDRED-1LOOP-ESD
3	1.40E-06	BDBE,RELEAS	LDRED-1LOOP-ESD-DTC
4	3.11E-06	BDBE,VESSEL	LDRED-1LOOP-ESD-DT-EXT
5	3.02E-06	BDBE	SD-RODS
6	1.86E-08	CSDRD	SD-RODS-LDRED-1LOOP-ESD
7	4.24E-11	NOT_CSDRD	SD-RODS-LDRED-1LOOP-ESD-DTC
8	9.40E-11	NOT_CSDRD	SD-RODS-LDRED-1LOOP-ESD-DT-EXT
9	2.32E-08	CSDRD,DBA	SD-RODS-FSI-EXT
10	5.29E-11	NOT_CSDRD	SD-RODS-FSI-EXT-DTC
11	1.17E-10	NOT_CSDRD	SD-RODS-FSI-EXT-DT-EXT



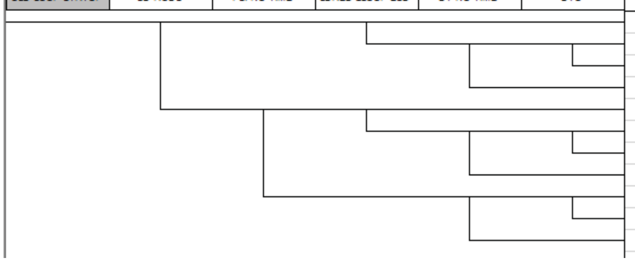
No.	Freq.	Conseq.	Code
1	2.00E-03	DBE	
2	4.56E-06	BDBE,RELEAS	DTC
3	1.41E-05	BDBE,VESSEL	DT-N
4	6.04E-08	CSDRD	SD-RODS
5	1.38E-10	NOT_CSDRD	SD-RODS-DTC
6	4.25E-10	NOT_CSDRD	SD-RODS-DT-N
7	5.83E-10	NOT_CSDRD,	SD-RODS-FSI-N
8	1.33E-12	NOT_CSDRD	SD-RODS-FSI-N-DTC
9	4.10E-12	NOT_CSDRD	SD-RODS-FSI-N-DT-N

Two loops secondary pump trip				
2LOOP-2PMP-TRIP	SD-RODS	FSI-N	DT-N	DTC



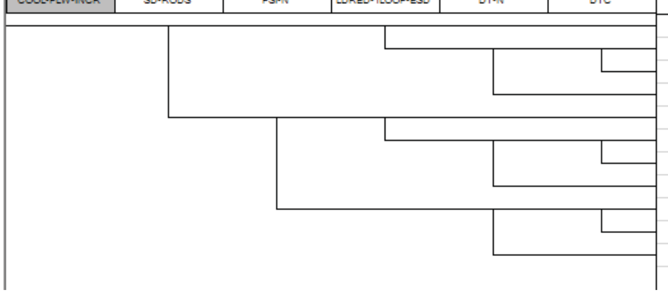
No.	Freq.	Conseq.	Code
1	2.00E-02	AOO	
2	4.56E-05	BDBE,RELEAS	DTC
3	1.41E-04	DBE,VESSEL_	DT-N
4	6.04E-07	BDBE	SD-RODS
5	1.38E-09	NOT_CSDRD	SD-RODS-DTC
6	4.25E-09	NOT_CSDRD	SD-RODS-DT-N
7	5.83E-09	NOT_CSDRD,	SD-RODS-FSI-N
8	1.33E-11	NOT_CSDRD	SD-RODS-FSI-N-DTC
9	4.10E-11	NOT_CSDRD	SD-RODS-FSI-N-DT-N

Cold loop startup					
CLD-LOOP-STRTUP	SD-RODS	FSI-NO-TIME	LDRED-2LOOP-ESD	DT-NO-TIME	DTC



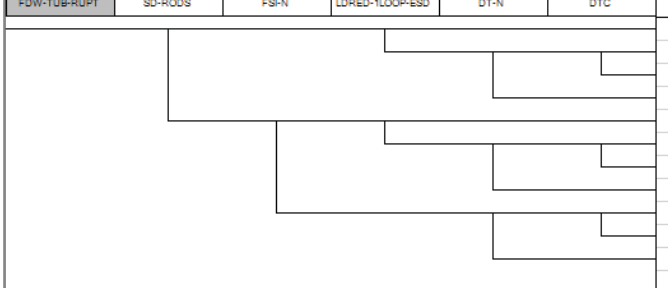
No.	Freq.	Conseq.	Code
1	1.00E-02	DBE	
2	7.87E-05	BDBE	LDRED-2LOOP-ESD
3	1.79E-07	CSDRD	LDRED-2LOOP-ESD-DTC
4	1.96E-06	BDBE,VESSEL	LDRED-2LOOP-ESD-DT-NO-TIME
5	3.02E-07	CSDRD	SD-RODS
6	2.38E-09	NOT_CSDRD	SD-RODS-LDRED-2LOOP-ESD
7	5.42E-12	NOT_CSDRD	SD-RODS-LDRED-2LOOP-ESD-DTC
8	5.93E-11	NOT_CSDRD	SD-RODS-LDRED-2LOOP-ESD-DT-NO-TIME
9	1.73E-08	CSDRD,DBA	SD-RODS-FSI-NO-TIME
10	3.94E-11	NOT_CSDRD	SD-RODS-FSI-NO-TIME-DTC
11	4.31E-10	NOT_CSDRD	SD-RODS-FSI-NO-TIME-DT-NO-TIME

Water cooling flow increase					
COOL-FLW-INCR	SD-RODS	FSI-N	LDRED-1LOOP-ESD	DT-N	DTC

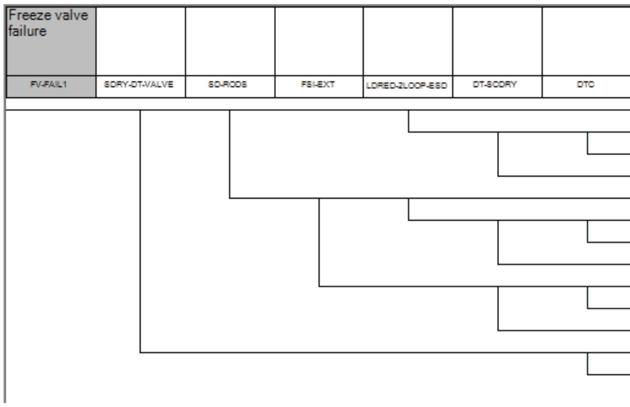


No.	Freq.	Conseq.	Code
1	3.10E-01	AOO	
2	1.91E-03	DBE	LDRED-1LOOP-ESD
3	4.35E-06	BDBE,RELEAS	LDRED-1LOOP-ESD-DTC
4	1.34E-05	BDBE,VESSEL	LDRED-1LOOP-ESD-DT-N
5	9.36E-06	BDBE	SD-RODS
6	5.76E-08	CSDRD	SD-RODS-LDRED-1LOOP-ESD
7	1.31E-10	NOT_CSDRD	SD-RODS-LDRED-1LOOP-ESD-DTC
8	4.05E-10	NOT_CSDRD	SD-RODS-LDRED-1LOOP-ESD-DT-N
9	9.03E-08	CSDRD,DBA	SD-RODS-FSI-N
10	2.06E-10	NOT_CSDRD	SD-RODS-FSI-N-DTC
11	6.35E-10	NOT_CSDRD	SD-RODS-FSI-N-DT-N

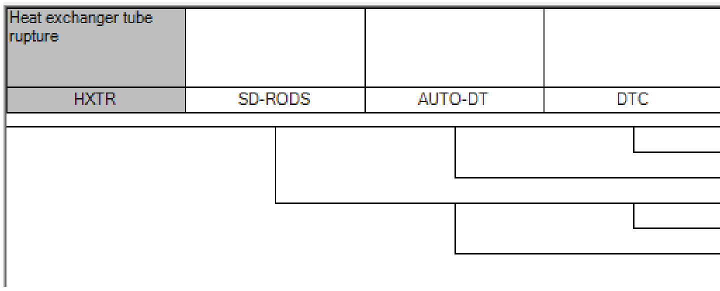
Feedwater tube rupture					
FDW-TUB-RUPT	SD-RODS	FSI-N	LDRED-1LOOP-ESD	DT-N	DTC



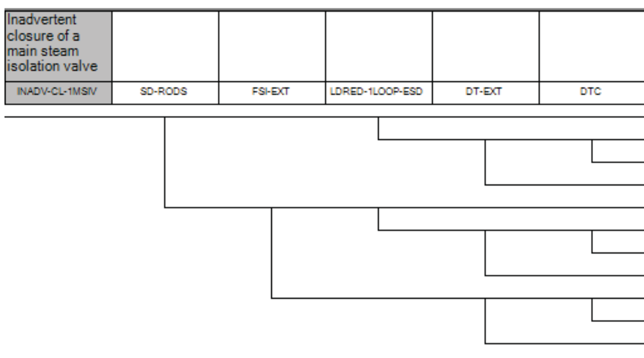
No.	Freq.	Conseq.	Code
1	5.00E-03	DBE	
2	3.08E-05	BDBE	LDRED-1LOOP-ESD
3	7.01E-08	CSDRD	LDRED-1LOOP-ESD-DTC
4	2.16E-07	CSDRD	LDRED-1LOOP-ESD-DT-N
5	1.51E-07	CSDRD	SD-RODS
6	9.29E-10	NOT_CSDRD	SD-RODS-LDRED-1LOOP-ESD
7	2.12E-12	NOT_CSDRD	SD-RODS-LDRED-1LOOP-ESD-DTC
8	6.53E-12	NOT_CSDRD	SD-RODS-LDRED-1LOOP-ESD-DT-N
9	1.46E-09	NOT_CSDRD,	SD-RODS-FSI-N
10	3.32E-12	NOT_CSDRD	SD-RODS-FSI-N-DTC
11	1.02E-11	NOT_CSDRD	SD-RODS-FSI-N-DT-N



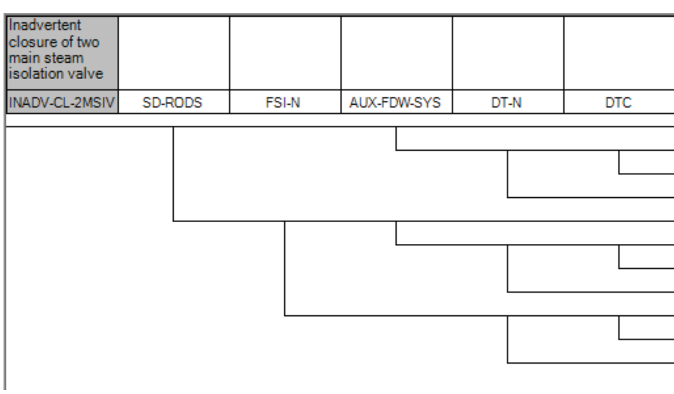
No.	Freq.	Conseq.	Code
1	4.83E-03	DBE	
2	3.80E-05	BDBE	LDRED-2LOOP-ESD
3	8.67E-08	CSDRD	LDRED-2LOOP-ESD-DTC
4	5.33E-07	CSDRD	LDRED-2LOOP-ESD-DT-SCDRY
5	1.46E-07	CSDRD	SD-RODS
6	1.15E-09	NOT_CSDRD	SD-RODS-LDRED-2LOOP-ESD
7	2.62E-12	NOT_CSDRD	SD-RODS-LDRED-2LOOP-ESD-DTC
8	1.61E-11	NOT_CSDRD	SD-RODS-LDRED-2LOOP-ESD-DT-SCDRY
9	1.12E-09	NOT_CSDRD	SD-RODS-FSI-EXT
10	2.55E-12	NOT_CSDRD	SD-RODS-FSI-EXT-DTC
11	1.57E-11	NOT_CSDRD	SD-RODS-FSI-EXT-DT-SCDRY
12	6.75E-05	BDBE,DBA	SDRY-DT-VALVE
13	1.54E-07	CSDRD	SDRY-DT-VALVE-DTC



No.	Freq.	Conseq.	Code
1	8.77E-03	DBE	
2	2.00E-05	BDBE,RELEAS	DTC
3	5.23E-05	BDBE,VESSEL	AUTO-DT
4	2.65E-07	CSDRD,DBA	SD-RODS
5	6.04E-10	NOT_CSDRD	SD-RODS-DTC
6	1.58E-09	NOT_CSDRD	SD-RODS-AUTO-DT

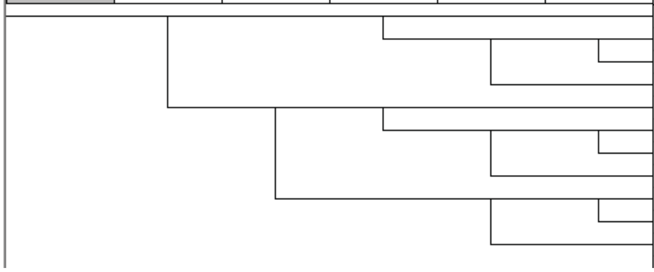


No.	Freq.	Conseq.	Code
1	2.40E-01	AOO	
2	1.48E-03	DBE	LDRED-1LOOP-ESD
3	3.37E-06	BDBE,RELEAS	LDRED-1LOOP-ESD-DTC
4	7.47E-06	BDBE,VESSEL	LDRED-1LOOP-ESD-DT-EXT
5	7.25E-06	BDBE	SD-RODS
6	4.46E-08	CSDRD	SD-RODS-LDRED-1LOOP-ESD
7	1.02E-10	NOT_CSDRD	SD-RODS-LDRED-1LOOP-ESD-DTC
8	2.26E-10	NOT_CSDRD	SD-RODS-LDRED-1LOOP-ESD-DT-EXT
9	5.57E-08	CSDRD,DBA	SD-RODS-FSI-EXT
10	1.27E-10	NOT_CSDRD	SD-RODS-FSI-EXT-DTC
11	2.82E-10	NOT_CSDRD	SD-RODS-FSI-EXT-DT-EXT



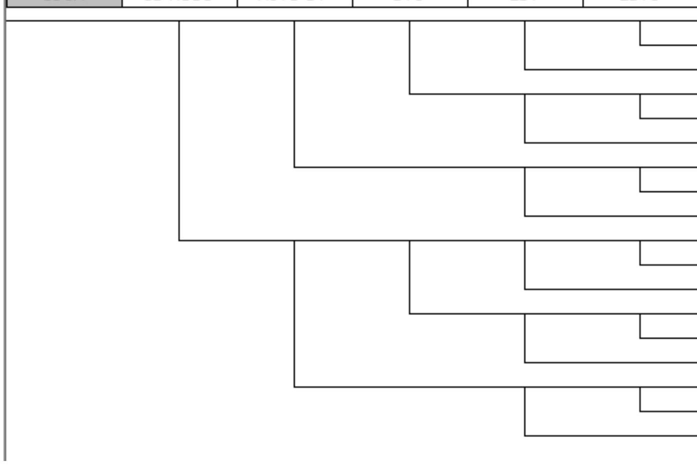
No.	Freq.	Conseq.	Code
1	6.14E-02	AOO	
2	2.09E-05	BDBE	AUX-FDW-SYS
3	4.77E-08	CSDRD	AUX-FDW-SYS-DTC
4	1.47E-07	CSDRD	AUX-FDW-SYS-DT-N
5	1.85E-06	BDBE	SD-RODS
6	6.32E-10	NOT_CSDRD	SD-RODS-AUX-FDW-SYS
7	1.44E-12	NOT_CSDRD	SD-RODS-AUX-FDW-SYS-DTC
8	4.44E-12	NOT_CSDRD	SD-RODS-AUX-FDW-SYS-DT-N
9	1.79E-08	CSDRD	SD-RODS-FSI-N
10	4.08E-11	NOT_CSDRD	SD-RODS-FSI-N-DTC
11	1.26E-10	NOT_CSDRD	SD-RODS-FSI-N-DT-N

Inadvertent opening of a steam generator relief					
INADV-OP-SGRV	SD-RODS	FSI-EXT	LDRED-1LOOP-ESD	DT-EXT	DTC



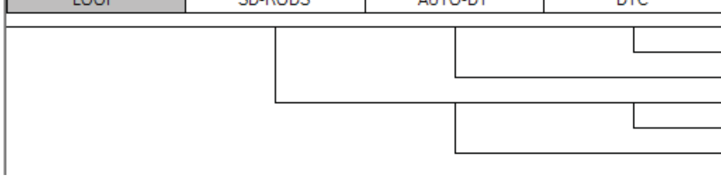
No.	Freq.	Conseq.	Code
1	1.40E-01	AOO	
2	8.62E-04	DBE	LDRED-1LOOP-ESD
3	1.96E-06	BDBE,RELEAS	LDRED-1LOOP-ESD-DTC
4	4.36E-06	BDBE,VESSEL	LDRED-1LOOP-ESD-DT-EXT
5	4.23E-06	BDBE	SD-RODS
6	2.60E-08	CSDRD	SD-RODS-LDRED-1LOOP-ESD
7	5.93E-11	NOT_CSDRD	SD-RODS-LDRED-1LOOP-ESD-DTC
8	1.32E-10	NOT_CSDRD	SD-RODS-LDRED-1LOOP-ESD-DT-EXT
9	3.25E-08	CSDRD,DBA	SD-RODS-FSI-EXT
10	7.41E-11	NOT_CSDRD	SD-RODS-FSI-EXT-DTC
11	1.64E-10	NOT_CSDRD	SD-RODS-FSI-EXT-DT-EXT

Leak from the primary circuit except the reactor vessel					
LOCA	SD-RODS	AUTO-DT	DTC	EDT	EDTC



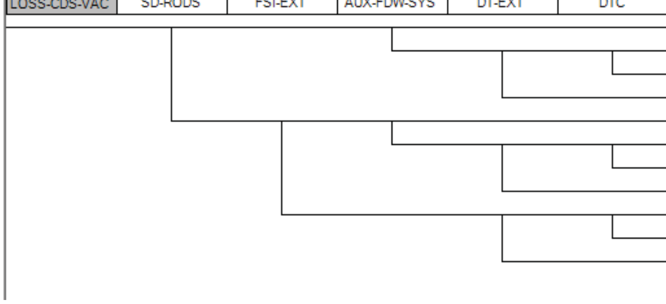
No.	Freq.	Conseq.	Code
1	2.00E-03	DBE	
2	2.19E-07	CSDRD	EDTC
3	7.95E-06	BDBE	EDT
4	4.56E-06	BDBE,RELEAS	DTC
5	5.00E-10	NOT_CSDRD	DTC-EDTC
6	1.81E-08	CSDRD	DTC-EDT
7	1.19E-05	BDBE	AUTO-DT
8	1.31E-09	NOT_CSDRD	AUTO-DT-EDTC
9	4.74E-08	CSDRD	AUTO-DT-EDT
10	6.04E-08	CSDRD,DBA	SD-RODS
11	6.63E-12	NOT_CSDRD	SD-RODS-EDTC
12	2.40E-10	NOT_CSDRD	SD-RODS-EDT
13	1.38E-10	NOT_CSDRD	SD-RODS-DTC
14	1.51E-14	NOT_CSDRD	SD-RODS-DTC-EDTC
15	5.47E-13	NOT_CSDRD	SD-RODS-DTC-EDT
16	3.60E-10	NOT_CSDRD	SD-RODS-AUTO-DT
17	3.95E-14	NOT_CSDRD	SD-RODS-AUTO-DT-EDTC
18	1.43E-12	NOT_CSDRD	SD-RODS-AUTO-DT-EDT

Loss of offsite power			
LOOP	SD-RODS	AUTO-DT	DTC

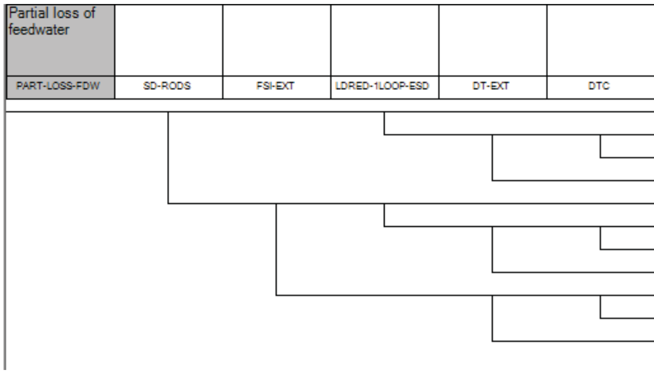


No.	Freq.	Conseq.	Code
1	1.50E-02	AOO	
2	3.42E-05	BDBE,RELEAS	DTC
3	8.94E-05	BDBE,VESSEL	AUTO-DT
4	4.53E-07	CSDRD	SD-RODS
5	1.03E-09	NOT_CSDRD	SD-RODS-DTC
6	2.70E-09	NOT_CSDRD	SD-RODS-AUTO-DT

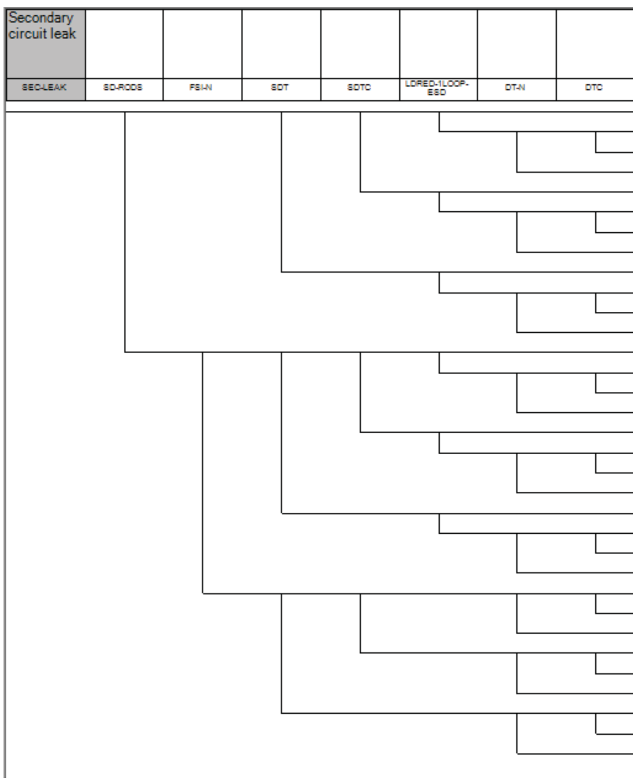
Loss of condenser vacuum					
LOSS-CDS-VAC	SD-RODS	FSI-EXT	AUX-FDW-SYS	DT-EXT	DTC



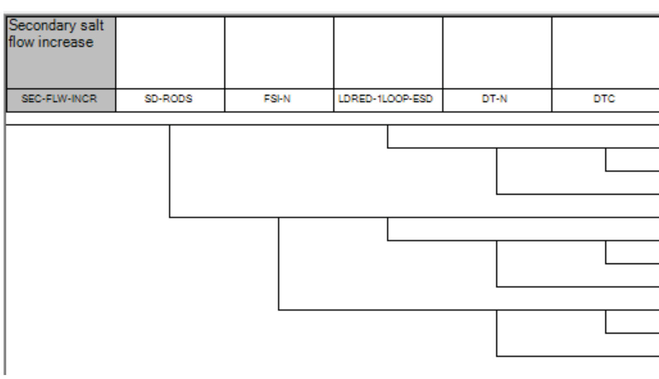
No.	Freq.	Conseq.	Code
1	4.10E-01	AOO	
2	1.40E-04	BDBE	AUX-FDW-SYS
3	3.19E-07	CSDRD	AUX-FDW-SYS-DTC
4	7.07E-07	BDBE,VESSEL	AUX-FDW-SYS-DT-EXT
5	1.24E-05	BDBE	SD-RODS
6	4.22E-09	NOT_CSDRD	SD-RODS-AUX-FDW-SYS
7	9.62E-12	NOT_CSDRD	SD-RODS-AUX-FDW-SYS-DTC
8	2.14E-11	NOT_CSDRD	SD-RODS-AUX-FDW-SYS-DT-EXT
9	9.52E-08	CSDRD	SD-RODS-FSI-EXT
10	2.17E-10	NOT_CSDRD	SD-RODS-FSI-EXT-DTC
11	4.81E-10	NOT_CSDRD	SD-RODS-FSI-EXT-DT-EXT



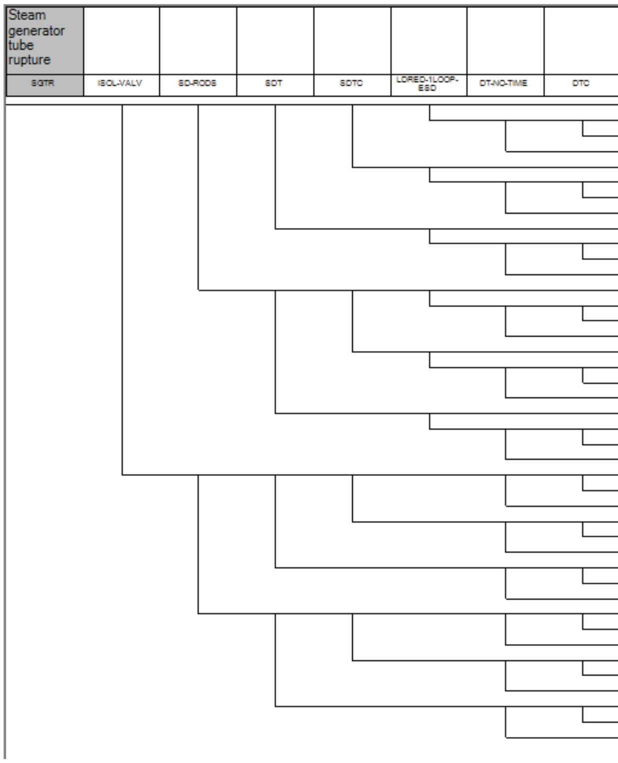
No.	Freq.	Conseq.	Code
1	1.00E-01	AOO	
2	6.15E-04	DBE	LDRED-1LOOP-ESD
3	1.40E-06	BDBE,RELEAS	LDRED-1LOOP-ESD-DTC
4	3.11E-06	BDBE,VESSEL	LDRED-1LOOP-ESD-DT-EXT
5	3.02E-06	BDBE	SD-RODS
6	1.86E-08	CSDRD	SD-RODS-LDRED-1LOOP-ESD
7	4.24E-11	NOT_CSDRD	SD-RODS-LDRED-1LOOP-ESD-DTC
8	9.40E-11	NOT_CSDRD	SD-RODS-LDRED-1LOOP-ESD-DT-EXT
9	2.32E-08	CSDRD,DBA	SD-RODS-FSI-EXT
10	5.29E-11	NOT_CSDRD	SD-RODS-FSI-EXT-DTC
11	1.17E-10	NOT_CSDRD	SD-RODS-FSI-EXT-DT-EXT



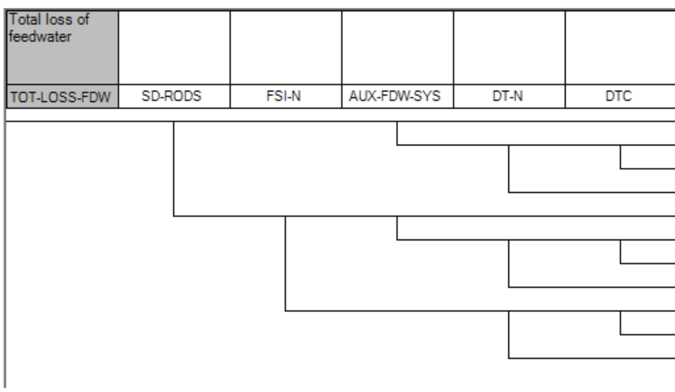
No.	Freq.	Conseq.	Code
1	2.00E-03	DBE	
2	1.23E-05	BDBE	LDRED-1LOOP-ESD
3	2.81E-08	CSDRD	LDRED-1LOOP-ESD-DTC
4	8.65E-08	CSDRD	LDRED-1LOOP-ESD-DT-N
5	1.12E-07	CSDRD	SDTC
6	6.89E-10	NOT_CSDRD	SDTC-LDRED-1LOOP-ESD
7	1.57E-12	NOT_CSDRD	SDTC-LDRED-1LOOP-ESD-DTC
8	4.84E-12	NOT_CSDRD	SDTC-LDRED-1LOOP-ESD-DT-N
9	1.26E-05	BDBE	SDT
10	7.78E-08	CSDRD	SDT-LDRED-1LOOP-ESD
11	1.77E-10	NOT_CSDRD	SDT-LDRED-1LOOP-ESD-DTC
12	5.47E-10	NOT_CSDRD	SDT-LDRED-1LOOP-ESD-DT-N
13	6.04E-08	CSDRD	SD-RODS
14	3.72E-10	NOT_CSDRD	SD-RODS-LDRED-1LOOP-ESD
15	8.47E-13	NOT_CSDRD	SD-RODS-LDRED-1LOOP-ESD-DTC
16	2.61E-12	NOT_CSDRD	SD-RODS-LDRED-1LOOP-ESD-DT-N
17	3.38E-12	NOT_CSDRD	SD-RODS-SDTC
18	2.08E-14	NOT_CSDRD	SD-RODS-SDTC-LDRED-1LOOP-ESD
19	4.74E-17	NOT_CSDRD	SD-RODS-SDTC-LDRED-1LOOP-ESD-DTC
20	1.46E-16	NOT_CSDRD	SD-RODS-SDTC-LDRED-1LOOP-ESD-DT-N
21	3.82E-10	NOT_CSDRD	SD-RODS-SDT
22	2.35E-12	NOT_CSDRD	SD-RODS-SDT-LDRED-1LOOP-ESD
23	5.36E-15	NOT_CSDRD	SD-RODS-SDT-LDRED-1LOOP-ESD-DTC
24	1.65E-14	NOT_CSDRD	SD-RODS-SDT-LDRED-1LOOP-ESD-DT-N
25	5.83E-10	NOT_CSDRD	SD-RODS-FSI-N
26	1.33E-12	NOT_CSDRD	SD-RODS-FSI-N-DTC
27	4.10E-12	NOT_CSDRD	SD-RODS-FSI-N-DT-N
28	3.26E-14	NOT_CSDRD	SD-RODS-FSI-N-SDTC
29	7.44E-17	NOT_CSDRD	SD-RODS-FSI-N-SDTC-DTC
30	2.29E-16	NOT_CSDRD	SD-RODS-FSI-N-SDTC-DT-N
31	3.68E-12	NOT_CSDRD,	SD-RODS-FSI-N-SDT
32	8.40E-15	NOT_CSDRD	SD-RODS-FSI-N-SDT-DTC
33	2.59E-14	NOT_CSDRD	SD-RODS-FSI-N-SDT-DT-N



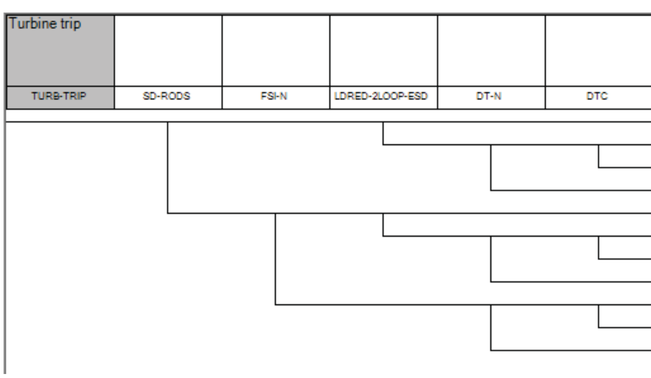
No.	Freq.	Conseq.	Code
1	3.10E-01	AOO	
2	1.91E-03	DBE	LDRED-1LOOP-ESD
3	4.35E-06	BDBE	LDRED-1LOOP-ESD-DTC
4	1.34E-05	BDBE	LDRED-1LOOP-ESD-DT-N
5	9.36E-06	BDBE	SD-RODS
6	5.76E-08	CSDRD	SD-RODS-LDRED-1LOOP-ESD
7	1.31E-10	NOT_CSDRD	SD-RODS-LDRED-1LOOP-ESD-DTC
8	4.05E-10	NOT_CSDRD	SD-RODS-LDRED-1LOOP-ESD-DT-N
9	9.03E-08	CSDRD,DBA	SD-RODS-FSI-N
10	2.06E-10	NOT_CSDRD	SD-RODS-FSI-N-DTC
11	6.35E-10	NOT_CSDRD	SD-RODS-FSI-N-DT-N



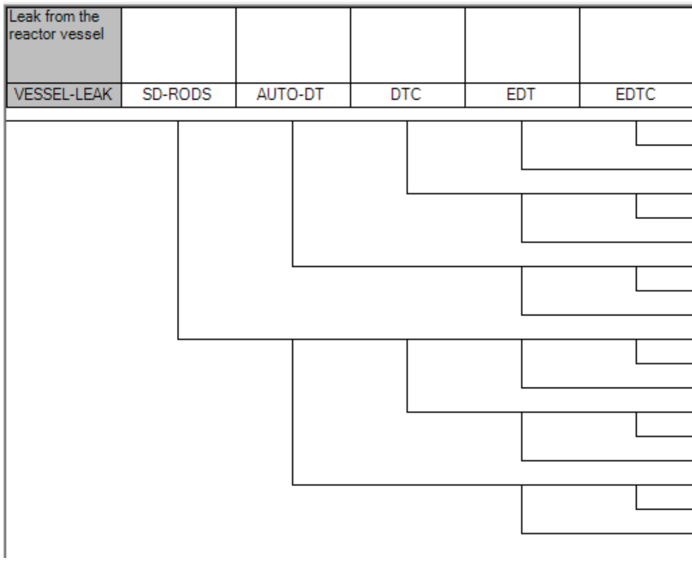
No.	Freq.	Conseq.	Code
1	5.52E-02	AOO	
2	3.40E-04	DBE	LDRED-1LOOP-ESD
3	7.74E-07	BDBE,RELEAS	LDRED-1LOOP-ESD-DTC
4	8.47E-06	BDBE,VESSEL_	LDRED-1LOOP-ESD-DT-NO-TIME
5	3.09E-06	BDBE,RELEAS	SDTC
6	1.90E-08	CSDRD	SDTC-LDRED-1LOOP-ESD
7	4.33E-11	NOT_CSDRD	SDTC-LDRED-1LOOP-ESD-DTC
8	4.74E-10	NOT_CSDRD	SDTC-LDRED-1LOOP-ESD-DT-NO-TIME
9	3.49E-04	DBE	SDT
10	2.15E-06	BDBE	SDT-LDRED-1LOOP-ESD
11	4.89E-09	NOT_CSDRD	SDT-LDRED-1LOOP-ESD-DTC
12	5.36E-08	CSDRD	SDT-LDRED-1LOOP-ESD-DT-NO-TIME
13	1.67E-06	BDBE	SD-RODS
14	1.03E-08	CSDRD	SD-RODS-LDRED-1LOOP-ESD
15	2.34E-11	NOT_CSDRD	SD-RODS-LDRED-1LOOP-ESD-DTC
16	2.56E-10	NOT_CSDRD	SD-RODS-LDRED-1LOOP-ESD-DT-NO-TIME
17	9.33E-11	NOT_CSDRD	SD-RODS-SDTC
18	5.74E-13	NOT_CSDRD	SD-RODS-SDTC-LDRED-1LOOP-ESD
19	1.31E-15	NOT_CSDRD	SD-RODS-SDTC-LDRED-1LOOP-ESD-DTC
20	1.43E-14	NOT_CSDRD	SD-RODS-SDTC-LDRED-1LOOP-ESD-DT-NO-TIME
21	1.05E-08	CSDRD	SD-RODS-SDT
22	6.49E-11	NOT_CSDRD,D	SD-RODS-SDT-LDRED-1LOOP-ESD
23	1.48E-13	NOT_CSDRD	SD-RODS-SDT-LDRED-1LOOP-ESD-DTC
24	1.62E-12	NOT_CSDRD	SD-RODS-SDT-LDRED-1LOOP-ESD-DT-NO-TIME
25	2.01E-04	DBE,VESSEL_D	ISOL-VALV
26	4.58E-07	CSDRD	ISOL-VALV-DTC
27	5.01E-06	BDBE,VESSEL_	ISOL-VALV-DT-NO-TIME
28	1.12E-08	CSDRD	ISOL-VALV-SDTC
29	2.56E-11	NOT_CSDRD	ISOL-VALV-SDTC-DTC
30	2.81E-10	NOT_CSDRD	ISOL-VALV-SDTC-DT-NO-TIME
31	1.27E-06	BDBE,VESSEL_	ISOL-VALV-SDT
32	2.90E-09	NOT_CSDRD	ISOL-VALV-SDT-DTC
33	3.17E-08	CSDRD	ISOL-VALV-SDT-DT-NO-TIME
34	6.07E-09	NOT_CSDRD	ISOL-VALV-SD-RODS
35	1.38E-11	NOT_CSDRD	ISOL-VALV-SD-RODS-DTC
36	1.51E-10	NOT_CSDRD	ISOL-VALV-SD-RODS-DT-NO-TIME
37	3.40E-13	NOT_CSDRD	ISOL-VALV-SD-RODS-SDTC
38	7.74E-16	NOT_CSDRD	ISOL-VALV-SD-RODS-SDTC-DTC
39	8.47E-15	NOT_CSDRD	ISOL-VALV-SD-RODS-SDTC-DT-NO-TIME
40	3.84E-11	NOT_CSDRD	ISOL-VALV-SD-RODS-SDT
41	8.74E-14	NOT_CSDRD	ISOL-VALV-SD-RODS-SDT-DTC
42	9.57E-13	NOT_CSDRD	ISOL-VALV-SD-RODS-SDT-DT-NO-TIME



No.	Freq.	Conseq.	Code
1	1.00E-02	AOO	
2	3.41E-06	BDBE	AUX-FDW-SYS
3	7.77E-09	NOT_CSDRD	AUX-FDW-SYS-DTC
4	2.40E-08	CSDRD	AUX-FDW-SYS-DT-N
5	3.02E-07	CSDRD	SD-RODS
6	1.03E-10	NOT_CSDRD	SD-RODS-AUX-FDW-SYS
7	2.35E-13	NOT_CSDRD	SD-RODS-AUX-FDW-SYS-DTC
8	7.24E-13	NOT_CSDRD	SD-RODS-AUX-FDW-SYS-DT-N
9	2.91E-09	NOT_CSDRD	SD-RODS-FSI-N
10	6.64E-12	NOT_CSDRD	SD-RODS-FSI-N-DTC
11	2.05E-11	NOT_CSDRD	SD-RODS-FSI-N-DT-N



No.	Freq.	Conseq.	Code
1	1.00E-01	AOO	
2	7.87E-04	DBE	LDRED-2LOOP-ESD
3	1.79E-06	BDBE,RELEAS	LDRED-2LOOP-ESD-DTC
4	5.54E-06	BDBE,VESSEL	LDRED-2LOOP-ESD-DT-N
5	3.02E-06	BDBE	SD-RODS
6	2.38E-08	CSDRD	SD-RODS-LDRED-2LOOP-ESD
7	5.42E-11	NOT_CSDRD	SD-RODS-LDRED-2LOOP-ESD-DTC
8	1.67E-10	NOT_CSDRD	SD-RODS-LDRED-2LOOP-ESD-DT-N
9	2.91E-08	CSDRD,DBA	SD-RODS-FSI-N
10	6.64E-11	NOT_CSDRD	SD-RODS-FSI-N-DTC
11	2.05E-10	NOT_CSDRD	SD-RODS-FSI-N-DT-N



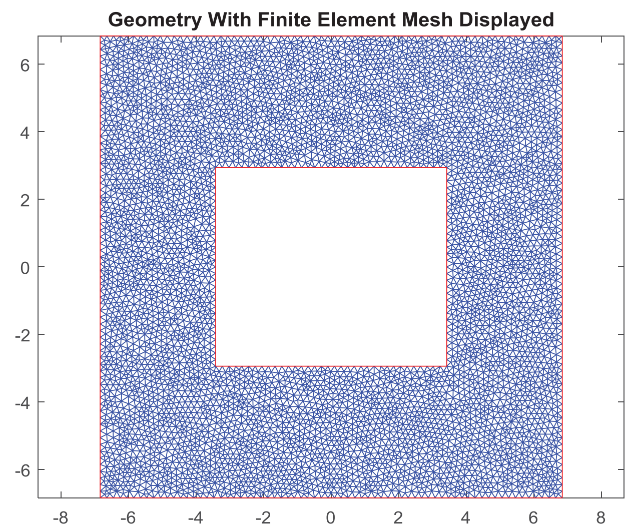
No.	Freq.	Conseq.	Code
1	8.00E-05	BDBE	
2	8.78E-09	NOT_CSDRD	EDTC
3	3.18E-07	CSDRD	EDT
4	1.82E-07	CSDRD	DTC
5	2.00E-11	NOT_CSDRD	DTC-EDTC
6	7.25E-10	NOT_CSDRD	DTC-EDT
7	4.77E-07	CSDRD	AUTO-DT
8	5.23E-11	NOT_CSDRD	AUTO-DT-EDTC
9	1.89E-09	NOT_CSDRD	AUTO-DT-EDT
10	2.42E-09	NOT_CSDRD	SD-RODS
11	2.65E-13	NOT_CSDRD	SD-RODS-EDTC
12	9.60E-12	NOT_CSDRD	SD-RODS-EDT
13	5.51E-12	NOT_CSDRD	SD-RODS-DTC
14	6.04E-16	NOT_CSDRD	SD-RODS-DTC-EDTC
15	2.19E-14	NOT_CSDRD	SD-RODS-DTC-EDT
16	1.44E-11	NOT_CSDRD	SD-RODS-AUTO-DT
17	1.58E-15	NOT_CSDRD	SD-RODS-AUTO-DT-EDTC
18	5.72E-14	NOT_CSDRD	SD-RODS-AUTO-DT-EDT

Table 19: Key for FTs and ETs top events

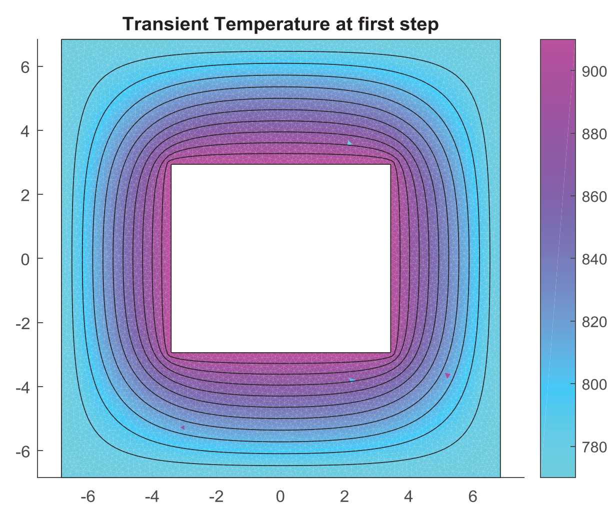
ID	Function	Failure
SD_RODS	Insertion of shutdown rods	Failure to insert
FSI	Inject fertile fuel salt into the primary circuit	Failure to inject
DT	Use of the freeze valve to drain the primary fuel salt	Freeze valve failure to open
DTC	Cooling of the drain tank	Failure to cool
SDT	Use of the freeze valve to drain the secondary fuel salt	Freeze valve failure to open
SDTC	Cooling of the secondary drain tank	Failure to cool
EDT	Collect of the fuel salt in case of a LOCA	Valve failure to open
EDTC	Cooling of the emergency drain tank	Failure to cool
SCDRY_VALVE	Use of the secondary valve to keep the fuel salt in the primary circuit	Failure to close the valve
AUTO-DT	Automatic use of the DT	Freeze valve failure to open
ISOL_VALVE	Use of a secondary relief valve	Failure to open
AUX-FDW-SYS	Auxiliary feedwater system	Failure to operate
LDRED-1LOOP-ESD	Load reduction after emergency shutdown with only one loop	Failure to operate
LDRED-2LOOPS-ESD	Load reduction after emergency shutdown with two loops	Failure to operate

Appendix 6: Heat transfer inside the HTC

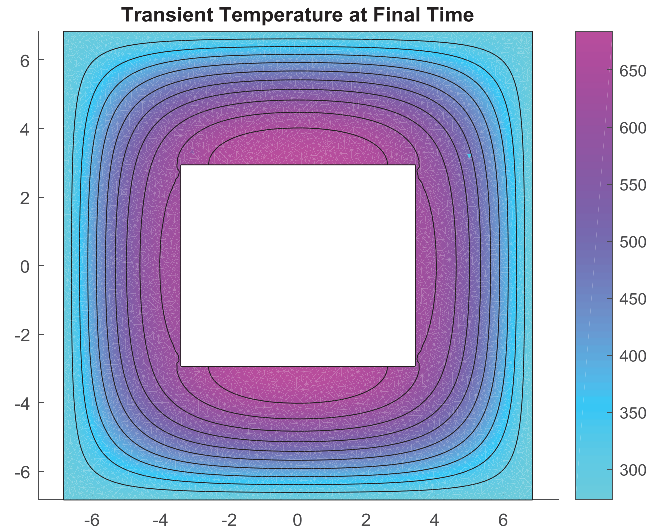
The heat transfer inside the High Temperature Containment is studied in order to screen out the IE "loss of power supply to the HTC" if it has almost no consequence for the reactor operation. The time necessary to freeze the fuel salt at the reactor vessel is estimated, supposing that the containment is inertized by argon, and conservatively supposing that no heat is produced by the primary loop (no decay heat). The reactor and the HTC are cylinders, so that we can model the problem in two dimensions. The model of the reactor vessel and its containment is shown below, together with its meshing for the simulation. The heat equation is solved on the different nodes of the mesh. The dimensions in the graphs are in meters.

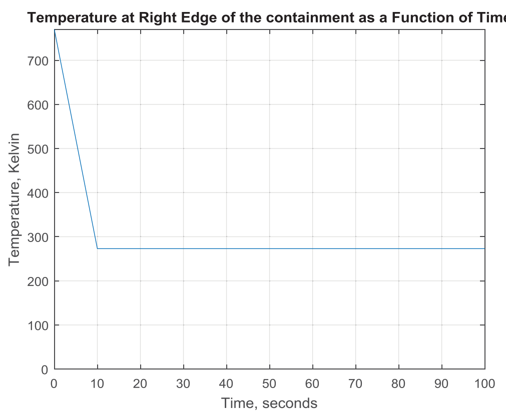


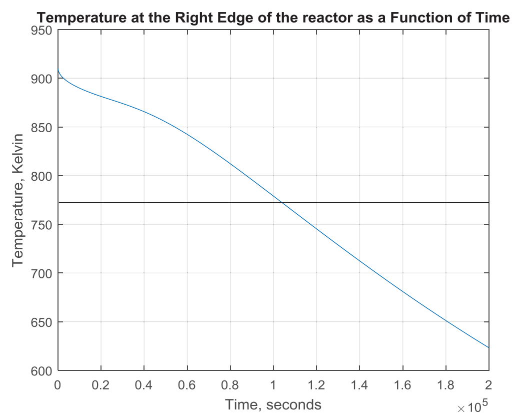
The initial state of the system calculated at steady state is shown below:

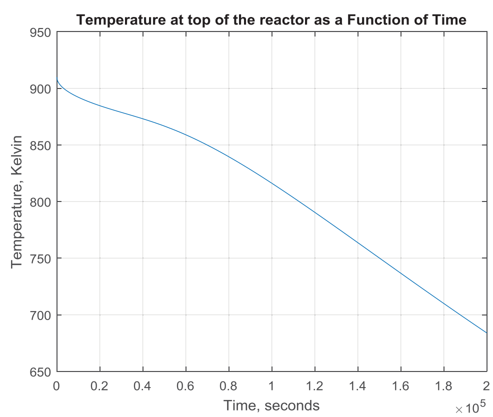


Then High Temperature Containment heating is removed. It is conservatively assumed that the temperature of the containment drops in 10 s to 273 K. The temperatures at the final step, together with the temperature at the reactor boundary and containment boundary are shown below:









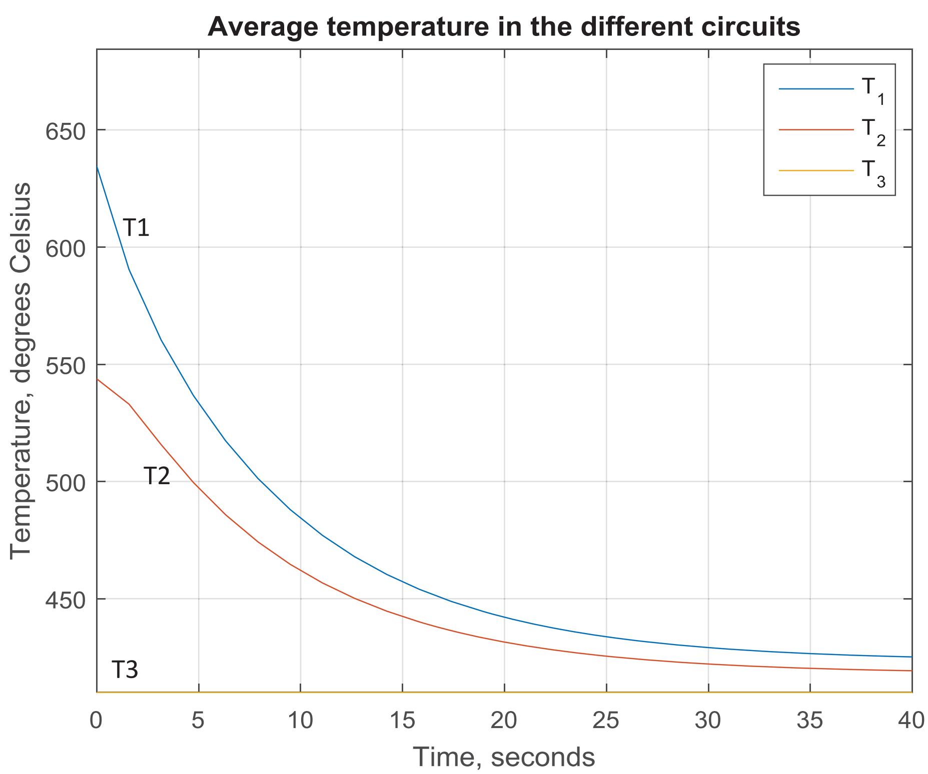
Despite the conservative assumptions, the simulation showed that more than 26 hours are necessary to freeze the salt at the reactor vessel if the reactor is tripped given the freeze valve failure. It is sufficient to react to this accident by manually opening the freeze valve (external heating for instance). That is why the HTC failure is assumed not to be a threat for the reactor operation. Therefore, its failure is not developed in the event trees.

Appendix 7: Heat transfer at the heat exchangers

The heat transfer at the heat exchangers is studied in order to assess if human action can be considered to reduce the load after an emergency shutdown. Indeed, if the flow rates of the secondary and tertiary loops are not reduced, then freezing at the heat exchangers could occur. In order to evaluate the time necessary for the freezing to happen, three heat exchange models between the three circuits of the FUJI-233Um reactor and the environment have been implemented. The model used is very simple:

- The initial temperatures of the circuits are constant and equal to their means
- The heat exchange is modelled by the Newton's law of cooling (heat transfer coefficient given in reference [20])
- The power is represented by a tuned coefficient, so that the temperatures are constant at operating conditions
- When the reactor trip is initiated, the power is set at the decay heat level
- When a temperature change is initiated, the temperature change is exponential

The result for the reactor trip is presented below:



The numbers 1, 2 and 3 represent the primary, secondary and tertiary circuits respectively. The result of this study is that if the cooling is not reduced after a reactor trip, then freezing occurs in some seconds. That is why human action is not credited for this system.