

---

---

# 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



## 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 feasibility 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 a interesting history.



## TABLE OF CONTENTS

	<b>Page</b>
<b>List of Tables</b>	<b>v</b>
<b>List of Figures</b>	<b>vii</b>
<b>List of Acronyms</b>	<b>ix</b>
<b>1 Introduction</b>	<b>1</b>
1.1 A brief design introduction . . . . .	1
1.2 A bit of history . . . . .	2
1.2.1 A focus on SUPERPHENIX . . . . .	3
1.2.2 International feedback . . . . .	5
<b>2 Case study</b>	<b>7</b>
2.1 Advanced Sodium Technological Reactor for Industrial Demonstration (ASTRID)	7
2.2 Case study . . . . .	8
2.2.1 Generic . . . . .	9
2.2.2 Reactor core . . . . .	9
2.2.3 Reactor structure . . . . .	10
2.2.4 Primary circuit components . . . . .	11
2.2.5 Secondary circuit components . . . . .	11
2.2.6 Tertiary circuit components . . . . .	12
<b>3 Identification of potential system failures</b>	<b>13</b>
3.1 Primary circuit components failure . . . . .	14
3.2 Secondary circuit components failure . . . . .	15
3.3 Tertiary circuit components failure . . . . .	15
3.4 Reactor structure components failure . . . . .	16
3.5 Aggressions . . . . .	16
<b>4 High-level failure identification</b>	<b>17</b>
4.1 Reliability Block Diagram . . . . .	17

## TABLE OF CONTENTS

---

4.2	Failure Modes and Effects Analysis . . . . .	18
<b>5</b>	<b>Probabilistic Risk Assessment</b>	<b>23</b>
5.1	PRA model . . . . .	23
5.2	PRA model applied to the case study . . . . .	24
<b>6</b>	<b>Functional models</b>	<b>25</b>
6.1	Functional model . . . . .	25
6.2	Function Failure Design Method . . . . .	26
6.3	Function Failure Identification and Propagation . . . . .	29
<b>A</b>	<b>Reliability Block Diagram</b>	<b>33</b>
A.1	Global system . . . . .	33
A.2	Primary system . . . . .	35
A.2.1	Primary system redundancies . . . . .	36
A.3	Secondary system . . . . .	41
A.3.1	Secondary system redundancies . . . . .	42
A.4	Tertiary system . . . . .	45
A.4.1	Tertiary system redundancies . . . . .	46
<b>B</b>	<b>Failure Modes and Effects Analysis</b>	<b>49</b>
<b>C</b>	<b>Probabilistic Risk Assessments</b>	<b>57</b>
	<b>Bibliography</b>	<b>59</b>

## LIST OF TABLES

TABLE	Page
1.1 Highly simplified advantages/inconvenients table for the SFR design . . . . .	2
4.1 Probability index . . . . .	20
4.2 Detectability index for a risk-centered method . . . . .	20
4.3 Detectability index for a reliability-centered method . . . . .	20
4.4 Detectability index . . . . .	21
4.5 Excerpt from TableB.1 presenting the (P, S, D)-triplet for the perceived most severe failure modes . . . . .	21
4.6 Excerpt from Table B.2 presenting the RPN and possible mitigation strategy for the perceived most severe failure modes . . . . .	21
6.1 Excerpt from the functional basis reconciled function set . . . . .	26
6.2 Excerpt from the functional basis reconciled flow set . . . . .	26
6.3 FFDM database . . . . .	28
6.4 FFDM normalized database . . . . .	28
B.1 FMEA . . . . .	53
B.2 FMEA: RPN and mitigation . . . . .	56
C.1 PRA: basic events . . . . .	58





## LIST OF FIGURES

FIGURE	Page
1.1 Pool type sodium-cooled fast reactor . . . . .	2
1.2 Pool-type vs Loop-type sodium-cooled fast reactor . . . . .	3
1.3 Operation timeline for the SUPERPHENIX reactor . . . . .	4
2.1 ASTRID reactor building generic schematics . . . . .	8
4.1 Reliability Block Diagram for the primary system . . . . .	18
6.1 High-level simplified FBED representation of ASTRID reactor. . . . .	31
A.1 Main Reliability Block Diagram architecture . . . . .	33
A.2 Reliability Block Diagram for the primary system . . . . .	35
A.3 Reliability Block Diagram for the core sensors in the primary system . . . . .	36
A.4 Reliability Block Diagram for the primary pumps in the primary system . . . . .	37
A.5 Reliability Block Diagram for the heat exchangers in the primary system . . . . .	38
A.6 Reliability Block Diagram for the safety injection system in the primary system . . . . .	39
A.7 Reliability Block Diagram for the decay heat removal in the primary system . . . . .	40
A.8 Reliability Block Diagram for the secondary system . . . . .	41
A.9 Reliability Block Diagram for the secondary pumps in the secondary system . . . . .	42
A.10 Reliability Block Diagram for the steam generators in the secondary system . . . . .	43
A.11 Reliability Block Diagram for the tertiary system . . . . .	45
A.12 Reliability Block Diagram for the condensers in the tertiary system . . . . .	46
A.13 Reliability Block Diagram for the tertiary-secondary pumps in the tertiary system . . . . .	46
A.14 Reliability Block Diagram for the boundary-tertiary pumps in the tertiary system . . . . .	47
A.15 Reliability Block Diagram for the turbines in the tertiary system . . . . .	47
A.16 Reliability Block Diagram for the generators in the tertiary system . . . . .	48



## LIST OF ACRONYMS

**ASTRID** Advanced Sodium Technological Reactor for Industrial Demonstration.

**CFV** Coeur a Faible Vidange, Low Void Worth Core.

**EBR** Experimental Breeder Reactor.

**FBED** Functional Basis for Engineering Design.

**FFDM** Function Failure Design Method.

**FFIP** Function Failure Identification and Propagation.

**FMEA** Failure Modes and Effects Analysis.

**FMECA** Failure Modes, Effects and Criticality Analysis.

**PHM** Prognostic Health Management.

**PRA** Probabilistic Risk Assessment.

**RBD** Reliability Block Diagram.

**RPN** Risk Priority Number.

**SFR** Sodium-cooled Fast Reactor.

**UFFSR** Uncoupled Flow Failure State Reasoning.



## 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) [16]. 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.

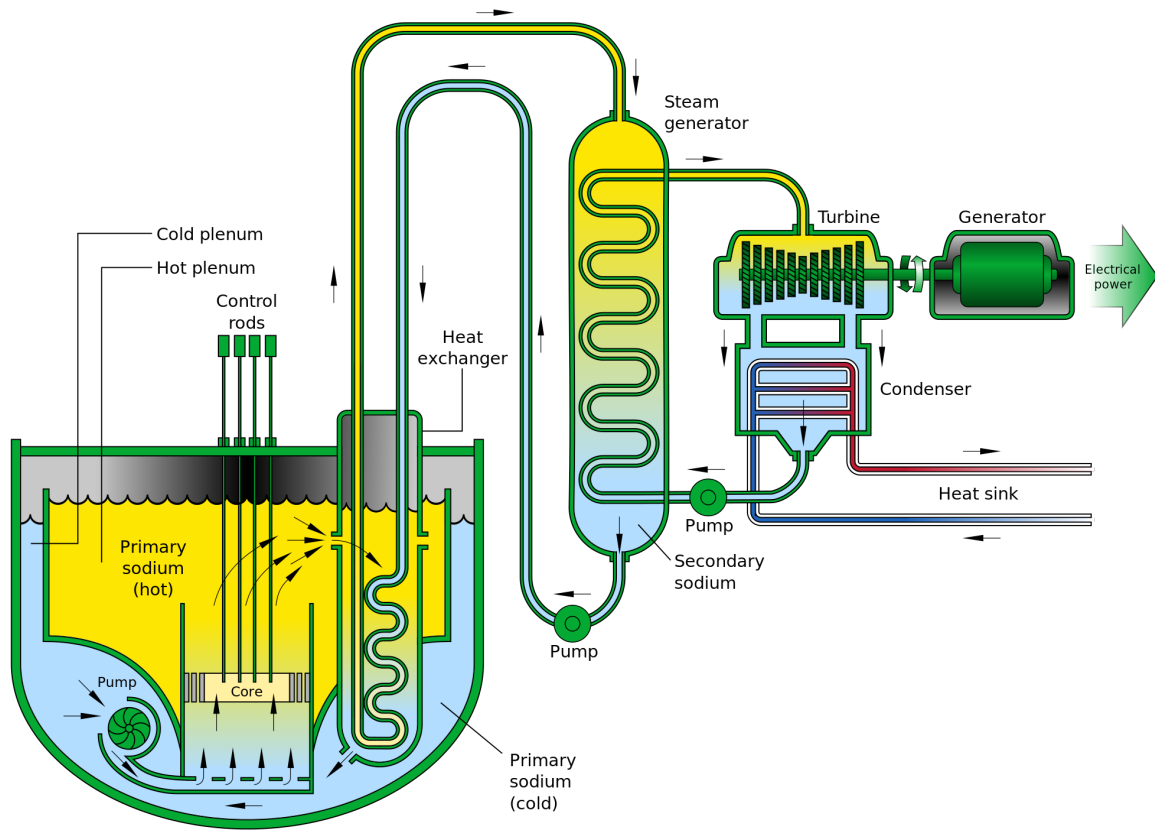


FIGURE 1.1. Pool type sodium-cooled fast reactor.

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

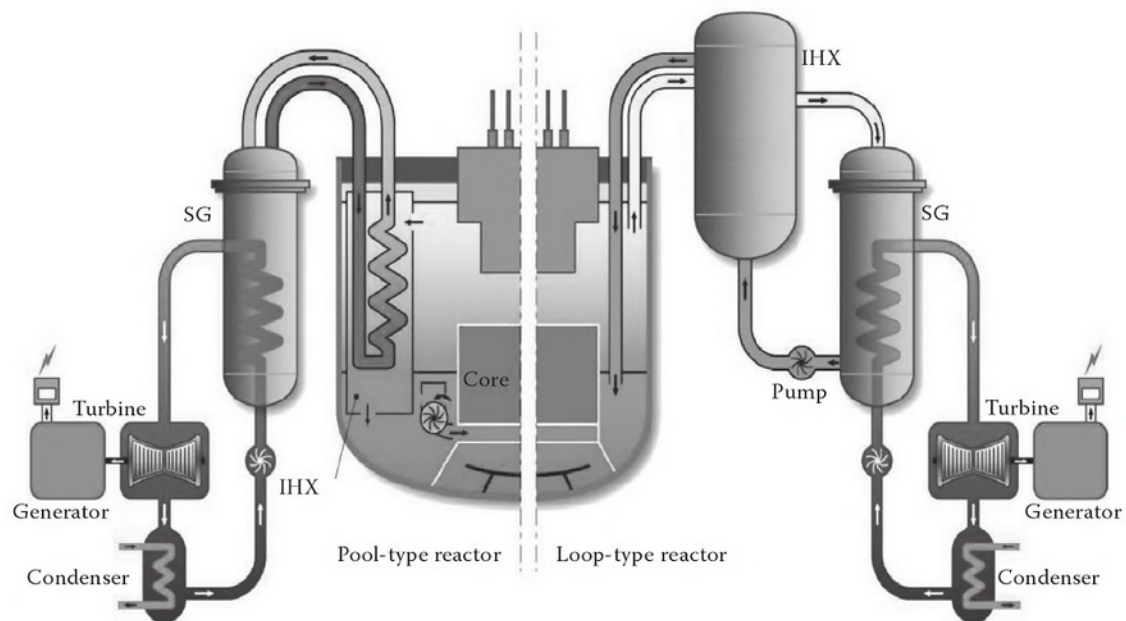


FIGURE 1.2. Pool-type vs Loop-type sodium-cooled fast reactor.

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 Superphenix 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

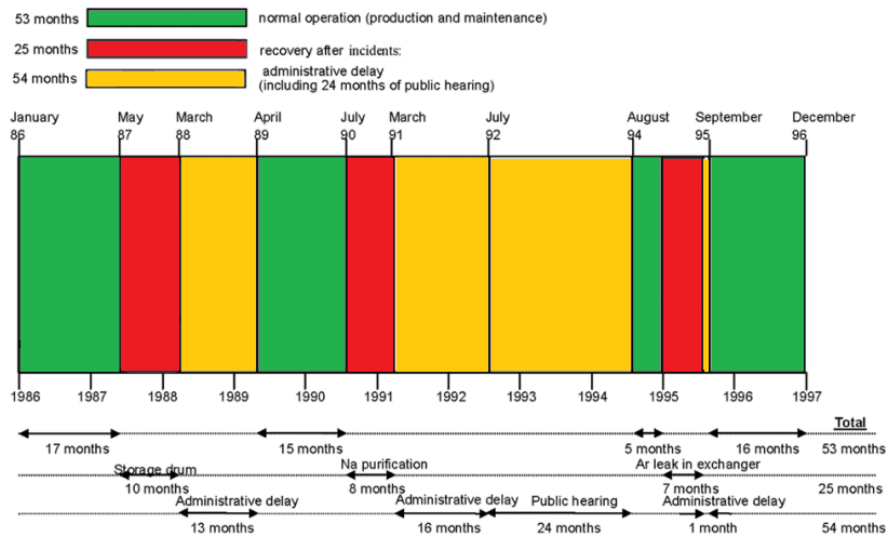


FIGURE 1.3. Operation timeline for the SUPERPHENIX reactor [6].

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 [7], 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 feasibility of breeding [11]. 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 ??, 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.

## 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.

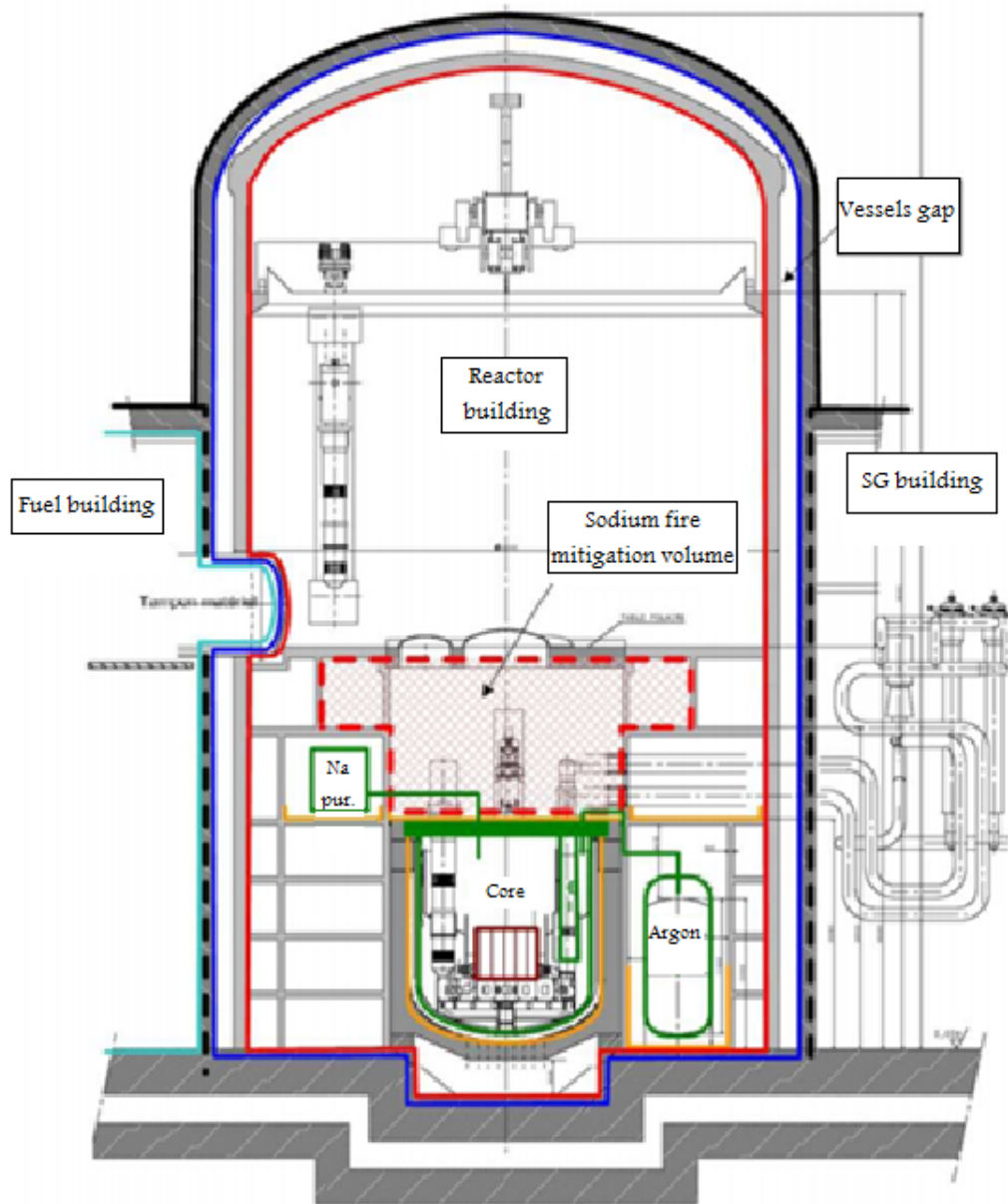


FIGURE 2.1. ASTRID reactor building generic schematics

## 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



## 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.

### 3.1 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 and 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 these 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 cladding 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 distortion 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 [15]. 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 through 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.

## 3.2 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 electromagnetic 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 immersed, 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.

## 3.3 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.

### 3.4 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 terms of 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.

### 3.5 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.

## 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.

### 4.1 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 4.1.

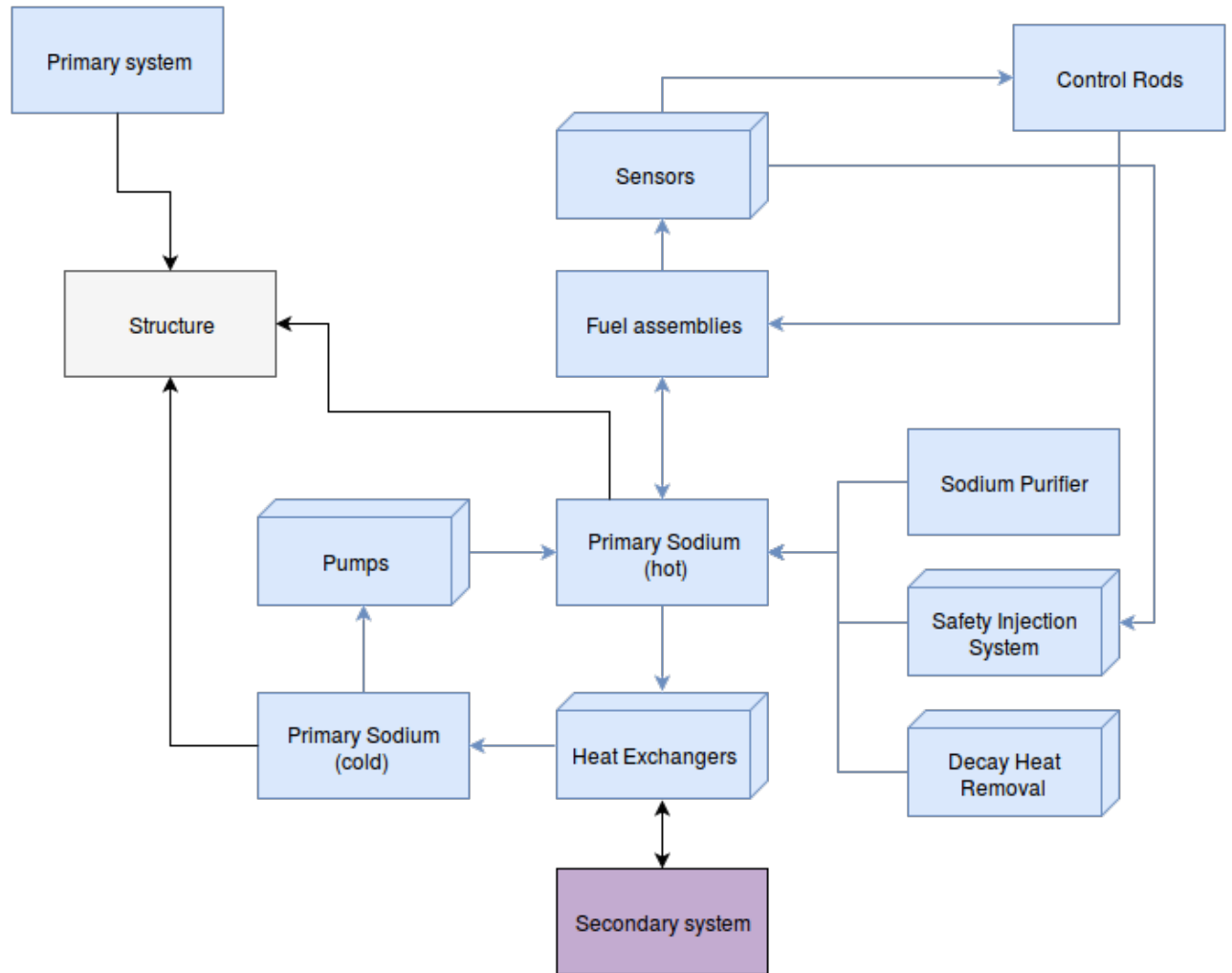


FIGURE 4.1. Reliability Block Diagram for the primary system

## 4.2 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.

$$(4.1) \quad RPN = P * S * D$$

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 [9]. 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 competition 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 occurring 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 conclusions.

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 between 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 explicated in details in this paper for clarity reasons. The risk-FMEA englobes the reliability ones, with of course a different emphasis.

Following 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 4.1, 4.2, 4.3 and 4.4.

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

Table 4.1: 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 4.2: 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 4.3: 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 aforementioned reference tables for the different



Detectability	Index	Detectability estimate
Very high	1	86% to 100%
High	2	76% to 85%
	3	66% to 75%
	4	56% to 65%
Moderate	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 4.4: 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 4.5 and 4.6.

ID	Component	Failure	Cause	<i>P</i>	<i>S</i>	<i>D</i>
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 4.5: 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 4.6: 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.

## PROBABILISTIC RISK ASSESSMENT

**R**isks assessments include the identification and analysis of initiating event, safety functions and accident sequences. The initiating events are the circumstances that put a system in an off-normal condition. The safety functions represent 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.

### 5.1 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.

## 5.2 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 aforementioned 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.

## FUNCTIONAL MODELS

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. Functions are interconnected by flows. One of the main advantages 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 ?. 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) [13], which reconciled sets of functions 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) [12], Function Failure Identification and Propagation (FFIP) [8] or Uncoupled Flow Failure State Reasoning (UFFSR) [14], [10].

### 6.1 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 6.1 and 6.2 give a few examples 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 allows for some level of interpretation as to how to categorize a function or flow.

A FBED model can be compared to a RBD. They both can take various degrees of details,

Table 6.1: 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 6.2: Excerpt from the functional basis reconciled flow set

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

high-level to low-level model description. One of the advantages that FBED exhibits as opposed to RBD is that it considers explicitly 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 6.1 show an example of a functional model applied to the present case study. One can note that the level of details can be modified. Moreover, to simplify the drawing, the redundancies displayed by the system are not explicated as separate functions and flows. They are instead encoded within the probabilities associated with each function or flow failure propagation.

## 6.2 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 during 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 6.3 shows several failure modes occurrences 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 occurrences is then computed into Table 6.3. Table 6.4 presents the normalized data, computed using Equation 6.1.

$$(6.1) \quad f_{i,n} = \frac{f_i}{\sum_j F_j}$$

Table 6.3: 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
...								

Table 6.4: 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
...								

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 explicated 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 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 failure 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 an informed decision. Consequently, this method can be judged insufficient for larger complex systems, but proves useful in the context of a concept generator, to choose a component that is better than another for a given functionality. 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.

### **6.3 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.

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 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 zero-liquid flow will then

potentially fail the next function in line and the failure propagate.

---

**Algorithm 1** FFIP pseudocode - Function 1

---

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

---



---

**Algorithm 2** FFIP pseudocode - Function 2

---

1: **procedure** SIGNAL - PROCESS  
**Require:** *Material - Human*, *Energy - Electrical*, *Signal*  
**Ensure:** *Signal - Control*  
2:   **if** *Material - Human*<sub>in</sub> = 0 and *Energy - Electrical*<sub>in</sub> = 0 **then return** procedure failed  
3:   **else if** *Material - Human*<sub>in</sub> = 0 and *Signal*<sub>in</sub> = 0 **then return** procedure failed  
4:   **else if** *Signal - Control*<sub>out</sub> = 0 **then return** procedure failed  
5:   **else return** procedure operative

---



---

**Algorithm 3** FFIP pseudocode - Function 3

---

1: **procedure** CONTROL MAGNITUDE - REGULATE  
**Require:** *Signal - Control*, *Energy - Electrical*  
**Ensure:** *Signal - Control*  
2:   **if** not *Signal - Control*<sub>in</sub> **then return** procedure SCRAM  
3:   **else if** *Signal - Control*<sub>in</sub> = 0 and *Signal - Control*<sub>out</sub> ≠ 0 **then return** procedure failed  
4:   **else if** *Signal - Control*<sub>in</sub> = ±1 and *Signal - Control*<sub>out</sub> in [0, ∓*Signal - Control*<sub>in</sub>] **then return** procedure failed  
5:   **else if** *Signal - Control*<sub>in</sub> and *Energy - Electrical*<sub>in</sub> = 0 **then return** procedure failed  
6:   **else return** procedure operative

---

In the case study at hand, several failure flow propagation were studied.

---

**Algorithm 4** FFIP pseudocode - Function 3

---

1: **procedure** CONVERT - CONVERT

**Require:** *Signal - Control, Energy - Electrical*

**Ensure:** *Energy - Mechanical*

2:   **if** not *Signal - Control*<sub>in</sub> **then return** procedure SCRAM

3:   **else if** *Signal - Control*<sub>in</sub> and *Energy - Electrical*<sub>in</sub> = 0 **then return** procedure failed

4:   **else if** *Signal - Control*<sub>in</sub> and *Energy - Mechanical*<sub>out</sub> = 0 **then return** procedure failed

5:   **else return** procedure operative

---

---

**Algorithm 5** FFIP pseudocode - Function 3

---

1: **procedure** CHANNEL - GUIDE - TRANSLATE

**Require:** *Material - Mixture - Solid-Solid, Energy - Mechanical*

**Ensure:** *Energy - Radioactive*

2:   **if** *Energy - Radioactive*<sub>out</sub> not change **then return** procedure failed

3:   **else return** procedure operative

---

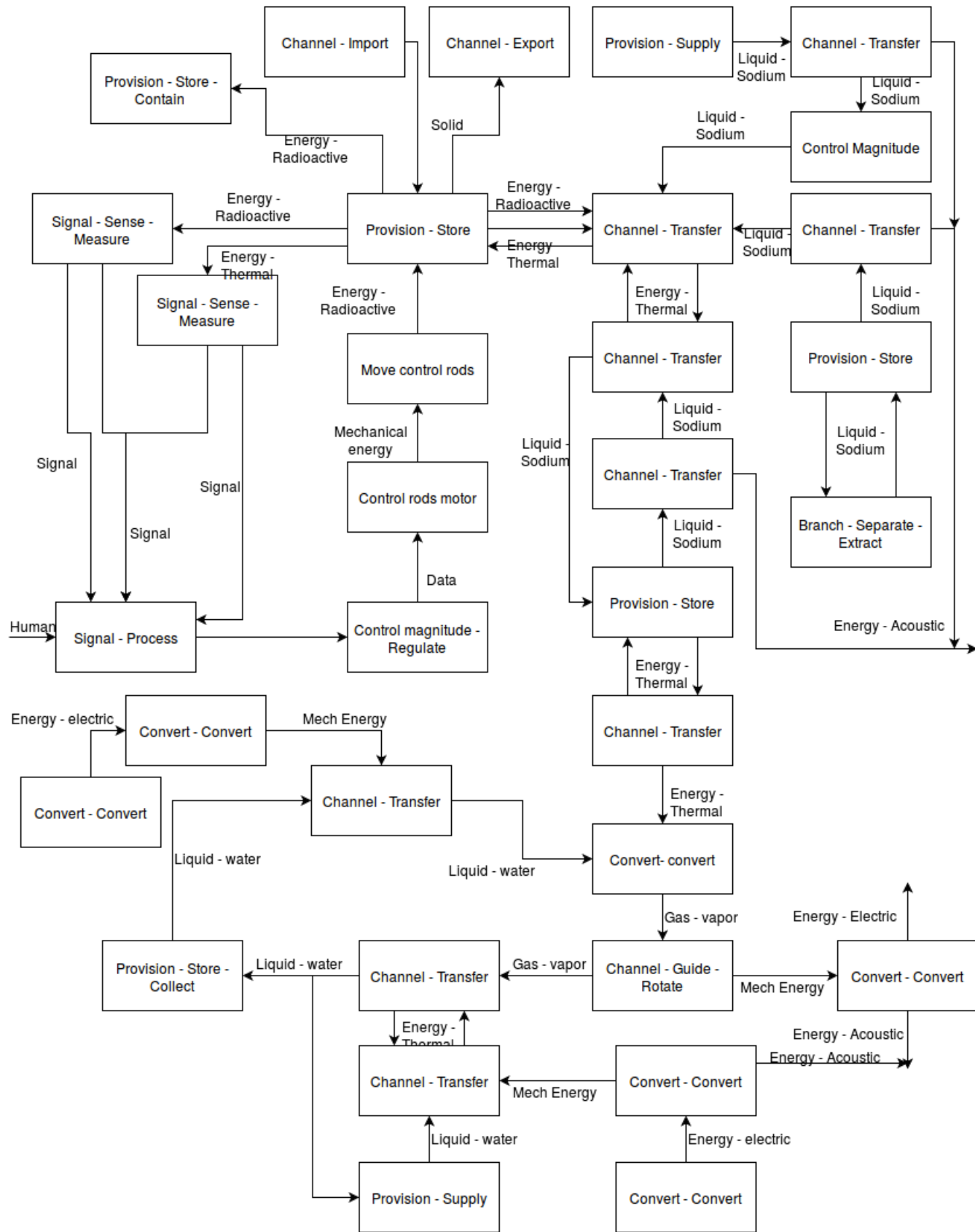


Figure 6.1: High-level simplified FBED representation of ASTRID reactor.

## 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.

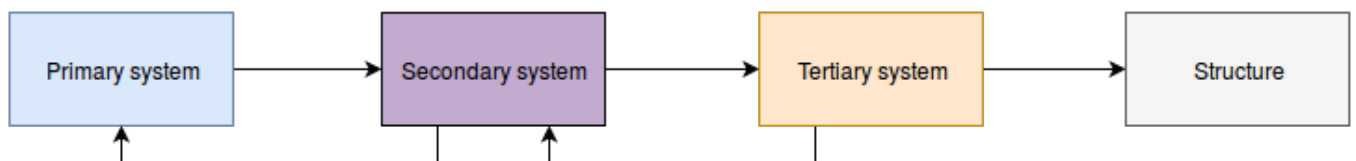


FIGURE A.1. Main RBD architecture



## A.2 Primary system

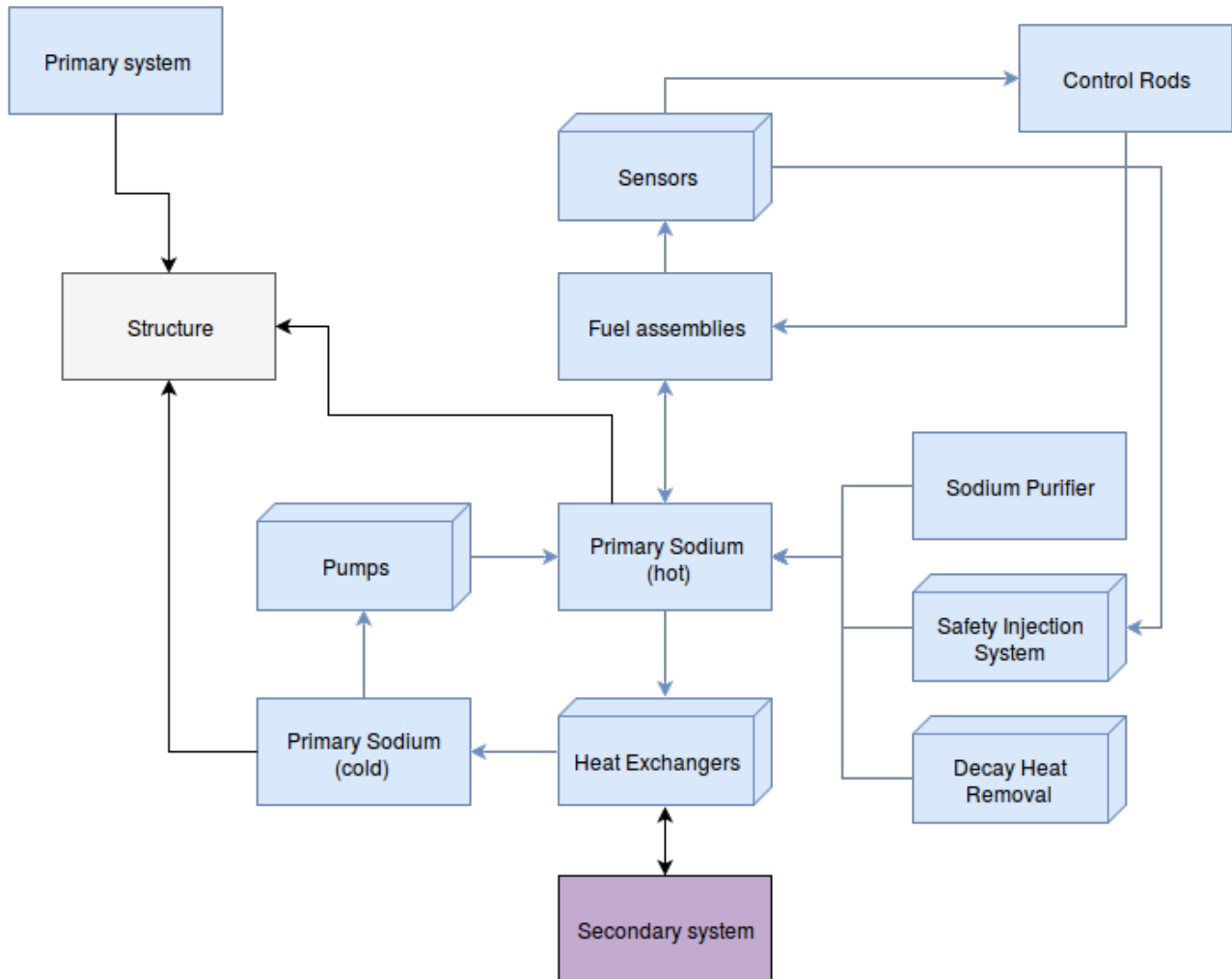


FIGURE A.2. Reliability Block Diagram for the primary system

### A.2.1 Primary system redundancies

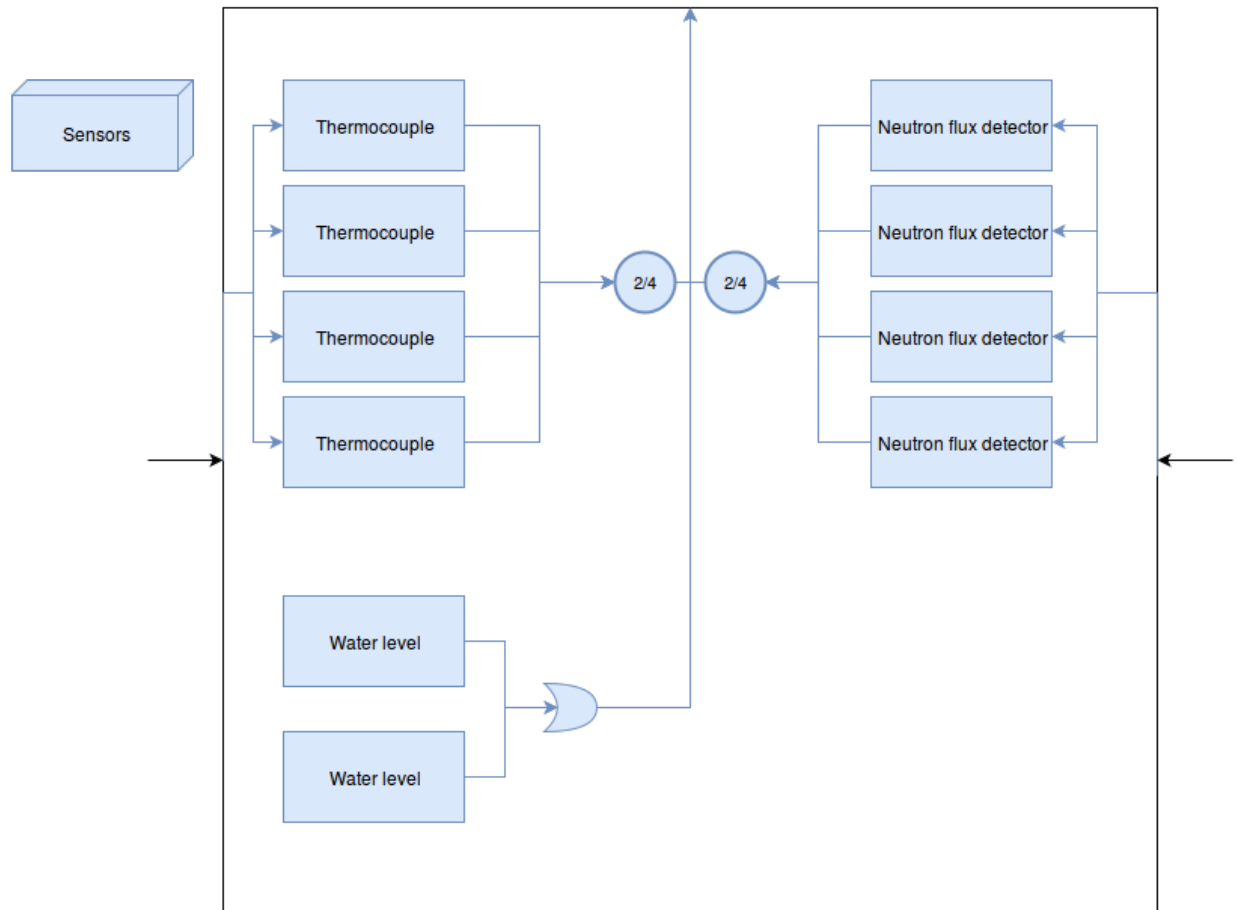


FIGURE A.3. Reliability Block Diagram for the core sensors in the primary system



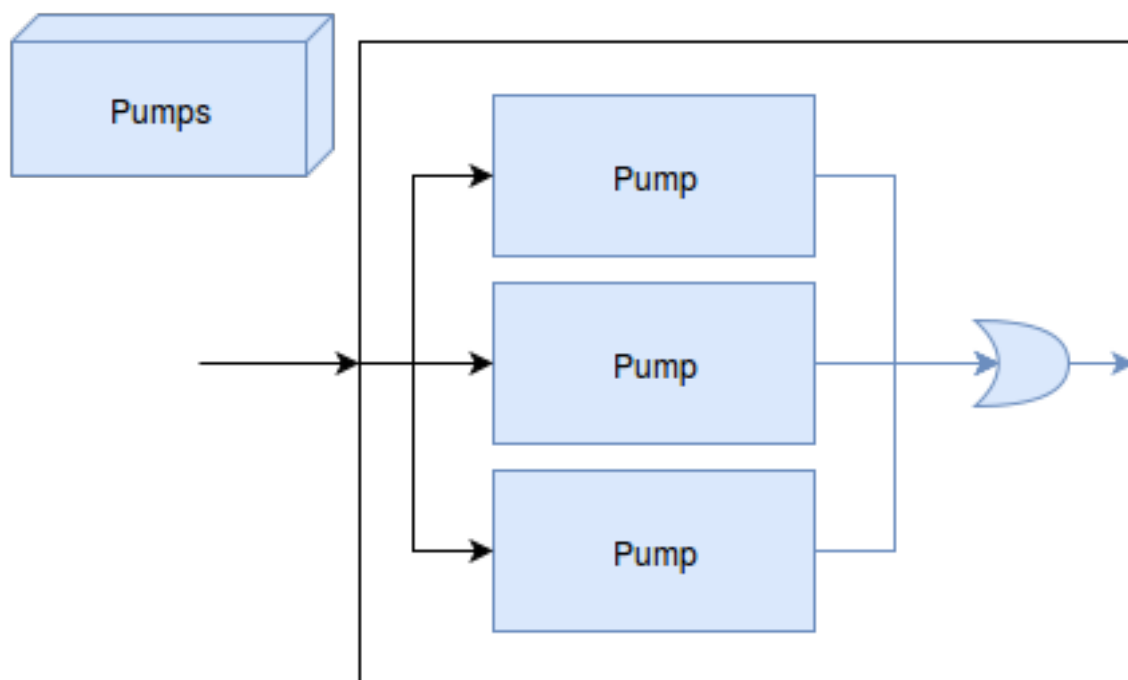


FIGURE A.4. Reliability Block Diagram for the primary pumps in the primary system

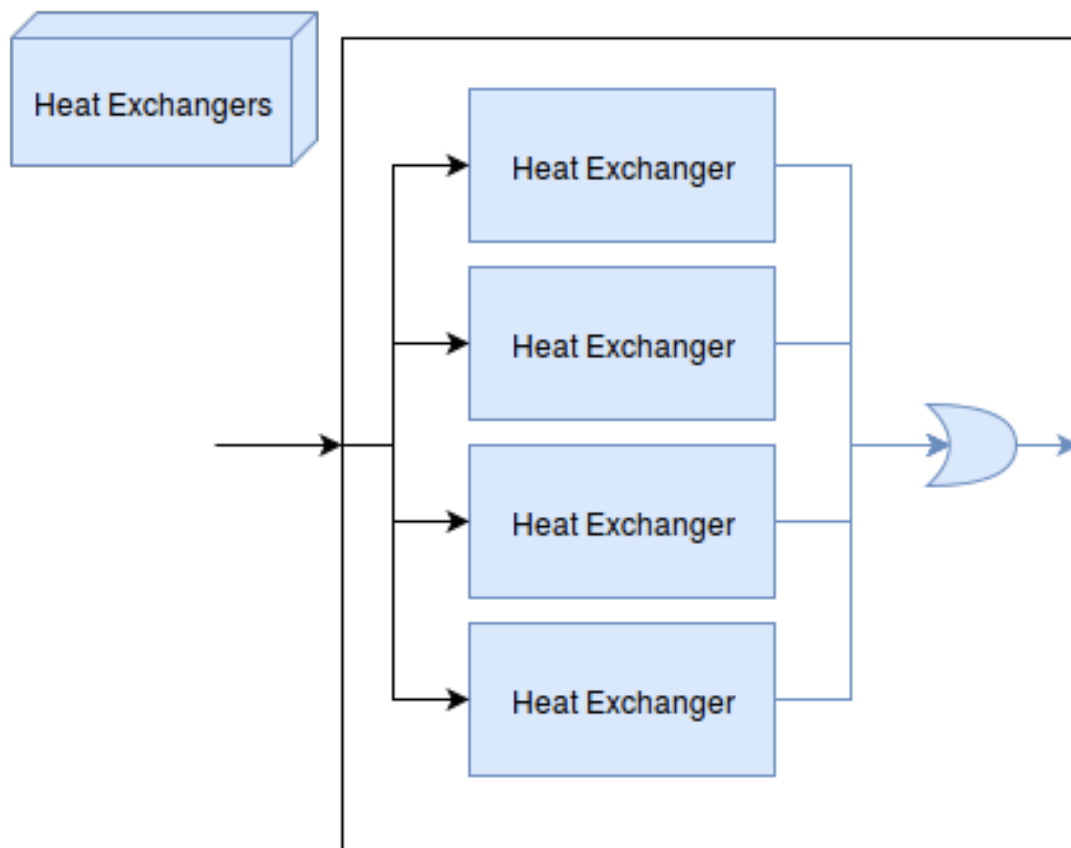


FIGURE A.5. Reliability Block Diagram for the heat exchangers in the primary system

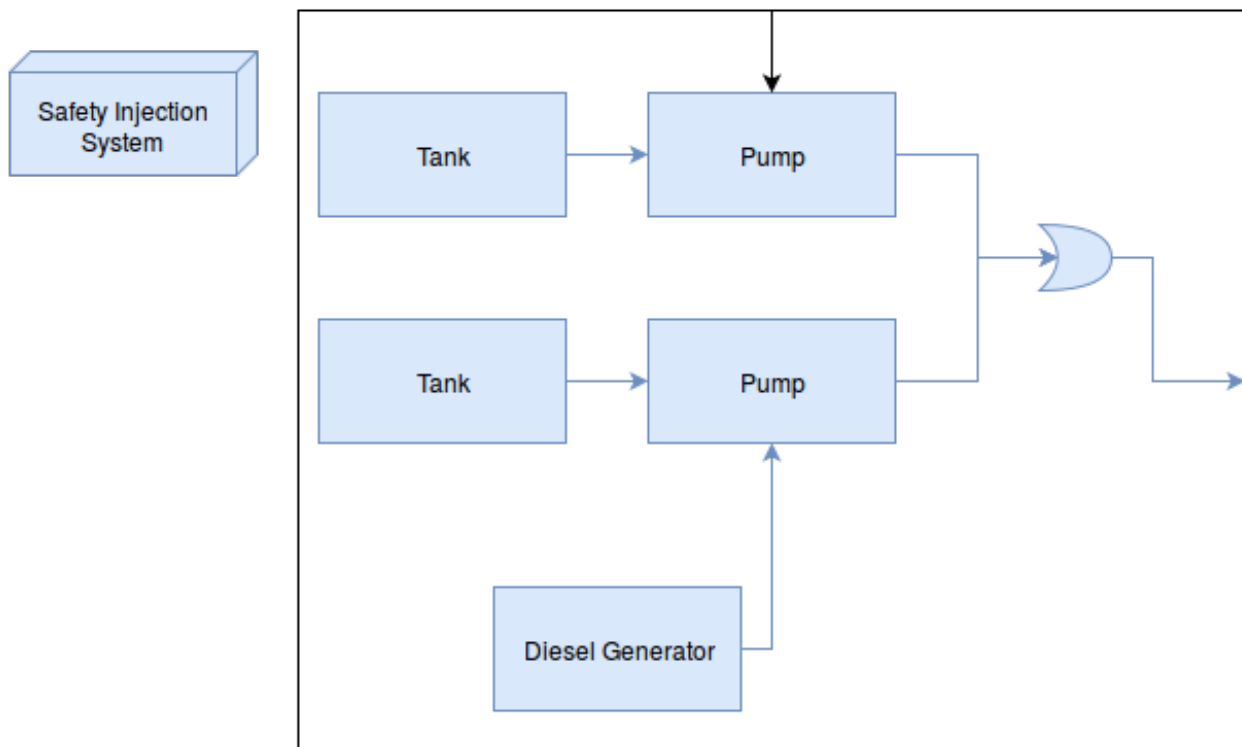


FIGURE A.6. Reliability Block Diagram for the safety injection system in the primary system

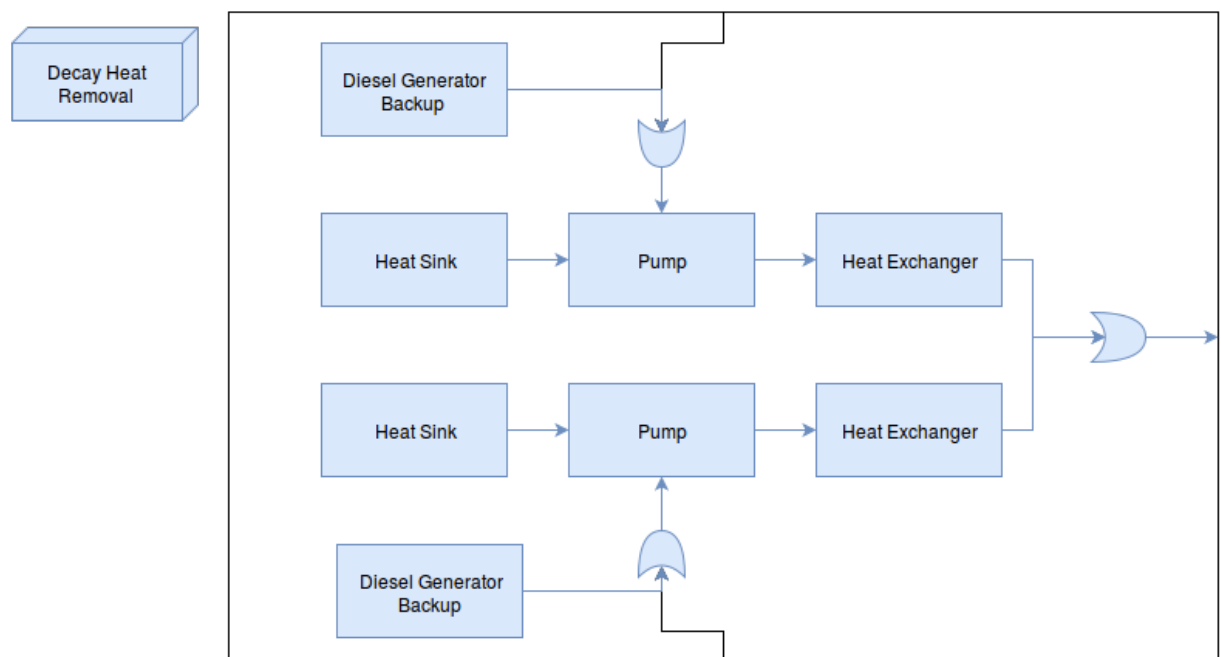


FIGURE A.7. Reliability Block Diagram for the decay heat removal in the primary system

### A.3 Secondary system

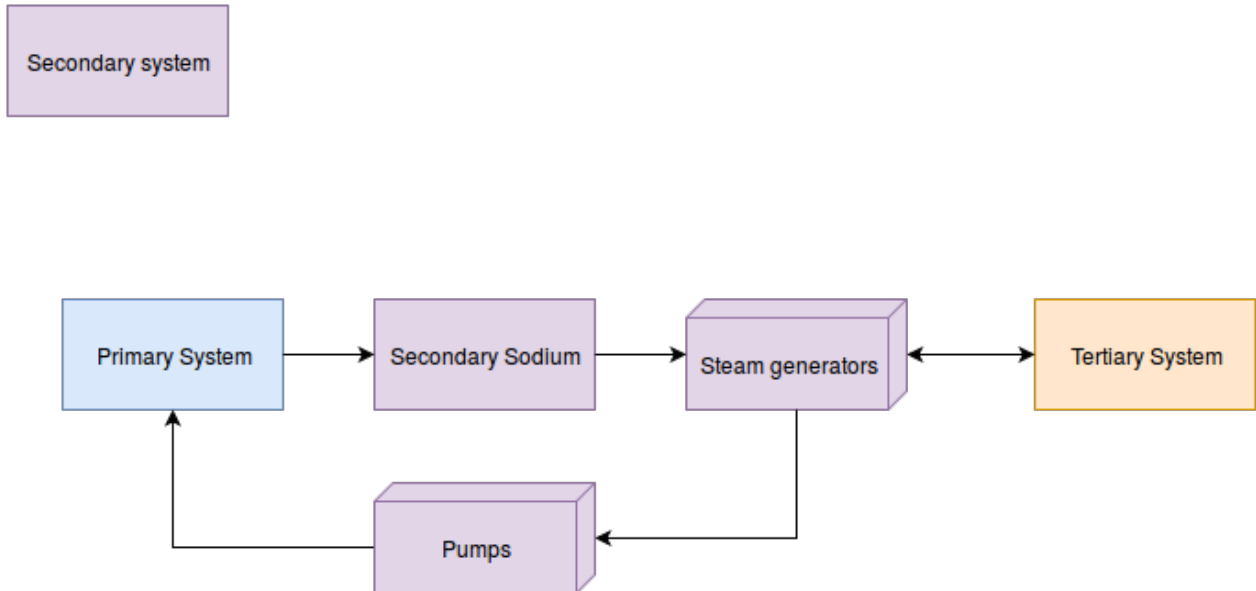


FIGURE A.8. Reliability Block Diagram for the secondary system

### A.3.1 Secondary system redundancies

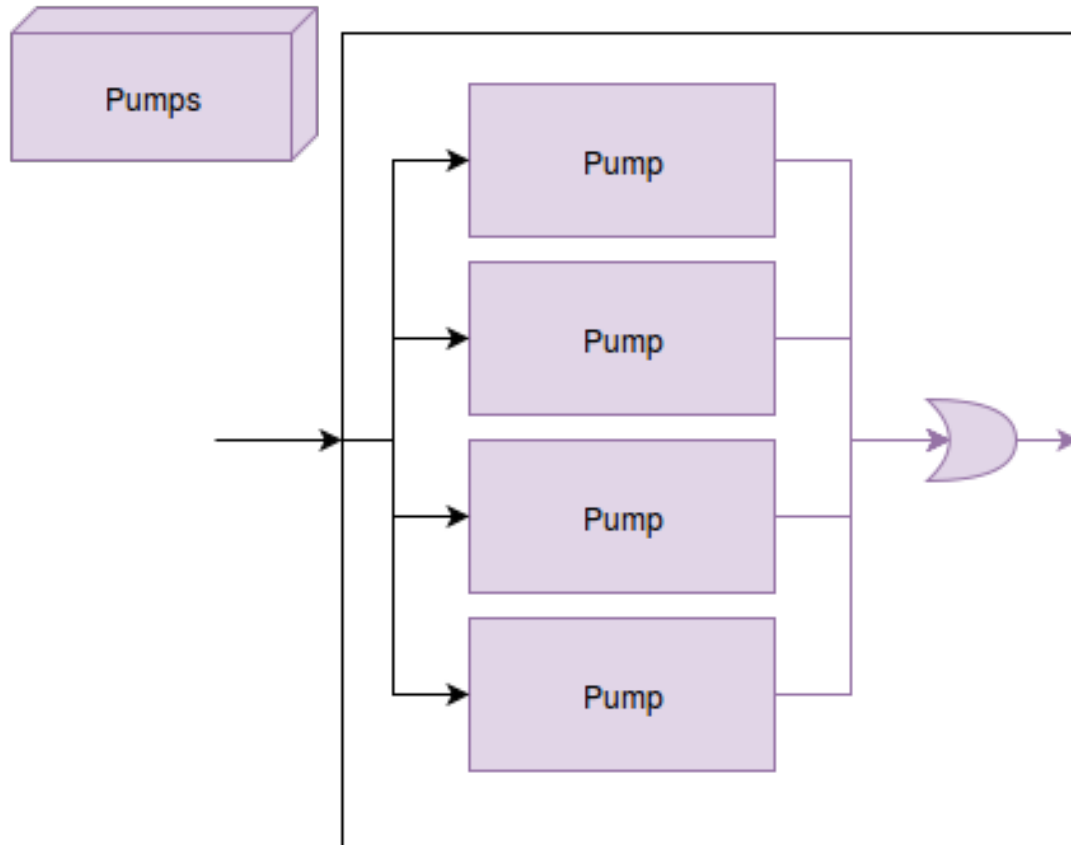


FIGURE A.9. Reliability Block Diagram for the secondary pumps in the secondary system

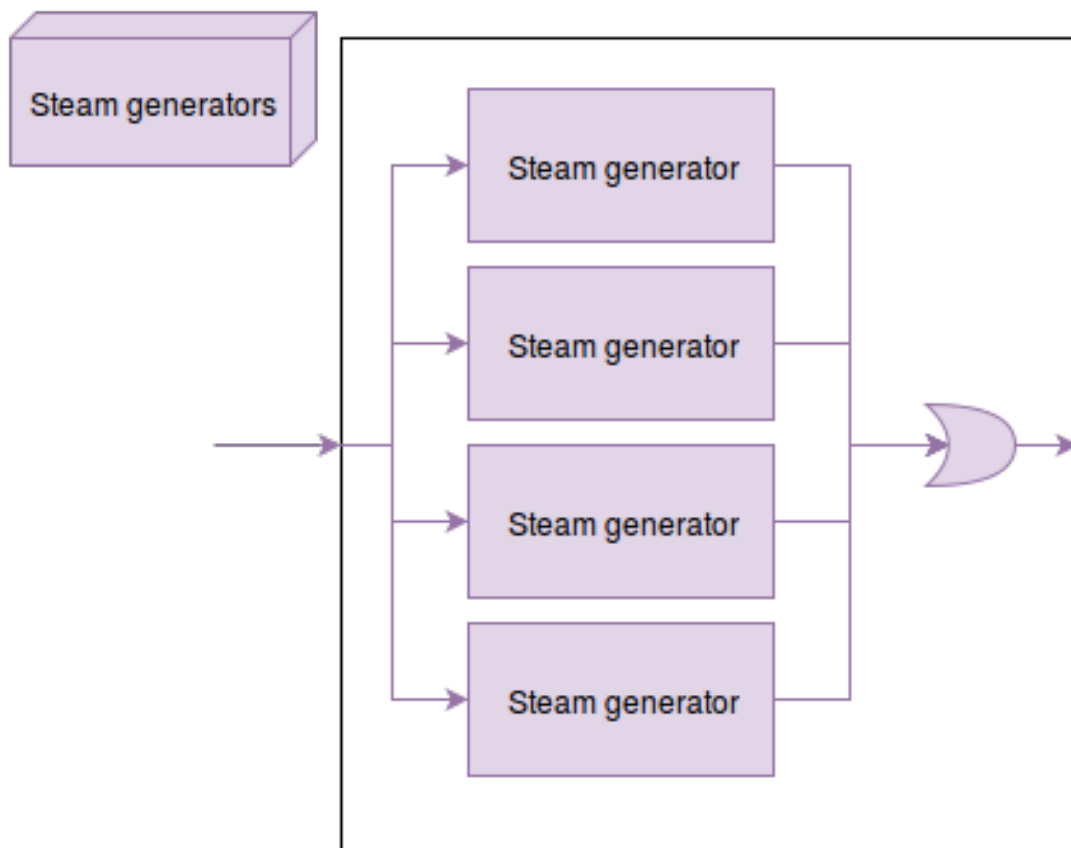


FIGURE A.10. Reliability Block Diagram for the steam generators in the secondary system





## A.4 Tertiary system

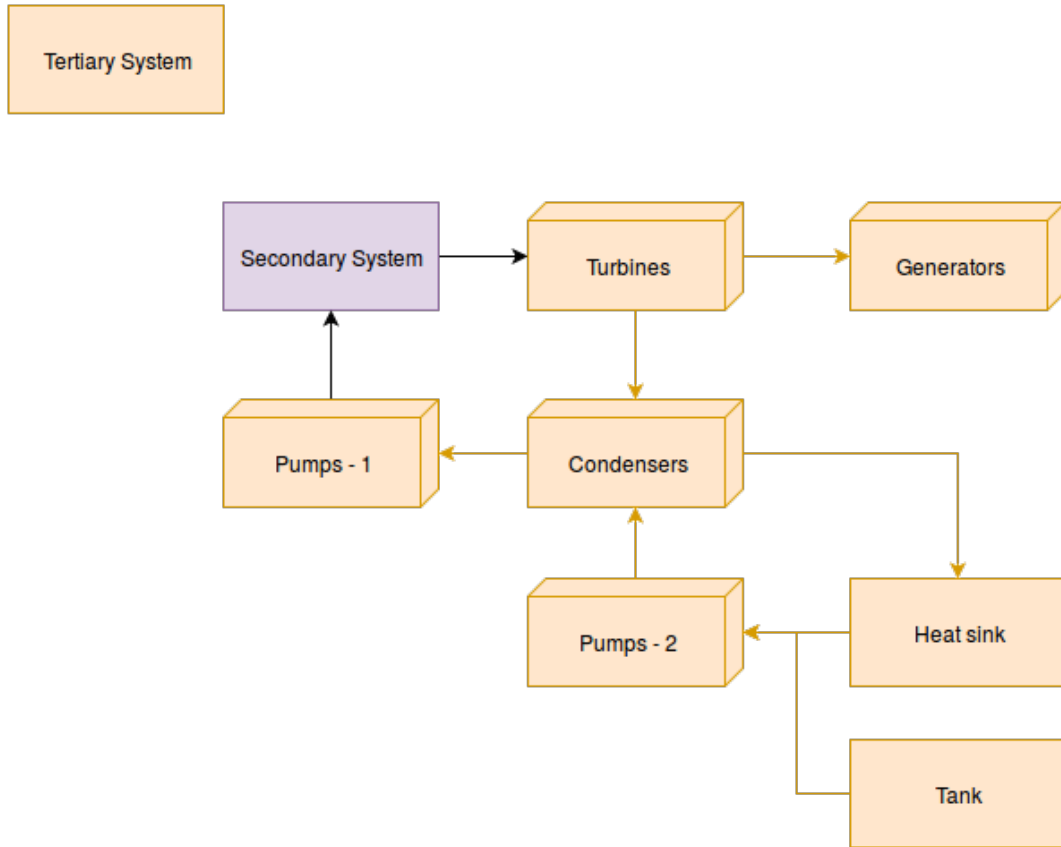


FIGURE A.11. Reliability Block Diagram for the tertiary system

#### A.4.1 Tertiary system redundancies

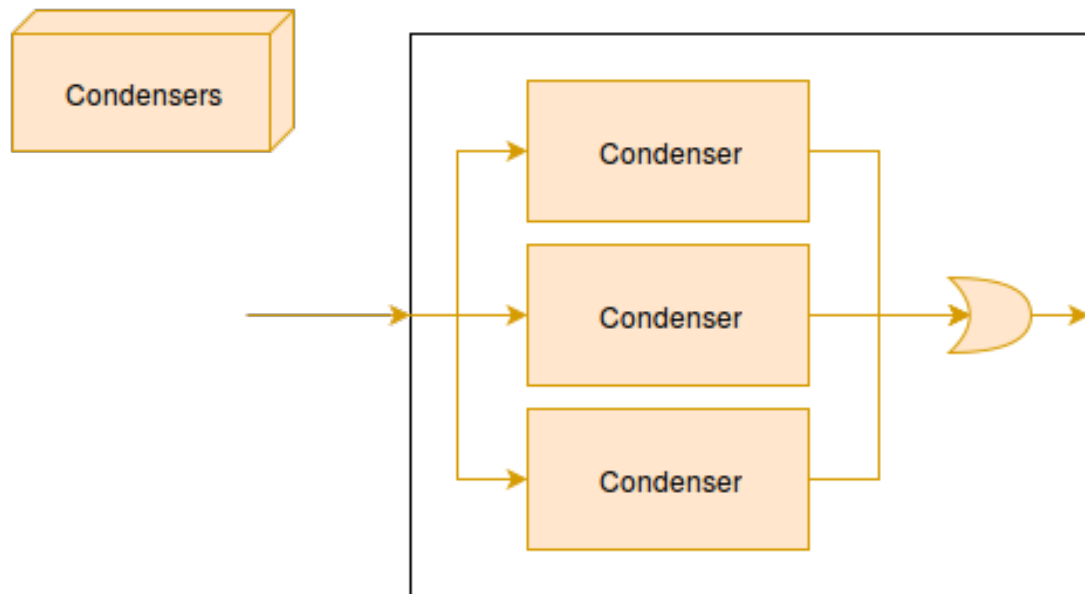


FIGURE A.12. Reliability Block Diagram for the condensers in the tertiary system

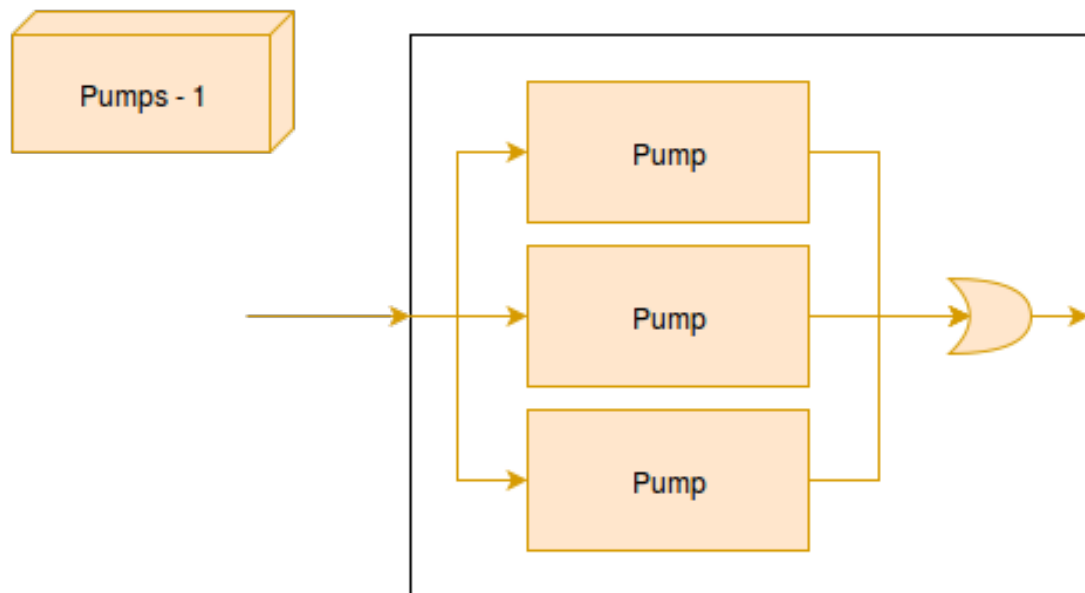


FIGURE A.13. Reliability Block Diagram for the tertiary-secondary pumps in the tertiary system

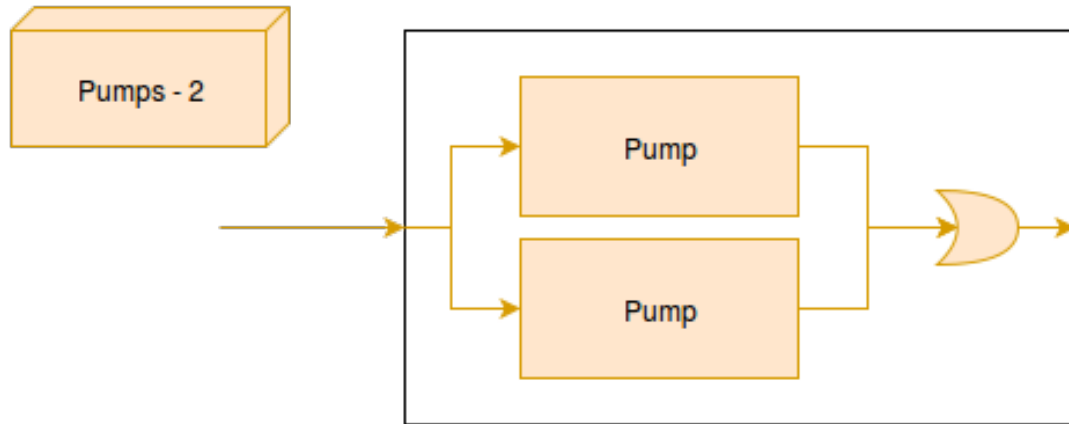


FIGURE A.14. Reliability Block Diagram for the boundary-tertiary pumps in the tertiary system

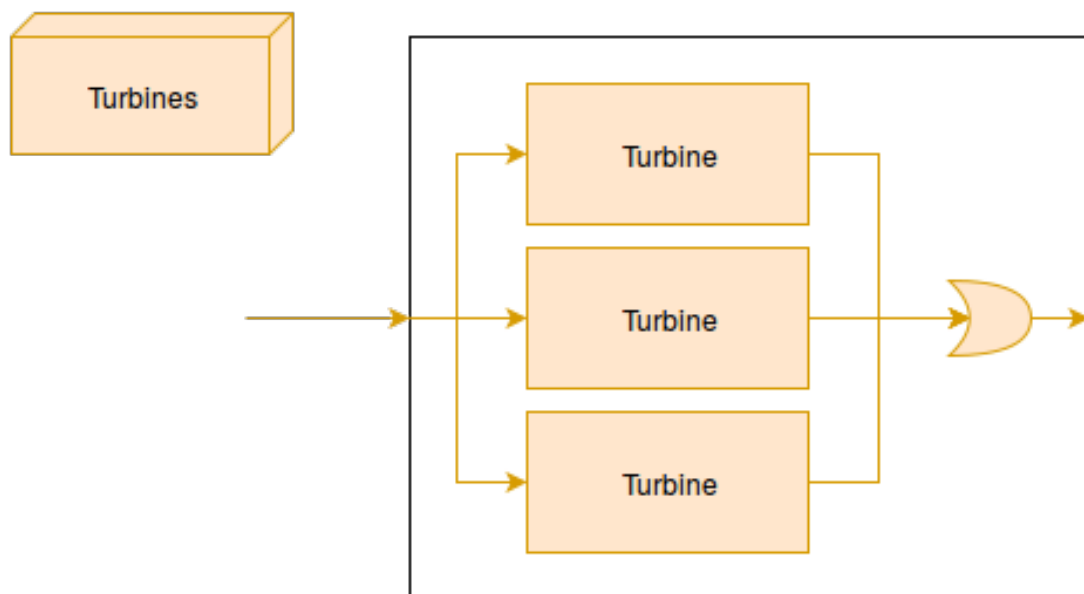


FIGURE A.15. Reliability Block Diagram for the turbines in the tertiary system

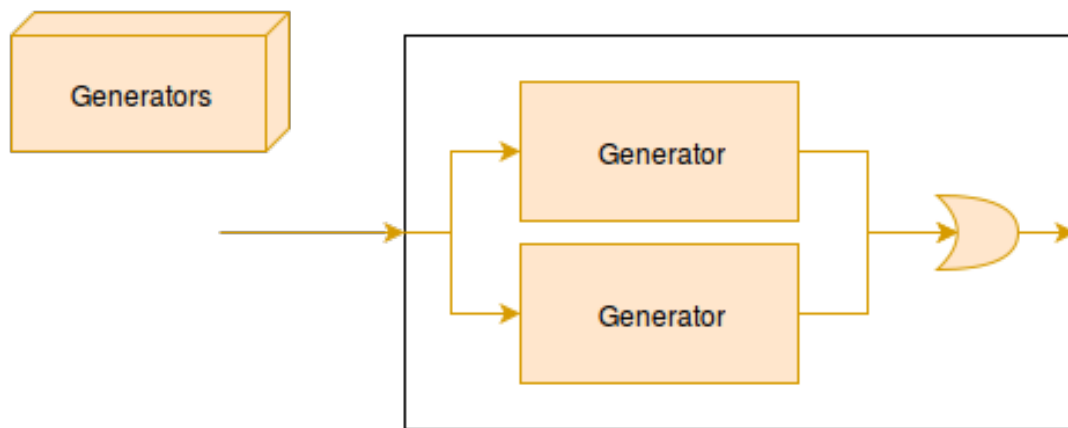


FIGURE A.16. Reliability Block Diagram for the generators in the tertiary system

## 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	<i>P</i>	<i>S</i>	<i>D</i>
1.1	Fuel Assemblies	Pin cladding (< 5%)	Local peak power	8	2	2
1.2		Pin cladding (> 10%)	Global peak power	5	9	2
1.3		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	Primary pumps	Partial loss of capability for one pump	Wear	4	5	4
2.2		Complete loss of capability for one pump	Bad maintenance	3	6	3
2.3		Partial loss of capability for all pumps	Wear and bad maintenance	2	9	2

## APPENDIX B. FAILURE MODES AND EFFECTS ANALYSIS

... continued

ID	Component	Failure	Cause	<i>P</i>	<i>S</i>	<i>D</i>
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		One rod does not fall	Gripped mechanical release	3	6	4
3.2		One rod fall too slowly	Distorsion	6	4	2
3.3	Control rods	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		Large leak in one of the two	Faulty material	2	7	7
4.2	Decay heat exchangers	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		Partial loss of capability for one pump	Wear	4	5	4
5.2	Heat removal system pumps	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

...continued

ID	Component	Failure	Cause	<i>P</i>	<i>S</i>	<i>D</i>
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
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

# APPENDIX B. FAILURE MODES AND EFFECTS ANALYSIS

... continued

ID	Component	Failure	Cause	<i>P</i>	<i>S</i>	<i>D</i>
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
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



...continued

ID	Component	Failure	Cause	<i>P</i>	<i>S</i>	<i>D</i>
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 Prognostic Health Management (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 distorted assemblies
3.5	20	Extend PHM to detect the failure, go toward a electromagnetic attachment, improve startup checks

... continued

ID	RPN	Mitigation
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
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
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

... continued

ID	RPN	Mitigation
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

## 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.

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	$1 \times 10^{-3}$
No fuel for the generator	GENERATOR_NO_FUEL	$1 \times 10^{-3}$
No oil for the generator	GENERATOR_NO_OIL	$1 \times 10^{-3}$
Other failure (bearing, rust, etc)	GENERATOR_OTHER_FAIL	$1 \times 10^{-2}$
No signal sent to the generator	GENERATOR_NO_SIGNAL	$1 \times 10^{-2}$
Fuel probes signal transmission	CORE_DET_FUEL_TRANS	$1 \times 10^{-6}$
Fuel temperature sensor	CORE_DET_FUEL	$1 \times 10^{-2}$
Neutron detectors signal transmission	CORE_DET_NEUT_TRANS	$1 \times 10^{-5}$
Neutron flux detector	CORE_DET_NEUT	$1 \times 10^{-3}$
Thermocouples signal transmission	CORE_DET_THER_TRANS	$1 \times 10^{-5}$
Thermocouple	CORE_DET_THER	$1 \times 10^{-2}$
Sensor detection of flow efficiency	SENSOR_DETECTION	$1 \times 10^{-3}$
Sensor communication	SENSOR_NO_COMM	$1 \times 10^{-3}$
Check if the power if off	AUTO_POWER_CHACK	$1 \times 10^{-7}$

# APPENDIX C. PROBABILISTIC RISK ASSESSMENTS

Event	ID	Failure probability
Signal communication	COMM_SIGNAL_POWER_OFF	$1 \times 10^{-3}$
Decay heat removal system heat exchanger	DHR_IHX	$1 \times 10^{-4}$
DHR system pump	DHR_PUMP	$1 \times 10^{-4}$
Heat sink availability	HEAT_SINK	$1 \times 10^{-3}$
Regular DHR power	DHR_POWER	$1 \times 10^{-4}$
Maintenance access to generator	MAINTENANCE_NOT_POSSIBLE	$1 \times 10^{-3}$
Repair of generator	GENERATOR_REPAIR	$1 \times 10^{-1}$
Signal to let rods fall	CORE_RODS_SIGNAL	$1 \times 10^{-5}$
Signal to let rods fall	CORE_RODS_SIGNAL_MANU	$1 \times 10^{-5}$
Mechanical release of control rods	CORE_RODS_MECH	$1 \times 10^{-4}$
Safety Injection System pump	SIS_PUMP	$1 \times 10^{-4}$
SIS Tank	SIS_TANK	$1 \times 10^{-5}$
Regular SIS power	SIS_POWER	$1 \times 10^{-4}$
SIS valve	SIS_VALVE	$1 \times 10^{-2}$
Breach in the main vessel	PRE_BREACH_CONT_MAIN	$1 \times 10^{-5}$
Breach in the safety vessel	PRE_BREACH_CONT_SAFE	$1 \times 10^{-5}$
Operator interpretation to manually detect LOCA	INTERPRET_OPERATOR	$5 \times 10^{-2}$
Control room communication isolated	OUTSIDE_COMMUNICATION	$1 \times 10^{-4}$
Operator unavailable	OPERATOR_PROBLEM	$1 \times 10^{-4}$
Manually add sodium to the core	MANU_COOL	$5 \times 10^{-1}$
Strenght of the cladding	CORE_CLAD_STREN	$1 \times 10^{-2}$

Table C.1: PRA: basic events

## 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] R. J. GARCIER AND Y.-F. L. LAY, *Déconstruire superphénix.*, *EspacesTemps.net*, (2015).
- [7] IAEA, *Power reactor information system - superphenix.*  
<https://www.iaea.org/PRIS/CountryStatistics/ReactorDetails.aspx?current=178>.  
Accessed: 2016-09-02.
- [8] T. KURTOGLU AND I. Y. TUMER, *FFIP: A framework for early assessment of functional failure in complex systems*, *International conference on Engineering Design*, (2007).
- [9] 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.
- [10] 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).
- [11] A. N. SOCIETY, *Fermi-I: New Age for Nuclear Power*, *American Nuclear Society*, 1979.
- [12] R. B. STONE, I. Y. TUMER, AND M. V. WIE, *FFDM: The function failure design method*, *Journal of Mechanical Design*, (2005).

## BIBLIOGRAPHY

---

- [13] R. B. STONE AND K. L. WOOD, *Development of a Functional Basis for Design*, Journal of Mechanica Design, 122 (2000), pp. 359–370.
- [14] D. VAN BOSSUYT AND I. RAMP, *Toward an automated model-based geometric method of representing function failure propagation across uncoupled systems*, ASME, (2014).
- [15] A. VERDIER, *Évaluation de la sous-criticité lors des opérations de chargement d'un réacteur nucléaire REP*, 2005.
- [16] 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).