A Risk and Reliability Analysis of a Sodium-Cooled Fast Nuclear Reactor

The ASTRID Prototype

By

GUILLAUME L'HER

Department of Mechanical Engineering
COLORADO SCHOOL OF MINES

A project submitted for the Risk and Reliability Engineering class at the Colorado School of Mines.

DECEMBER 2016

Executive Summary

Various risk and reliability analysis methods were applied to the ASTRID nuclear reactor design. The design demonstrated remarkable safety features, with exceedingly low chances of accidents causing the release of radioactivity in the environment. A more complete analysis could reveal potential cost savings actions while keeping the system safety extremely high.

This improved safety comes at the cost of a slightly downgraded reliability, with the reactor being shutdown preemptively in numerous cases as part of the defense system. It is recommended to consider a coupled system for electricity generation to cover for most of the plant downtime and drastically increase cost effectiveness.

One of the point of interest seen in this analysis that would merit a more in depth analysis is the loss of offsite power, forcing the use of numerous, historically often unreliable, backup generators and shutting down the plant due to lack of powered sensors in the core. Alternative electricity generation solution should be studied.

This analysis should be repeated with greater details once the design is more advanced, in order to confirm the findings of this document and potentially make informed cost-saving modifications.

The numbers and design choices considered in this study are based on the author's engineering background and may not reflect the reality. While the qualitative conclusions can be taken with a reasonable degree of confidence, the values given in this document should not be reused for an official risk and reliability analysis. Due to time constraints, several subsystems and paths to failure have been ignored in this document. Those intentional omission may prove to be more limitating than the ones explicited.

Abstract

The importance of understanding, assessing, communicating, and making decisions based in part upon risk, reliability, robustness, and uncertainty is rapidly increasing in a variety of industries (e.g.: petroleum, electric power production, etc.) and has been a focus of some industries for many decades (e.g.: nuclear power, aerospace, automotive, etc). This project aims at applying a number of different risk and reliability analysis methods to gain insight on a particular complex system.

One of the leading industry in the risk and reliability engineering field is the nuclear power industry. Nuclear power is coming to a turning point, which will likely decide its future. Second generation reactors designs, developed in the 50s and 60s, are used today to generate most of the world's nuclear energy. Accidents like Chernobyl and Fukushima have led to heavy criticism of the nuclear industry by a large number of lay people.

Several third generation reactor designs are being built today to replace the world aging nuclear fleet, but they are already under criticism, being considered too risky. The fourth generation reactor design developments are still underway, and have the ability to change lay people's view on this source of energy. This can be accomplished only if the risks are analyzed and taken into account to the best of our abilities, and if these studies' results are communicated efficiently to the unforgiving public opinion.

In that regard, a fourth generation nuclear reactor prototype, the Advanced Sodium Technological Reactor for Industrial Demonstration (ASTRID), is under development by the CEA in France. Its goal is to demonstrate the feasability of such designs, from a technical and economical standpoint. A particularly interesting point in light of this study is that this Sodium-cooled design presents some obvious risks, sodium-water and sodium-air interactions, and an interesting history.

TABLE OF CONTENTS

List of Tables

List of Figures

List of Acronyms

ASTRID Advanced Sodium Technological Reactor for Industrial Demonstration.

CFV Coeur a Faible Vidange, Low Void Worth Core.

CRFFA Cable Routing Function Failure Analysis.

EBR Experimental Breeder Reactor.

FBED Functional Basis for Engineering Design.

FFDM Function Failure Design Method.

FFIP Funtion Failure Identification and Propagation.

FMEA Failure Modes and Effects Analysis.

FMECA Failure Modes, Effects and Criticality Analysis.

FSL Function State Logic.

HRA Human Reliability Assessment.

PHM Prognostic Health Management.

PRA Probabilistic Risk Assessment.

RBD Reliability Block Diagram.

RPN Risk Priority Number.

SFR Sodium-cooled Fast Reactor.

STA Success Tree Analysis.

UFFSR Uncoupled Flow Failure State Reasoning.

CHAPTER 1

INTRODUCTION

Nuclear power is coming to a turning point, which will likely decide its future. Second generation reactors designs, developed in the 50s and 60s, are used today to generate most of the world's nuclear energy. Accidents like Chernobyl and Fukushima have led to heavy criticism of the nuclear industry by a large number of lay people.

Several third generation reactor designs are being built today to replace the world aging nuclear fleet, but they are already under criticism, being considered too risky. The fourth generation reactor design developments are still underway, and have the ability to change lay people's view on this source of energy. This can be accomplished only if the risks are analyzed and taken into account to the best of our abilities, and if these studies' results are communicated efficiently to the unforgiving public opinion.

1.1 A brief design introduction

One of the designs currently under development is the Sodium-cooled Fast Reactor (SFR). This is the most advanced fourth generation reactor design, and around twenty SFRs have already been operated throughout the world. First introduced by the USA in 1951 in Idaho Falls, Russia, France and Japan are today the main players, with India and China having also recently developed their prototypes. Two different designs exist for the SFR, pool-type (figure 1.1, figure 1.2) and loop-type (figure 1.2) [21]. This study will focus on the pool-type design.

Table 1.1 shows a simplified comparison of the pros and cons of this fourth generation design, not inherently specific to the SFR. Some advantages and inconvenients are found in other GEN IV designs.

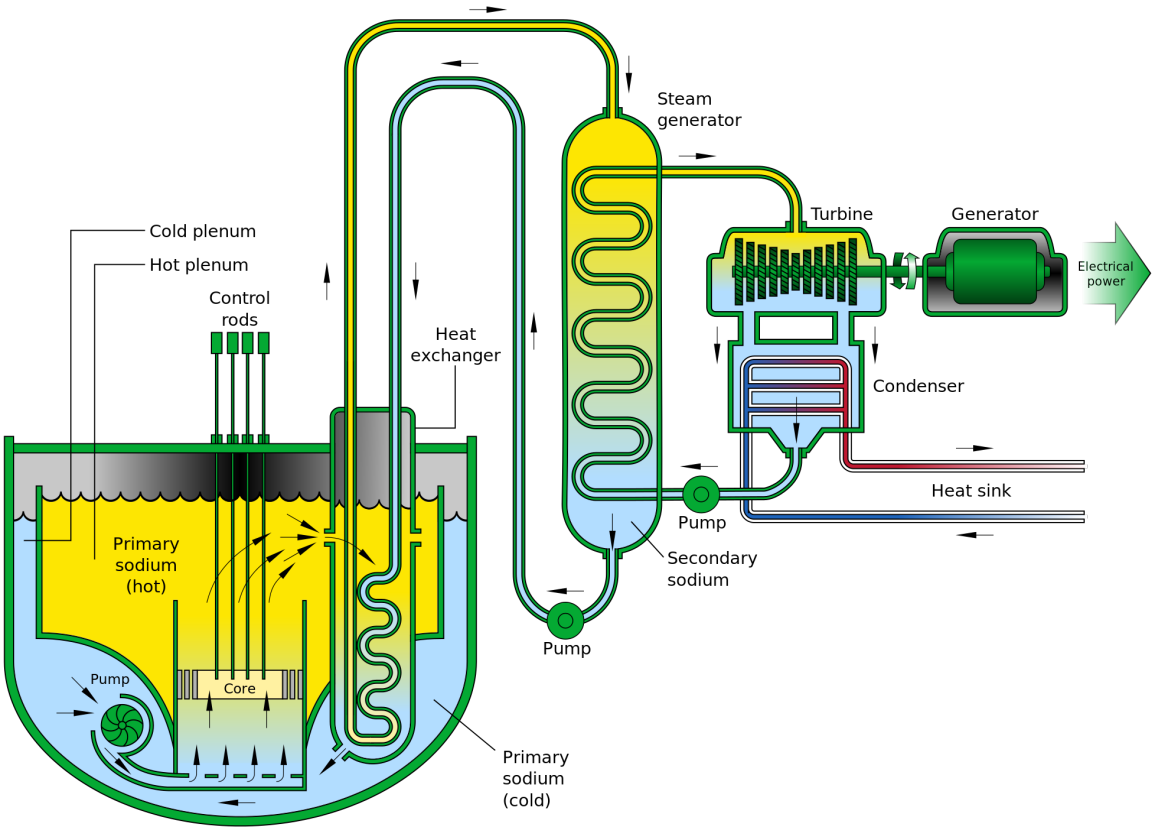

FIGURE 1.1. Pool type sodium-cooled fast reactor.

Category	Pros	Cons
Technology	Flexible fuel cycle (U, Pu, Th) Breeding and Transmutation Core power density High thermal efficiency	Opaqueness of Na Na reacts with air and water Shielding fast spectrum High operation temperatures
Economics		Expensive R&D Expensive design
Politics		New set of regulations
Environment	Waste reduction	
Opinions		Hostile public opinion

Table 1.1: Highly simplified advantages/inconvenients table for the SFR design

1.2 A bit of history

Several SFR have been in operation in the world, accumulating around 400 reactor-years of feedback. Even though the technologies used in each reactor design is not identical, similarities

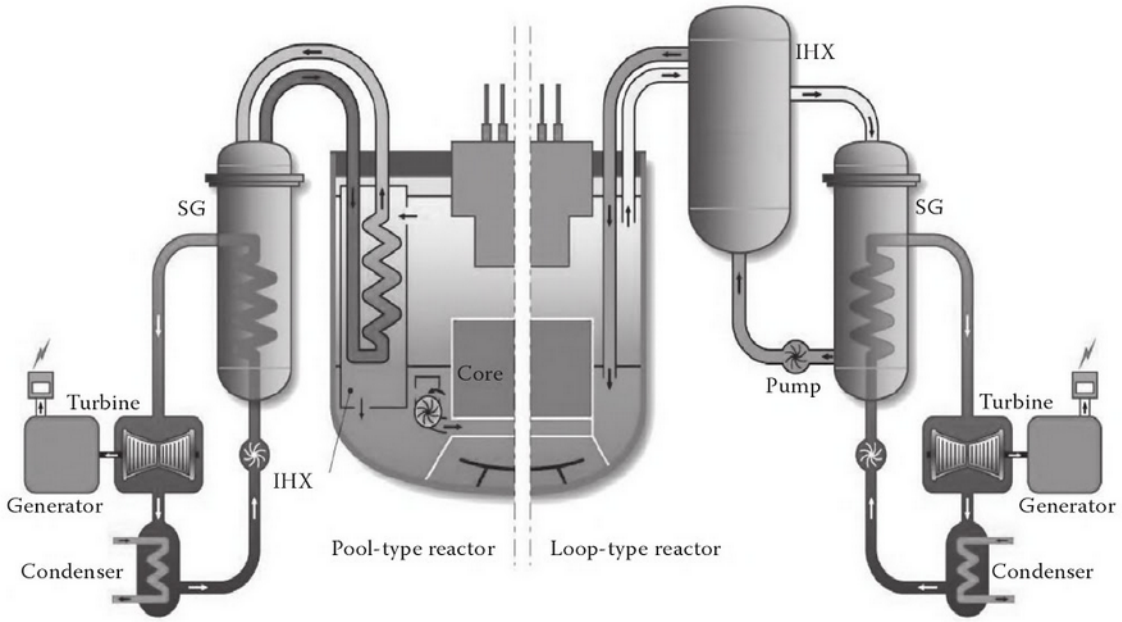

FIGURE 1.2. Pool-type vs Loop-type sodium-cooled fast reactor.

are such that parallels can be drawn and applied to our case study design. Some of the reactors in this international feedback are loop-type, instead of the pool-type design considered in this study, but most incidents and repairs would be applicable to both designs.

The feedback from the different reactors show one recurrent failure, sodium leaks. Even though the consequence of this failure have not had catastrophic consequences, they could potentially be important. Notably, they will be one of the main point of interest during public debates. Failure modes causing sodium leak (loss of coolant, fire and explosion hazard), especially on a large scale, will thus be considered with attention.

1.2.1 A focus on SUPERPHENIX

The French Superhenix reactor demonstrates the impact of politics, public opinion and risk communication in the nuclear industry.

The reactor diverged in 1985 and was connected to the grid and reached full power in 1986, just as Chernobyl was happening. The worries that arose from the well-known accident caused an extremely violent opposition to the project. Several anti-nuclear organizations hence protested the project after Chernobyl, causing one death. It is to be noted that a rocket was even fired at the power plant.

Consequently, due to growing concerns from the general public and political sides, the plant was shut down for extended periods of time not prominently for safety reasons, but mostly for

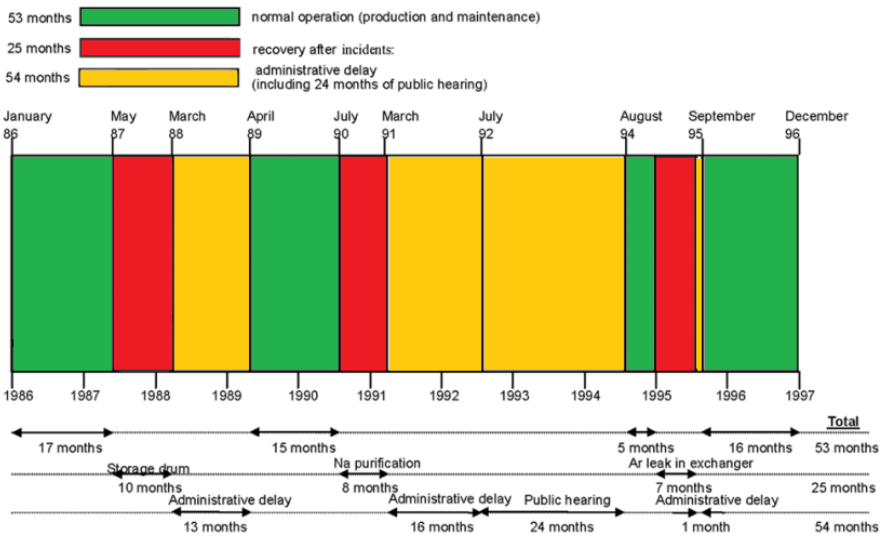

FIGURE 1.3. Operation timeline for the SUPERPHENIX reactor [7].

administrative ones, and finally closed in 1997 following a political decision in an election period. In total, the plant was shut down 54 months due to purely administrative reasons [8], when it would have been perfectly able to operate, over its 10 years operation (figure 1.3).

This decision happened after the most productive year yet in the plant operation history, and caused a substantial loss, as the plant had to shut down in the middle of its cycle, wasting partially burnt up assemblies in the core and a whole new core refuel already assembled. The plant was supposed to stay online until at least 2015, and its early termination caused the operating company, EDF, to lose around roughly 4 billions dollars (lost fuel and partners reimbursement), on top of the lost revenues.

However, even though the decision to suddenly terminate the Superphenix project was mostly political, and driven by public opinion in the wake of Chernobyl, it would be wrong to consider that the technology used in this plant design was flawless and mastered, as obviously no system can be perfectly safe and reliable, and this was after all a prototype. The experts working on the project could not efficiently prove the system's safety to the (albeit ferociously opposed and potentially irrational) public. Failing such a crucial project in a "Nuclear country" could be a sign of an endangered industry going forward, a lack of communication skills from the experts, or a faulty design which could not be solidly defended.

The shortfalls of Superphenix notably, and a few other SFR designs, will be used in this analysis to derive potential design flaws and communication problems and find some possible mitigations for the new French prototype ASTRID, coming in the wake of yet another nuclear accident, Fukushima.

1.2.2 International feedback

1.2.2.1 American power plants

After World War II, the USA were undeniably leaders in the nuclear industry, experimenting on a variety of audacious designs. They were the first to experiment with liquid-metal fast reactors, and in particular sodium-cooled reactors.

SODIUM REACTOR EXPERIMENT (1957-1964) was built to demonstrate the feasibility of a sodium-cooled reactor as the heat source for a commercial power reactor to produce electricity. It actually experienced the first consequent meltdown of part of its (small) core in July 1959 [2].

FERMI-I (1963-1972) was a 70MWe plant designed to test the feasability of breeding [15]. It also suffered a partial meltdown in 1966, following a loss of coolant incident that was detected too late.

EBR-I (1951-1964) and EBR-II (1965-1994) were two Experimental Breeder Reactor (EBR), prototype of sodium-cooled fast reactors. EBR-II was one of the first reactors to exhibit passive safety systems that were tested and proven functional.

1.2.2.2 French power plants

France has favored the Sodium-cooled fast reactors design in its history, following some american ideas and experiments.

RAPSODIE (1967-1983) was a pool-type prototype, the first of its kind built in France. Sodium aerosols were detected in the main vessel at some point, indicating a leak, which was not found. After the prototype was shut down, during the decommissioning, an explosion caused by an overpressure occurred in a sodium tank, killing one engineer and injuring four others.

PHENIX (1973-2010) followed in RAPSODIE footsteps. Several issues arose during the operation of this reactor. Those issues were identified and solved. They included numerous (32) sodium leaks and several (5) sodium-water reactions. In 2002, an explosion occurred in an almost empty sodium tank, due to water infiltrations after heavy rains. In 2008, an audit revealed important flaws in the plant anti-fire surveillance software.

SUPERPHENIX (1985-1997), discussed in greater details in 1.2.1, also exhibited sodium leaks, including, in 1987, one near the safety vessel, due to steel-corrosion from an alloy not tested in its predecessors. Fixing this problem actually caused the loss of the fuel assemblies stockage ability, which penalized the subsequent plant operations. In 1990, the primary sodium got polluted, due to a defective membrane in a compressor. All in all though, the incidents in the primary circuit were scarce.

However, the plant underwent some more conventional troubles that impacted strongly the power generation. The machines room roof gave in after a snowstorm in 1990, and the initial design called for a 1200 MWe turbine, but the plant was finally equipped with two 600 MWe instead, impacting the plant grid availability.

1.2.2.3 Russian power plants

The reactors BN-350 (1973-1999) and BN-600 (1980-present) both experienced several sodium leaks, causing sodium fires for a couple hours. Not a lot of information is publicly available for those reactors.

1.2.2.4 Japanese power plants

Japan decided to go toward the loop-type design reffig:c1f2. JOYO was in operation for 30 years (1977-2007), and stopped its operations after an incident during fuel handling, preventing any subsequent core reload until removal of a bent subassembly. On december 8, 1995, the secondary circuit of MONJU (1986-present, but never in full operation) started vibrating, causing the leak of several hundreds kilograms of sodium. A fire happened with no automatic reactor shutdown. The reactor had to be shut down manually more than a hour later.

CHAPTER 2

CASE STUDY

The case study that will be considered for this project is a new SFR technological demonstration reactor design, the ASTRID. Studying such a huge complex system as a nuclear reactor can be daunting and unfeasible in a limited amount of time. In the context of this project, the systems and components that will be studied, as well as the level of details that will be considered, are described in this chapter.

2.1 ASTRID

The ASTRID prototype, a Sodium-cooled pool-type Fast Reactor design, is currently designed by the CEA in Cadarache, France. This research reactor will have a thermal output of 1500 MWth, generating around 600 MWe. The goal of this prototype is to show the improvement in the sodium-cooled fast reactors design area since Superphenix, and most notably demonstrate the minor actinides transmutation possibilities offered by this design.

As it represents the future of this reactor design option in France, and, if successful, potentially a larger scope internationally, this reactor will act as the case study. In that regards, this document aims to show how well the design respond to recent engineering methods for risk and reliability analysis, in the event of significant incidents and loss of functionality, and to discuss how the findings can be accurately passed onto the public opinion. Moreover, it will consider the reliability aspect during some transient situation, in order to identify and mitigate the loss of electrical power generation.

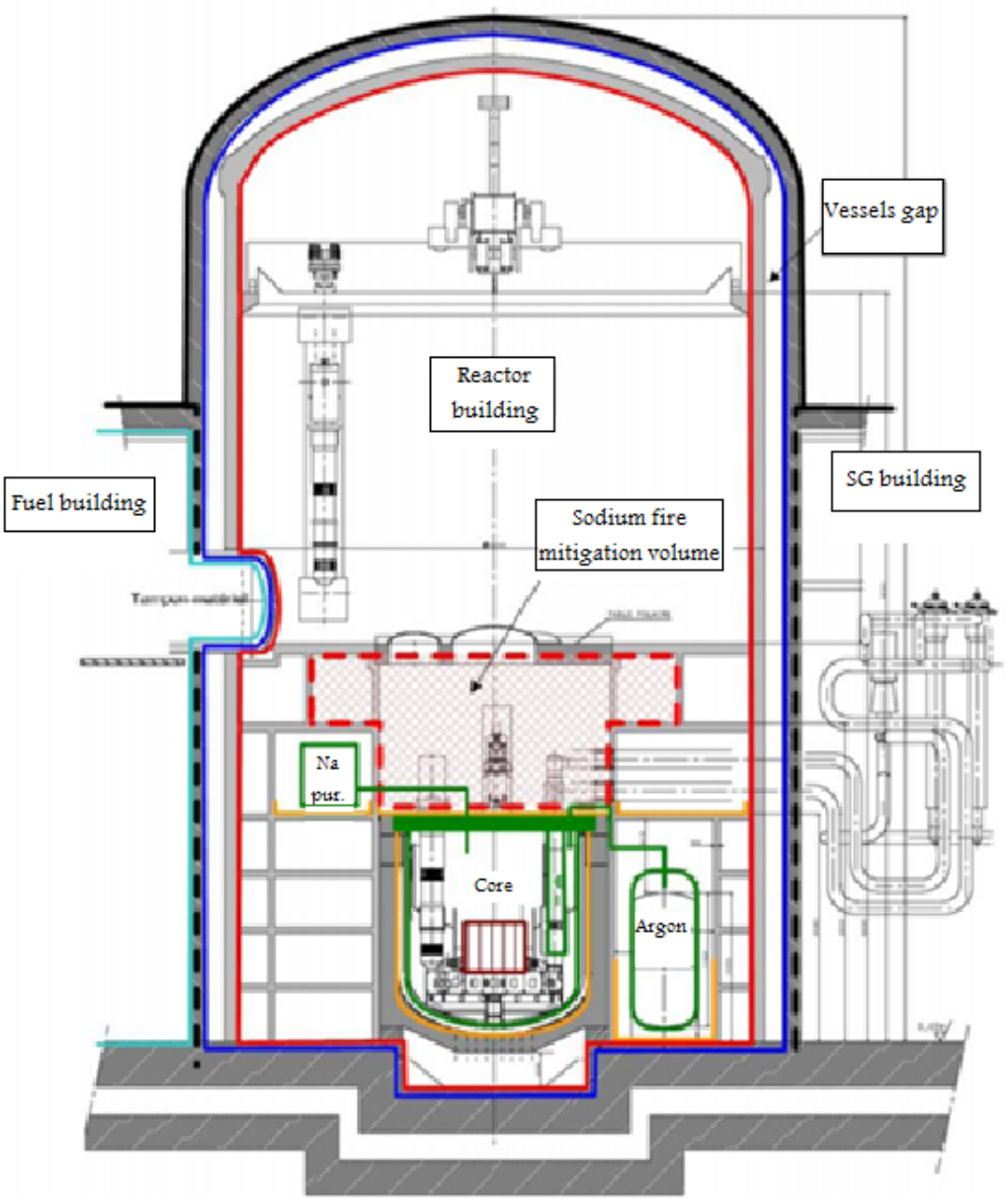

FIGURE 2.1. ASTRID reactor building generic schematics

2.2 Case study

During this case study, state-of-the-art risk and reliability analysis methods will be applied to the system. The main failures of interest will be put in two categories, risk and reliability. The risk, or safety, failures are those that can cause a core meltdown or a radioactive contamination of the environment or workforce, either by themselves or combined with one or more uncoupled failures. The reliability failures are the ones that would cause a loss of electricity generation, and

thus render the whole system mostly inoperant. It is interesting to consider the fact that for this particular system, the loss of electricity generation capability is not by itself sufficient to deem the system inoperable, since the secondary plant objective, minor actinides transmutation, could still be taking place. Thus, by intended system goals, reliability issues are mitigated due to their diversity.

The system of interest is defined as including the components identified within the following sections. Due to scarce publicly available information on the detailed reactor designed, notably redundancies, the author has exerted his judgement and experience as a nuclear engineer to use a model deemed representative of reality.

2.2.1 Generic

This category contains components which are found throughout the plant and are identified as a cause of likely failures, according to historical data. For example, pipes and valves can be found in this sections. Depending on the level of details, bolts, screws, and other small component could also be identified.

2.2.2 Reactor core

This reactor core design presents several natural objectives:

- No sodium boiling
- Negative sodium void effect
- No fuel pellet meltdown
- High performance (cycle length and fuel burn-up)

Those objectives should be met by design. Consequently, a type of core (Coeur a Faible Vidange, Low Void Worth Core (CFV), [5]), optimized for low sodium void effect, has been developed by the CEA. This does not mean that such risk or reliability failures will now be ignored, but they will be classified as less likely to occur.

The main components of the reactor core that will be considered are:

- Fuel assemblies

  The fuel assemblies contains the radioactive fuel elements

- Control rods

  The control rods allows the emergency shutdown of the chain reaction and the modulation of the power output.

- Neutron detectors

  These detectors gives precious information on the neutron activity inside the core.

- Thermocouples

  These temperature detectors give needed information on the temperature within the fuel and in the primary sodium.

2.2.3 Reactor structure

This category includes the different vessels and concrete elements in the whole system. Two main types can be identified, the structure surrounding the primary circuit and the ones surrounding the secondary circuit and other. For the primary circuit, those are notably:

- Inner vessel

  This structure separates the hot primary sodium from the cold primary sodium.

- Main vessel

  This is the main vessel, separating the primary circuit from the secondary circuit and the environment.

- Safety vessel

  This is an envelope of the main vessel insuring supplementary containment.

- Roof

  This can be considered part of the main vessel, but it does support other components, and as such is treated differently.

- Core catcher

  This is a safety system in case of a meltdown, to prevent the corium from spilling out of a controlled area.

For the secondary circuit and other systems, those can be:

- Command room

  This structure houses the command controls.

- Intervention paths

  This includes the tunnels or hallways leading to different parts of the site.

- Secondary systems building

  This building houses the turbines, condensers, secondary electromagnetic pumps, and other secondary systems and elements.

- Spent fuel pools

  This element allows for stocking the spent and new fuel assemblies before, during or after a fuel loading.

In this case study, only the primary systems structure will be considered. However, secondary structures failures might also be identified in some failure modes.

2.2.4 Primary circuit components

The considered components in the primary circuit are:

- Reactor Core

  This component was introduced in greater details in 2.2.2. It could be separated from the primary circuit depending on the depth of the analysis.

- Intermediate heat exchanger (redundancy: 4)

  This component transfers heat from the sodium in the primary circuit to the sodium in the secondary circuit.

- Primary mechanical pump (redundancy: 3)

  This component allows for circulating the primary sodium through the core.

- Decay heat removal components (redundancy: 2)

  These components and systems insure the safety function associated with cooling the core.

- Argon tank

  This element permits to keep the sodium away from oxygen, with which it can react.

- Sodium purifier

  This component purifies the primary sodium to clean it from foreign elements and chemicals

2.2.5 Secondary circuit components

The considered components in the secondary circuit are:

- Secondary electromagnetic pump (redundancy: 4)

- Steam generator (redundancy: 4)

2.2.6 Tertiary circuit components

The considered components in the tertiary circuits are:

- Turbine (redundancy: 3)
- Generator (redundancy: 2)
- Condenser (redundancy: 3)
- Heat sink

CHAPTER 3

RISK ANALYSIS TAKEAWAY

Risk analyses are mostly useless if their results cannot be communicated. Several methods can be used to efficiently communicate risk and allow for easy decisions to be made. Often, those decisions need to account for cost to the system in case of a failure, which is the cost of the repair (C_r) as well as the cost of the time during which the system is unusable (C_e). This has to be compared to the cost of preventive actions (C_p), whether these are changes in design or modified maintenance program.

3.1 Decision making

In order to make efficient decisions for a system, the risks to the system must be given, from a regulation standpoint as well as a cost standpoint. As mentionned, the cost effectiveness can be explicited as:

$$\text{cost effectiveness} = \text{risk probability} * (C_r + C_e) - C_p \tag{3.1}$$

As long as the cost effectiveness is positive, the decision seems to be obvious. However, what happens when the design improvement cost is very high, and unaffordable to the company? In such cases, it is useful to present different scenarios, coming from various analysis methods. Indeed, a method such as Probabilistic Risk Assessment (PRA) could make the engineering team recommend adding an expensive redundancy to the system, when a method such as Prognostics in Early Functional Design could lower the risk probability to the system by adding a monitoring function and a paragraph in the procedures, at a low cost.

The use of different methods on a system, though time-consuming, is highly recommended. A method could be better than another, at detecting potential faults or defining adequate

workarounds for example, but they all by essence propose a narrow set of solutions. When confronted with decision making, the more options are available, with all the associated parameters (cost, time, likelihood, benefits, inconvenients), the easier the decision can be.

Probabilities are often misunderstood by people. A solution is to present the probability values obtained as time and unit occurence. Thus, a probability of $1 \times 10^{-2}\ y^{-1}$ would be translated to *"It will happen on average once every hundred years for a unit. Build 100 units, and it will happen every year on one of the unit at least"*. Even though not correct per se, this wordy approximation gets the point across.

3.2 The case of ASTRID

Several methods were used on the case study, the Sodium-cooled fast reactor ASTRID. Even though the scope of these performed analyses might vary, with the system failure defined as reliability issue to the its impact on the environment, important facts can be taken from them.

First and foremost, one thing appear from the present study. Nuclear systems, with all their existing redundancies, are extremely safe. ASTRID is a prototype for a new kind of reactors, taking into account thousands of years of historical data from existing nuclear plants, as well as a lot of even more relevant Sodium-cooled reactor data. The redundancies introduced in the system are the fruit of thousands of PRA and FMEA studies. It is however important to note that the state of the art in risk and reliability analyses changes, and that other methods can give more information and discern fault propagation path unseen by classical methods. Notably, what happens in today's engineering world is that a fault will be discovered in a similar system, or after a "close call", and a fix will be introduced to the system after that. Those are often times known as uncoupled failure, an unexpected, non nominal flow entering a component and failing it. Moreover, in recent years, the field of prognostics and health management has grown and sensors allowing to predict imminent failures are used more and more in complex systems, rendering recovery maintenance possible and cost-effective. Classical methods cannot account for such events, and new methods have been derived to consider these paths and mitigate them.

3.2.1 FMEA

More details on FMEA are given in section 5.

A FMEA was carried out on the case study. It revealed several points where attention was necessary. Notably, the calibration of the detectors. Badly calibrated neutron flux detectors can give frankly erroneous flux values, which are used to compute the power level in the core. This false inforamtion can lead to high local temperature in the core without the operator's knowledge and damage the fuel. Frequent calibration are thus recommended to mitigate this issue, already reduced by the redundant detectors used.

Another important risk to the system identified through FMEA, in terms of core damage and radioactivity release, is the external agressions risks, whether it is natural or human caused. This risk is relative to the strenght of the vessels separating the core from the outside world, and potential breaches caused. A reinforced vessel is recommended, as well as a heightened security to predict such event and take measures.

That being said, one of the main issues of this kind of analysis is its subjectivity and the needs for expert elicitations to cover various physical ways of propagating a failure through the Reliability Block Diagram (RBD). Another engineer will likely obtain different scores and probably a different set of principal recommendations depending on their background.

It would thus be interesting to have at least five independent FMEA studies of the same system in order to discern patterns and improve the confidence in the results.

3.2.2 PRA

More details on PRA are given in section 6.

On selected PRA trees, the likelihood of our system releasing radioactivity in the atmosphere is estimated at one in a billion in a year. This means that we expect a radioactivity accident once every billion years for our system. The PRA methods applied consequently show the system as being extremely safe. One of the takeaway is actually that some costly redundant system could be scraped off in order to increase the probability while still staying under reasonable threshold.

It is a risky move, since regulations agencies and public opinions would not react well to a step backward in safety. Thus, if this were to be done, communications about it should be kept to a minimum and worded carefully.

This is especially true considering the expertise needed to compute an accurate PRA model, with all the various parameters for the tiniest components, as well as the correct failure paths.

3.2.3 FFDM

More details on FFDM are given in section 7.2.

In the absence of adequate functional historical data for a nuclear power plant specific environment, failure modes defined in the FMEA analysis were used to compute function failure scores. Using this dataset, and the limitations it entails, notably from the expertise point of view as discussed previously, several function failure modes appear as noteworthy. The analysis revealed that corrosion fatigue was a failure mode to seriously consider when selecting appropriate materials. The function exhibited by the control rods insertion is deemed at high risk of mechanical stress failure, due to the distorsion of the irradiatied control rods. Finally, the electronic failure of the detectors appears to be a point of interest for the system.

This demonstrates one of the weakness of FFDM when compared to more simple FMEA method, it does not account for the severity of an event, only its probability. It will thus detect more failure modes when used in conjonction with an adequate historical failure database, but it

does not help any decision making, because the severity of the failure and its consequences on the studied system are not computed.

Precious information can still be obtained by using FFDM, whether it is as a part of an improved FMEA or to help select material options.

3.2.4 FFIP

More details on FFIP are given in section 7.3.

FFIP can use the failure modes identified by FFDM and propagate those failures through a functional model. This makes this methods really interesting from a risk and reliability analysis view point, as it requires less time-consuming, error-prone, human-made nominal propagation path as seen in PRA or hinted at in FMEA. This method is applied to the case study of ASTRID.

In the scenario modeled, we see that the loss of power to one neutron flux detector and the propagation of this failure causes the reactor shutdown with a probability of roughly 1×10^{-3}, hence a loss of reliability. We also compute that it causes a catastrophic failure, with a release of radioactivity in the environment, with a likelihood of 5×10^{-11}, exceedingly low. To give a perspective on this number, a meteor utterly destroying the plant would be more likely to happen.

3.2.5 UFFSR

More details on UFFSR are given in section 7.4.

In every complex system, uncoupled flows, defined as flows that are not nominally expected, can fail any number of functions within the system. These failure flows can not be taken into account within PRA or FFIP methods, and are cumbersome to account for in FMEA. Integrating a functional model with a physics-based model, principal uncoupled flows can be identified and propagated using FFIP-like algorithm. The number of combinations of potential paths is extremely consequent.

A catastrophic turbine failure (explosion with shrapnel) is considered to demonstrate the method. It is computed that the shrapnel can reach at least 125 meters from the turbine location, damaging a lot of uncoupled systems. From the results obtained, it is thus recommended not to move the turbine away, as it would result in efficiency loss, but to rotate the turbine so that shrapnel would not reach critical components, and to reinforce the building concrete if the cost increase is not prohibitive.

The probability of a radioactivity release following this accident is calculated as being 1×10^{-10}, low enough to be ignored. Thus, the final recommendation would be that the turbine and its building are oriented in such a way that shrapnel would not damage the rest of the plant extensively.

3.2.6 HRA and Prognostics in Early Design

More details on Prognostics in Early Design are given in section 7.5.

This method is used to account for potential Prognostic and Health Management (PHM) equipment in the plant, and their impact on the maintenance and recovery actions taken after the detection of an imminent failure. Human Reliability Assessment (HRA) is used to estimate the likelihood of a successful recovery as well as the potential failure introduced by a maintenance team to the system due to faulty actions. Doing so, we can see for example that the probability of recovering from a detected imminent failure of the turbine is 98.5%, and the chance of introducing a failure mode is 0.15%. Using those numbers, we see that for an adequate sensor on the turbine, the probability of failure is reduced by an order of magnitude, going from once every thousand years to once every ten thousand years.

This can be used to justify not adding redundancies but instead placing more sensors in the system. In the case of the turbine, this does not necessarily apply, since the cost of the turbine can be offset by the operation benefits. However, in the case of other type of components, such as backup generators, this can be used to eliminate unnecessary and expensive redundancies.

3.2.7 CRFFA

More details on CRFFA are given in section 7.6.

The Cable Routing Function Failure Analysis (CRFFA) method can be used to select the best cable paths configuration, minimizing common-cause failure propagating through the system. In the case of a nuclear reactor, watchdogs limit the usefulness of this method in the case of risk analysis for power and signal cables, since the shutdown is initiated passively if no signal is received. However, it is quite interesting when considering the reliability side of it.

It is thus recommended to isolate the various signal and power cables from and to the various detectors equipment in the core, in order to avoid potential common-cause failure mode that would render the operator blind to what is going on in the reactor and thus impact directly the reliability of the plant.

But more importantly, the cables should be ordered and labeled correctly, since one of the main common failure cause in this case would be human mistake. An organized cable route would also allow for swift repairs.

CHAPTER 4

IDENTIFICATION OF POTENTIAL SYSTEM FAILURES

Based on the historical data gathered, from SFRs design and other nuclear power generation design, a list of common macro failure modes can be computed. Different serious failures can now be identified, in order to assess their impact on the plant. Five main categories of impacting events have been considered:

- Primary circuit component functional failure,
- Secondary circuit component functional failure,
- Tertiary circuit component functional failure,
- Reactor structure failure,
- Aggressions.

Generic components (e.g. pipes, valves) failures can by definition happen in any subsystem, and thus will be considered accross all of them.

The following sections present a non-echaustive list of different past and potential failures, and describe succinctly the foreseen impact on the plant safety and reliability. Three main categories can be seen: the failures which do not lead to a catastrophic failure by themselves but are likely aggravating factors in the event of another issue, the failures which are mainly responsible for a disastrous event, and the failures which cause reliability-related issues.

This section does not fully consider the system as complex, its goal is to simply give a feel for the things that can go, and have gone wrong, in the system at a macro-level.

4.1 Primary circuit components failure

All the components in the primary circuit subsystem can fail, with varying probabilities, and they all can have various impacts on the whole system and the environment outside the system. To simplify this macrostudy, only the main components can be looked at to identify source of failures and their consequences. Those main components comprise the core, the primary mechanical pump, the decay heat removal system anf the intermediate heat exchanger.

The core will be discretized into the fuel assemblies, the control rods, the detectors and the fuel handling procedures. When looking at each of this components separately and applying past events or potential failures considered, one can estimate roughly the potential consequences on the system.

For example, a complete fuel cladding failure means that the radioactive materials held in the assemblies can be released in the primary circuit, the equivalent of a meltdown. A partial fuel caldding failure will not by itself cause a meltdown, but it can and will be an aggravating factor if something else happens. A problem that has been on the rise in some nuclear plants is the distorsion of assemblies, slowing the insertion of the control rods and potentially preventing an automatic shutdown of the reactor, and impacting its neighboring assemblies. It also causes a reliability issue, since the reloading of a distorted assembly is more difficult and time-consuming. Other issues can appear, notably a detector failure, causing the operators to operate blindly, or worse, a detector malfunction, causing the operators to misinterpret the actual state of the core. Moreover, human errors are not to be forgotten, as the Dampierre's reactor reloading error shows [20]. A mistake made when handling fuel can create a criticality event and put the workers and the environment at risk. Several other events have also been observed in reactor cores: a missing fuel pin in an assembly, a control rods pin stuck in another one, ... Those incidents did not cause the safety analyses to be proven wrong, thanks to the consequent uncertainties margin considered, but they make it more difficult to argue for a relaxation of those high margins.

Even though the core is a central element in a nuclear reactor, it can be seen that a failure in this subsystem would usually not by itself lead to a full meltdown of the fuel. Indeed, a loss of coolant is often needed for that to happen.

A failure in one of the other primary system components can cause a loss of cooling abilities and start a core meltdown. Redundancy, maintenance and emergency procedures are primordial in this part of the design.

The mechanical pump failure can indeed prevent the sodium coolant to circulate though the core, and thus potentially melting down the core. However, as tested in EBR-II, the negative void coefficient displayed by the selected core would shut down the reaction before the fuel assemblies melt down. The decay heat would still need to be dealt with though. A failure of the decay heat removal system might thus cause a meltdown of the fuel, having lost the cooling abilities. This is partly what happened in March 2011 at Fukushima, a loss of power caused a loss of the decay heat removal systems, and seawater had to be used on the core to cool it down. If the intermediate

heat exchanger failed, in case of a pipe rupture, the intermediate system (between the primary and secondary circuit) can be contaminated, and there is a loss of cooling abilities, potentially causing a meltdown.

Most of the primary system components are linked to the core cooling and moderation. Hence, if they fail, they are likely to have a consequential impact on the core, often leading to a meltdown.

4.2 Secondary circuit components failure

The secondary system is possibly even more impacting to the plant safety than the primary system. Most failures on this system would cause a loss of coolant, or a diminution of the cooling abilities. If the coolant is lost, then the core heat cannot be controlled and the fuel cladding will start to melt. As said previously, this adds an emphasis on the need for maintenance and redundancy and emergency systems and procedures.

The secondary system is defined by the secondary eletromagnetic pump and the steam generator. It contains the secondary circuit sodium, used to transfer heat from the primary circuit sodium to the tertiary circuit water. Any failure in this circuit endangers the whole system safety, by potentially causing a meltdown due to a loss of coolant abilities. A leak in this subsystem means that the secondary system is not able to get as much heat off of the primary circuit, and it may also cause a contamination, the sodium in the secondary circuit being weakly activated when passing through the intermediate heat exchanger. In the same vein, a failure of the pump means that sodium does not get to the heat exchanger, and cause a loss of cooling abilities. The core would still be immerged, until the temperature reaches the boiling point of sodium and starts to uncover the core. This is why a specific core design with a negative void coefficient is important.

4.3 Tertiary circuit components failure

The tertiary system does not contain sodium, but water, and is used primarily for electricity generation. It is also used for secondary sodium cooling. So, two subsystems can be considered here, the electricity generation system, containing the turbine and the generator, and the secondary/tertiary heat exchange system, containing the heat sink, the condenser, and the tertiary system pump. A failure in the former would cause a loss of electricity generation, i.e. a reliability issue, but would have no consequences on the reactor integrity. A failure in the latter would cause a lack of cooling of the secondary sodium, which would in turn impact negatively the heat exchange between the primary and secondary circuit. For example, a leak in the condenser, or a problem with the heat sink, could mean that vapor reaches the tertiary pump and fails it completely, hence no water sent to the steam generator and poor heat exchange capabilities.

Once again, this could be mitigated only with good maintenance, and most importantly redundancies in all the systems.

4.4 Reactor structure components failure

The reactor structure integrity is extremely important when it comes to radioactive contamination. The different vessels act as containment. In the eventuality of a large breach, or a small breach left unchecked, the core can even be uncovered and melt down. Reactor vessel integrity issues have been detected in the past [3] without safety consequences, but with high cost in termsof lost production time. The case study design has the added difficulty of having to prevent sodium interaction with air and water. One of the main source of failure for the reactor structure is aging, especially within a highly radioactive environment.

It is quite difficult to add redundancy in those cases. Different systems are thought of in case of a failure and a meltdown, e.g the core catcher. But these components require extensive surveillance and state-of-the-art conception and materials at the design stage.

4.5 Aggressions

When considering aggressions to the nuclear power plant, two types are discerned and analyzed, external and internal.

In the external category, the common-cause failure mode are considered. Those events usually happen site-wide, such as a flood or earthquake, or with the potential of spreading, such as fire. In a sodium-cooled power plant, fire is especially a concern, as demonstrated in the design operations feedback. Terrorism is also considered in this category, nuclear power plant being an ideal target for an attack. Plane crash, bomb and hacking should thus be taken into account.

Those external aggressions have a direct impact on the plant component, as well as an indirect impact, by preventing repairs or human intervention. For example, a flood can prevent repair crew and materials from getting on-site. An example of external aggression is the accident that happened in Fukushima. A seism caused all the powered unit to shut down quickly, as it was designed to. However, the flooding caused by the tsunami that followed was not considered, and caused a complete loss of on-site power, including the backup generators. The redundancy in this case existed, but was not designed to withstand a "Black Swan" event.

The internal threat has been defined as the failure of a component affecting an uncoupled other, and human error, whether it is operations, maintenance, engineering or manufacturing. Three Miles island is an example of such event, where human engineering caused an erroneous interpretations from the operators who then followed incomplete procedures to counter automatic plant actions. This category will be difficult to address fully, and design should aim at diminishing the amount of procedures by increasing the number of passive safety systems, and avoiding complexity when possible. Surveillance systems should also be made redundant in the design part to prevent erroneous readings and interpretations in the control room and during maintenance.

CHAPTER 5

HIGH-LEVEL FAILURE IDENTIFICATION

High-level reasoning about a system necessitates to know how the system's component interact with one another. This allows for the estimation of the impact of different component failures on the whole system. System mapping can be achieved through what is known as the Reliability Block Diagram (RBD). Armed with that graphical visualisation of the system at hand, it is possible to perform Failure Modes and Effects Analysis (FMEA) to estimate how it might fail and an associated score.

5.1 Reliability Block Diagram

In this paper, RBD will only be used as a graphical tool, a way to communicate about the system components and their interactions. It can however also be used to compute unreliability probability, by computing the probability of failure of each component within the system, in series, parallels or in a hybrid mix. This is mostly useful for simple straightforward system. The main interest of RBD in our case study is to define the system and various interactions, and get a first feel for risk and reliability issues.

The diagrams are presented in appendix A. In order to facilitate the reading, the case study has been divided in four systems, as defined in section 2.2: primary, secondary, tertiary and structure (figure A.1). For each of those systems, the redundant components are indicated by a block instead of a simple rectangle. Those blocks are then analyzed in more details in subsequent figures. An example is also given in figure 5.1.

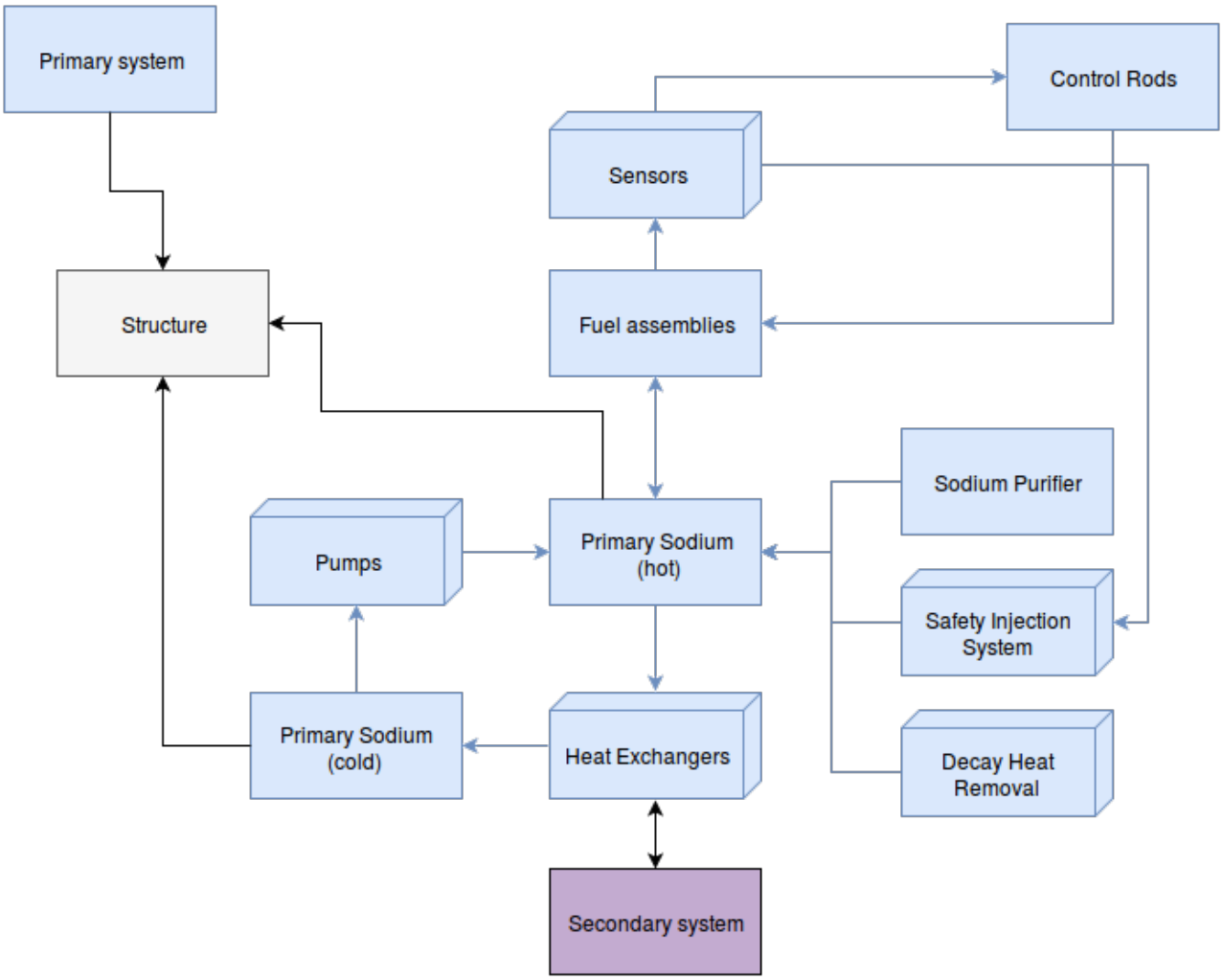

FIGURE 5.1. Reliability Block Diagram for the primary system

5.2 Failure Modes and Effects Analysis

Failure Modes and Effects Analysis is a method that ultimately allows designers to identify weaknesses in their systems, by taking into account the probability of a failure to occur (P), the severity of the consequences on the system (S) and the detectability (D). Let us first define these different factors.

Probability (P) On a scale from 0 to 10, this represents the probability of the given failure happening in the considered component, 1 being almost never and 10 being all the time.

Severity (S) On a scale from 0 to 10, this represents the consequence of the component failure on the whole system, 0 being no consequence and 10 being catastrophic failure.

Detectability (D) On a scale from 0 to 10, this represents the probability to detect the failure and to fix or mitigate the effects, 0 being easy detection and repair and 10 being no possible detection nor action.

Those three factors give the designers a score, the Risk Priority Number (RPN), for each identified potential failure throughout the system.

$$RPN = P * S * D \tag{5.1}$$

The designers can then estimate the need for corrections from the highest impacting failure to the lowest. Important shortcomings of this method are to be noted [11]. It heavily depends on the designers producing the analysis, and their biases (wishful thinking, knowledge, background, ...). Moreover, it can basically only take into account regular failures, that have happened before, and is not adequate for identifying possible "Black Swan" events. It is also not applicable to an early design stage, and thus can generate costly changes that could have been avoided before the conpetion became too advanced. Additionally, the coherence of the RPN formula has been debated. Indeed, one can see from table B.1 and B.2 that the RPN is higher for a (3, 6, 6) (P, S, D)-triplet than for a (2, 7, 7) one, implying that in this specific case, the probability of the event occuring is more important than both the severity and the detectability, which can obviously be contested. This also goes to show the huge impact a optimistic or pessimistic estimation can have on the whole RPN ranking and associated conlusions.

Several other FMEA-based methodologies have been developed over the years, to try and cover the shortcomings of FMEA, some examples being the Failure Modes, Effects and Criticality Analysis (FMECA) or the fuzzy rule-based system FMEA [4]. If a FMEA is to be performed, it is important for the designers to consider the best FMEA method for their project. A classic FMEA was applied to the case study presented in this paper. Even though it is an imperfect method, it can give, and do give, the designers precious information on a high-level.

This study will present a FMEA performed with relation to risks to the system. In the nuclear industry, this is the main one, since it directly impacts communication to the public.

Another FMEA could have been performed with relation to reliability, most useful to the plant operators. The major parameter impacted betwen the two different analyses is the severity. For example, the loss of a generator might be given a 8 on the 10-points scale in the "reliability" study, yet only a 1 in the "risk" study.

This categorization was chosen not to be explicited in details in this paper for clarity reasons. The risk-FMEA englobes the reliability ones, with of course a different emphasis.

Follwoing the literature found on the subject [1], the reference tables giving the meaning of each 10-point scale for the Probability, Severity (risk-oriented and reliability-oriented for information) and Detectability parameters score are displayed respectively in tables 5.1, 5.2, 5.3 and 5.4.

Probability	Index	Probability estimate
Inevitable	10	≥ 0.5
	9	0.1
Frequent	8	0.05
	7	0.02
Occasional	6	0.01
	5	0.005
	4	0.001
Minor	3	0.0005
	2	0.0001
Exceptionally	1	< 0.0001

Table 5.1: Probability index

Severity	Characteristics	Index
Very high	The effect can affect both the safety and operation, as the environment, potentially causing damage to property or persons and/or breaking any laws.	9 and 10
High	Reductions in the power level of the plant and/or weakening the plant safety.	7 and 8
Moderate	Reduce the system efficiency, generating work stresses which lead the plant to operate in level of risk over of the one in normal condition.	4, 5 and 6
Minor	The failure effects don't interfere in the plant operation, but reduce shortly the system performance.	2 and 3
Remote	The failure effect is almost not perceived.	1

Table 5.2: Detectability index for a risk-centered method

Severity	Characteristics	Index
Very high	The effect can affect the operation, potentially causing damage to property or persons and/or breaking any laws. Off-grid time.	9 and 10
High	Reductions in the power level of the plant.	6, 7 and 8
Moderate	Reduce the system efficiency, generating work stresses.	5
Low	The failure effects don't interfere in the plant operation, but reduce shortly the system performance.	3 and 4
Minor	The failure effect is almost not perceived.	2
Remote	The failure effect is not perceived on the plant power generation.	1

Table 5.3: Detectability index for a reliability-centered method

An extensive – yet incomplete, by essence of the method – FMEA has been performed on the system at hand. The failure modes, causes and (P, S, D)-triplets can be seen in table B.1 and the RPN and mitigation actions in table B.2.

The range of RPN values obtained using the aforementionned reference tables for the different

Detectability	Index	Detectability estimate
Very high	1	86% to 100%
High	2	76% to 85%
	3	66% to 75%
Moderate	4	56% to 65%
	5	46% to 55%
	6	36% to 45%
Low	7	26% to 35%
	8	13% to 25%
Minor	9	6% to 15%
	10	0% to 6%

Table 5.4: Detectability index

parameters goes from 4 for a large breach of the core catcher to 400 for an erroneous signal from every detectors. The perceived failure modes with the greatest RPN number have been selected and are presented in tables 5.5 and 5.6.

ID	Component	Failure	Cause	P	S	D
8.1	Detectors	Wrong signal from all	Electronic components	5	8	10
11.2	Main vessel	Small breach	Aggression	3	10	10
12.4	Safety vessel	Large breach	Aggression	3	9	10
12.2		Small breach	Aggression	3	8	10

Table 5.5: Excerpt from TableB.1 presenting the (P, S, D)-triplet for the perceived most severe failure modes

ID	RPN	Mitigation
8.4	400	Calibrate the detectors frequently, use different kind, use other ways to determine reactor power output
11.2	300	Good material and large width, external defense
12.4	270	Good material and large width, external defense
12.2	240	Good material and large width, external defense

Table 5.6: Excerpt from Table B.2 presenting the RPN and possible mitigation strategy for the perceived most severe failure modes

One of the main issues with the FMEA, as discussed previously, is the subjectivity of the data, highly dependable on the designer's experience and expertise. All the different systems (electronic, electric, mechanical, nuclear, ...) should be analyzed, and a large panel of experts is thus needed. The author of this paper applied engineering training and experience to deduce some of the (P, S, D)-triplets. The principal strength of this method resides in its simplicity and its capability to quickly give the designer an idea of potential problems to be fixed within the system.

In the present case study, one can notice that the failure modes perceived as having a bigger impact all have a detectability parameter of 10, meaning that it has very low chances of being detected before a catastrophic failure of the component happens. Aggressions and electronic failures were the culprits. This undetectability, tied with a highly consequential severity (between 8 and 10) and a probability estimated as minor (3), causes the RPN to spike.

One might want to look in priority at the mitigation strategies for those failure modes. For example, the detectors calibration failure RPN can be lowered by operational procedures, insuring the good calibration of the detectors at all times. The main vessel looks like a potential weak point too. It is not practical to make it redundant, and as such, studies on its strength and size should be carried, as well as stress tests.

CHAPTER 6

PROBABILISTIC RISK ASSESSMENT

Risks assessments include the identification and analysis of initiating event, safety functions and accident sequences. The initiating events are the circumstances taht put a system in an off-normal condition. The safety functions represents the mitigating actions designed in the system. The accident sequences are the combinations of safety functions successes and failures used to describe the accident after the initiator. A successful response is obtained when the system transitions to a safe and stable end-state for a given period of time after the initiating event.

Probabilistic Risk Assessment (PRA) is used to compute the frequency and consequences of not achieving this safe and stable end-state.

6.1 PRA model

The goal of the PRA model is to model the system as-built and as-operated. This can be done using the design information, system drawings, operating experience data, system operating procedures, maintenance practices and a variety of other sources of information.

PRA is based upon two primordial concepts, understanding the plant perturbation and understanding how the plant responds to the identified perturbations (physical responses, automatic system responses, operator responses).

Those concepts can be used to define the end states. One can note that several different failed end states can be considered. Indeed, the system can fail with several degree of severeness (core damage, release and radiological consequences are the three levels usually used in the nuclear industry). Moreover, the Probability Risks Assessment method can be used as a Probability Reliability Assessment.

It is thus important to properly define the goal of the analysis, as well as all the different hypotheses made.

A PRA model consists of:

1. Event trees

   They describe the accident sequences, from the initiating event to an end state. Each event in an event tree is usually given two possible states, failure or success. Intermediate states can also be used in more advanced models.

2. Fault trees

   They describe the failure of mitigating functions.

Frequency and probability estimates are given for the failure of components or the happenstance of initiating events. One of the biggest challenges of this type of analysis, which is true for most risk and reliability analysis methods, is the difficulty to obtain those estimates. They can mostly be computed from operating experience data, expert elicitation.

6.2 PRA model applied to the case study

The PRA model that will be applied to the case study of the ASTRID reactor will be classical. Level-2 end-state will be considered, that is the system will be considered in a failed state if there is an unexpected release of radioactive materials in the atmosphere. Only two states will be used throughout the study, success or failure.

Several initiating events will be analyzed:

1. Loss of offsite power
2. Loss of coolant
3. Power excursion

Moreover, two subtrees (event trees used by the main trees) will be used, the SCRAM failure and the containment failure. Those two subtrees will also be analyzed independently, since they can be applied to a variety of initiating events.

Due to the aforementionned difficulty to obtain real frequency and probability data for initiating and basic events, the values used in this study are estimated using the engineering knowledge of the author. The value presented are consequently used to illustrate the method, and should thus not be taken as face value.

Table C.1 presents the probability of each event considered in this study.

The cutsets generated by the PRA analysis, through the use of the software SAPHIRE [14], for the initiating events considered and the goal of the analysis, are exceedingly low. It is worth

Table 6.1: PRA cutsets

IE	Cutsets	Probability (y^{-1})
B1_LOSS_OFFSITE_POWER	IE, COMM_SIGNAL_POWER_OFF, OUTSIDE_COMMUNICATION	4×10^{-9}
	IE, COMM_SIGNAL_POWER_OFF, OPERATOR_PROBLEM	4×10^{-9}
	IE, AUTO_POWER_CHECK, OUTSIDE_COMMUNICATION	4×10^{-13}
	...	...
LOSS_OF_COOLANT	IE, INTERPRET_OPERATOR, SENSOR_DETECTION	5×10^{-9}
	IE, INTERPRET_OPERATOR, SENSOR_NO_COMM	5×10^{-9}
	IE, CORE_CLAD_STREN, GENERATOR_REPAIR, PRE_BREACH_CONT_MAIN, PRE_BREACH_CONT_SAFE, SIS_VALVE	1×10^{-19}
	...	...
POWER_EXCURSION	IE, CORE_CLAD_STREN, GENERATOR_REPAIR, PRE_BREACH_CONT_MAIN, PRE_BREACH_CONT_SAFE, SIS_VALVE	8×10^{-16}
	IE, CORE_CLAD_STREN, GENERATOR_REPAIR, MANU_COOL, PRE_BREACH_CONT_MAIN, PRE_BREACH_CONT_SAFE, SIS_VALVE	4×10^{-16}

repeating that the analysis that was carried out on the case study is a level-2 end-state. In other words, only the release of radioactive material in the atmosphere is considered. Had we performed a reliability analysis using PRA, or been interested in core damage only, the probability of failure would have been orders of magnitudes higher.

Table 6.1 shows the main cutsets for each initiating event considered, and their associated probability of happening.

CHAPTER 7

FUNCTIONAL ANALYSES

A different way of representing an engineering system is to embed it as a functional model. A functional model is a graphical representation of a system, that ties a component to a function, or a set of functions, fulfilled within the system. Function are interconnected by flows. One of the main advantage of functional modeling is its applicability in the early stages of design, when no components have been selected and the design is just a concept. Until recently, two main methods existed to create a functional method, NIST and the Functional Basis. Each had their own volatile taxonomy, which limited the widespread use of this technique to other ends than system description. Stone and Wood proposed the Functional Basis for Engineering Design (FBED) [18], which reconciled sets of function and flows notably with relation to mechanical engineering design nomenclature. This common taxonomy allowed for automatic analysis methods and database maintenance, which paved the way to various risk and reliability methods based on functional models, such as Function Failure Design Method (FFDM) [17], Funtion Failure Identification and Propagation (FFIP) [9], Uncoupled Flow Failure State Reasoning (UFFSR) [19], [12], Prognostics-based analysis in early design ([16] and [10]), or Cable Routing Function Failure Analysis (CRFFA) [13].

7.1 Functional model

A FBED description of a system uses the reconciled function set and flow set to name the various functions and flows necessary within a system. Tables 7.1 and 7.2 give a few example of such functions and flows. FBED is organized using three classes, primary, secondary and tertiary, each increasing the degree of specification. THose three classes cover every potential function seen in a mechanical design. It is to be noted that it still allow for some level of interpretation as to how

Table 7.1: Excerpt from the functional basis reconciled function set

Class (primary)	Secondary	Tertiary
Branch	Separate	Divide
		Extract
		Remove
	Distribute	
Channel	Import	
	Export	
	Transfer	Transport
		Transmit
	Guide	Translate
		Rotate
		Allow DOF
...		
Support	Position	

Table 7.2: Excerpt from the functional basis reconciled flow set

Class (primary)	Secondary	Tertiary
Material	Human	
	Gas	
	Liquid	
	Solid	Object
		Particulate
		Composite
...		
Energy	Thermal	

to categorize a function or flow.

A FBED model can be compared to a RBD. They both can take various degrees of details, high-level to low-level model description. One of the advantages that FBED exhibits as opposed to RBD is that it considers explicitely the flows linking the different functions. Moreover, it does not depend on the component selection, which allow the design team to explore a larger space of possible systems. Figure 7.1 show an example of a functional model applied to the present case study. One can note that the level of details can be modified. Moreoever, to simplify the drawing, the redundancies displayed by the system are not explicited as separate functions and flows. They are instead encoded within the probabilities associated with each function or flow failure propagation.

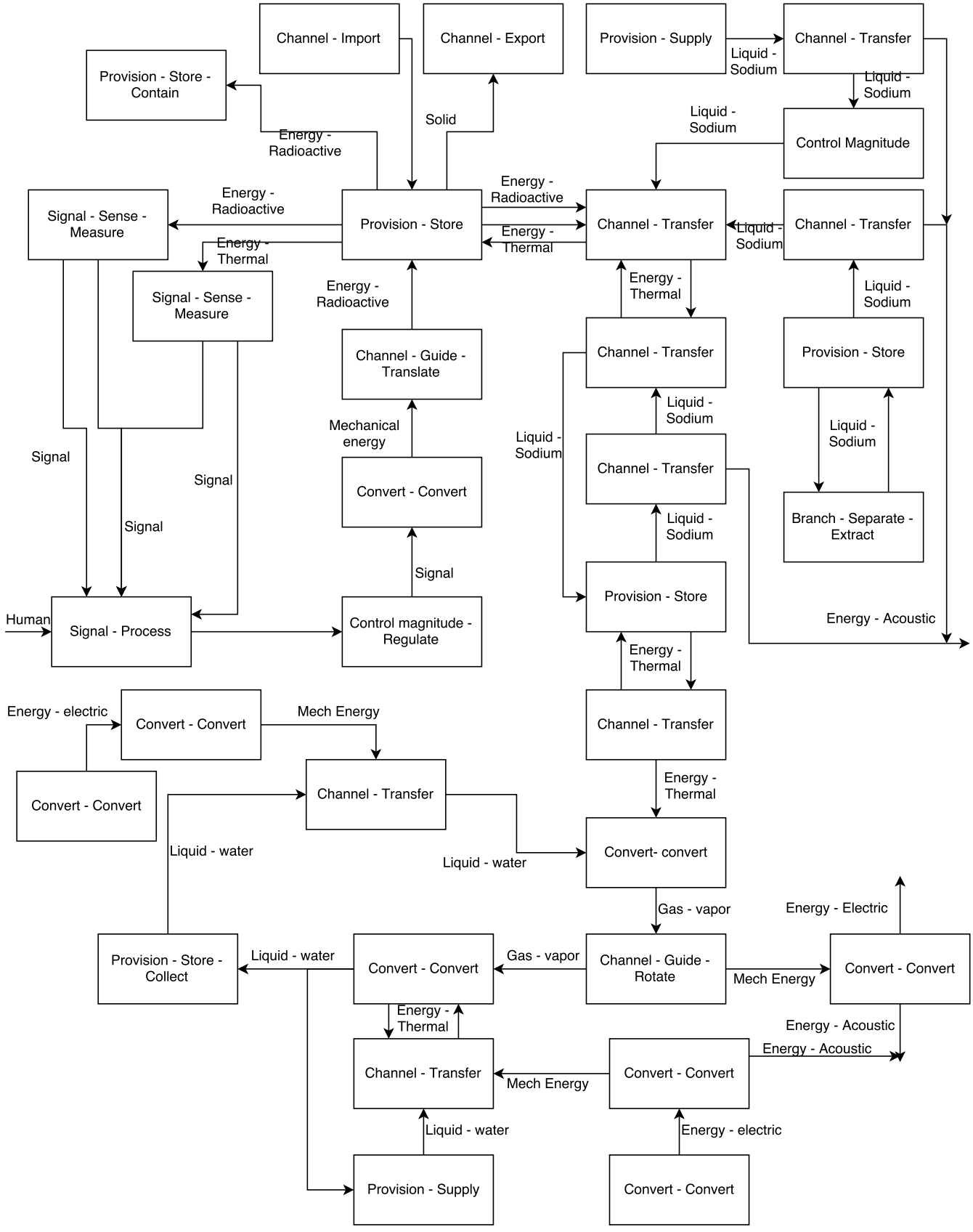

Figure 7.1: High-level simplified FBED representation of ASTRID reactor.

7.2 Function Failure Design Method

FFDM is a method whose main goal is to look at historical component failure data within a system, and estimate the different failure mode observed. Those failure modes are then linked to the functions in the design. Effectively, FFDM is similar to FMEA, but allow for a more generalized approach by taking on functions. The failure modes identified can then be mitigated by modifying the functions used in the system. It has been shown that given the right database available, FFDM gave more information on the potential risk and possible actions to mitigate them in a system than FMEA. Moreover, being based on functions-failure-modes database, this method is less likely to depend uniquely on expert opinion.

However, FFDM does not diagnose the root cause of a failure, nor does it take into account manufacturing and operating conditions. Indeed, FFDM does not differentiate various levels of stress durin operations and is very dependent on past operation data to derive information about failure modes. More importantly, FFDM does not consider the severity or the detectability of a failure mode. It only focuses on the likelihood of a failure mode for each function in the system. This is an important limitation of the methodology, since it doesn't allow the design team to make fully informed decisions.

To illustrate this method, let us assume that a repository of failure modes for a given system is available. An engineering team wants to improve upon the original design, or create a new design entirely. The first step is to translate the system to a functional black-box model. Then, for each function, the failure history is analyzed, and a susceptibility score is used to link a function to all potential failure mode. Given that information, a mitigation analysis is conducted, allowing to choose the most adequate components addressing the identified function failure modes.

The fact that this method is based upon functional model allow for its use in conceptual design. One of its limitation is the existence of a complete database, and the fact that a function can fail following different failure modes depending on operating stresses and component physical attributes.

Table 7.3 shows several failure modes occurences for a subset of the case study system functions.

One of the main difficulty of the FFDM method is to populate the database. Historical data is scarcely available for components, and those components must be decomposed into a functional model in order to link failure modes and functions. The failure modes considered should be drawn from a similar system, in terms of operating range and flows, to the system being analyzed. Indeed, a function "Channel - Transfer" would exhibit very different score for each failure mode in a system in which the flow is a potent acid versus a system in which the flow is room temperature water.

In order to compute the data needed for the FFDM analysis, in the absence of meaningful historical data, the FMEA analysis results presented in Table B.2 are considered. Each component was analyzed and a list of potential failure and their likelihood was obtained. The number of

Table 7.3: FFDM database

Function/Failure	Corrosion Fatigue	Human Attack	Thermal Stress	Mechanical Shock	...	Mechanical Stress	Radiation Damage	Electronic Failure
Channel - Transfer	18	12	0	8		0	6	0
Provision - Store - Contain	10	14	13	5		0	11	0
Signal - Sense - Measure	0	0	0	0	...	0	0	33
Convert - Convert	17	5	0	6		0	4	0
Branch - Separate - Extract	6	0	0	0		0	1	0
Channel - Guide - Translate	0	0	0	5		20	0	0
...								

occurences is then computed into Table 7.3. Table 7.4 presents the normalized data, computed using Equation 7.1.

$$f_{i,n} = \frac{f_i}{\sum_j F_j} \tag{7.1}$$

Where:

$f_{i,n}$ = Normalized failure score for the mode i

f_i = Failure score for the mode i

$\sum_j F_j$ = Number of functions considered

An example of the methodology applied to derive FFDM database from the FMEA analysis rather than historical data is explicited on the component *Fuel assemblies*. A fuel assembly can be translated into a *Provision - Store - Contain* function. FMEA analysis detected five different potential failure modes: a high power peaking factor, a very high power peaking factor, a human mistake (misidentification), wear and a damage to the head. We can categorize those five failure modes into various categories. The high power peaking factors can both be put in the thermal stress category. A human mistake to misidentify a fuel assembly can be categorized as a human attack. Damage to the assembly head can be sorted into the mechanical stress category. Once the main categories are computed, the likelihood of each events are taken from the FMEA analysis and incremented to the total value for each category. In this example, it would mean that *Thermal stress* has a score of 13 $(8+5)$, *Human attack* a score of 3, and so on.

Then, the other components exhibiting the function *Provision - Store - Contain*, such as the inner vessel or the core catcher, are analyzed and their failure modes scores are added to their relevant categories.

The FFDM database obtained shows that the failure mode *Corrosion fatigue* is present with a high score in a number of function. This is something the design team should consider, notably when deciding what material to use and the operating conditions that it will be subject to. A very high number can be seen, the *Mechanical stress* for the *Channel - Guide - Translate* function. The score displayed is 20. Moreover, a score of 16.5 can be seen for the *Electronic failure* of the function *Signal - Sense - Measure*. This is explained by the fact that the failure mode are highly

Table 7.4: FFDM normalized database

Function/Failure	Corrosion Fatigue	Human Attack	Thermal Stress	Mechanical Shock	...	Mechanical Stress	Radiation Damage	Electronic Failure
Channel - Transfer	4.5	3	0	2		0	1.5	0
Provision - Store - Contain	2	2.8	2.6	1		0	2.2	0
Signal - Sense - Measure	0	0	0	0	...	0	0	16.5
Convert - Convert	4.25	1.25	0	1.5		0	1	0
Branch - Separate - Extract	6	0	0	0		0	1	0
Channel - Guide - Translate	0	0	0	5		20	0	0
...								

likely for the given function. It can be seen that no other function exhibit those failure modes. A particular attention should thus be ported on the two functions, whether it is redundancies or improving the system.

A crucial information is missing from this analysis. The likelihood of a failure mode damaging a function can be computed, based on historical data and even based on expert judgement if needed. However, the consequences of these failures on the system cannot be calculated. This leaves a consequent unknown out of the design team reach, since they cannot, from this data alone, take a fully informed decision. Consequently, this method can be judged insufficient for larger complex systems, but proves useful in the context of a concept generator.A concept generator allow slight modifications and information to link functions and components, selecting the better component from a historical database for a given functionality in a given environment. FFDM can also be used in the very early stage of design to point toward the direction to follow for the design, potentially avoiding some costly changes late in the design phase. It cannot be used as a stand-alone tool to make decision on the risk and reliability aspect of a system for all its design phases.

7.3 Function Failure Identification and Propagation

FFDM can be used to select the most adequate components for a given functionality in a system, based upon historical failure data. However, it does not show how a failure caused by one of these componenets can propagate through the system. Reliability Block diagrams can be used to calculate the failure propagation through the components of a system, but this is limited to the end stages of design, when the whole system is mapped out. It is however crucial, in terms of risk and reliability analysis as well as in terms of design costs, to be able to compute potential failure propagation in the early phase of the design. This allows the engineers to make informed decisions about risk in the system and ways to mitigate them early on, thus saving a lot of redesign cost and time, from potential prototype modification to manufacturer contracts.

By applying a propagation method to a functional model, it is possible to get some insights about the system early on. FFDM data can be used to translate historical component failure to function failure probabilities. FFIP uses this data to propagate the failure through various flows in the system after a given initializing event. Analyzing the system in such a way can reveal

weak points in the design, where mitigation action could be taken at the design stage, such as adding a redundancy or redirecting a failure flow.

An algorithm can be used to determine the propagation of the failure and the probability associated. This algorithm is named Function State Logic (FSL). It estimates the flow coming into a function and the impact on the function and the outgoing flows. Consider a tank of water (*Provision - Store - Supply*). If the feeding pipe (*Channel - Transfer*) fails, then the liquid flow can be degraded or reduced to zero. This in turn does not fail the tank of water which can still function and store water. However, the outgoing flow will eventually fail if nothing is done, since the tank will run out of water. In this example, the function did not directly fail but can be considered to have failed indirectly by not being able to deliver its liquid flow for lack of incoming flow. The degraded or zero-liquid flow will then potentially fail the next function in line and the failure propagates.

Two different end results will be considered, showing the versatility of FFIP. Indeed, the system risk can be computed, by selecting the function representing the core containment, but the reliability of the system can be computed at the same time, by selecting the function representing the final electricity generation and outgoing flow. The failure of the first is a severe issue for the risk as well as the reliability of the system, while the second is mostly important to the operators. Hence, the reliability probability of failure can afford to be higher than the risk probability of failure.

In the case study at hand, several failure flow propagation were studied. Let us take the case of a loss of electrical power in all the neutron detectors. FFIP can give us precious information on how the failure propagates through the system and what can be done to mitigate this. Various scenarii are used to illustrate the method. A loss of the function representing the neutron detectors, a loss of the function representing the turbines and a loss of the function representing the condensers. In each case, FFIP is applied to propagate the failure and evaluate the impact on the critical risk function and the critical reliability function.

It is important to note that this represents an exponential problem. The complexity of the system grows exponentially with the size of the system. It is thus also important to define viable cutsets and a threshold, very much like in PRA. Using FSL algorithm as seen in algorithm 1 to 5 applied to the first scenario presented in figure D.1, the number of possible paths through a system, from the same initiating event, grows very quickly, according to equation 7.2

$$N = \prod_{i} \sum_{j} P_{i,j} \tag{7.2}$$

Where:

N = Number of possible cutsets

i = Function on the path

j = Algorithm possibility

For example, considering the loss of the neutron detectors power source, one can illustrate how quickly the number of cutsets grows. The initiating event is the loss of the incoming flow, *Energy - Electrical*. FSL can be used to compute the potential cutsets. The loss of the power source fails the function *Signal - Sense - Measure*. Consequently, several case can be considered. The power source to the control room might be turned and no human present to manually shut down the reactor, independently of the loss of detector signal. The next function in line is to *Regulate* the core output. Let us consider that it receives a zero signal if no action is asked, a negative signal to lower the control rods and a positive signal to raise the control rods. If no signal is received, a SCRAM procedure is initiated. If the output of this function does not correspond to the demand, the function is considered failed. If it does receive a signal, but is not alimented in power, the function fails. Eventually, each scenario create a cutset, and propagates to the next function, generating a failure tree.

In this case study, the cutsets studied extensively will be limited, the goal being to demonstrate the methodology. We will apply the full FFIP method to the risk assessment following the initiating event *loss of neutron detectors power source* D.1. Similar to the event tree in PRA, probabilities can be assigned to each potential failure propagation potential. These probabilities can then be used to compute the impact of the initiating event on the system risk assessment, according to equation 7.3.

The outcome of a function, as given by FSL, can be decided by the design team. In the simplest case, a binary choice can be taken, function failed or not. However, different impact on the outgoing flows can be considered, such as degraded flows or flows-back. For the sake of simplicity, we only consider a function failed or healthy.

$$P_f = \prod_i (P_i) \tag{7.3}$$

Where:

P_f = Probability of failure of the critical risk function

P_i = Probability associated to the outcome of the function (FSL cutset)

Considering the data given in Table 7.5 and 7.7, we can compute the probability of the failure of the power source to the neutron detectors propagating through the system. These probabilities correspond to the scenario explicited in figure D.1. We can see that in this case, the reactor is not at risk considering this cutset, since the lack of available flux information ensures an automatic or manual SCRAM of the reactor. The probability associated with this cutset is 9.995×10^{-4}. However, the reliability is impacted, since the forced shutdown implies that the electricity generation cannot be supplied. The probability of this happening is 1×10^{-3}, since nothing can obviously compensate the loss of the reactivity and thermal transfer in the core to generate electricity.

Table 7.5: Propagation of failure in risk analysis

Event	Probability of happenstance (y^{-1})
IE_PWR_DET	1×10^{-3}
FUNC_SIG_MEASURE	1
FLOW_SIG	1
FUNC_SIG_PROCESS	9.995×10^{-1}

Table 7.6: Propagation of failure in risk analysis - Alternative scenario

Event	Probability of happenstance (y^{-1})
IE_PWR_DET	1×10^{-4}
FUNC_SIG_MEASURE	1
FLOW_SIG	1
FUNC_SIG_PROCESS	5×10^{-4}
FLOW_SIG_CONTROL	1
FUNC_REGUL	1
FLOW_SIG_CONTROL	1
FUNC_PROV_STORE	1×10^{-3}

Hence, we see that the reliability should be improved, and it can be done by acting on the probability of failure of the initiating event. Adding batteries or alternative power sources would tremendously lower the likelihood of failure.

Table 7.6 illustrates a potential cutset presenting a safety risk, from the same initiating event, and the associated probability. In this scenario, displayed in figure D.4, the signal from the neutron detector is not received, and the absence of signal is not acted upon by the automatic or human system in place. No negative reactivity is inserted to the core, which is not surveyed anymore. A chance of a transient happening while the detectors are down is considered. The probability of this event is calculated to be 5×10^{-11}, exceedingly low. Indeed, the loss of a detector does not imply that the core is going to melt, only that a line of defense, the flux measurement part, is temporarily gone. FFIP would consequently not recommend anything to be modified in this case, from the risk to the system point of view.

7.4 Uncoupled Flow Failure State Reasoning

Analyzing the risk and reliability of a complex system using only nominal flow paths through the use of directed graph disregards potentially crucial information. In a lot of failed systems, particularly catastrophic failures, the failure was caused by an unexpected flow compromising a component functionality. For example, in the book *The Hunt for Red October* [6], the submarine nuclear reactor fails in a catastrophic way due, partly, to a clapper getting loose in the primary

Table 7.7: Propagation of failure in reliability analysis

Event	Probability of happenstance (y^{-1})
IE_PWR_DET	1×10^{-3}
FUNC_SIG_MEASURE	1
FLOW_SIG	1
FLOW_THER_CORE	1
FLOW_THER_PRIM_SEC	1
FLOW_THER_SEC_TER	1
FUNC_CONV_HEX	1
FLOW_VAPOR	1
FUNC_TURBINE	1
FLOW_MECH_ENER	1
FUNC_GENERATOR	1

circuit and obstruing part of a pipe, causing a series of unrecoverable failures through the system. This clapper, a *Material - Object* flow, was not expected to be taken in by the *Channel - Transfer*function. This work of fiction illustrates one part of uncoupled flow failure, an unexpected flow following the nominal flow path.

However, another category of uncoupled flows are often also not considered during risk and reliability analysis. Those are external flows incurring after a failure of a function in the system. In nuclear systems, a well-known uncoupled flow would be caused by the explosion of a turbine. This would project shrapnels at high speed, which could damage the containment vessel, the control room or other unlinked components. In order to systematically study potential uncoupled flows caused by the failure of a function and their impact on the system as a whole as early in the design phase as possible, functional models can be used.

Potential flows generated by a function failure, or dispersed following a function failure, are computed in this method. A tank (*Provision - Store*) can thus generate a flow made of the tank walls (*Material - Solid*) and the tank filler (*Material - Liquid*). These accidental flows can then attack other function in the vincinity of the failed function. THe liquid could spill and damage some electrical wires. Shrapnels from a tank explosion could damage other components. The goal of this methodology is to estimate the reach of accidental flows throughout the system boundaries. How far can the uncoupled flows go, and how much damage can they make? A physics-based model can be used to estimate the reach of an uncoupled flow.

Several cutsets are displayed in the appendix.

To mitigate the increased risk and reliability issues seen in the system by taking into account the uncoupled flows, two main options are available. The model geometry can be modified, hence moving different critical functions out of reach of potential uncoupled flows. However, this method is not always viable, as the reach can be extensive and the system size limited. Another option is

to add what we will call *Arrestor functions*, i.e. functions whose role it is to stop uncoupled flow to reach functions of interest in the system. An example of an arrestor function might be a wall dressed between two components.

The number of uncoupled flows grows exponentially with relation to the size of the system. This is a problem when considering the exhaustivity of the solutions in a computer program for example, as well as the memory size and computation time required to solve the system. In order to mitigate this computation problem, the approach taken is reversed from FFIP or PRA. Instead of considering an initiating event and propagating the failure through the system, critical functions are defined, and UFFSR methodology estimates the potential paths (cutsets) that can fail these functions. Effectively, it disregards all cutsets that do not reach the critical functions with a probability higher than a given threshold.

Considering the scenario presented in figure E.1, the potential paths to reach either the failure of the risk critical function or the reliability critical function, as defined in the FFIP analysis, are computed. In the scenario considered, the turbine fails and explodes. This failure generates uncoupled flows, shrapnels (*Material - Object*). The range of the shrapnels are considered, and the scenario assume the destruction of vital equipment in the control room, the destruction of the condensers, the destruction of the tertiary pumps or some attched piping. However, in the analyzed cutset, the containment building is not failed, the concrete being able to whistand the incoming uncoupled flow.

The probability of failure of the components depends on the geometric layout of the plant and on the resistance of each component. This implies that several level of analysis are possible with this methodology. In the early design stage, this method can be used to generate new cutsets, that will be later investigated. Compared to nominal paths methods such as FFIP or PRA, more information is provided. FMEA is able to compute such uncoupled flows, but it does not come with an algorithm to systematically detect such uncoupled cutsets. However, in the early design stages, probability associated with a defined uncoupled cutset is difficult to estimate, since the probability depends, as said previously, on information unavailable to the design team. The engineers can however enter more details into their models as the design progresses. Components can be linked to functions and flows, using for example concept generators with FFDM. In those cases, information on the strength and the historical failure and potential uncoupled flows can be gathered and used to get a better idea of the system risk and reliability. Early conditions on the system layout can be obtained by simulating several possible layout and estimating the uncoupled flows propagation. Finally, once the components and layouts are chosen, UFFSR can be used to inform the designers about necessary or recommended arrestor functions to introduce in order to mitigate risks.

In 2009, a similar event happened in Russia, where a turbine exploded and destroyed a plant. The 1500-ton turbine went up approximately 50 feet before crashing back down. Debris were also sent laterally. In the case study, this means that instead of placing the turbines hall parallel

to the control room and the reactor building, it is recommended to place it such that the debris would not go in the direction of these buildings. One could also move the turbine hall away from the reactor and the control room, but this would not be very practical.

Physics-based models can be used to compute the probability of a failure propagation through an uncoupled flow. In the example of the turbine exploding considered, the speed and direction of the resulting shrapnels can be assumed. From this information, the distance the shrapnels can cover and the perforation power they hold can be modeled. The impact of this can be compared to the position and strength of various components.

Say that the turbine catastrophic failure cause shrapnel to be emitted vertically and along the sides of the turbine, with a speed of s $m.s^{-1}$. The range of a projectile is computed using Equation 7.4, considering no air resistance. This will give us a higher bound for the range. Of course, the range does not tell the full story, since the incoming speed and force applied to other components is paramount to its health. In the case of the scenario E.1 applied to the case study, the height of the turbine can be considered to be 2 meters. It may be so to facilitate maintenance as well as preventing against flood damages. The direction of the debris expulsed following a turbine explosion is considered isotropic, ranges from 0 to 360 degrees radially. We consider that the projectile cannot be launched axially, due to the turbine intrinsic motion. The initial speed can vary. An initial velocity of 50 $m.s^{-1}$ is considered in this example.

Plugging these numbers into equation 7.4 would give a maximum range of around 257 m. The reality would be lower, considering air resistance. Even if air resistance caused the range to be half of this value, say around 125 m, this is still very consequent and the solution cannot realistically be to increase the distance between the components. However, by orientating the turbines correctly with regards to the other components, that is, avoid placing components on the sides of the turbines, most of the uncoupled flows consequences can be mitigated. In the considered scenario, an arrestor function seems also very important. Concrete walls can be erected around the turbines hall in order to stop most of the shrapnel from such an event. This is explicited in figure E.2. It can be seen that due to the loss of the SIS, even though the rods can be lowered in the core, decay heat is not taken out and thus the core melt down anyway, despite the arrestor function preventing widespread damages to the plant. However, the likelihood of this event, as computed by FFIP analysis, is deemed very low (less than 10^{-10}). The fact that the probability is this low is due to the fact that, in reality, a decay heat exchange system, with its own *Provision - Supply* function, is included within the *Channel - Transfer* function (top right corner of the functional model). This distinction between two different system with a similar goal was intentionally left out for the sake of simplicity, and the redundancy coded in the failure probability.

$$d = \frac{v\cos(\theta)}{g}\left(v\sin(\theta) + \sqrt{v^2\sin^2(\theta) + 2gy_0}\right) \tag{7.4}$$

Where, as explicited on figure 7.2:

d = Range

v = Initial velocity

g = Gravitational acceleration

y_0 = Initial height

θ = Initial angle

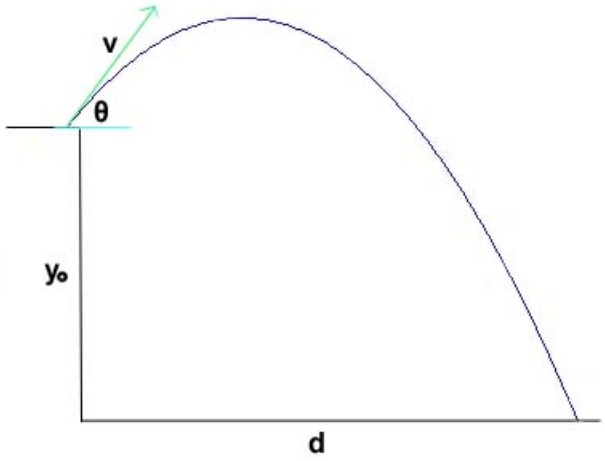

Figure 7.2: Range of a projectile.

Consequently, UFFSR can show cutsets that other methods either do not consider at all (PRA, FFIP, RBD, ...), or do not consider in a consistent manner (FMEA, ...). It requires a lot of time and computational power to be performed on a large system scale. However, UFFSR can quickly gives precious information about the system risks and reliability, though the conclusions drawn need to be refined as more details are available. In this case study, we saw that the turbine explosion was a real risk to the system, and that simple measures could be taken, such as the turbines orientations and a concrete wall, in order to mitigate the risks. The analysis done is a simplified case of what UFFSR can do. Indeed, the probability of an uncoupled flow was not considered in the scenario studied, only the possibility. The probability of an uncoupled flow reaching other functions in the system is a function of the distance between the initiating event and the analyzed function $d_{i,f}$, as well as the analyzed function resistance to the incoming flow $s_{f,i}$. It can be written $P = f(d_{i,f}, s_{f,i})$. There resides the real future strength of UFFSR, once a computational framework is created.

7.5 Prognostics in Early Functional Design

More and more systems use Prognostic Health Management (PHM) hardware to detect future failures and allow for preventive maintenance and recovery actions, automated or manual.

However, the hardware is often added on after the system has been built or during the late stages of the design. In the early stages of the design, PHM is currently not seriously considered, despite the consequent impact it can have on the system failure and the subsequent design choices made. Hence, a system can be designed with unnecessary expensive redundancies which could be deprecated by PHM hardware. The earlier in the design phase a system fault is discovered, the less costly the design required modifications can be. Being able to consider prognosis in the early phases by modeling the impact of PHM hardware allow the designer to limit the costly system changes and increase the system reliability.

Probabilistic Risk Assessment (PRA) method is able to model failure detection and recovery actions, but is limited by its rigidness, time-consuming changes, and by its use in the late phases of design. FMEA or functional failure methods, such as FFDM or FFIP, are not able to model recovery actions in a dedicated framework.

The Prognostics in Early Design method proposed in this paper creates a framework that enable the use of a functional failure method in various stages of design, notably early on, coupled with PHM hardware considerations. A Bayesian network is used to compute the functional failure propagation probabilities. The optimized configuration for PHM equipment positioning is automatically given to the system designer, who can then decide to move forward with it or modify the system, according to the system failure probability returned by the algorithm.

7.5.1 Methodology

The methodology can be discretized into four main parts. This method is based upon a functional representation of a system as developed by Stone [18], augmented with Success Tree Analysis (STA), the logical opposite of FTA. Four distinct databases are necessary to represent various system information. They comprise information about PHM hardware efficiency, emergent function weaknesses, impacts of function failure on subsequent linked flows quality, and tie the probability of corrective action success to each particular system function and flow. The selection and positioning of PHM hardware through the designed system is generated. The Bayesian network representing the complex system is consequently built following the framework shown in figure 7.3. A risk and reliability analysis is performed on the system. The positioning of PHM equipment can then iterately be modified to compute the best possible system configuration and supports the decision making.

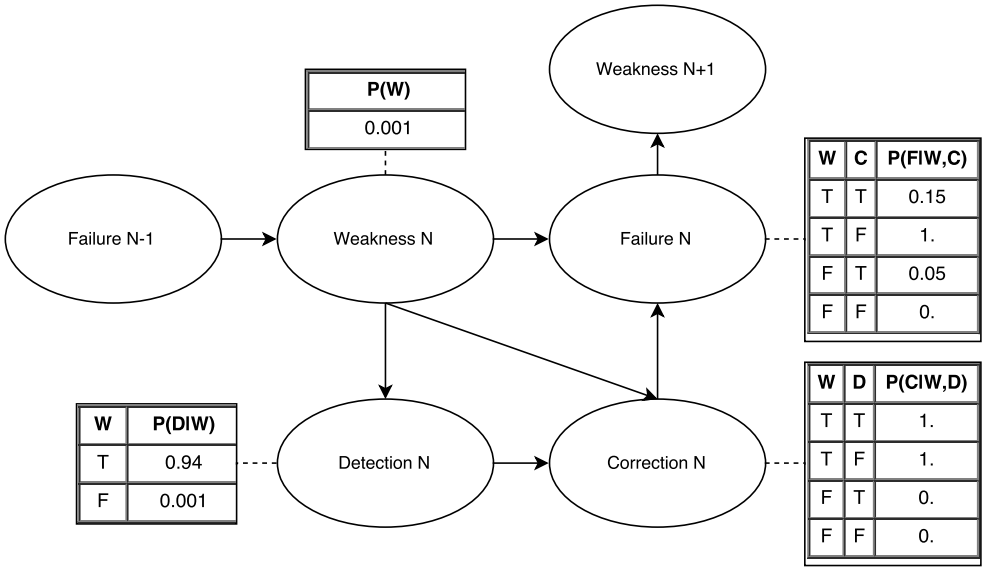

Figure 7.3: Example of the method prognostic bayes net.

In order to illustrate the algorithm presented, a small example is given. Figure 7.4 presents a very simple functional model, and Figure 7.5 its translation into the proposed method model, provided each function and flow are linked to a PHM device. The interaction with the various database, $\mathscr{F}$, $\mathscr{H}$, $\mathscr{M}$, $\mathscr{P}$ and $\mathscr{W}$ is also shown in Figure 7.5. If the designer were to force the flow f_{12} not to be equipped with a PHM hardware, the nodes *Detection* f_{12} and *Correction* f_{12} would disappear from the model, along with the connections.

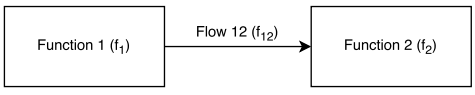

Figure 7.4: Simple functional model.

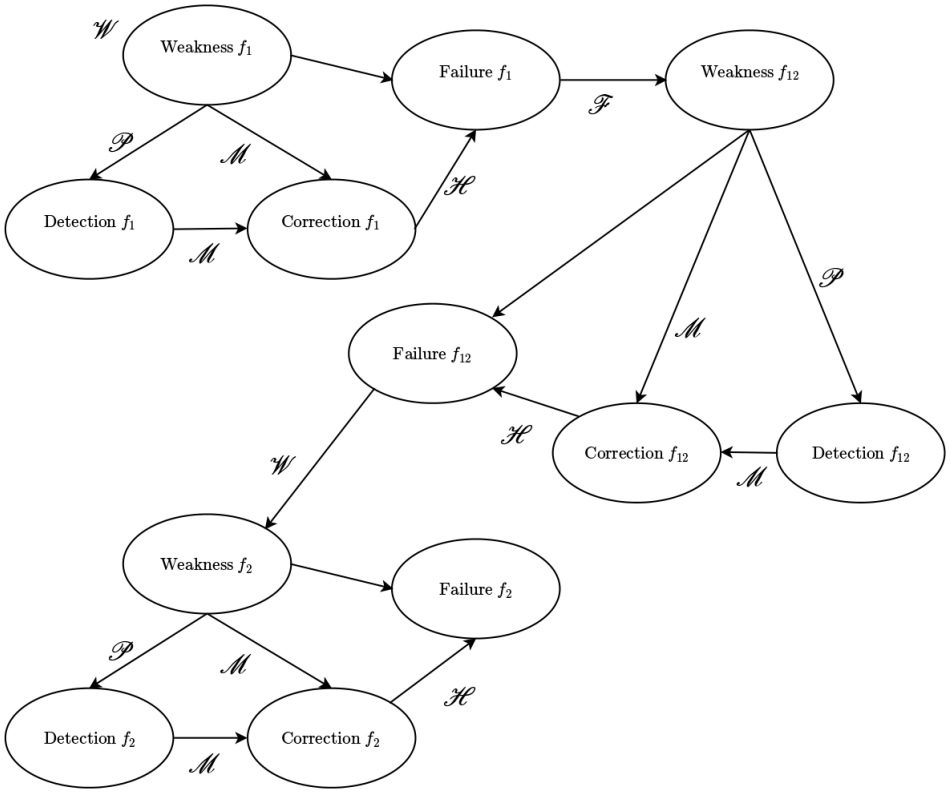

Figure 7.5: Translation of a simple function model (Figure 7.4) to its functional prognostic Bayesian network form.

The Bayesian network used to describe the whole system is based upon the following algorithm steps.

Step 0 This step is optional. In a Bayesian network, the designer can set the states of several functions and flows. While not particularly useful to generate the risk and reliability analysis on the system during the early design phase, it can be noted that this feature can be used simultaneously as a Prognostics and Diagnostics tool during the operational lifetime of the system.

Step 1 The algorithm computes the probability of a function weakness, given the observed evidence (step 0) or $\mathscr{W}$. The function weakness nodes is a binary event, meaning that it can only take one of two potential states. Consequently, either there is a weakness or the function is in a nominal state, as represented by W in Equation 7.5 for the function f_1.

$$P(W_{f_1}) = \begin{matrix} state \\ Y \\ N \end{matrix} \begin{bmatrix} \omega_{f_1} \\ \bar{\omega_{f_1}} = 1 - \omega_{f_1} \end{bmatrix} \tag{7.5}$$

Table 7.8: Conditional probability tables for the weakness detection, correction and failure of a function f_1

$P(D_{f_1}\|W_{f_1})$	Weakness f_1	Y	N
Detection f_1	Y	ε_{phm,f_1}	e_{phm,f_1}
	N	$1-\varepsilon_{phm,f_1}$	$1-e_{phm,f_1}$

$P(C_{f_1}\|W_{f_1},D_{f_1})$	Weakness f_1	Y		N	
	Detection f_1	Y	N	Y	N
Correction f_1	Y	γ_{f_1}	μ_{f_1}	γ_{f_1}	μ_{f_1}
	N	$1-\gamma_{f_1}$	$1-\mu_{f_1}$	$1-\gamma_{f_1}$	$1-\mu_{f_1}$

$P(F_{f_1}\|W_{f_1},C_{f_1})$	Weakness f_1	Y		N	
	Correction f_1	Y	N	Y	N
Failure f_1	Y	$1-\rho_{f_1}$	1	β_{f_1}	0
	N	ρ_{f_1}	0	$1-\beta_{f_1}$	1

Step 2 The weakness probability associated with f_1 has been computed in step 1. The probability of being in a state of detection by a PHM hardware can now be calculated. Several potential states can be described to link a weakness of a function to its detection. There could effectively be a weakness, and this weakness could be detected according to the attached hardware efficiency ε_{phm,f_1}. The probability of this event will be noted d_{ε,f_1}. Alternatively, there might be no function weakness, but a false alarm is raised by the hardware according to its false alarm rate e_{phm,f_1}. The probability of this event will be noted d_{e,f_1}. The combination of these two events forms the probability of a detection.

The probability of being in the state of non detection, is trivially the complement of the probability of detection. Either the weakness is present and not detected, or there is no weakness, and no false alarm is raised.

The different probability path leading to the probability of detection are represented in Table 7.8.

Given the function weakness probability, the detection conditional probability matrix $P(D_{f_1}|W_{f_1})$ obtained is displayed in Equation 7.6.

$$P(D_{f_1}|W_{f_1}) = \begin{matrix} \\ Y \\ N \end{matrix} \overset{state}{\begin{bmatrix} d_{\varepsilon,f_1}+d_{e,f_1} \\ d'_{\varepsilon,f_1}+d'_{e,f_1} \end{bmatrix}} \tag{7.6}$$

Where:

$$d_{\varepsilon,f_1} = \omega_{f_1}\varepsilon_{phm,f_1}$$

$$d_{e,f_1} = (1-\omega_{f_1})e_{phm,f_1}$$

$$d'_{\varepsilon,f_1} = \omega_{f_1}(1-\varepsilon_{phm,f_1})$$

$$d'_{e,f_1} = (1-\omega_{f_1})(1-e_{phm,f_1})$$

This step is performed if and only if the function of interest is equipped with a PHM hardware. Indeed, if a PHM hardware is not attached to the function, the detection is trivially non-existent, implying $\varepsilon_{phm,f_1} = 0$ and $e_{phm,f_1} = 0$. Entering these numbers in Equation 7.6, we obtain the relation 7.7.

$$P(D_{f_1}|W_{f_1}) = \begin{matrix} \\ Y \\ N \end{matrix} \overset{state}{\begin{bmatrix} 0 \\ 1 \end{bmatrix}} \tag{7.7}$$

Step 3 The weakness probability and the detection probability have been computed respectively in step 1 and step 2. This third step estimates the probability of a corrective action being attempted. The potential scenarii leading to the corrective action are treated by the conditional probability table presented in Table 7.8. In the case of an actual weakness, the detector could detect the weakness (d_{ε,f_1}). Then, the maintenance team is sent to repair according to a decision probability γ_{f_1} given by $\mathscr{M}$. Alternatively, the weakness is not detected (d'_{ε,f_1}) but a scheduled non required maintenance is done on the function, according to a probability μ_{f_1} also given by $\mathscr{M}$. The combination of these two events translate to a probability noted c_{ω,f_1}. Maintenance can also be carried out on the function if no weakness actually happened. This event is true if a false alarm (d_{e,f_1}) caused the maintenance team to mobilize or if a scheduled non required maintence is performed. These two events can be combined to obtain a probability noted $c_{\bar{\omega},f_1}$. Finally, the corrective action probability can be calculated by combining c_{ω,f_1} with $c_{\bar{\omega},f_1}$.

Considering the fact that the corrective action is a binary event, the probability of no corrective action being carried out is trivially the complement of the probability that a corrective action is performed.

Given the function weakness probability $P(W_{f_1})$ and the detection probability matrice $P(D_{f_1}|W_{f_1})$, the conditional corrective action matrice obtained is displayed in Equation 7.8.

$$P(C_{f_1}|W_{f_1},D_{f_1}) = \begin{matrix} \\ Y \\ N \end{matrix} \overset{state}{\begin{bmatrix} c_{\omega,f_1} + c_{\bar{\omega},f_1} \\ c'_{\omega,f_1} + c'_{\bar{\omega},f_1} \end{bmatrix}} \tag{7.8}$$

Where:

$$c_{\omega,f_1} = d_{\varepsilon,f_1}\gamma_{f_1} + d'_{\varepsilon,f_1}\mu_{f_1}$$

$$c_{\bar{\omega},f_1} = d_{e,f_1}\gamma_{f_1} + d'_{e,f_1}\mu_{f_1}$$

$$c'_{\omega,f_1} = d_{\varepsilon,f_1}(1-\gamma_{f_1}) + d'_{\varepsilon,f_1}(1-\mu_{f_1})$$

$$c'_{\bar{\omega},f_1} = d_{e,f_1}(1-\gamma_{f_1}) + d'_{e,f_1}(1-\mu_{f_1})$$

Step 4 Based on the weakness probability and the corrective action probability, calculated respectively in step 1 and step 3, the algorithm computes the probability of the function failure using the conditional probability table displayed in Table 7.8. In the case of an actual weakness, the path leading to a failure can be that no corrective action was performed (c'_{ω,f_1}), or that a corrective action was performed (c_{ω,f_1}) but was unsuccessful, according to the ρ_{f_1} value given in $\mathscr{H}$. Alternatively, a function can fail if there was no weakness but a corrective action was still performed ($c_{\bar{\omega},f_1}$) and generated a function failure according to the mishandling probability β_{f_1} given by $\mathscr{H}$. The failure probability of f_1 is obtained by combining these different scenarii.

The probability that the function does not fail is obtained if a weakness was present but was corrected following the ρ_{f_1} value, or no weakness was present and either no action were performed or the performed action did not fail the function, according to the mishandling probability β_{f_1}. This corresponds to the complement of the probability of failure.

Given the function weakness probability $P(W_{f_1})$ and the correction probability matrice $P(C_{f_1}|W_{f_1},D_{f_1})$, the conditional failure matrice obtained is displayed in Equation 7.9.

$$P(F_{f_1}|W_{f_1},C_{f_1}) = \begin{matrix} \\ Y \\ N \end{matrix} \overset{state}{\begin{bmatrix} f_{f_1} \\ f'_{f_1} \end{bmatrix}} \tag{7.9}$$

Where:

$$f_{f_1} = c_{\omega,f_1}(1-\rho_{f_1}) + c'_{\omega,f_1} + c_{\bar{\omega},f_1}\beta_{f_1}$$

$$f'_{f_1} = c_{\omega,f_1}(\rho_{f_1}) + c'_{\bar{\omega},f_1} + c_{\bar{\omega},f_1}(1-\beta_{f_1})$$

Step 5 A function failure can be linked to different outgoing flow quality. The flow quality represents a state of weakness and is modeled by a *s*-event. A *s*-event is an event that can take four distinct states of flow quality. The quality of a flow can be categorized as failed (λ_f), of low concern (λ_l), of high concern (λ_h), or nominal (λ_n). The algortihm considers that the quality of a flow cannot spontaneously change without an impact on the last function acting on it. This

represents one of the simulation limitation, as discussed previously. Indeed, it does not allow for the treatment of failure flows going through a function without failing it.

$\mathscr{F}$ contains the detailed data for each specific function-flow connection. The probability of weakness $P(W_{f_{12}}|F_{f_1})$ is displayed in Equation 7.10.

$$P(W_{f_{12}}|F_{f_1}) = \begin{matrix} state \\ f \\ l \\ h \\ n \end{matrix} \begin{bmatrix} w_{f,f_{12}} \\ w_{l,f_{12}} \\ w_{h,f_{12}} \\ w_{n,f_{12}} \end{bmatrix} \tag{7.10}$$

Where:

$$w_{f,f_{12}} = \lambda_{f,f_{12}} f_{f_1}$$
$$w_{l,f_{12}} = \lambda_{l,f_{12}} f_{f_1}$$
$$w_{h,f_{12}} = \lambda_{h,f_{12}} f_{f_1}$$
$$w_{n,f_{12}} = f_{f_1} + f'_{f_1} - \sum_{i\in[f,h,l]} f_{f_1} \lambda_i$$

Step 6 The weakness probability of f_{12} has been computed in step 5. The probability of a detection can now be calculated. Similarily to step 2, several potential states can be described to link a weakness of a flow to its detection. There could effectively be a flow quality weakness, which is detected according to the attached hardware efficiencies. The hardware efficiencies for a flow are given for the three states of degraded operation, low concern ($\varepsilon_{phm,l,f_{12}}$), high concern ($\varepsilon_{phm,h,f_{12}}$) and failed ($\varepsilon_{phm,f,f_{12}}$). The probability of a scenario in which a weakness is present and detected will be noted $d_{\varepsilon_i,f_{12}}$, for $i \in [f,l,h]$. Alternatively, a detection might occur if there is no flow weakness, but a false alarm is raised by the hardware according to its false alarm rate $e_{phm,f_{12}}$. The probability of this event will be noted $d_{e,f_{12}}$. The combination of these two events forms the probability of a detection. This can be seen in Table 7.9.

The probability of not having a detection is the complement of the probability of having a detection. Indeed, if the flow quality is not nominal, the detector might fail to detect it, with a probability depending on its efficiency. If the flow quality is nominal, the detector can also not signal any issue, based on its false alarm rate.

Given the flow weakness probability, the detection conditional probability matrice $P(D_{f_{12}}|W_{f_{12}})$ obtained is displayed in Equation 7.11.

Table 7.9: Conditional probability tables for the weakness detection, correction and failure of a flow f_{12}

$P(D_{f_{12}}\|W_{f_{12}})$	Weakness f_{12}	Failed	Low concern	High concern	Nominal
Detection f_{12}	Y	$\varepsilon_{phm,f,f_{12}}$	$\varepsilon_{phm,l,f_{12}}$	$\varepsilon_{phm,h,f_{12}}$	$e_{phm,f_{12}}$
	N	$1-\varepsilon_{phm,f,f_{12}}$	$1-\varepsilon_{phm,l,f_{12}}$	$1-\varepsilon_{phm,h,f_{12}}$	$1-e_{phm,f_{12}}$

$P(C_{f_{12}}\|W_{f_{12}},D_{f_{12}})$	Weakness f_{12}	Failed		Low concern		High concern		Nominal	
	Detection f_{12}	Y	N	Y	N	Y	N	Y	N
Correction f_{12}	Y	$\gamma_{f,f_{12}}$	$\mu_{f,f_{12}}$	$\gamma_{l,f_{12}}$	$\mu_{l,f_{12}}$	$\gamma_{h,f_{12}}$	$\mu_{h,f_{12}}$	$\gamma_{n,f_{12}}$	$\mu_{n,f_{12}}$
	N	$1-\gamma_{f,f_{12}}$	$1-\mu_{f,f_{12}}$	$1-\gamma_{l,f_{12}}$	$1-\mu_{l,f_{12}}$	$1-\gamma_{h,f_{12}}$	$1-\mu_{h,f_{12}}$	$1-\gamma_{n,f_{12}}$	$1-\mu_{n,f_{12}}$

$P(F_{f_{12}}\|W_{f_{12}},C_{f_{12}})$	Weakness f_{12}	Failed		Low concern		High concern		Nominal	
	Correction f_{12}	Y	N	Y	N	Y	N	Y	N
Failure f_{12}	Y	$1-\rho_{f,f_{12}}$	1	$1-\rho_{l,f_{12}}$	1	$1-\rho_{h,f_{12}}$	1	$\beta_{f_{12}}$	0
	N	$\rho_{f,f_{12}}$	0	$\rho_{l,f_{12}}$	0	$\rho_{h,f_{12}}$	0	$1-\beta_{f_{12}}$	1

$$P(D_{f_{12}}|W_{f_{12}}) = \begin{matrix} \\ Y \\ N \end{matrix} \overset{state}{\begin{bmatrix} \sum_{i\in[f,h,l]} d_{\varepsilon_i,f_{12}} + d_{e,f_{12}} \\ \sum_{i\in[f,h,l]} d'_{\varepsilon_i,f_{12}} + d'_{e,f_{12}} \end{bmatrix}} \tag{7.11}$$

Where:

$$d_{\varepsilon_i,f_{12}} = \omega_{i,f_{12}} \varepsilon_{phm,i,f_{12}}$$

$$d_{e,f_{12}} = \omega_{n,f_{12}} e_{phm,f_{12}}$$

$$d'_{\varepsilon_i,f_{12}} = \omega_{i,f_{12}} (1-\varepsilon_{phm,i,f_{12}})$$

$$d'_{e,f_{12}} = \omega_{n,f_{12}} (1-e_{phm,f_{12}})$$

This step is performed if and only if the function of interest is equipped with a PHM hardware. Indeed, if a PHM hardware is not attached to the function, the detection is trivially in a false state.

Step 7 The flow weakness probability and the detection probability have been computed respectively in step 5 and step 6. This next step estimates the probability of a corrective action being attempted. The potential scenario leading to the corrective action are treated by the conditional probability table presented in Table 7.9. In the case of an actual weakness, the detector could detect the weakness according to the corresponding hardware efficiency for each flow quality ($d_{\varepsilon_i,f_{12}}$ for $i \in [f,l,h]$). If the event is detected, the maintenance team is sent to repair according to a decision probability $\gamma_{i,f_{12}}$ for $i \in [f,l,h]$, based on the team management and the detected flow quality weakness. The decision probability is given by $\mathscr{M}$. Alternatively, the weakness could be undetected ($d'_{\varepsilon_i,f_{12}}$ for $i \in [f,l,h]$) but a scheduled non required maintenance could be performed on the system which would impact the flow, according to a probability $\mu_{f_{12}}$

also given by $\mathscr{M}$. The combination of these two events translates to a probability noted $c_{\omega,i,f_{12}}$ for $i \in [f,l,h]$. Maintenance can also be carried out on the system, with a direct impact on the flow f_{12} if no weakness actually happened. This event is true if a false alarm ($d_{e,f_{12}}$) caused the maintenance team to mobilize or if a scheduled non required maintence is performed. These two events can be combined to obtain a probability noted $c_{\bar{\omega},f_{12}}$. Finally, the corrective action probability can be calculated by combining $c_{\omega,i,f_{12}}$ with $c_{\bar{\omega},f_{12}}$ for $i \in [f,l,h]$.

The probability that no corrective action is attempted is the complement of the probability that a corrective action is carried out.

Given the function weakness probability $P(W_{f_{12}}|F_{f_1})$ and the detection probability matrice $P(D_{f_{12}}|W_{f_{12}})$, the conditional corrective action matrice obtained is displayed in Equation 7.12.

$$P(C_{f_{12}}|W_{f_{12}},D_{f_{12}}) = \begin{matrix} \\ Y \\ N \end{matrix} \overset{state}{\begin{bmatrix} \\ \sum_{i\in[f,l,h,n]} c_{\omega_i,f_{12}} \\ \\ \sum_{i\in[f,l,h,n]} c'_{\omega_i,f_{12}} \\ \end{bmatrix}} \tag{7.12}$$

Where, for $i \in [f,l,h]$:

$$\begin{aligned}
c_{\omega_i,f_{12}} &= d_{\varepsilon_i,f_{12}}\gamma_{i,f_{12}} + d'_{\varepsilon_i,f_{12}}\mu_{f_{12}} \\
c_{\omega_n,f_{12}} &= d_{e,f_{12}}\gamma_{n,f_{12}} + d'_{e,f_{12}}\mu_{f_{12}} \\
c'_{\omega_i,f_{12}} &= d_{\varepsilon_i,f_{12}}(1-\gamma_{i,f_{12}}) + d'_{\varepsilon_i,f_{12}}(1-\mu_{f_{12}}) \\
c'_{\omega_n,f_{12}} &= d_{e,f_{12}}(1-\gamma_{n,f_{12}}) + d'_{e,f_{12}}(1-\mu_{f_{12}})
\end{aligned}$$

Step 8 Based on the flow weakness probability and the corrective action probability, calculated respectively in step 5 and step 7, the algorithm computes the probability of the flow failure using the conditional probability table displayed in Table 7.9.

In the case of an actual weakness, either of low concern, of high concern, or failed, the path leading to a failure can be that no corrective action was performed $\left(\sum_{i\in[f,l,h]} c'_{\omega_i,f_{12}}\right)$, or that a corrective action was performed $\left(\sum_{i\in[f,l,h]} c_{\omega_i,f_{12}}\right)$ but was unsuccessful, according to the $\rho_{i,f_{12}}$ values for $i \in [f,l,h]$ given in $\mathscr{H}$. Alternatively, the flow can fail if there was no weakness but a corrective action was still performed on the system ($c_{\omega_n,f_{12}}$) and generated a function failure according to the mishandling probability $\beta_{f_{12}}$ given by $\mathscr{H}$.

Given the function weakness probability $P(W_{f_1})$ and the correction probability matrice $P(C_{f_1}|W_{f_1},D_{f_1})$, the conditional failure matrice obtained is displayed in Equation 7.13.

$$P(F_{f_{12}}|W_{f_{12}},C_{f_{12}}) = \begin{matrix} state \\ Y \\ N \end{matrix} \begin{bmatrix} f_{f_{12}} \\ f'_{f_{12}} \end{bmatrix} \tag{7.13}$$

Where:

$f_{f_{12}} = c_{\omega_n,f_{12}}\beta_{f_{12}} + \sum_{i\in[f,l,h]} c_{\omega_i,f_{12}}(1-\rho_{i,f_{12}}) + c'_{\omega_i,f_{12}}$

$f'_{f_{12}} = c_{\omega_n,f_{12}}(1-\beta_{f_{12}}) + c'_{\omega_n,f_{12}} + \sum_{i\in[f,l,h]} c_{\omega_i,f_{12}}\rho_{i,f_{12}}$

If the next Bayesian node in the model is a logical gate, the algorithm goes to step 9-b. Else, it goes back to step 9-a.

Step 9-a A failed flow is considered to fail a receiving function, since the function will not be able to perform its task without a necessary flow. The failure probability obtained in step 8 for the flow is thus passed fully to the next function in the model. The emergent weakness of the next function in the model is also considered. Consequently, given $P(F_{f_{12}}|W_{f_{12}},C_{f_{12}})$, the weakness probability seen by the next function is displayed in the conditional failure matrice in Equation 7.14.

$$P(W_{f_2}|F_{f_{12}}) = \begin{matrix} state \\ Y \\ N \end{matrix} \begin{bmatrix} f_{f_{12}} + \omega_{f_2} \\ f'_{f_{12}} - \omega_{f_2} \end{bmatrix} \tag{7.14}$$

The algorithm returns to step 1.

Step 9-b Logical gates can combine several flows and compute the next function weakness associated. Consider another flow, f_{32}, supplying a redundant flow to function f_2. An OR-gate is placed in the model, so that only one flow, f_{12} or f_{32} is needed for function f_2 to operate nominally.

The probability that the flow failures propagate through the gate $g_{12,32}$ to the next function weakness, $P(F_{f_2}|F_{f_{12}},F_{f_{32}})$, is explicited in Equation 7.15.

$$P(F_{g_{12,32}}|F_{f_{12}},F_{f_{23}}) =$$

$$\begin{matrix} state \\ Y \\ N \end{matrix} \begin{bmatrix} f_{f_{12}}f_{f_{32}} \\ f'_{f_{12}}f_{f_{32}} + f_{f_{12}}f'_{f_{32}} + f'_{f_{12}}f'_{f_{32}} \end{bmatrix} \tag{7.15}$$

The gate failure probability becomes the new flow failure probability. The algorithm returns to step 9-a.

Table 7.10: Detectors considered

Detector	ε	e
S	0.80	0.001
Q	0.98	0.1

7.5.2 Application to the case study

The existing automatic tools to compute the optimized combination of PHM hardware in the system and the associated probability of failure is not yet able to run the simulation of a quite large functional models such as the one presented in figure 7.1 on a local computer in a reasonable amount of time. Work is ongoing to parallelize the algorithm and optimize its runtime. In order to illustrate part of the method, a subset of the system will be considered. The failure of the turbine, as studied in the work relative to FFIP and UFFSR, is going to be considered. Two different sensors can be used to detect a weakness of the function. The change in the final probability of failure after taking into account the PHM hardware will be computed.

Two different kind of sensors could be used to detect a potential failure of the function fo interest. In our case, we will consider a sensor giving the rotation speed of the turbine (S) and a sensor giving the vapor quality and flow (Q). S is taken as having a 85% chance of detecting an anomaly leading to a function failure. A false alarm rate of 0.001 is imagined. Alternatively, Q has a 98% chance of detecting an anomaly and a false alarm rate of 0.1.

Table 7.10 shows the chosen parameters.

An "ideal" management is considered, based uniquely on PHM hardware data. Consequently, $\gamma = 1$ and $\mu = 0$. This implies that a maintenance team is sent if and only if a detector indicates a potential weakness.

After detection of an anomaly, the repair success is computed according to Human Reliability Assessment (HRA). In our case, we will consider that should a weakness be detected on the function *Channel - Guide - Rotate* representing the turbine, the following algorithm should be followed to obtain the repair success probability. The assumptions made are presented in table 7.11. The human error probability (HEP) is defined from the combination of the Performance Shaping Factors (PSF_c) corresponding to different essential parts of the maintenance success such as stress factor or task complexity. It follows Equation 7.16. $NHEP$ is defined in HRA as being equal to 0.001 for action-based maintenance. The mishandling probability is computed from PSF_c disregarding the time component.

$$HEP = \frac{NHEP * PSF_c}{NHEP * (PSF_c - 1) + 1} \tag{7.16}$$

Consequently, we can compute $\rho = 0.985$ and $\beta = 0.0015$.

Table 7.11: Estimates of the different HRA categories

Category	Level
available time	Time available = time required
stress	Nominal
complexity	Nominal
human training	Low
procedures	Insufficient information
ergonomics	Nominal
fitness for duty	Nominal
processes	Good

Using these information, it is now possible to compute the impact of a detector on the probability of failure of the function of interest. We will consider an initial probability of weakness of 1, in order to compute directly the impact of the prognostics in early design method. The probability of failure is reduced to 0.035 using Q and 0.21 using S. The higher false alarm rate is not a big enough issue to make up for the efficiency difference. This is due to the fact that the repair or corrective action is considered simple. We consequently consider that the probability of failure of this function is lowered by almost two orders of magnitudes. This translates to the subsequent FFIP analysis of the system, lowering the probability of failure of the initiating event.

A more detailed analysis of several functions and sensors accross the system is performed. In this analysis, we consider $gamma = 1$ and $\mu = 0$, meaning that every time, and only if, a detection occur, a maintenance team is sent. Several sensors are used, including two types of vibration sensors (VIB_1 and VIB_2), two types of flux sensors (FLU_1 and FLU_2), a flow sensor (FLW), a video camera (VID) and an acoustic sensor (ACO). The sensors exhibit different parameters dependiong on the monitored function. The results can be seen in table 7.12.

It is interesting to note that in the case of the turbine, the repair is considered easy with a low chance of causing a failure. The best sensor for the monitoring of this function is the flow sensor, while the least adequate is the video camera one. The video camera use does reduce the probability of failure by a factor 3, and can be considered low cost. However, its high false alarm rate implies that the maintenance team will make a lot of trip to check the turbine, impacting the productivity of the component and the availability of the maintenance team for other tasks. When looking at the vessel, due to a low chance of being able to fix it if a problem is detected, the efficiency of the sensors is a secondary impact. In that case, considering the low probability of failure, a scheduled visual inspection should be enough and a PHM hardware would not bring much. Finally, we consider the backup generators. The generators are considered quite unreliable

Table 7.12: Example of the impact of PHM sensors on the failure probability for specific functions/components

Function	Component	Function parameters		Sensor	Sensors parameters		Weakness	Failure
		ρ	β		ε	e	(y^{-1})	(y^{-1})
Channel - Guide - Rotate	Turbine	0.985	0.0015	VIB_1	0.91	0.1	3×10^{-3}	4.6×10^{-4}
				VIB_2	0.85	0.002		4.9×10^{-4}
				FLW	0.97	0.05		2.1×10^{-4}
				VID	0.7	0.2		1.2×10^{-3}
				ACO	0.77	0.01		7.4×10^{-4}
Provision - Store - Contain	Vessel	0.3	0.	FLU_1	0.94	0.01	5×10^{-5}	3.6×10^{-5}
				FLU_2	0.999	0.001		3.5×10^{-5}
				VID	0.85	0.3		3.7×10^{-5}
Convert - Convert	Backup generator	0.6	0.1	ACO	0.7	0.1	1×10^{-2}	1.5×10^{-2}
				VIB_1	0.89	0.15		1.9×10^{-2}
				VIB_2	0.95	0.01		5.3×10^{-3}

and difficult to fix, notably because of the time frame to perform the maintenance. Moreover, a very high chance of maintenance mistake is considered. With those parameters, we can see that the sensors with a low efficiency and high false alarm rate cause the function to be less reliable. A factor of two can be gained by using an efficient vibration detector. Considering such a high chance of the maintenance team generating a failure and the low chance of actually fixing an issue, it can be deemed detrimental to use PHM systems here until the team is better trained, or until the generator are easier to fix.

This demonstrates a small part of what this method can actually accomplish, seeing as it is not limited to one function or flow in the system but also its impact on the whole system, and that it can attribute sensors to potentially every function or flow in the model. A more detailed case study, on a simplified pressurized water reactor design, is performed in [10].

Taking into account Prognostics and Health Management systems early in the design can reduce cost, by avoiding costly and redundancies and using the strength of PHM instead. It can also allow to detect weak maintenance point on which training and component ergonomy should be improved.

7.6 Cable and Pipe Routing

In a complex systems, a large number of cables and pipes are used for various purposes. The failure of a cable or pipe section can thus impact several components in the system if the cables are not properly isolated. The CRFFA method looks at the optimum path for the cables, avoiding configurations where common-cause failure can fail several functions of the system at once.

In the case study at hand, a risk often seen is a fire hazard. Indeed, the use of Sodium and its reactivity with air and water make the Sodium-cooled fast reactor prone to exhibit fires. Fire can easily damage cables and fail their associated function. Fire can be caused by two pipes, one

carrying sodium, the other water, being too close to one another. However, interaction of Sodium with air renders this routing problem secondary.

In our system, several routing configurations must be avoided, especially in regards to the redundant systems, such as the neutron flux detectors or temperature detectors. The redundancy is jeopardized if the signal or power cables all run along the same path for an extended section length. Indeed, a failure in this section, whether it is fire or human mistake, would fail every detector at once, forcing a reactor shutdown. If the cables cannot physically be separated due to geometric constraints, or if maintenance is hindered by the isolation of these cables, the section at risk should be monitored to detect potential failures (degraded cables, etc). This would help improve the system's reliability.

In our system, safeguards exist to prevent damage to the core in case of a loss of power or signal. Watchdogs are put in place along with "passive" safety system. One example is the watchdog that control the rods falling mechanism. If no signal is received, the mechanism is designed to let go of the rods and shut down the reactor. This implies that any cable routing configuration is fine from a risk standpoint. Watchdogs allow for the CRFFA method to be used only in reliability analysis. This allow the designer to consider the CRFFA constraints as secondary and possible in the late stages of design.

Arguably more important than the cable routing itself, an efficient, labeled and orderly cable layout should be used. Color-coded, labeled cables will drastically reduce potential human error during maintenance, potentially more so than their routing.

As mentionned, CRFFA can also be applied to pipes routing configuration within the system. The main issue in our piping will come from leaky pipes causing water to spray electrical component and sodium to interact with air or water. Consequently, it should be seen to, during the final geographical design of the plant, that water pipes avoid passing over electrical component as much as possible. This ties in with the UFFSR analysis, and the potential use of arrestor functions in the system.

APPENDIX A

RELIABILITY BLOCK DIAGRAM

Reliability block diagrams, for a system as complex as a nuclear plant especially, can become huge and hard to read. In order to facilitate the reading, the case study has been divided in four systems: primary, secondary, tertiary and structure A.1. For each of those systems, the redundant components are indicated by a block instead of a simple rectangle. Those blocks are then analyzed in more details in subsequent figures.

A.1 Global system

The structure is considered only for the primary circuit in the present case study. However, we could also choose to consider the secondary and tertiary circuits structure in our analyses. This would be, for example, the control room roof caving in or a plane falling on the steam generator building, etc.

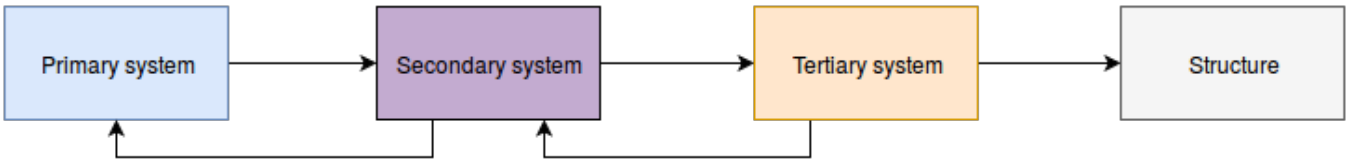

FIGURE A.1. Main RBD architecture

A.2 Primary system

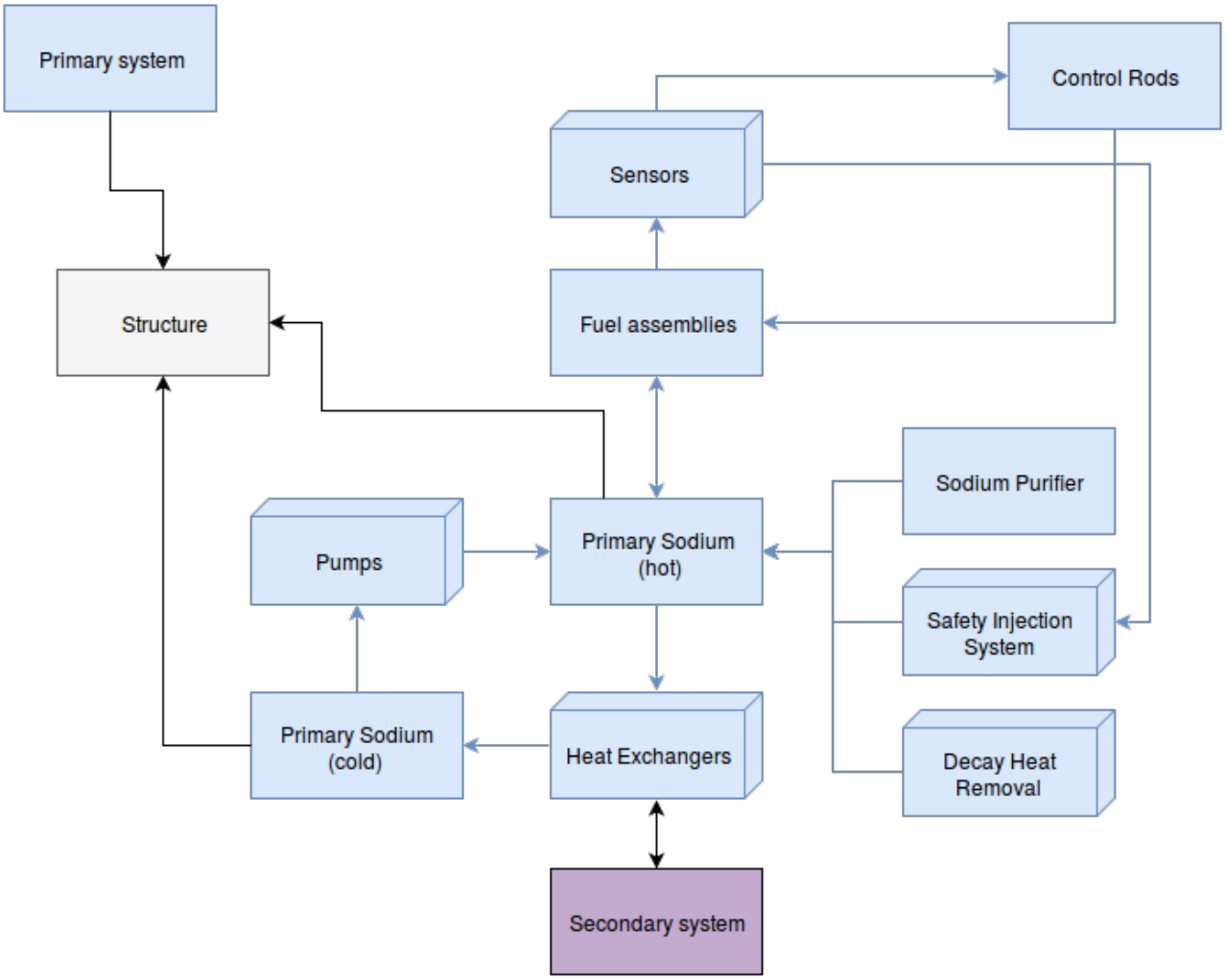

FIGURE A.2. Reliability Block Diagram for the primary system

A.2.1 Primary system redundancies

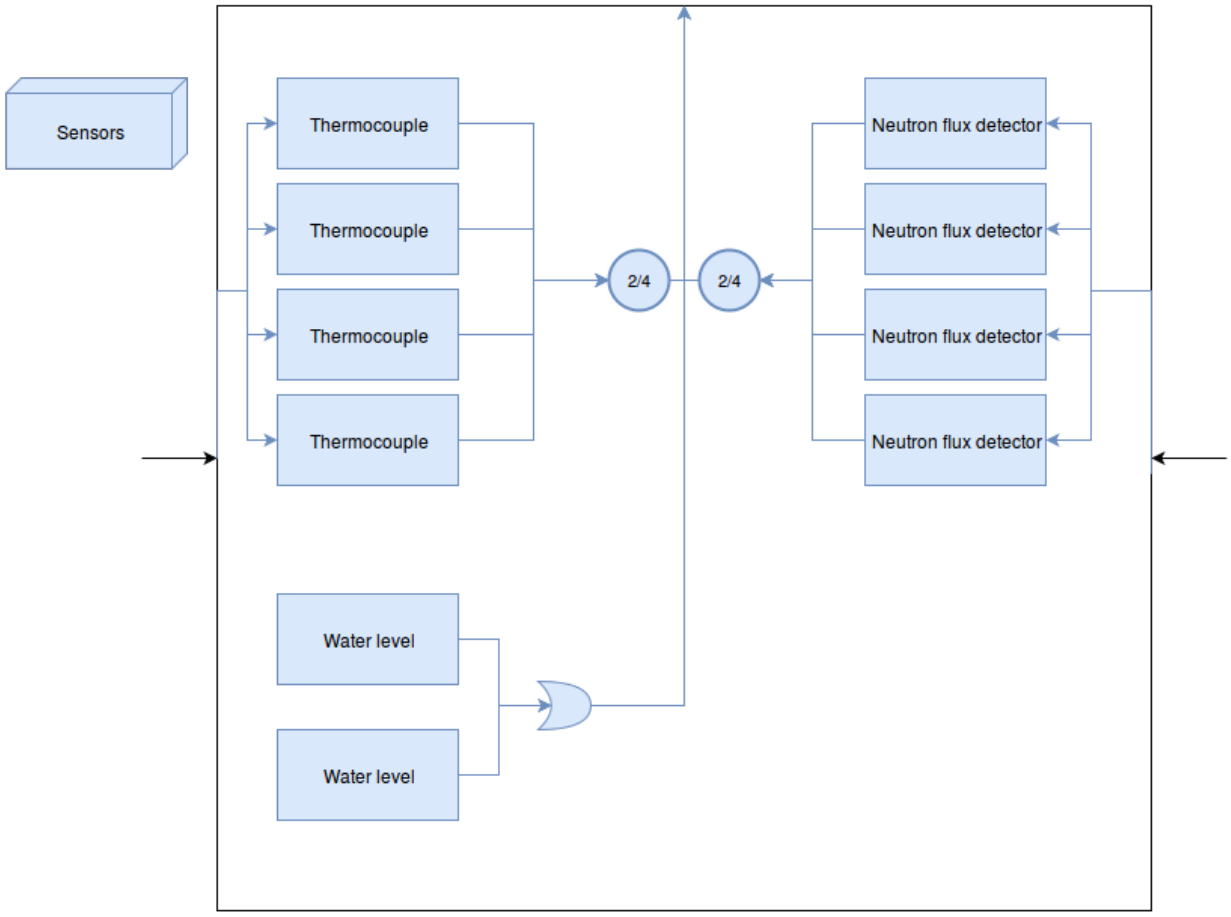

FIGURE A.3. Reliability Block Diagram for the core sensors in the primary system

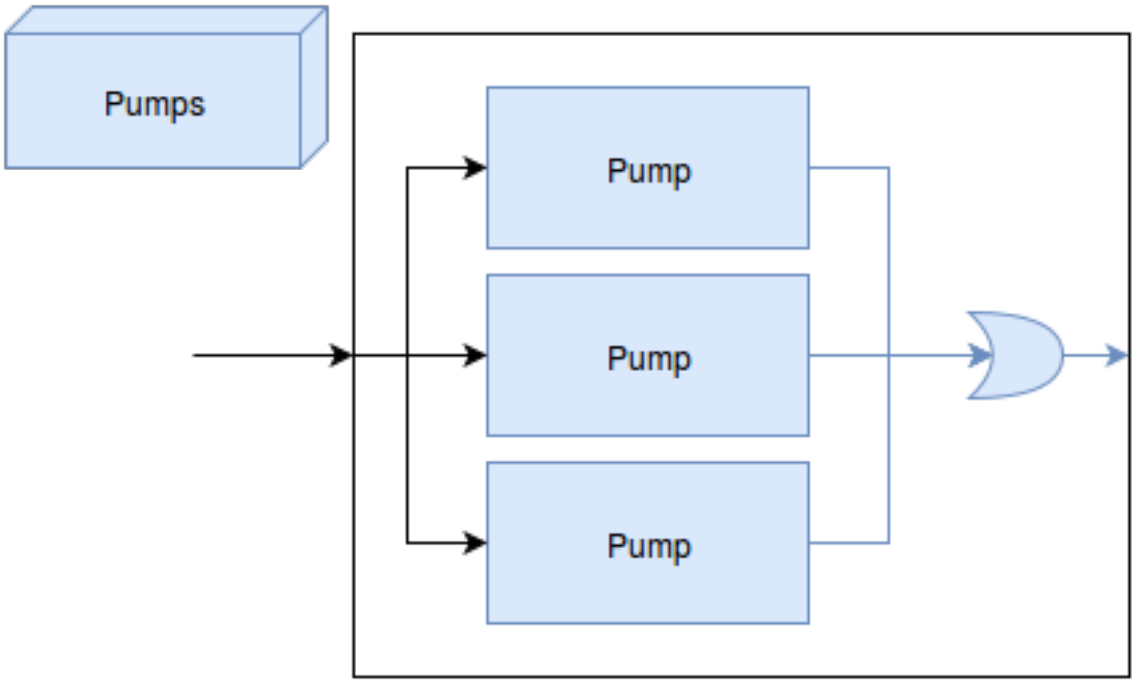

FIGURE A.4. Reliability Block Diagram for the primary pumps in the primary system

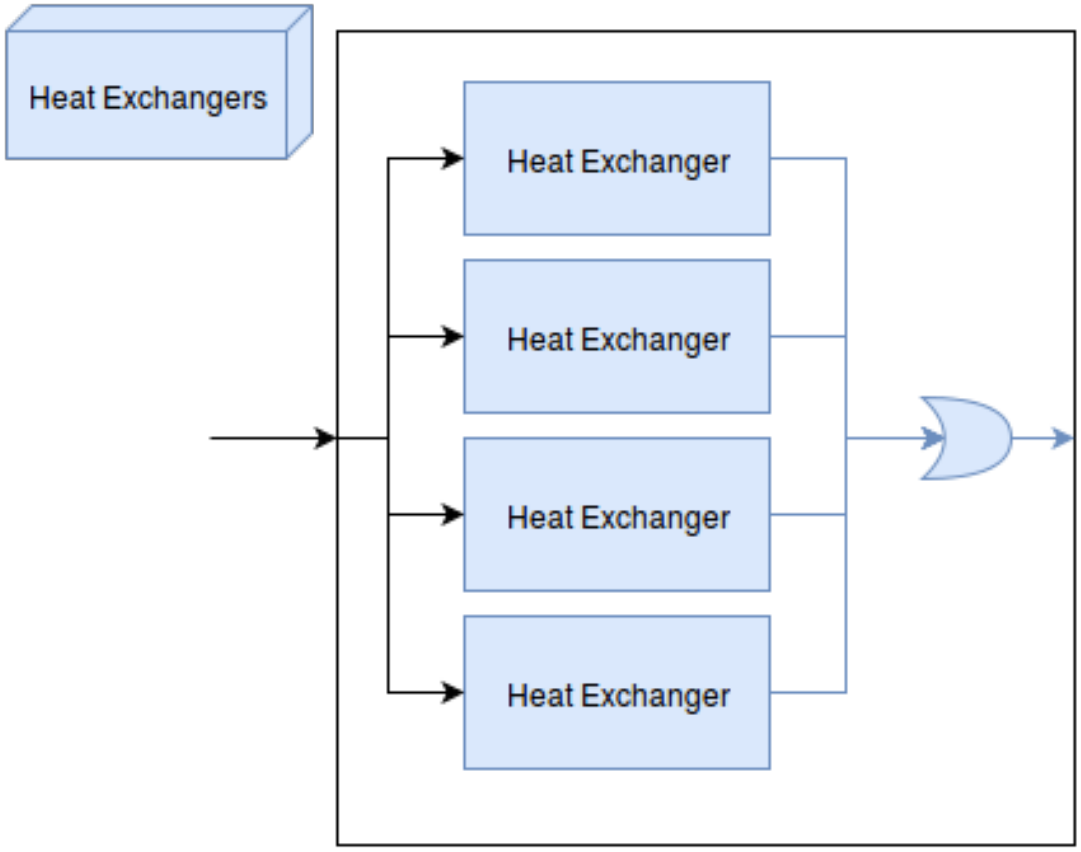

FIGURE A.5. Reliability Block Diagram for the heat exchangers in the primary system

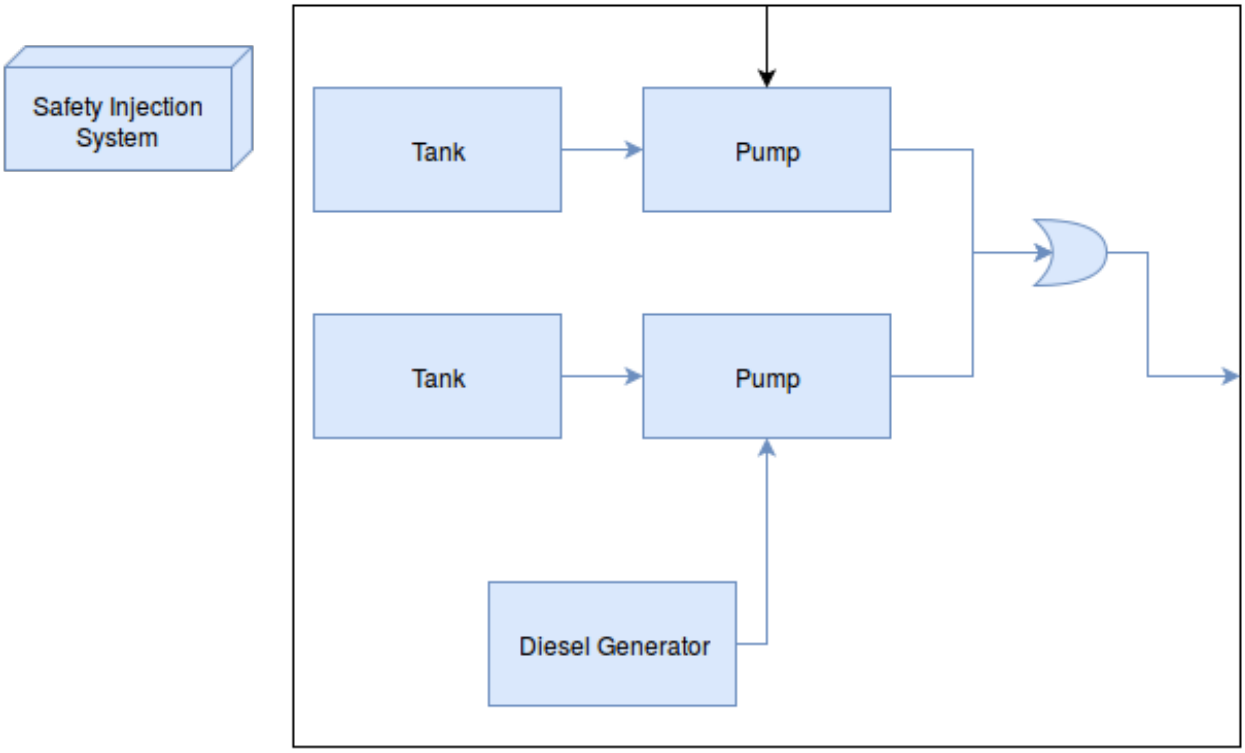

FIGURE A.6. Reliability Block Diagram for the safety injection system in the primary system

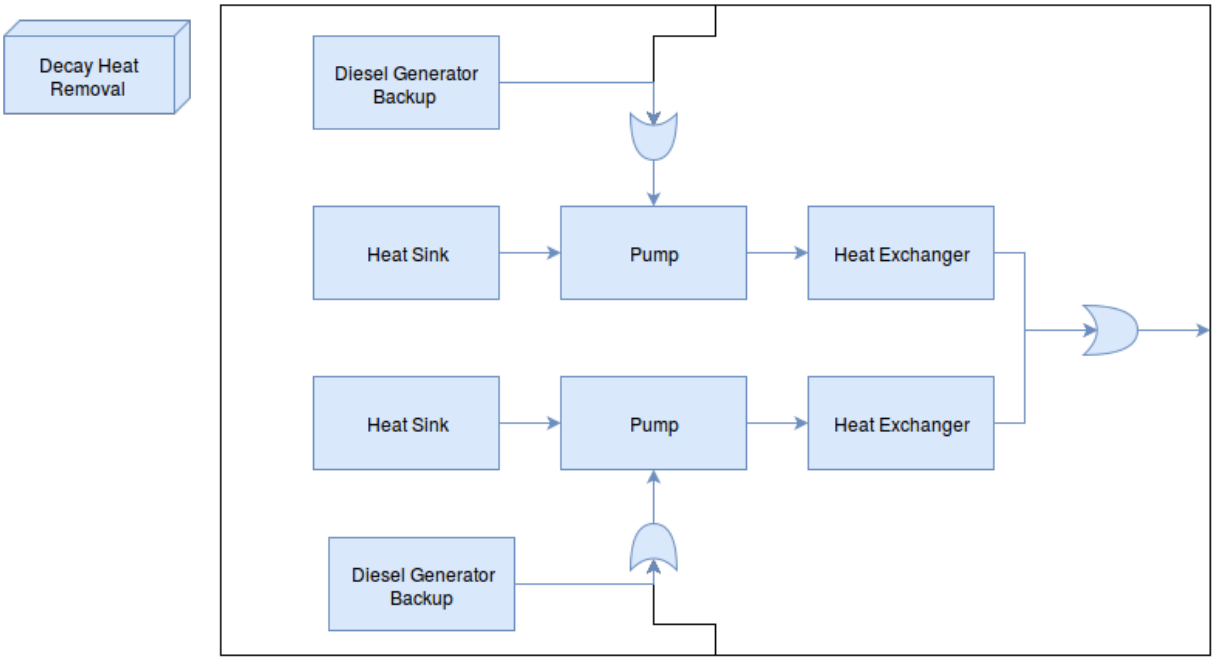

FIGURE A.7. Reliability Block Diagram for the decay heat removal in the primary system

A.3 Secondary system

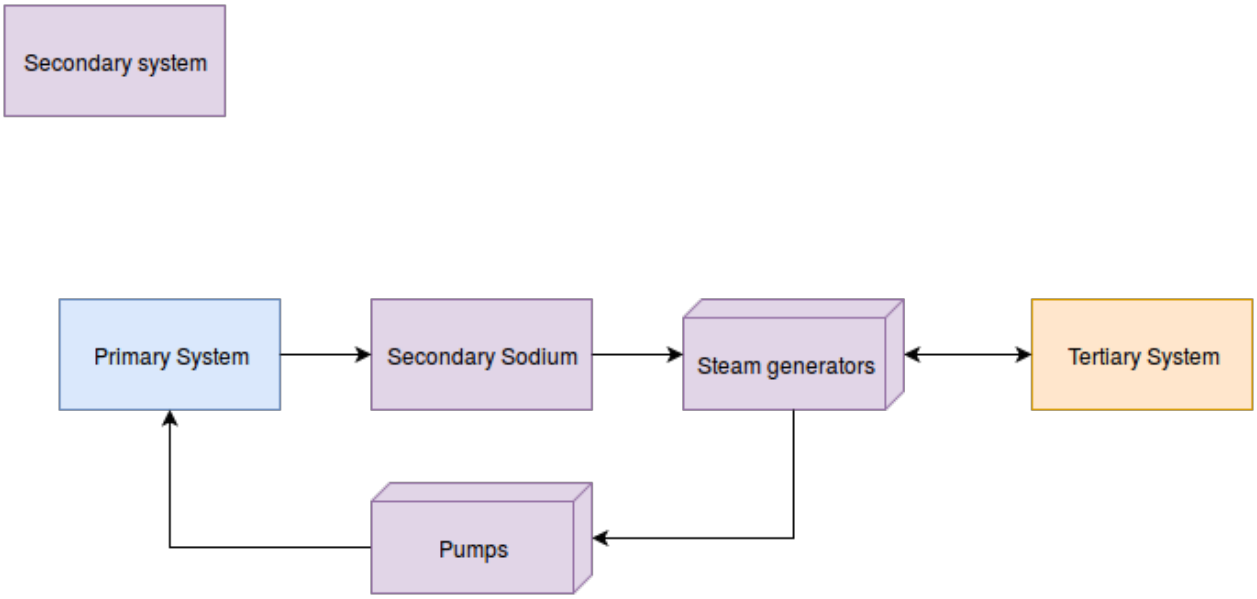

FIGURE A.8. Reliability Block Diagram for the secondary system

A.3.1 Secondary system redundancies

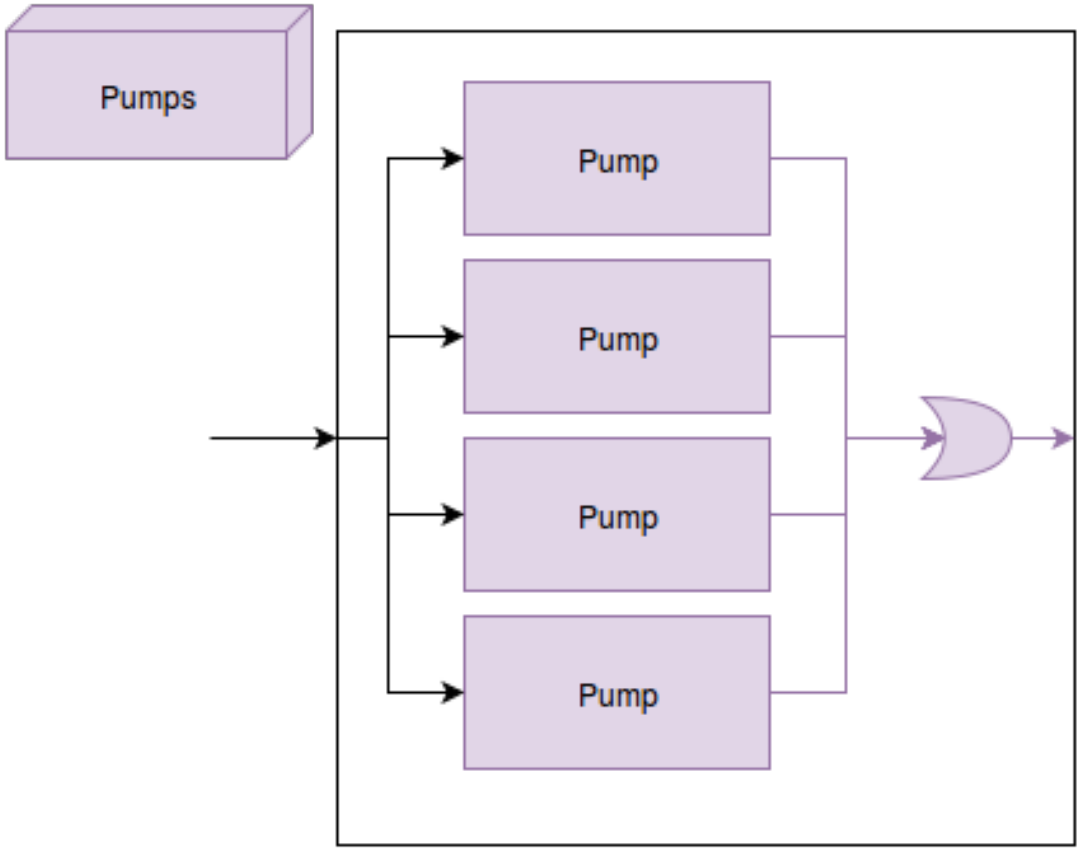

FIGURE A.9. Reliability Block Diagram for the secondary pumps in the secondary system

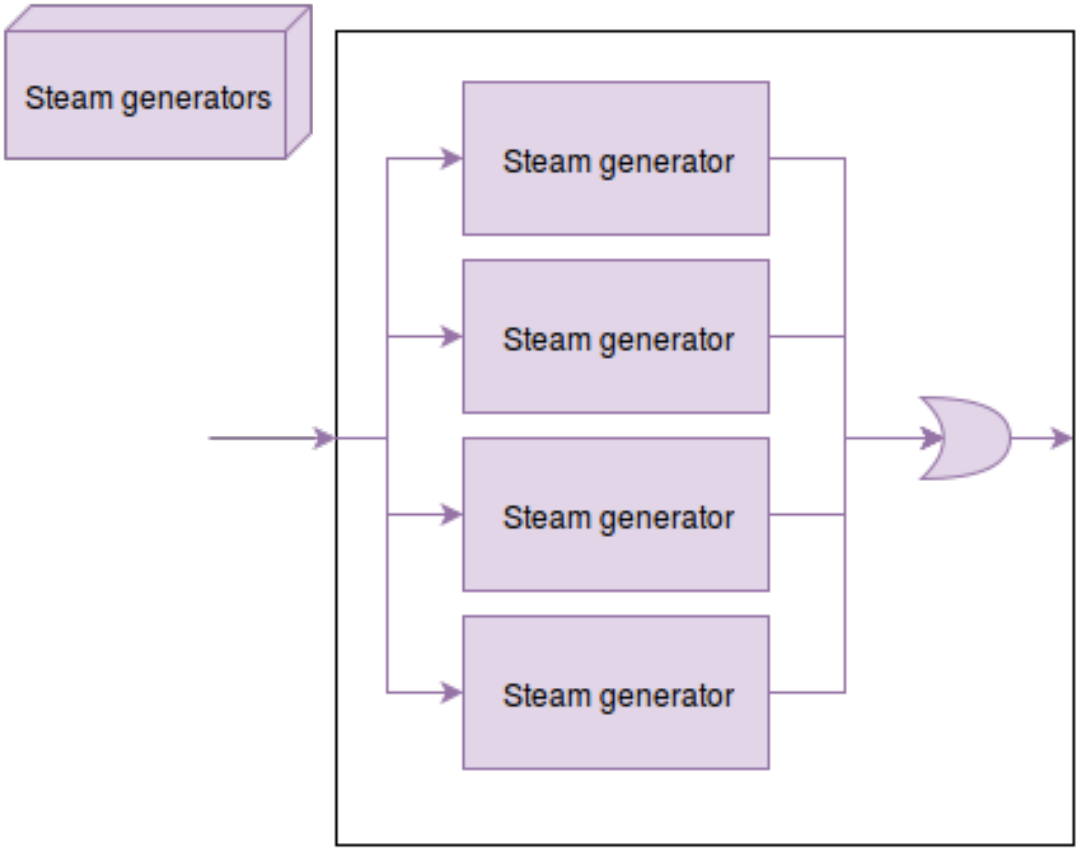

FIGURE A.10. Reliability Block Diagram for the steam generators in the secondary system

A.4 Tertiary system

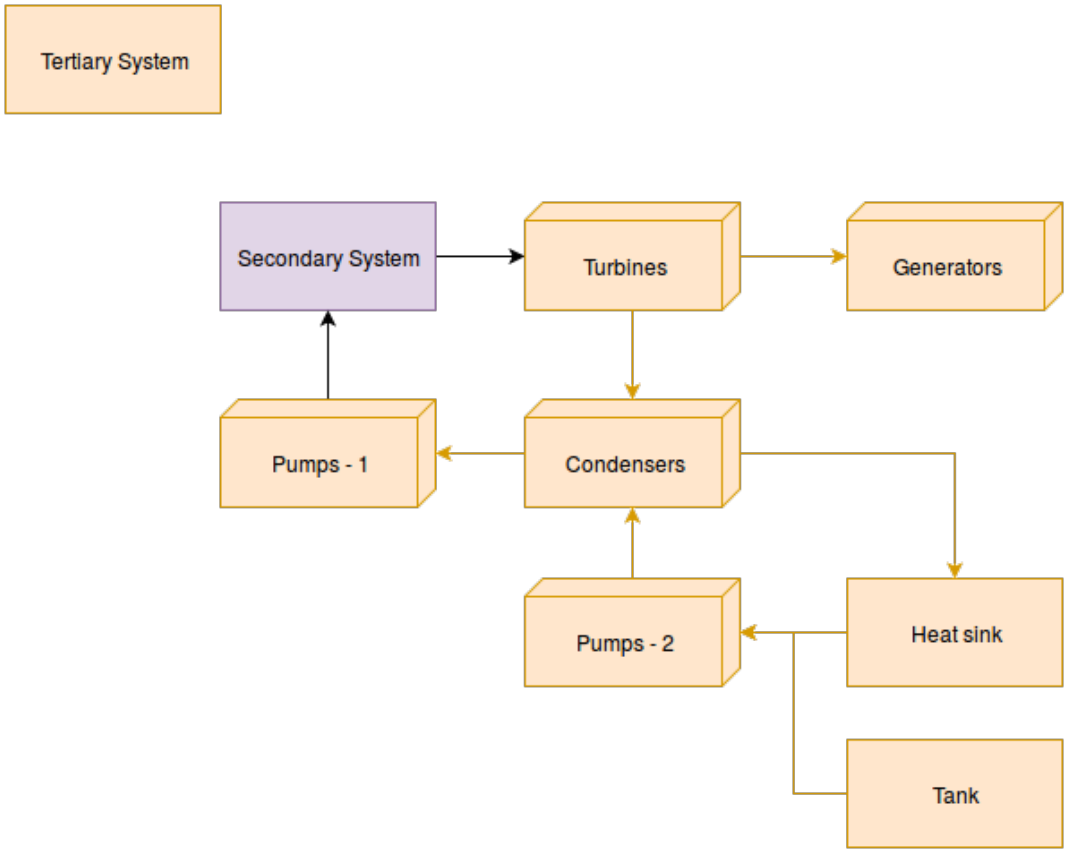

FIGURE A.11. Reliability Block Diagram for the tertiary system

A.4.1 Tertiary system redundancies

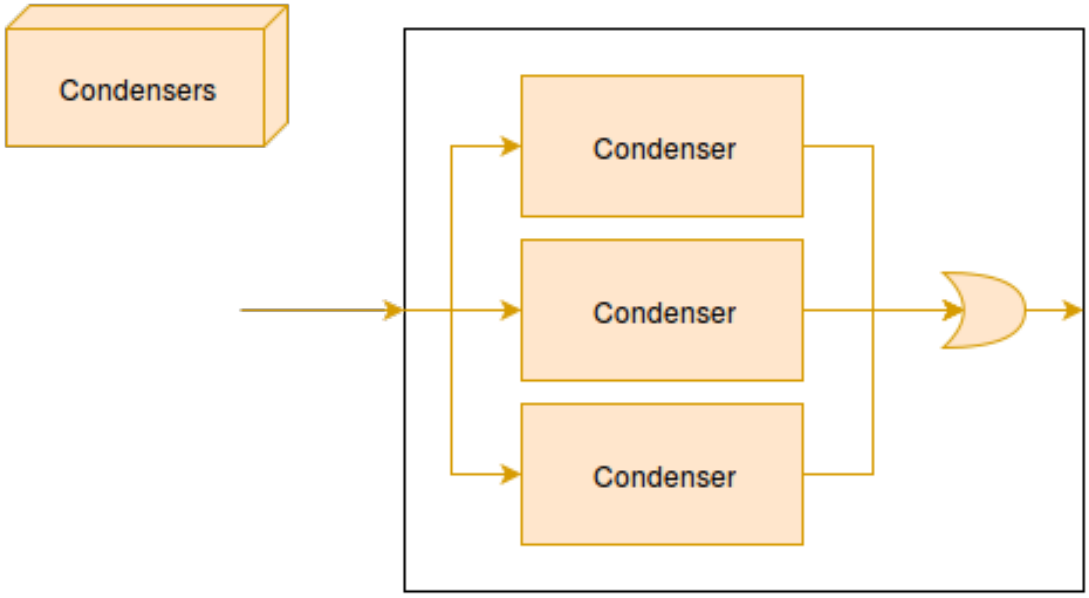

FIGURE A.12. Reliability Block Diagram for the condensers in the tertiary system

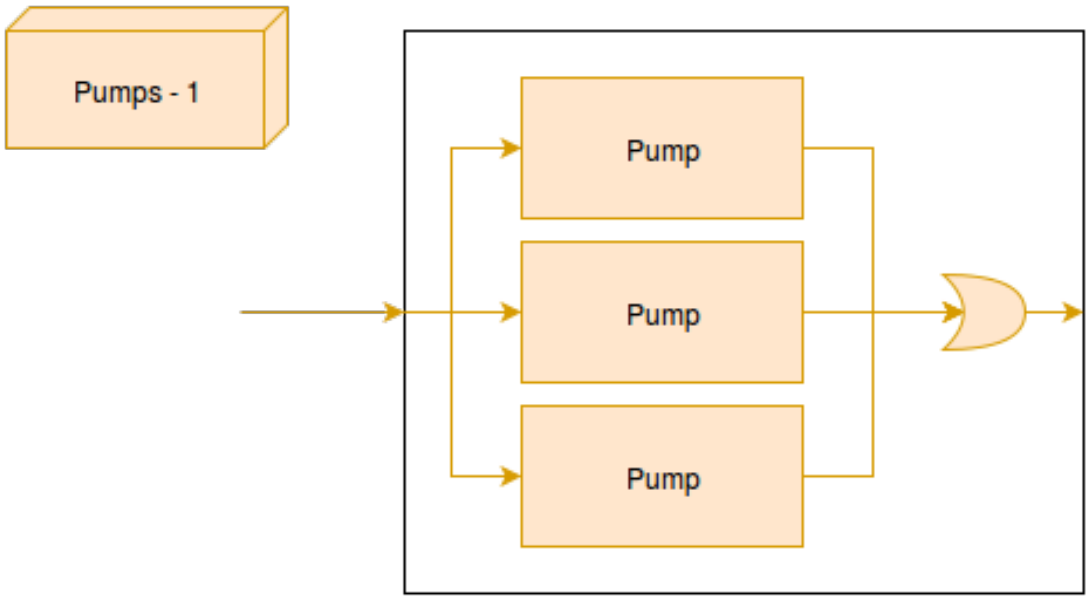

FIGURE A.13. Reliability Block Diagram for the tertiary-secondary pumps in the tertiary system

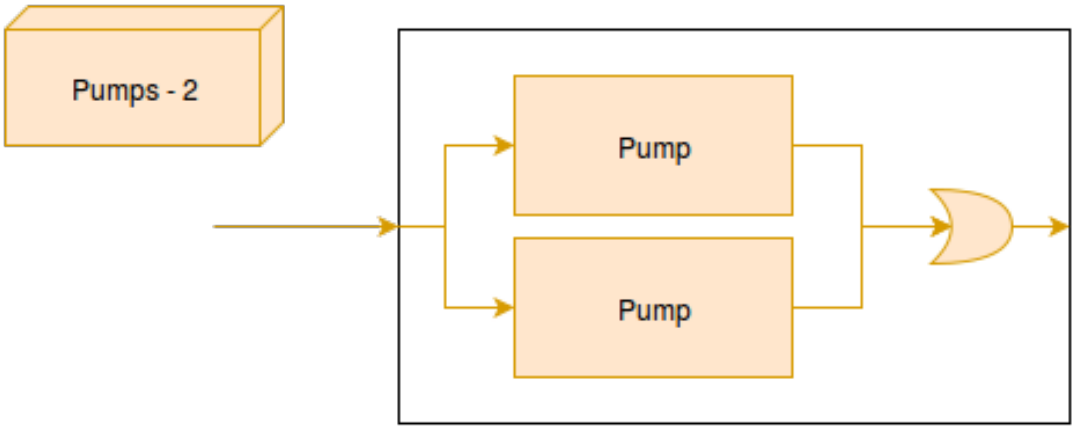

FIGURE A.14. Reliability Block Diagram for the boundary-tertiary pumps in the tertiary system

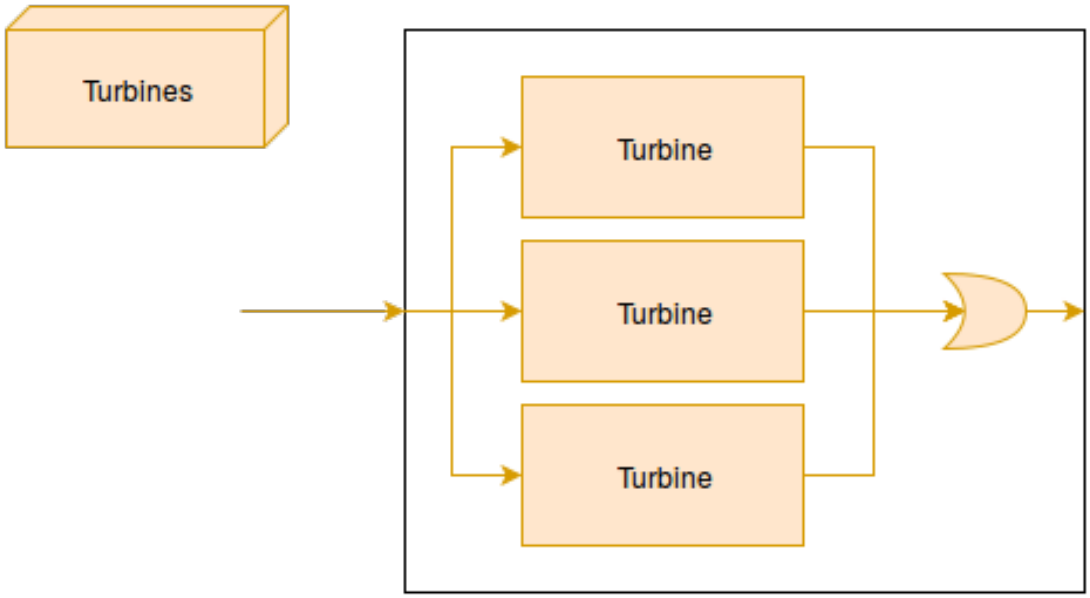

FIGURE A.15. Reliability Block Diagram for the turbines in the tertiary system

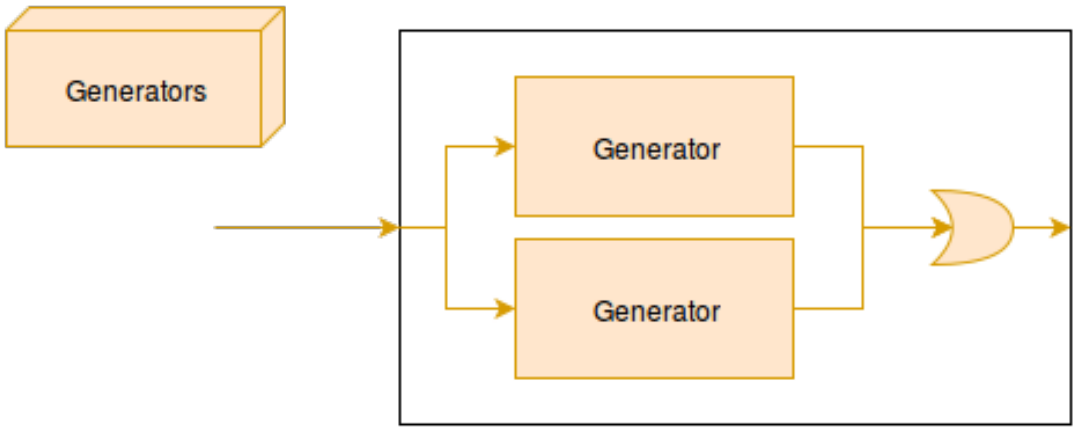

FIGURE A.16. Reliability Block Diagram for the generators in the tertiary system

APPENDIX B

FAILURE MODES AND EFFECTS ANALYSIS

FMEA asks for the creation of a table which associate a (Probability, Severity, Detectability)-triplet and a corresponding RPN to a (failure mode, cause)-doublet of a component. Potential mitigation action can also be added, as well as its cost and other useful information during the design process. Table B.1 presents the(P, S, D)-triplets associated with a number of potential failures and causes. It is to be noted that, by essence of the real-world FMEA in a complex system, the list presented is not exhaustive. It shows the failure modes that the author thought were most likely to have a higher RPN.

Table B.2 presents, for each and every identified failure modes, possible mitigation action that could be taken.

ID	Component	Failure	Cause	P	S	D
1.1		Pin cladding (< 5%)	Local peak power	8	2	2
1.2		Pin cladding (> 10%)	Global peak power	5	9	2
1.3	Fuel Assemblies	Assemblies distorsion	Wear	5	4	4
1.4		Assemblies handling	Bad identification	3	8	4
1.5		Assemblies handling	Head damage	5	2	10
2.1		Partial loss of capability for one pump	Wear	4	5	4
2.2	Primary pumps	Complete loss of capability for one pump	Bad maintenance	3	6	3

. . . continued

ID	Component	Failure	Cause	P	S	D
2.3		Partial loss of capability for all pumps	Wear and bad maintenance	2	9	2
2.4		Complete loss of capability for all pumps	Repeated bad maintenance	1	9	3
2.5		Complete loss of capability for all pumps	External aggression	2	9	10
3.1	Control rods	One rod does not fall	Gripped mechanical release	3	6	4
3.2		One rod fall too slowly	Distorsion	6	4	2
3.3		One rod gets stuck in	Distorsion	4	2	3
3.4		One rod gets stuck in	Seism	2	5	8
3.5		More than one rod don't fall	Gripped mechanical release	2	10	1
3.6		More than one rods fall too slowly	Distorsion	5	6	2
3.7		More than one rods get stuck in	Distorsion	3	7	3
4.1	Decay heat exchangers	Large leak in one of the two	Faulty material	2	7	7
4.2		Small leak in one of the two	Wear	3	6	6
4.3		Large leak in the two	Faulty material and inspection	1	9	7
4.4		Small leak in the two	Wear and insufficient inspection	2	8	6
5.1	Heat removal system pumps	Partial loss of capability for one pump	Wear	4	5	4

. . . continued

ID	Component	Failure	Cause	P	S	D
5.2		Complete loss of capability for one pump	Bad maintenance	3	7	3
5.3		Partial loss of capability for all pumps	Wear and bad maintenance	2	7	2
5.4		Complete loss of capability for all pumps	Repeated bad maintenance	1	9	3
5.5		Complete loss of capability for all pumps	External aggression	2	9	10
6.1	Sodium purifier	Partial loss of capability	Wear	4	4	3
6.2		Partial loss of capability	Aggression	2	4	10
6.3		Complete loss of capability	Wear	3	8	2
6.4		Complete loss of capability	Aggression	1	8	10
7.1	Argon tank	Small leak	Wear	3	3	3
7.2		Large leak	Aggression	2	7	10
8.1	Detectors	No signal from one	Electronic components	6	1	9
8.2		No signal from any	Electronic components	2	8	8
8.3		Wrong signal from one	Electronic components	7	1	3
8.4		Wrong signal from all	Electronic components	5	8	10
9.1	Thermocouples	No signal from one	Electronic components	4	1	9
9.2		No signal from any	Electronic components	1	8	8
9.3		Wrong signal from one	Electronic components	5	1	3
9.4		Wrong signal from all	Electronic components	3	7	10
10.1	Inner vessel	Small breach	Wear	3	7	3

. . . continued

ID	Component	Failure	Cause	P	S	D
10.2		Large breach	Wear	1	8	1
11.1	Main vessel	Small breach	Wear	3	8	1
11.2		Small breach	Aggression	3	10	10
11.3		Large breach	Wear	2	9	1
11.4		Large breach	Aggression	2	10	10
12.1	Safety vessel	Small breach	Wear	2	8	1
12.2		Small breach	Aggression	3	8	10
12.3		Large breach	Wear	2	9	1
12.4		Large breach	Aggression	3	9	10
13.1	Core catcher	Small breach	Wear	2	2	3
13.2		Large breach	Wear	1	4	1
14.1	Heat exchangers	Small breach in one of them	Wear	3	4	6
14.2		Large breach in one of them	Wear	3	7	5
14.3		Small breach in all of them	Wear	2	8	4
14.4		Large breach in all of them	Wear	1	9	3
15.1	Steam generators	Small breach in one of them	Wear	3	4	5
15.2		Large breach in one of them	Wear	3	7	4
15.3		Small breach in all of them	Wear	2	8	3

. . . continued

ID	Component	Failure	Cause	P	S	D
15.4		Large breach in all of them	Wear	1	9	2
16.1	Secondary pumps	Partial loss of capability for one pump	Wear	4	4	4
16.2		Complete loss of capability for one pump	Air in the pump	3	5	3
16.3		Partial loss of capability for all pumps	Wear and bad maintenance	2	7	2
16.4		Complete loss of capability for all pumps	Repeated bad maintenance	2	7	3
16.5		Complete loss of capability for all pumps	External aggression	2	7	10
17.1	Turbine	Failure of one	Wear	6	5	7
17.2		Failure of all	Wear	2	7	6
18.1	Condenser	Failure of one	Wear	4	7	6
18.2		Failure of all	Wear	1	8	5
19.1	Tertiary pumps	Partial loss of capability for one pump	Wear	4	4	4
19.2		Complete loss of capability for one pump	Air in the pump	3	5	3
19.3		Partial loss of capability for all pumps	Wear and bad maintenance	2	7	2
19.4		Complete loss of capability for all pumps	Repeated bad maintenance	2	7	3
19.5		Complete loss of capability for all pumps	External aggression	2	7	10

Table B.1: FMEA

ID	RPN	Mitigation
1.1	32	Better material, stay in the normal operation range
1.2	90	Better material, stay in the normal operation range
1.3	80	Better detectability and positioning in the core
1.4	96	Better cameras and labels
1.5	100	Solid assembly heads, maintenance training
2.1	80	Better PHM
2.2	54	Better maintenance and inspection
2.3	36	Better PHM, maintenance and inspection
2.4	27	Better PHM to limit maintenance
2.5	180	Protect the pumps physically
3.1	72	Extend PHM to detect the failure, go toward a electromagnetic attachment
3.2	48	Check the assemblies when unloading to know their distorsion and mitigate the effects
3.3	24	Check the assemblies when unloading to know their distorsion and mitigate the effects
3.4	80	Take seisms into account when reloading distorded assemblies
3.5	20	Extend PHM to detect the failure, go toward a electromagnetic attachment, improve startup checks
3.6	60	Check the assemblies when unloading to know their distorsion and mitigate the effects
3.7	63	Check the assemblies when unloading to know their distorsion and mitigate the effects
4.1	98	Good testing of the material, regular inspection
4.2	108	Regular inspection
4.3	63	Good testing of the material, regular inspection

. . . continued

ID	RPN	Mitigation
4.4	96	Regular inspection
5.1	80	Regular inspection
5.2	63	Regular inspection, maintenance training
5.3	28	Regular inspection, maintenance training, PHM
5.4	27	Regular inspection, maintenance training, better PHM to limit the maintenance
5.5	180	Protect the pumps physically
6.1	48	Inspection, PHM
6.2	80	Protect from physical threats
6.3	48	Inspection, PHM
6.4	80	Protect from physical threats
7.1	27	Inspection and PHM
7.2	140	Protect the tank physically
8.1	54	Check the detectors
8.2	128	Check the detectors
8.3	21	Calibrate the detectors
8.4	400	Calibrate the detectors frequently, use different kind, use other ways to determine reactor power output
9.1	36	Check the sensors
9.2	64	Check the sensors
9.3	15	Calibrate the sensors
9.4	210	Calibrate the sensors frequently, use different kind, use other ways to determine reactor power output
10.1	63	Good material testing, inspection and fluence reduction

. . . continued

ID	RPN	Mitigation
10.2	8	Good material testing and inspection and fluence reduction
11.1	24	Good material testing and inspection and fluence reduction
11.2	300	Good material and large width, external defense
11.3	18	Good material testing and inspection and fluence reduction
11.4	200	Good material and large width, external defense
12.1	16	Good material testing and inspection and fluence reduction
12.2	240	Good material and large width, external defense
12.3	18	Good material testing and inspection and fluence reduction
12.4	270	Good material and large width, external defense
13.1	12	Good material testing and inspection
13.2	4	Good material and inspection
14.1	72	Inspection
14.2	105	Inspection
14.3	64	Inspection
14.4	27	Inspection
15.1	60	Inspection
15.2	84	Inspection
15.3	48	Inspection
15.4	18	Inspection
16.1	64	Inspection
16.2	45	PHM, stop the pump when it detects vapor
16.3	28	Inspection
16.4	42	Inspection

. . . continued

ID	RPN	Mitigation
16.5	140	Protect the pumps physically from falling objects or other
17.1	210	Redundancies, stay within operational range
17.2	84	Redundancies, stay within operational range, diversify technologies
18.1	168	Inspection
18.2	40	Inspection
19.1	64	Inspection
19.2	45	PHM, stop the pump when it detects vapor
19.3	28	Inspection
19.4	42	Inspection
19.5	140	Protect the pumps physically from falling objects or other

Table B.2: FMEA: RPN and mitigation

APPENDIX C

PROBABILISTIC RISK ASSESSMENTS

Probabilistic risk assessments consists of three categories of data, the event trees, the fault trees, and the frequencies associated with each basic and initiating events. This appendix lists in details the data used in the study. It also shows the model implementation for the event trees and selected fault trees.

Table C.1 presents, for each and every identified basic event, their probability, on a per year basis.

Event	ID	Failure probability
No signal sent to the generator to start	NO_START_SIGNAL	1×10^{-3}
No fuel for the generator	GENERATOR_NO_FUEL	1×10^{-3}
No oil for the generator	GENERATOR_NO_OIL	1×10^{-3}
Other failure (bearing, rust, etc)	GENERATOR_OTHER_FAIL	1×10^{-2}
No signal sent to the generator	GENERATOR_NO_SIGNAL	1×10^{-2}
Fuel probes signal transmission	CORE_DET_FUEL_TRANS	1×10^{-6}
Fuel temperature sensor	CORE_DET_FUEL	1×10^{-2}
Neutron detectors signal transmission	CORE_DET_NEUT_TRANS	1×10^{-5}
Neutron flux detector	CORE_DET_NEUT	1×10^{-3}
Thermocouples signal transmission	CORE_DET_THER_TRANS	1×10^{-5}

Event	ID	Failure probability
Thermocouple	CORE_DET_THER	1×10^{-2}
Sensor detection of flow efficiency	SENSOR_DETECTION	1×10^{-3}
Sensor communication	SENSOR_NO_COMM	1×10^{-3}
Check if the power if off	AUTO_POWER_CHACK	1×10^{-7}
Signal communication	COMM_SIGNAL_POWER_OFF	1×10^{-3}
Decay heat removal system heat exchanger	DHR_IHX	1×10^{-4}
DHR system pump	DHR_PUMP	1×10^{-4}
Heat sink availability	HEAT_SINK	1×10^{-3}
Regular DHR power	DHR_POWER	1×10^{-4}
Maintenance access to generator	MAINTENANCE_NOT_POSSIBLE	1×10^{-3}
Repair of generator	GENERATOR_REPAIR	1×10^{-1}
Signal to let rods fall	CORE_RODS_SIGNAL	1×10^{-5}
Signal to let rods fall	CORE_RODS_SIGNAL_MANU	1×10^{-5}
Mechanical release of control rods	CORE_RODS_MECH	1×10^{-4}
Safety Injection System pump	SIS_PUMP	1×10^{-4}
SIS Tank	SIS_TANK	1×10^{-5}
Regular SIS power	SIS_POWER	1×10^{-4}
SIS valve	SIS_VALVE	1×10^{-2}
Breach in the main vessel	PRE_BREACH_CONT_MAIN	1×10^{-5}
Breach in the safety vessel	PRE_BREACH_CONT_SAFE	1×10^{-5}
Operator interpretation to manually detect LOCA	INTERPRET_OPERATOR	5×10^{-2}
Control room communication isolated	OUTSIDE_COMMUNICATION	1×10^{-4}
Operator unavailable	OPERATOR_PROBLEM	1×10^{-4}

Event	ID	Failure probability
Manually add sodium to the core	MANU_COOL	5×10^{-1}
Strenght of the cladding	CORE_CLAD_STREN	1×10^{-2}

Table C.1: PRA: basic events

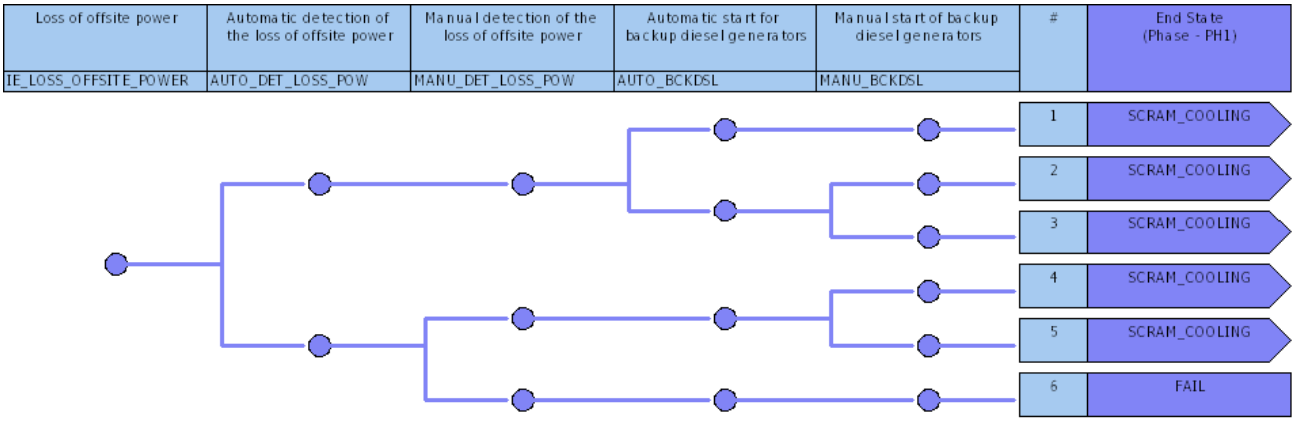

FIGURE C.1. Event tree for the loss of offsite power.

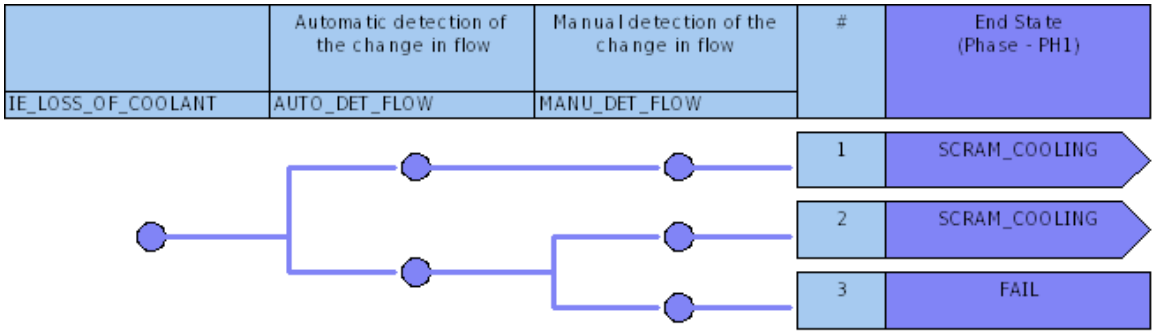

FIGURE C.2. Event tree for the loss of coolant.

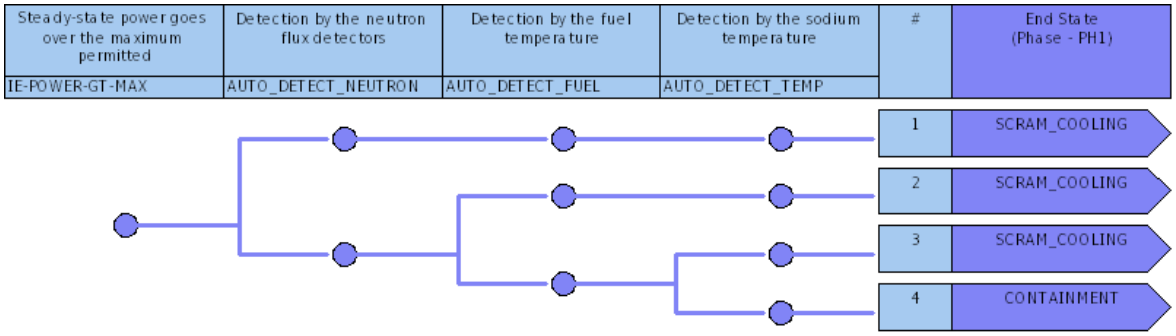

FIGURE C.3. Event tree for power excursion.

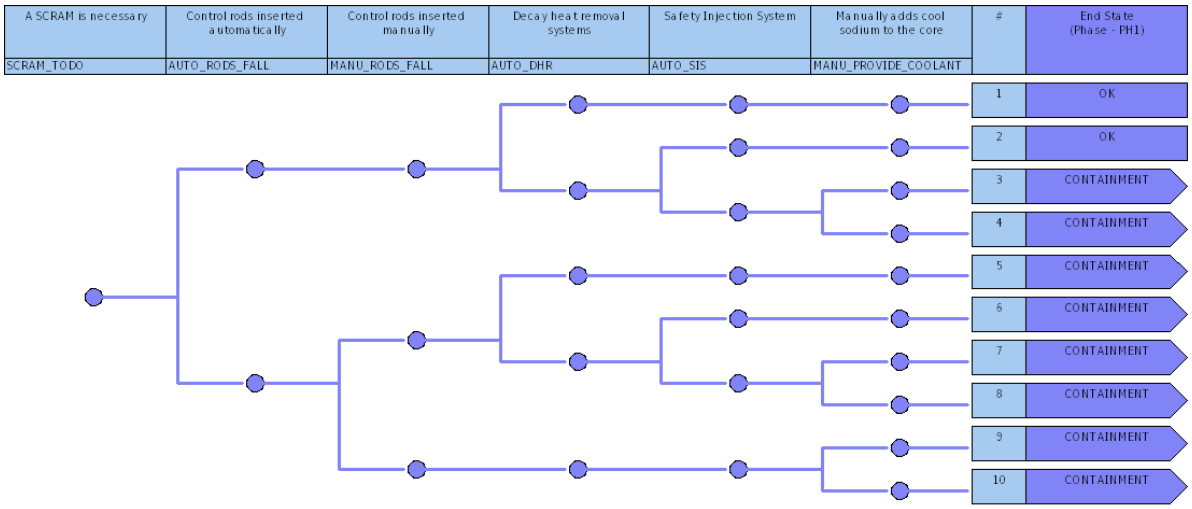

FIGURE C.4. Event tree for the SCRAM and cooling.

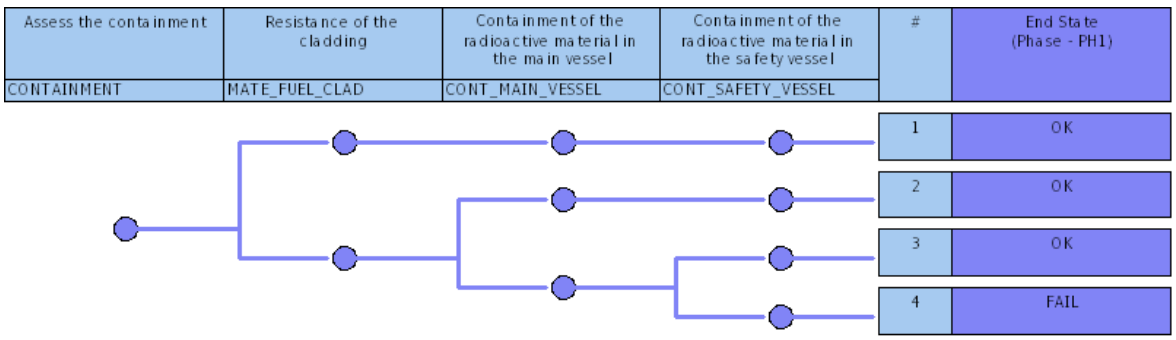

FIGURE C.5. Event tree for the containment.

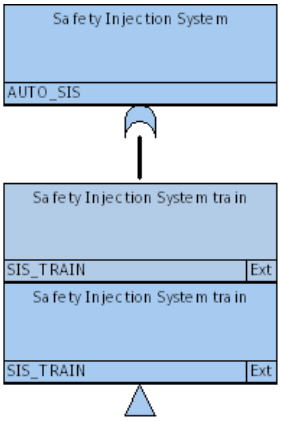

FIGURE C.6. Fault tree for the safety injection system.

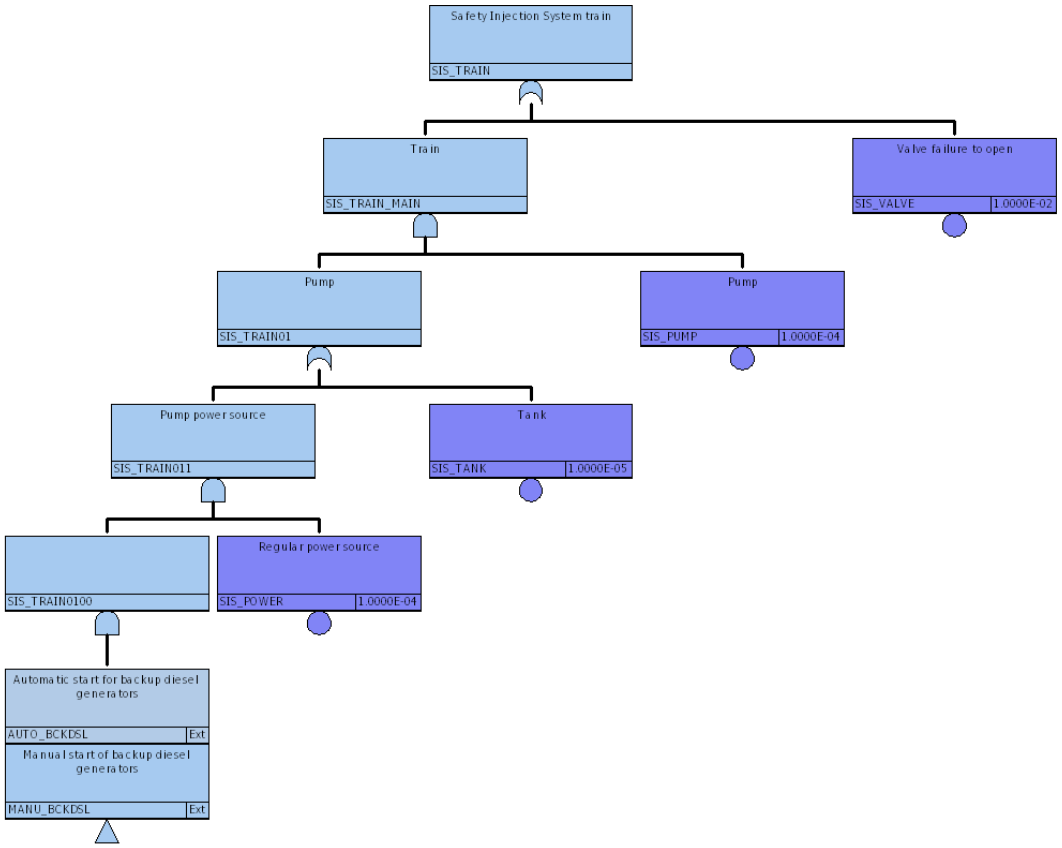

FIGURE C.7. Detailed fault tree for the safety injection system.

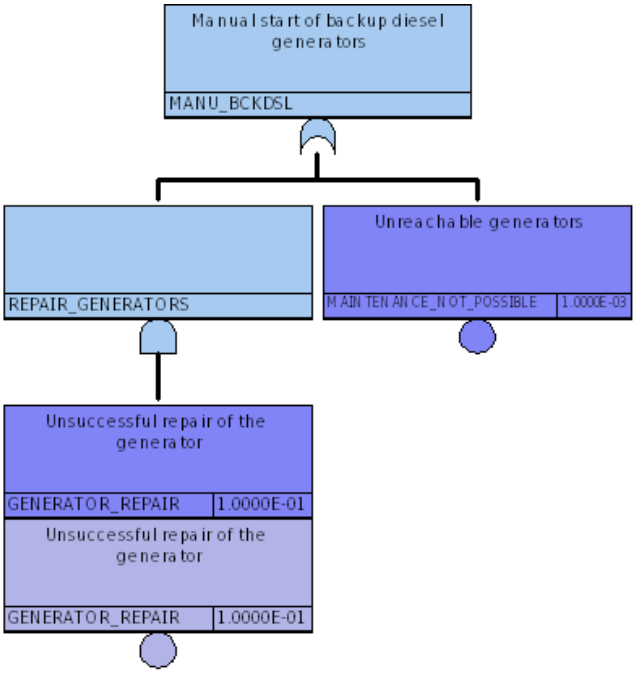

FIGURE C.8. Fault tree for the manual use of the backup generator.

APPENDIX D

FUNCTION FAILURE IDENTIFICATION AND PROPAGATION

Several initiating events are considered, and the propagation of the failures is computed using FFIP methodology. The loss of the function *Signal - Sense - Measure* linked to the *Energy - Radioactive* flow is propagated on figure D.1. This is equivalent to the loss of neutron detectors in a RBD. Next, the loss of the function Channel - Guide - Rotate, which connect the flow *Material - Gas* with *Energy - Mechanical* is propagated on figure D.2. This is equivalent to the loss of the turbines in a RBD. Furthermore, the loss of the function *Convert - Convert* converting vapor flow to liquid flow is propagated on figure D.3. This is equivalent to the loss of the condensers in a RBD.

Two critical functions are defined. These functions are the one that are critical to the system reliability (electricity generation) and the system risks (preventing a core meltdown).

Algorithm 1 FFIP pseudocode - Function 1

1: **procedure** SIGNAL - SENSE - MEASURE
Require: *Energy - Electrical*, *Energy - Radioactive*
Ensure: *Signal*
2: **if** *Energy - Electrical*$_{in} = 0$ **then return** procedure failed
3: **else if** *Energy - Radioactive*$_{in} >$ max(range) **then return** procedure failed
4: **else if** *Energy - Radioactive*$_{in} <$ min(range) **then return** procedure failed
5: **else if** *Signal*$_{out} = 0$ **then return** procedure failed
6: **else return** procedure operative

Algorithm 2 FFIP pseudocode - Function 2

procedure SIGNAL - PROCESS
Require: *Material - Human*, *Energy - Electrical*, *Signal*
Ensure: *Signal - Control*
    if $Material\text{ - }Human_{in} = 0$ and $Energy\text{ - }Electrical_{in} = 0$ **then return** procedure failed
    else if $Material\text{ - }Human_{in} = 0$ and $Signal_{in} = 0$ **then return** procedure failed
    else if $Signal\text{ - }Control_{out} = 0$ **then return** procedure failed
    else return procedure operative

Algorithm 3 FFIP pseudocode - Function 3

procedure CONTROL MAGNITUDE - REGULATE
Require: *Signal - Control*, *Energy - Electrical*
Ensure: *Signal - Control*
    if not $Signal\text{ - }Control_{in}$ **then return** procedure SCRAM
    else if $Signal\text{ - }Control_{in} = 0$ and $Signal\text{ - }Control_{out} != 0$ **then return** procedure failed
    else if $Signal\text{ - }Control_{in} = \pm 1$ and $Signal\text{ - }Control_{out}\ in\ [0, \mp Signal\text{ - }Control_{in}]$ **then return** procedure failed
    else if $Signal\text{ - }Control_{in}$ and $Energy\text{ - }Electrical_{in} = 0$ **then return** procedure failed
    else return procedure operative

Algorithm 4 FFIP pseudocode - Function 4

procedure CONVERT - CONVERT
Require: *Signal - Control*, *Energy - Electrical*
Ensure: *Energy - Mechanical*
    if not $Signal\text{ - }Control_{in}$ **then return** procedure SCRAM
    else if $Signal\text{ - }Control_{in}$ and $Energy\text{ - }Electrical_{in} = 0$ **then return** procedure failed
    else if $Signal\text{ - }Control_{in}$ and $Energy\text{ - }Mechanical_{out} = 0$ **then return** procedure failed
    else return procedure operative

Algorithm 5 FFIP pseudocode - Function 5

procedure CHANNEL - GUIDE - TRANSLATE
Require: *Material - Mixture - Solid-Solid*, *Energy - Mechanical*
Ensure: *Energy - Radioactive*
    if $Energy\text{ - }Radioactive_{out}$ not change **then return** procedure failed
    else return procedure operative

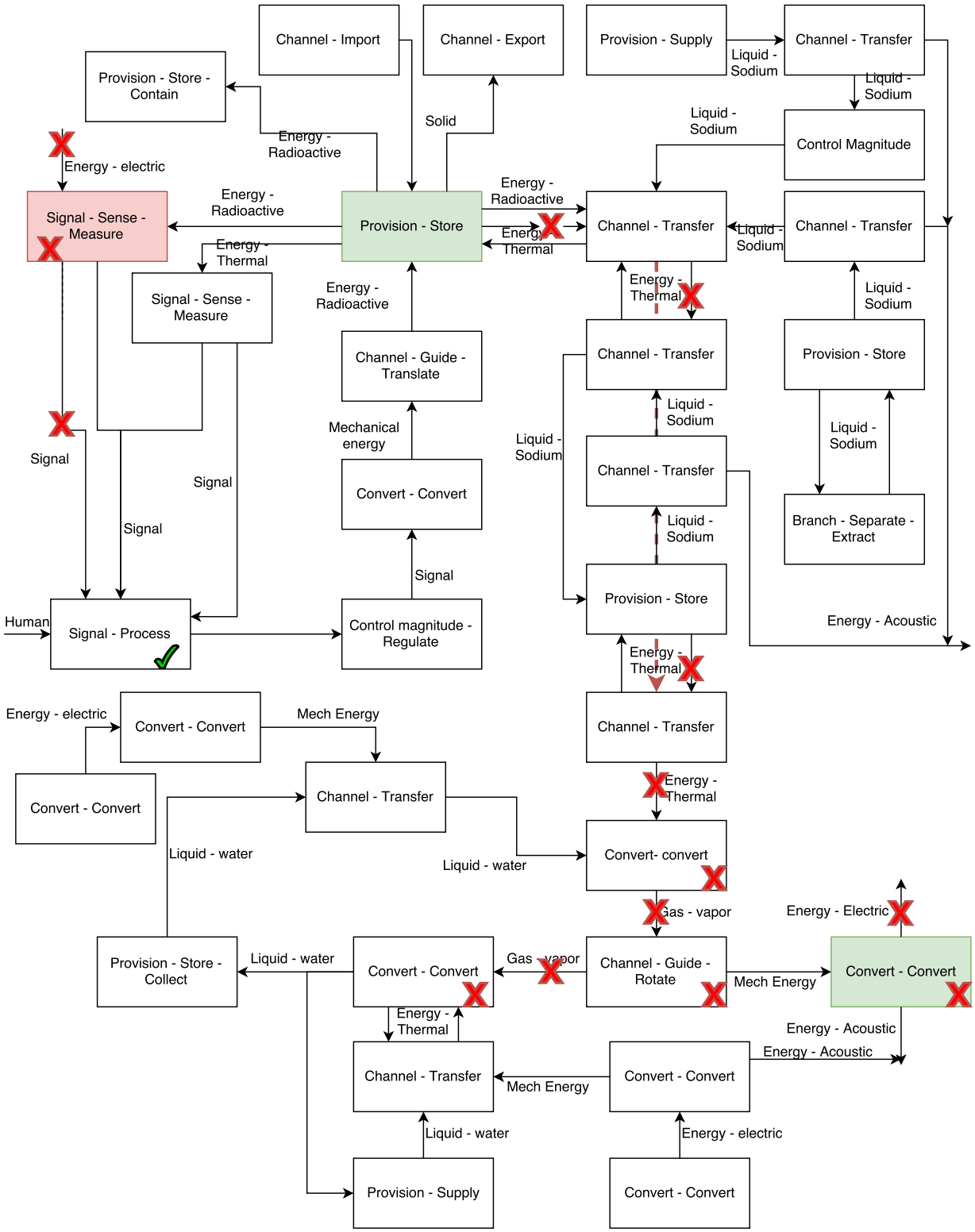

Figure D.1: FFIP - Initiating event: Loss of signal for the neutron detectors.

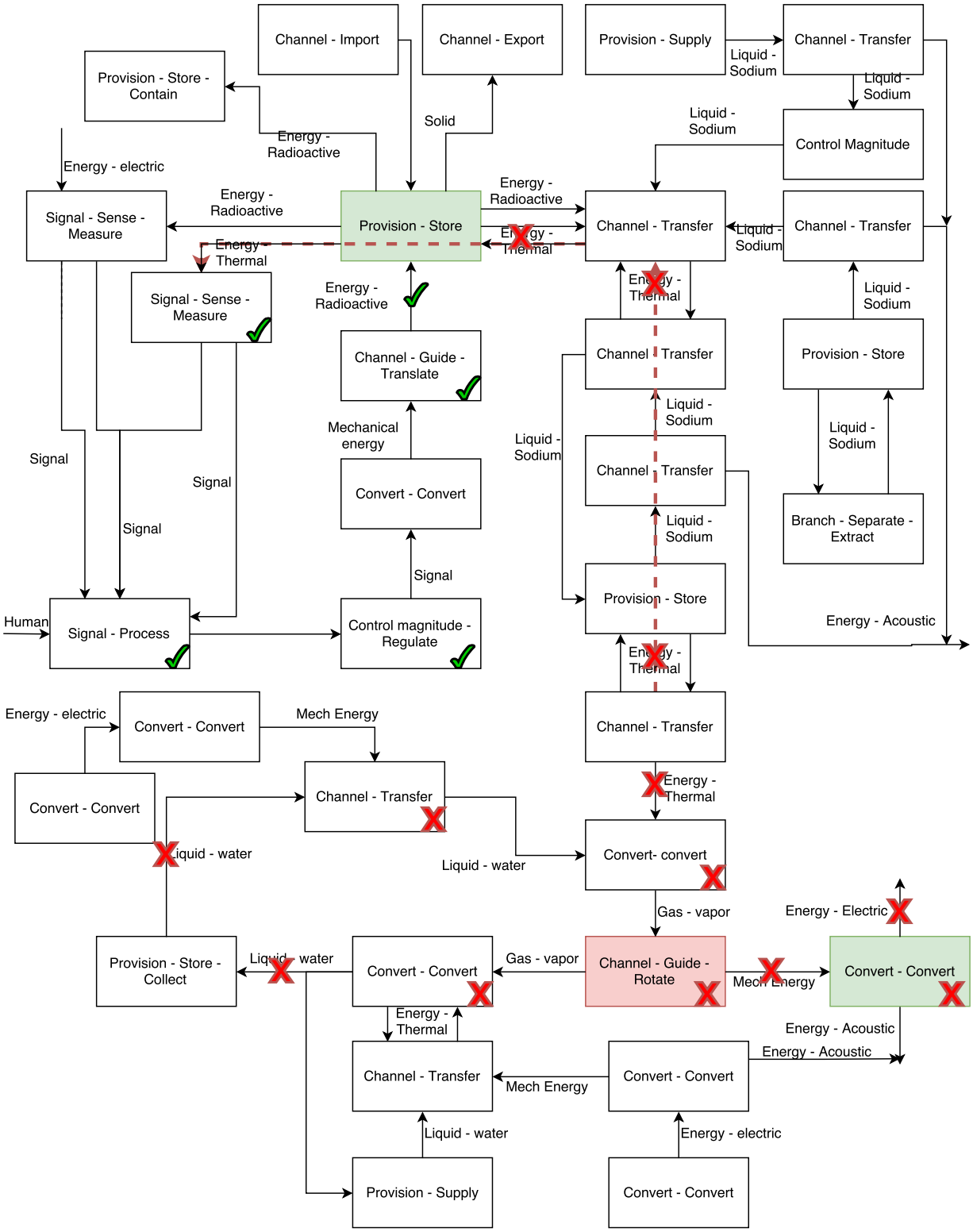

Figure D.2: FFIP - Initiating event: Loss of turbines.

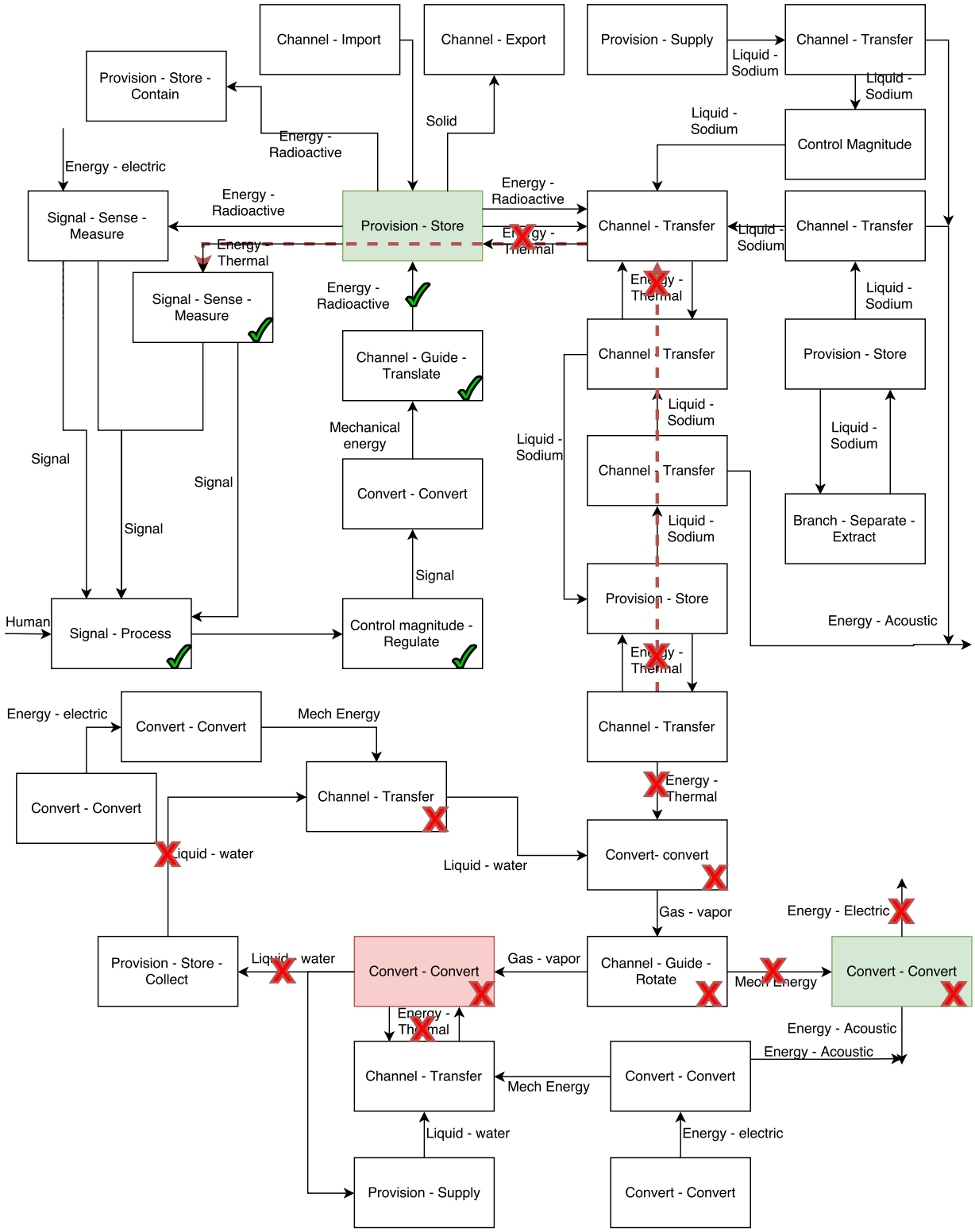

Figure D.3: FFIP - Initiating event: Loss of condensers.

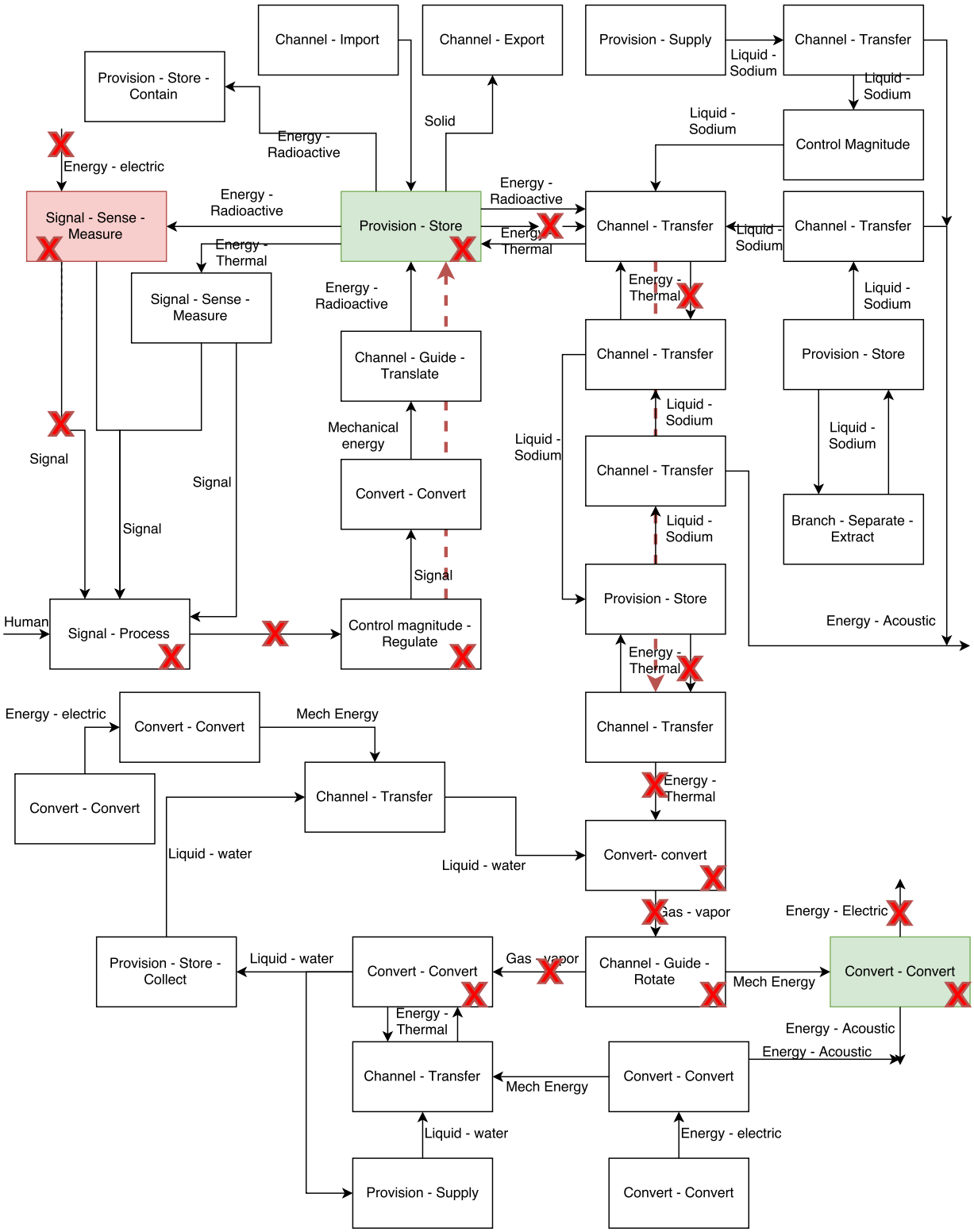

Figure D.4: FFIP - Initiating event: Loss of signal for the neutron detectors - Alternative scenario

APPENDIX E

UNCOUPLED FLOW FAILURE STATE REASONING

Similarly to FFIP analysis, several initiating events are considered. For each function on the cutsets path, a FFIP analysis is carried to understand the impact on the nominal flow paths. Then, a UFFSR analysis is performed to compute potential new cutsets. The loss of the function Channel - Guide - Rotate, which connect the flow *Material - Gas* with *Energy - Mechanical* is propagated on figure D.2, and a UFFSR analysis graphical example is shown on figure E.1. This is equivalent to the loss of the turbines in a RBD, and, in a UFFSR analysis, the explosion of the turbine. Figure E.2 shows the same event, with an arrestor function (green hexagon) considered on the way (a thick concrete wall in this case).

As in FFIP, two critical functions are defined. These functions are the one that are critical to the system reliability (electricity generation) and the system risks (preventing a core meltdown).

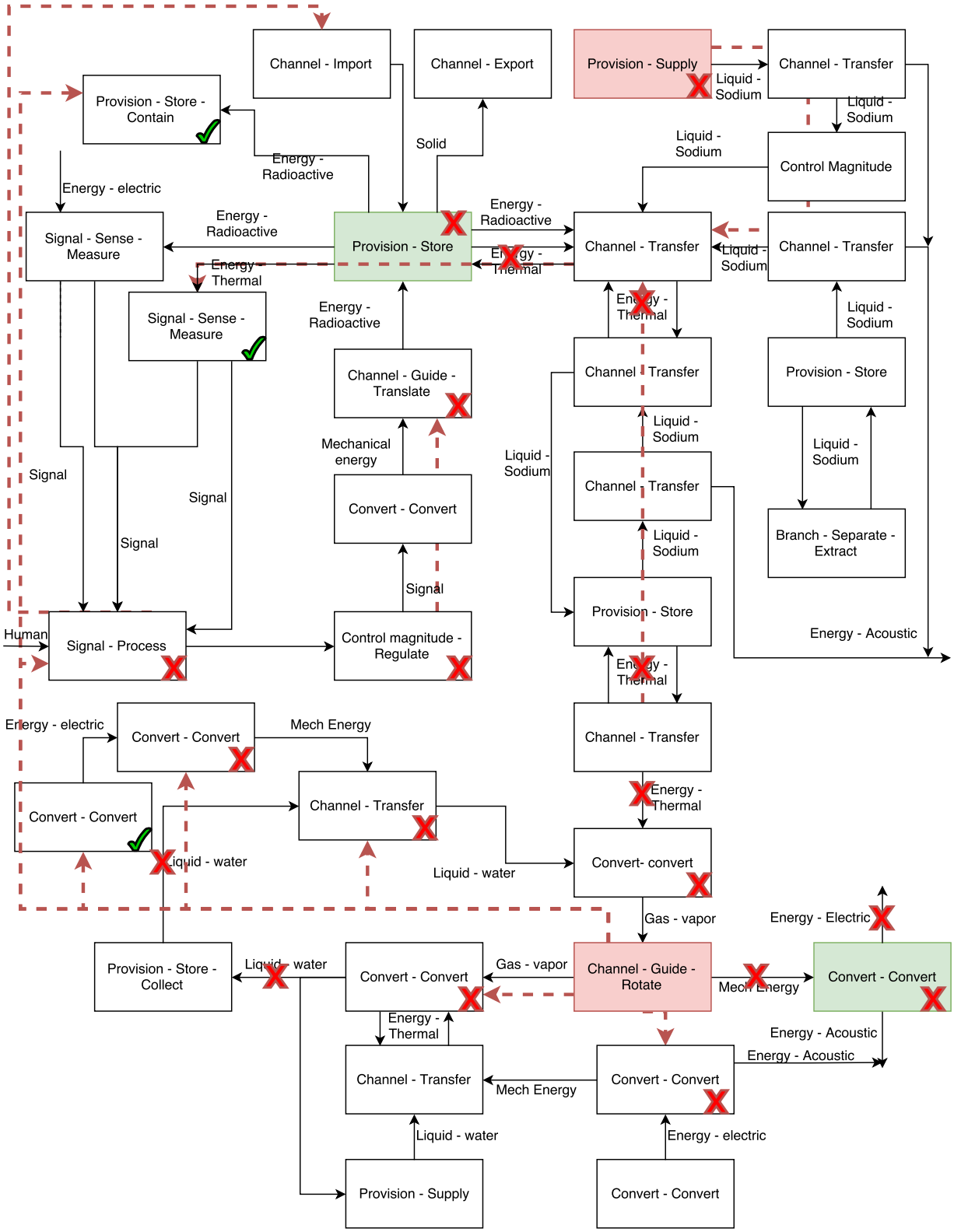

Figure E.1: UFFSR - Initiating event: Turbine explosion - Secondary event: Loss of sodium supply for the SIS

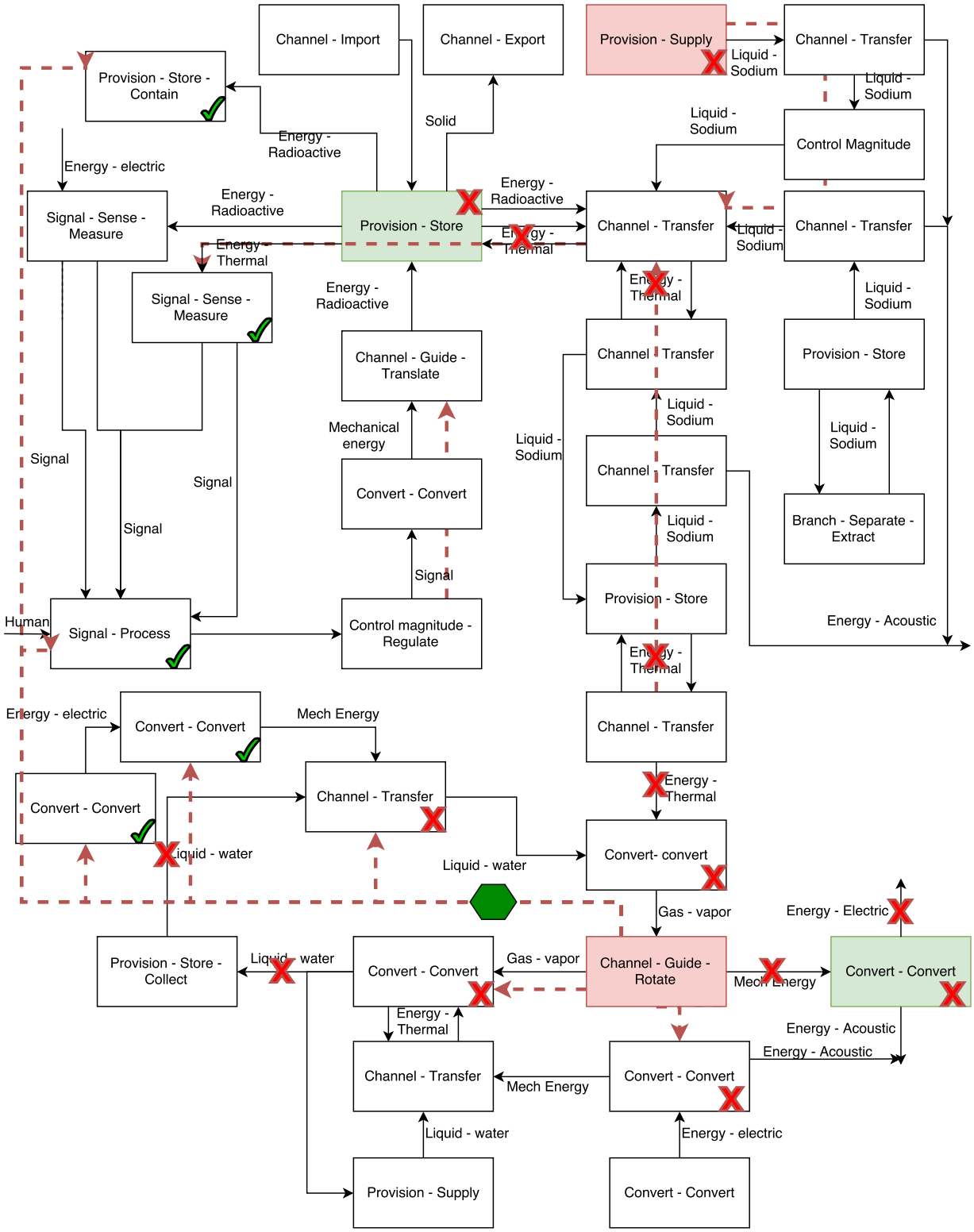

Figure E.2: UFFSR - Arrestor Function - Initiating event: Turbine explosion - Secondary event: Loss of sodium supply for the SIS

BIBLIOGRAPHY

[1] P. ADRIANO DE ALMADA GARCIA, I. CURTY, L. JUNIOR, AND M. A. OLIVEIRA, *A weight restricted dea model for fmea risk prioritization*, Producao, 23 (2013), pp. 500–507.

[2] R. ASHLEY ET AL., *SRE fuel element damage - final report*, Atomics International, (1961).

[3] W. D. BECKNER, *Reactor pressure vessel head degradation and reactor coolant pressure boundary integrity*, NRC Bulletin, (2002).

[4] J. B. BOWLES AND C. E. PELAEZ, *Fuzzy logic prioritization of failures in a system failure mode, effects and criticality analysis.*, Reliability Engineering and System Safety, 50 (1995), pp. 203–213.

[5] M.-S. CHENAUD ET AL., *Status of the astrid core at the end of the pre-conceptual design phase 1*, Nuclear Engineering And Technology, 45 (2013).

[6] T. CLANCY, *The Hunt for Red October*, 1984.

[7] R. J. GARCIER AND Y.-F. L. LAY, *Déconstruire superphénix.*, EspacesTemps.net, (2015).

[8] IAEA, *Power reactor information system - superphenix*.
`https://www.iaea.org/PRIS/CountryStatistics/ReactorDetails.aspx?current=178`.
Accessed: 2016-09-02.

[9] T. KURTOGLU AND I. Y. TUMER, *FFIP: A framework for early assessment of functional failure in complex systems* , International conference on Engineering Design, (2007).

[10] G. L'HER AND D. L. VAN BOSSUYT, *Prognostic systems representation in a function-based Bayesian model during engineering design*, TBD, (TBD).

[11] H.-C. LIU, L. LIU, AND N. LIU, *Risk evaluation approaches in failure mode and effects analysis: A literature review*, Expert Systems With Applications, 40 (2013), pp. 828–838.

[12] B. M. O'HALLORAN, N. PAPAKONSTANTINOU, AND D. L. VAN BOSSUYT, *Modeling of function failure propagation across uncoupled systems*, Proceedings - Annual Reliability and Maintainability Symposium, 2015-May (2015).

[13] ——, *Cable routing modeling in early system design to prevent cable failure propagation events*, Proceedings - Annual Reliability and Maintainability Symposium, 2016-Jan (2016).

[14] C. SMITH, J. KNUDSEN, ET AL., *SAPHIRE basics - An Introduction to Probabilistic Risk Assessment via the Systems Analysis Program for Hands-On Integrated Reliability Evaluations (SAPHIRE) Software*, Idaho National Laboratory, (2009).

[15] A. N. SOCIETY, *Fermi-I: New Age for Nuclear Power*, American Nuclear Society, 1979.

[16] C. STACK AND D. L. VAN BOSSUYT, *Toward a Functional Failure Modeling Method of Representing Prognostic Systems During the Early Phases of Design*, Proceedings of the ASME 2015 International Design Engineering Technical Conference & Computers and Information in Engineering Conference, (2015), pp. DETC2015–46400.

[17] R. B. STONE, I. Y. TUMER, AND M. V. WIE, *FFDM: The function failure design method* , Journal of Mechanical Design, (2005).

[18] R. B. STONE AND K. L. WOOD, *Development of a Functional Basis for Design*, Journal of Mechanical Design, 122 (2000), pp. 359–370.

[19] D. VAN BOSSUYT AND I. RAMP, *Toward an automated model-based geometric method of representing function failure propagation across uncoupled systems* , ASME, (2014).

[20] A. VERDIER, *Évaluation de la sous-criticité lors des opérations de chargement d'un réacteur nucléaire REP*, 2005.

[21] IAEA, *Status of innovative fast reactor designs and concepts: A supplement to the IAEA advanced reactors information system (ARIS)*, Department of Nuclear Energy, Division of Nuclear Power, Nuclear Power Technology Development Section, (2013).