Construction of a generic PSA model for Swedish BWRs

Based on SSMFS 2008:17 design requirements for Swedish BWRs

Master's Thesis in Nuclear Engineering

ROGER HURTIG

Division of Nuclear Engineering
Department of Applied Physics
Chalmers University of Technology
Gothenburg, Sweden 2015
CTH-NT-310

ISSN 1653-4662

CTH-NT-310

Construction of a generic PSA model for Swedish BWRs

Master's Degree Thesis
Master's Program in Nuclear Engineering
CHALMERS UNIVERSITY OF TECHNOLOGY

ROGER HURTIG

Department of Applied Physics
Division of Nuclear Engineering
CHALMERS UNIVERSITY OF TECHNOLOGY

Gothenburg, Sweden 2015

Construction of a generic PSA model for Swedish BWRs
Master's Degree Thesis
ROGER HURTIG

Master's thesis
CTH-NT-310
ISSN 1653-4662
Department of Applied Physics
Division of Nuclear Engineer
Chalmers University of Technology
SE-412 96 Gothenburg
Sweden
E-mail: hroger@student.chalmers.se

Cover:
Oskarshamn 2
http://www.okg.se/sv/Press/Bildbank/

Master's thesis in Master Program in Nuclear Engineering
ROGER HURTIG
Department of Applied Physics
Division of Nuclear Engineering
Chalmers University of Technology

Abstract

The focus of this study is to develop and document a generic PSA model, based on SSM deterministic design requirements. The objective is to be able to use this model as a benchmark tool in the evaluation of new methods for probabilistic safety analysis, or in the evaluation of new design requirements.

Three designs that fulfill SSMF 2008:17 design requirements were constructed and implemented into the computer code RiskSpectrum. The results from RiskSpectrum were compared to the results available in the safety reports of Oskarshamn 1, 2 and 3.

The conclusions of this thesis are that the results show consistency between construction 1, 2 and 3. Sensitivity analysis of the probabilistic results demonstrates that the PSA models 1, 2 and 3 are robust. A robust concept can operate without failure under a variety of conditions. The study also indicates that models based SSMFS 2008:17 design requirements can lead to a design that is fire resistant. Both construction 1 and 3 live up to the requirements that are essential to represent the generic PSA model, however, construction 3 is more suitable as a benchmark tool as extraordinary fire mitigation measures do not need to be taken into consideration. Lesson to be learned is that one generic design/construction that fulfills SSMFS 2008:17 requirements may satisfactorily describe the plant and provide results with a sufficient level of details. Therefore future efforts should be directed towards the development and use of generic design/PSA models.

Acknowledgements

I would like to thank the colleagues on OKG; especially my thesis advisor Pär Lindahl and PSA specialists Michael Landelius and Lovisa Nordlöf for taking time to answer my questions and providing solutions when it was needed. I would also like to thank Morgan Lindqvist for the help with the construction requirements.

Table of contents

1 Introduction

1.1 Background

1.1.1 About OKG

OKG was founded in 1965 and today owns and operates three nuclear reactor units – Oskarshamn 1 (O1), Oskarshamn 2 (O2) and Oskarshamn 3 (O3) – which together account for ten per cent of the total electricity generation in Sweden.

1.1.2 Safety Analysis for Nuclear Power Plants

Safety Analysis of Nuclear Power Plants (NPPs) is based on two different approaches that may complement each other. One approach is deterministic: the physical response of the system is simulated under transient/accidental conditions using deterministic codes. In this case, the objective is to investigate the variation of reactor parameters relevant to safety and show if the requirements on the system design are fulfilled. The second approach corresponds to the so-called Probabilistic Safety Analysis (PSA) which is primarily used to calculate quantitative measures of risk such as core damage frequency and large release frequency. The current work focuses on the latter.

1.2 Scope of the thesis

The purpose of this master thesis is to develop and document a generic PSA model, based on SSM[1] deterministic design requirements. Such PSA model would be a valuable tool in the evaluation of new methods of probabilistic safety analysis or the evaluation of new design requirements.

The advantage of using a generic model compared to using plant models is that the generic model is relatively simple and transparent. The generic model has no connection to the plant-specific conditions so the results are generally valid for facilities that meet or that will fulfill SSM requirements.

The objective is to build a generic PSA model mainly based on SSM deterministic design requirements.

1.3 Methodology

This thesis is divided into four stages.

- The first stage is to familiarize and interpret the design requirements from SSMFS 2008:17 that provide the conditions for the generic PSA model.
    - How many designs are required to obtain a generic set of models for Swedish BWRs?
- The second step is to construct the actual PSA model with the use of the computer program RiskSpectrum[2].
    - PSA Level 1 analysis – which initiating events have the largest effect on the core damage frequency?
    - Is there any significant difference between different generic models?

[1] SSM is the Swedish Radiation Safety Authority

[2] RiskSpectrum is an advanced fault tree and event tree software tool licensed for use at half of the world's nuclear power plants. [46]

- The third step addresses the analysis of the results of the preparatory work in step 1 and 2. This is done by making use of RiskSpectrum and by possibly comparing of the results with the corresponding PSA results in the safety reports for plants O1, O2 and O3.
    - Can the developed generic PSA models represent O1, O2 and O3?
- The fourth step involves the validation of the generic PSA-models by comparing them with the results obtained from a safety evaluation method developed by OKG.
    - Are the generic PSA-models robust?

1.4 Abbreviations and definitions

The main abbreviations that are used in this document are summarized in Table 1.1. Definitions of relevant and basic concepts are reported in Table 1.2.

Table 1.1: Main abbreviations.

Term	Explanation
BC	Boundary Condition
BWR	Boiling Water Reactor
CCF	Common Cause Failure
CCI	Common Cause Initiator
CET	Containment Event Tree
DSA	Deterministic Safety Analysis
FMEA	Failure mode and effect analysis
HS	Core Damage
HS1	Core damage due to loss of reactivity control
HS2	Core damage due to loss of core cooling
HS3	Core damage due to loss of residual heat removal
HS4	Core damage due to overpressure
IAEA	International Atomic Energy Agency
IE	Initial Event
LOCA	Loss of Coolant Accident
MCS	Minimal Cut Sets
PDS	Plant Damage State
PSA	Probabilistic Safety Analysis
SAR	Safety Analysis Rapport
FC	Fractional Contribution
RIF	Risk Increase Factor

Table 1.2: Relevant definitions.

Term	Explanation
Basic event	""The basic event" in a fault tree model for which no further development of the fault tree logic is made. It is the selected system boundary for the level of detail in the model." [34]
Significance Analysis	"The process to calculate the significance (impact) different basic events or groups of basic events has on the result. Different types of relevance metrics are used to analyze the significance of all the important basic events. Examples of important dimensions are Fractional Contribution (FC) and Risk Increase Factor (RIF). The significance of the basic events are translated to the importance of the plant input components and systems." [34]

Fire cell	Fire is assumed to not be able to spread further than the limits of the fire cell. [34]
CCF	"Multiple faults that occurs simultaneously or in a short period of time and can be attributed to the same cause." [34]
Fault tree	"A tree structure that starts with a predefined top event which is logically broken down to possible causes. " [34]
Frequency	"Frequency is the expected number of errors for a time period. The term frequency in PSA is the term for a time-independent value for an event that is usually used for initiating events, which are usually described with unit events per year." [34]
Function event	"Function event is a safety function or an event such as fire or explosion in an event tree. In PSA Level 1 it is typically a safety function which is challenged due to a disturbance in normal operation. A probability of its outcome (for example, safety function fails or explosion occurs) can be connected to the function event." [34]
Generic data	"The fault data collected and compiled from several plants." [34]
Event Tree	"A logic diagram that starts with an initial event and covering all scenarios determined by analyzing the function events and consequences." [34]
Core damage	Damage to the reactor core as a result of any of the following consequences: HS1, HS2, HS3 and HS4.
Initiating event	"Initiating event is a disturbance that starts a sequence that requires safety systems." [34]
Component	"A unit in a nuclear power plant such as tank, pump, valve or switch." [34]
LOCA	"Loss of Coolant Accidents is events that lead to loss of coolant for example through pipe break in the primary system." [34]
PSA level 1	"Identification and quantification of the sequences leading to core damage." [34]
PSA level 2	"Identification and quantification of the sequences leading to a radioactive release" [34]
Boundary conditions	"A boundary condition reflects the conditions for which the analysis is carried out. The boundary conditions are controlled by boundary condition sets in RiskSpectrum. " [34]
Risk	"Risk is an entity which is an aggregate of the probability and consequences of a given event." [34]
Fraction Contribution	"Fraction contribution indicates the proportion of the total result which depends on the initiating event or group of initiating events." [34]
Risk Increase Factor	"Risk increase factor indicates how much the total result would increase if the current basic event always fails, i.e. the probability of 1." [34]
Area event	"Area event is an initial event that occurs outside the process but within the plant buildings. Primarily, this is internal fire and internal flood." [34]
Sequence	"A sequence describes a sequence of events in an event tree which starts with an initiating event and concludes with a consequence." [34]
Transient	"Transients is a generic name for all events (except LOCA) leading to imbalance between input and abducted heat in reactor core." [34]
Grace time	A design principle for Swedish BWRs is that no operator actions shall be required within 30 minutes after an initiating event. Therefore no operator actions are credited within 30 minutes in analysis. Known as "Rådrumsregeln" in Swedish.

1.5 Basics of a general Boiling Water Reactor

The basic design of a typical Boiling Water Reactor can be seen in Figure 1.1. Heat is produced via nuclear fission reactions that are obtained from the splitting of uranium atoms with neutrons. The uranium is contained in the so-called fuel rods that are arranged in the nuclear reactor core. Cooling water flows throughout the core and steam is generated by the energy released in the nuclear process. The steam-water mixture leaves the top of the core and enters the moisture separator. Water droplets are removed before the steam is directed to the turbine through the steamline. The turbine is connected to the electricity generator. The pressure difference caused by the steam makes the turbine blades rotate and thereby producing electricity that is transported out through the electrical grid.

The steam temperature is much lower after passing the turbine but not low enough to become water. The unused steam is thus fed into a condenser consisting of a large number of narrow pipes that is filled with sea water. The sea water is pumped through the pipes and back out into the sea. The water from the condenser is pumped back into the reactor to be heated again. The water is circulated using electrically powered pumps. These pumps and other operating systems in the plant receive their power from the electrical grid. If offsite power is lost, emergency cooling water is supplied by other pumps, which can be powered by onsite diesel generators. The water that is in the reactor system forms a closed cycle and is never in direct contact with the sea water. [48]

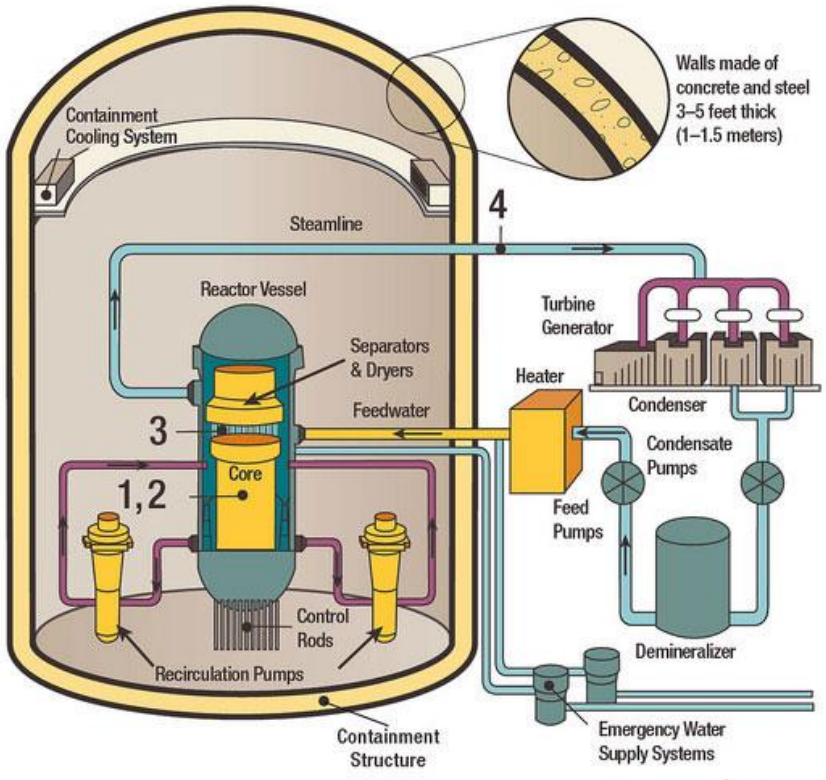


Figure 1.1: Typical design concept of a commercial BWR. [47]

Multiple barriers and safety systems are constructed to prevent radiation and radioactive substances from affecting the surrounding, figure 1.2 displays the barriers and provides a sense of the size of them.

The first barrier is the fuel which consist of *ceramic uranium pellets* that have low solubility in water, air and binds the radioactive substances. The second barrier is the *cladding tubes* that are made of *zirconium alloy*. This metal alloy tube surrounds the uranium pellet and is completely gas-proof. The third barrier consists of the *reactor tank and associated pipe systems*. The reactor tank is made of 15-20 cm thick steel and weighs around 400 tons. The fourth barrier is the *reactor containment* that surrounds the reactor. It is made of meter-thick concrete with infused gas-proof steel plates. The fifth barrier is the *building itself* (aka *secondary containment*). The building is designed to withstand strong forces from both inside and outside. More detailed information will be provided in chapter 2.1. [48]

There are also multiple safety systems that are protecting the barriers to be overrun, more detailed information will be provided in chapter 2.3.

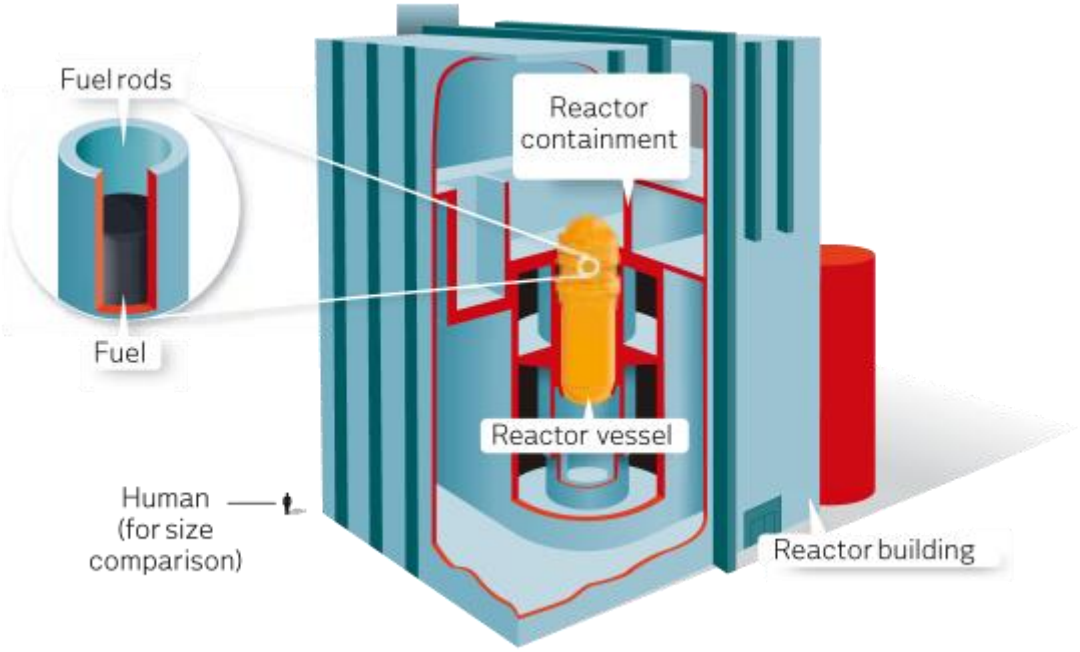


Figure 1.2: Safety barriers in a BWR. [48]

1.6 Structure of the thesis

The report is structured as follows. In Chapter 2 and 3 the theory and the SSM requirements for Boling Water Reactors are described. In Chapter 4 the model that has been developed and the results are discussed. In Chapter 5 conclusions are drawn and future work is illustrated.

2 Theory

2.1 Barrier

For protection against the release of radioactive fission products into the environment the concept of defense in depth is applied. This consist of the implementation of several physical barriers between the radioactive substances and the environment, and engineering features (safety functions) that can preserve the integrity of the barriers under a wider spectrum of possible conditions (see figure 2.1). If integrity is lost for a barrier then the next barrier will still work. The barriers are the fuel pellet ceramic crystal structure, the fuel cladding, the reactor primary system, the reactor containment and the secondary containment. [1]

The safety functions ensure that barrier design limits (mainly related to pressure and temperature) are not exceeded. In addition, there are systems that will protect the reactor containment and mitigate the impact on the environment if the barriers would not work as intended in highly improbable event combinations. [1]

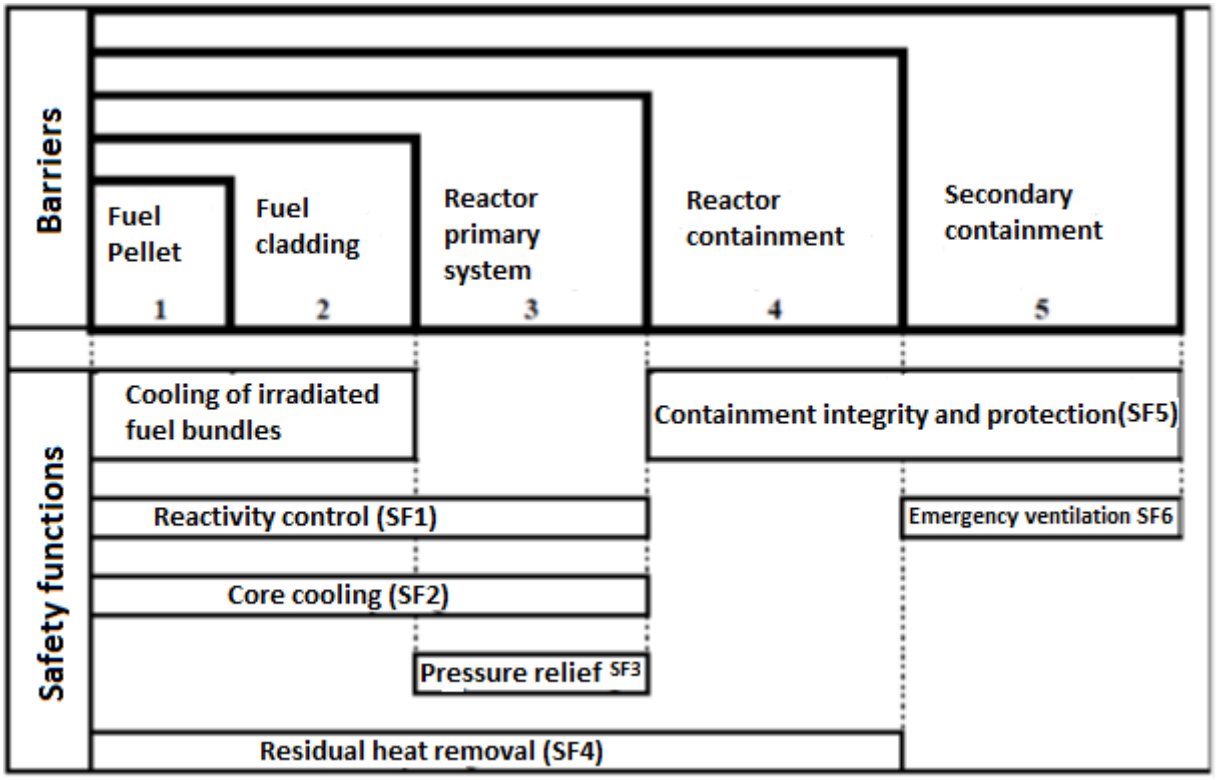


Figure 2.1: Relationship between barriers and safety functions.

2.1.1 Fuel pellet and the fuel cladding (barrier 1 and 2)

The first barrier "Fuel pellet matrix" and the second barrier "Fuel cladding" is protected by the safety functions "Reactivity control", "Core Cooling" and "Residual heat removal". Reactivity control function limits the power production of the fuel by interrupting the chain reaction, after which only the decay heat is generated. Core cooling and residual heat removal limits the temperature of the fuel and cladding and thus also in the third barrier, reactor primary system (RCPB). Irradiated nuclear

fuel bundles stored in fuel pools are protected by the safety function "cooling of irradiated fuel bundles". [1]

2.1.2 Reactor primary system (barrier 3)

The third barrier "reactor primary system" consists of the reactor tank and connecting piping through the outer shell valves. The reactor primary system is protected against overpressure mainly by the safety function "pressure relief of the reactor primary system". [1]

2.1.3 The reactor containment (barrier 4)

The fourth barrier "The reactor containment (RI)" consists of the containment shell with grommets and stop devices such as dome, person gates, isolation valves and blind flanges. [1]

In the case of a pipe break or other events that can lead to a damage of the core, isolation valves can be used to isolate the containment and avoid possible radioactive leakages through the barrier. This isolation function depends on the room monitor chains. [1]

Following a pipe break of the reactor primary cooling system, the structural integrity of the reactor containment is dependent on the PS function (Pressure-Suppression principle). The PS function means that the steam flowing out and pressurizes the primary space through the vent tube is forced down below the surface of the condensation pool in the secondary space. The condensation pool can store a large amount of energy supplied in a very short time. This stored energy can then be carried away by the cooling chain for the condensation pool to the ultimate heat sink, e.g. the sea. [1]

The PS function with condensation pool and its cooling system has as main tasks to limit the pressure increase so that the design limit for the containment is not exceeded. The containment atmosphere should be treated after a possible internal pipe break in order to bring down the amount of airborne activity and prevent hydrogen fire. [1]

2.1.4 Secondary Containment (barrier 5)

The fifth barrier "Secondary Containment", consists of the reactor building's exterior walls with doors, gates and ventilating grommets. Its function is to limit soil emission in all the events that belong to the event class H2-H4[3], and it depends on the "emergency ventilation" which isolates the reactor building and maintains directed flow paths for filtered emission through the chimney. Barrier integrity is protected primarily by the isolation of the pipe breaks outside the reactor containment and by passive protection features such as prepared blow paths and flooding paths. [1]

2.2 Safety critical structures

Safety-critical structures include such structures that are crucial for maintaining barriers and safety features. This section describes fire management and flood protection. [1]

2.2.1 Fire protection

The fire protection has the task, in addition to conventional personal and property protection, to prevent third parties from damage by ionizing radiation from radioactive releases caused by fire. This

[3] See chapter 2.5.1 for overall description of event class H2-H4.

means that the barriers and safety functions that are necessary to prevent unacceptable releases must not be compromised in a fire. [1]

The principle of defense in depth is also applied to the area of fire protection where it is interpreted according to the following three lines of defense:

1. Fire should be prevented by *minimizing the combustible substances and reducing and controlling ignition sources*.
2. Fire that arises should be quickly detected and extinguished in order to limit any damage by *fire detection systems, fire extinguishing systems and manual actions.*
3. Fire that has not been extinguished shall be prevented from spreading to the safety functions. In view of this, the plant design needs to be consistent with specific *fire technical requirements for surface layer and installations, distance separation and fire cell and fire zone division.* [1]

Dividing the building into separate fire zones and compartments contributes to a facility that is single failure tolerant and common cause failure (CCF) tolerant. [3]

2.2.2 Protection against internal flooding

Plant protection against internal events including flooding shall prevent damage to the barriers and safety functions, so that unacceptable releases can be avoided after the primary event. This means that the protection function should isolate the rupture site and divert water emanated. [1]

The plant flood protection consists of both passive and active functions. Structural design and layout is such that, regardless of the rupture site and rupture size, only one of the redundant subsystems belonging to a safety function may be affected by the escaping water. The intended runoff pathways through floor drainage system, unloading hatches, doors and shafts, limit the water level in the respective areas, thus also limiting the load on the current building structure. A prerequisite for the passive flood protection is that the tightness between separating parts of the building is maintained. The priority action in the case of pipe break outside the reactor containment is to isolate the location of the rupture instead of restricting coolant loss from the reactor. [1]

2.3 Safety functions (Barrier Protective Functions)

The barrier protective functions that are required shortly after an initial event are automatically initiated by the reactor protection system. [1]

The need for safety functions is dependent on the initial event and the need of functioning also varies. The safety functions and the logics that come into play during an accident depends on the initiating event and the time after its initiation. [1]

The basic safety functions shall be able to manage all initial events that are related to classes between H2 and H4 (see section 2.5.1). There is mitigating functions for initiating events in class H5 and for situations where the safety functions completely fail. The latter determine the extent of the radiological releases to the environment. [1]

Every initial event places specific demands on the various safety functions which constitute protection against reactor core damage. The initial events may be grouped according to various characteristics, such as likelihood of occurrence and with respect to the required safety functions. [1]

2.3.1 Reactivity control (SF1)

The reactivity control safety function interrupts the nuclear chain reaction any time an event of class H2 to H4 occurs. Moreover, this system is capable to keep the reactor subcritical. The safety function protects primarily the fuel pellets and the cladding against overheating, but is also a prerequisite for the integrity of the containment barrier. [1]

Reactivity control is performed during operation by means of the movable control rods (system 1 for SF1) and the speed of the main circulation pumps. These functions are also used for all events in the event classes H2-H4. Additionally there is a system for automatic pumping of boron solution (system 2 for SF1). [1]

2.3.2 Core cooling (SF2)

The core cooling function should supply water to the reactor vessel in sufficient quantities to ensure core cooling. [1]

The core is normally supplied with coolant by the feed water system (System 1 for SF2). There are two functions with different pressure set and dilute feed capability for supply of water to the reactor vessel in all events with the exception of the earthquake in the event classes H2-H4. [1]

Auxiliary feed water system (system 2 for SF2) can, with two of four identical but physically and functionally separate circuits, supply the reactor with water after a small pipe break or after an expected event that causes interruption in the main feed water flow. [1]

2.3.3 Pressure relief of the reactor primary system (SF3)

A pressure relief system is implemented to ensure the integrity of the primary coolant system, i.e. the primary system should be able to maintain its pressure and load carrying capacity without leakages. The ordinary pressure relief system has the capability to limit the pressure in the reactor primary system up to 110% of the design pressure in the event class H2-H4. [1]

Pressure relief should also limit the pressure in the reactor primary system to:

- 120% of design pressure for an expected event (H2) and common cause failures (CCF) in the reactor shutdown system, for example, complex sequences that lead to missed hydraulic scram "(system 1 for SF1) or non-automatic pumping of boron solution (system 2 for SF1) .
- 130% of design pressure for expected events H2, non-expected events H3 (pipe break excluded), and common cause failures of the regular pressure relief.

Pressure relief with (System 1 for SF3) is activated partly by events that are expected to increase the pressure in the reactor, partly when high pressure has been reached. An operational disturbance initiates (system 2 for SF3) pressure relief valves which are activated by electricity, the system is dependent on the power level. A number of additional safety or pressure relief valves can open at higher pressure set-points. This includes spring based impulse valves which are activated by system pressure. [1]

2.3.4 Residual heat removal (SF4)

Residual heat removal and/or emergency core cooling ensures core cooling immediately after a disturbance, such as abnormal conditions occurrence and/or reactor core shutdown. In a longer perspective, the core decay heat must be transferred to the final heat sink. [1]

By restricting the pressure and temperature shall the safety function "residual heat removal" mainly protect the fuel and its cladding, but also the barriers “reactor primary system” and the “containment integrity”. In addition, the reactor can be cooled down to atmospheric pressure within a reasonable time after a disturbance. [1]

Residual heat removal is accommodated in most anticipated events by the steam turbine condenser that is cooled in (System 1 for SF4) by seawater. The residual heat removal is done through steam bubbling with (System 2 for SF4) to the condensation pool when the turbine condenser is not available. [1]

2.3.4 Containment integrity and protection (SF5)

Containment integrity and its protection shall reduce activity releases to the environment in the event class H2-H4 which caused previous barriers to be broken. The primary tasks in an internal pipe break are to isolate the reactor containment and prevent the increase in pressure that can impair the integrity of the containment. In addition, the reactor containment atmosphere is treated to limit the amount of airborne activity and prevent hydrogen fire during events associated event class H4. The task in case of outer pipe break is to insulate the site of the fracture in order to limit the coolant loss from the reactor. [1]

The surveillance chains (system 1 for SF5 or System 2 for SF5) initiate active functions that are needed for isolation and protection of the reactor containment immediately after an initial event. Other safeguards necessary as a prerequisite for successful containment function are initiated depending on the triggering condition. [1]

In case of pipe break in the reactor containment or other event that trigger the surveillance chain, all scale and insulation valves are closed with the exception of those valves needed for the instrumentation, the scram, the core cooling, and the systems (1 and 2 of SF5). [1]

2.3.5 Emergency ventilation (SF6 at PSA level 2 analysis)

The objective of the emergency ventilation system is to limit the amount of radioactivity released by isolating the reactor building and filter the exhaust air prior to emission through the main chimney. [1]

Isolation of the secondary containment (i.e., the reactor building) and start of emergency ventilation means that the normal ventilation is stopped and insulation damper closes. Fans in System 1 or 2 for SF6 are started and create a powerful under-pressure in the reactor building. The evacuated air is passed through filter banks, where most of the iodine content and particles are removed. [1]

2.3.6 Cooling of irradiated fuel bundles (incorporated in SF4)

Effective cooling shall be provided for irradiated fuel bundles so that the fuel pellet and the fuel cladding barriers are properly protected. This includes both the irradiated and exhausted fuel that is stored in the fuel pools, and the irradiated fuel in the reactor tank. The temperature of the water pool is restricted to ensure adequate water coverage. [1]

Cooling of irradiated fuel bundles are continuously in operation and is thus not initiated. The pool cooling shall manually be switched over to specific cold chain, in case of failure of the cooling system. [1]

2.4 Design basis events and acceptance criteria

The design and the operations of a nuclear reactor should take in account a variety of possible conditions. These conditions range from various normal operating modes to highly improbable events that may cause severe damage of the core. The different operating conditions and different initial events that can occur, however, have very different frequency: from normal operational modes that occur during each year of operation down to very unlikely events that are estimated to occur with a frequency below once in a ten million reactor years. [4]

In this context a balanced risk profile of the plant is estimated. The risk is defined as the product of frequency and consequence. Consequences are primarily related to radiological ambient effects, radiological impact on personnel, and to the re-qualification of the facility after the event. Therefore the expected state (events with high frequency) allows extremely limited consequences while the hypothetical state (events with very low frequency) allows larger, but still acceptable, consequences. [4]

A balanced risk profile can generally be achieved by using event classification. In fact one divides different operating conditions, events or event sequences in different classes where each class includes events within a given frequency range. Each class is characterized by proper acceptance criteria (i.e., the consequences of events of the same class do not have to exceed the same limits). The effectiveness of the barriers and of the defense-in-depth strategy needs to be demonstrated with a careful analysis. [4]

2.5 Requirements for event classification

To analyze the safety of Swedish nuclear plants, initiating events shall be considered in the deterministic safety analysis, according to the approach described in the Radiation Safety Regulations SSMFS 2008:1 [5]. The different operating situations, events and event sequences that a facility may face are divided into event classes [4]. The event classes cover normal operation, anticipated events, unanticipated events, unlikely events and highly improbable events. In the analysis of events that have not been considered in the reactor design, customized assumptions and acceptance criteria may be applied (beyond design basis accidents) [3]. Events that do not fall into the general system of event classes linked to the analysis assumptions are handled as beyond design basis event. [4]

The selection of the initiating events should be based on probability analysis. Some initiating events should be included as postulates, to verify the robustness of the plant design, regardless of the likelihood of these events to occur. Examples of such an event are loss of coolant at a break in the biggest pipe or at a location adjacent to the reactor pressure vessel. [3]

The safety analyzes should be based on a systematic inventory of the events, sequences of events and conditions that could lead to a nuclear accident (SSMFS 2008:1 Chapter 4, § 1). [5]

The methodology for event classification has been based on ANSI/ANS 52.1-1983. [4]

For each event class defines acceptable consequences. This is done mainly by indicating how much impact that can be allowed on the barriers to release of radioactivity. The acceptable consequences are usually stated as limits for critical parameters which must not be passed as a consequence of the event. Acceptable consequences that can be quantified in such values are called acceptance criteria.

These acceptance criteria include the requirement prerequisites and methodology that will be used to confirm that the critical parameters meet the acceptance criteria. [4]

In the design of nuclear power plants it is taken into account events with very low probability as part of the defense in depth principle. However, there is a probability level that is so low that it can be practically neglected. This probability level is usually called "Extremely improbable events (residual risks)" according SSMFS 2008:17 [3]. The reason for that, in this way one may neglect a large reactor tank rupture is that one have done everything reasonably practicable to prevent this from happening. [4]

2.5.1 Initiating events and event classification

An initiating event is defined as a process disturbance that requires one or more automatic or operator initiated action to shut down the reactor and / or bring the facility to a safe and stable condition. Failure to take action entails significant risk of an accident with damage to the core / fuel. Initiating events is normally divided into internal and external events that reflect the origin of an event. [30]

The identification of initiating events is an important part of a PSA. IEs directly affect the core damage frequency in PSAs. [29]

The Swedish regulations given in SSMFS 2008:17 [3] identify five event-classes[4] according to the frequency limits.

2.5.1.1 Normal operation (H1)

Normal operations include disturbances which are controlled by the usual operating- and control-systems without interruption. [3]

The frequency is such that these occurrences can be considered as normal operating modes. [4]

2.5.1.2 Expected events (H2)

These events are expected to occur during a nuclear reactor lifetime. [3]

The frequency is smaller than **10^{-2} per year**. This value should be used as a way to assess whether other identified initiating events other than the examples given in a prescribed list falls within the event class H2. [4]

2.5.1.3 Unanticipated events (H3)

Unanticipated events are not expected to occur in a nuclear reactor lifetime, but can be expected to occur if multiple reactors are considered. [3]

Their frequency F is between **10^{-2} and 10^{-4} per year**. This value should be used as a way to assess whether other identified initiating events other than the examples provided by the nuclear authority falls within the event class H3. [4]

[4] Classification of events made in safety assessment and reflecting an expected probability of an event occurring and affecting reactor functions. [3]

2.5.1.4 Improbable events (H4)

This category groups events that cannot be expected to occur. It also includes a number of overall events (despite their frequency) that are analyzed to verify reactor robustness. These events are often called design basis events. [3]

The frequency is between **10^{-4} and 10^{-6} per year**. This value should be used as a way to assess whether other identified initiating events other than the examples provided by the nuclear authority falls within the event class H4. [4]

2.5.1.5 Highly improbable events (H5)

Highly improbable events are not expected to occur. If the event should nevertheless occur, then it can lead to significant damage to the core. These events form the basis of the mitigating systems that may be used during severe accidents. [3]

The frequency of events H5 is between **10^{-6} and 10^{-7} per year**. This event class includes events that are taken into account as they may pose a significant risk to the environment. This can mean either that the events in question have an excessive impact on core damage frequency according to the PSA studies or that the consequences for the environment, if they should occur without current protection is in place, would be unacceptable. [4]

2.5.1.6 Extremely improbable events (residual risk)

Events that is so improbable that they need not be taken into account as initiating events in connection with safety analysis. [3]

Frequency is larger than **10^{-7} per year**. According to Government Decision No. 12 of 1986-02-27 and SSMFS 2008:17, sequences with very low frequency can be ignored for Swedish plants. [4]

2.5.1.7 Special events

Special events that do not fall into the above described general classification may be analyzed and special assumptions and acceptance criteria may be applied to them. [3]

2.6 Initiating events

2.6.1 Purpose of defining the initiating events

In the development of a comprehensive plant model for PSA a list of IEs, as complete as possible, is required. The consequences of ill-defined IEs are various. A missing IE in a PSA means that core damage frequency would be underestimated by the value of the IE frequency multiplied by the conditional probability of safety system failure given the occurrence of the IE. A larger list of IEs than necessary (for example, due to inappropriate grouping) would result in waste of resources because of the analyses of additional unnecessary accident sequences. An IE list that is incomplete or is insufficiently precise in its frequency determination would generally result in an incorrect estimation of the core damage frequencies. [29]

2.6.2 Internal events

The internal initiating events consist of three main categories:

- LOCAs
- Transients

- Special common cause initiating events (common cause initiators (CCIs)) [28]

2.6.2.1 LOCAs

The loss of coolant accident (LOCA) initiators includes primary system breaks resulting in loss of primary coolant. Pipe breaks and ruptures of different sizes, inadvertent opening and failures to re-close (stuck open) of valves are being considered in this category. [29]

2.6.2.2 Transients

Transients are a generic name for all the events that lead to imbalance between heat input and output in the reactor. [30]

The initiating events for transients are those which introduce the disturbance in normal plant operation, without loss of primary coolant and which require an automatic or manual shutdown of the reactor. Typical examples of transient initiators include disturbance in feed water flow, turbine/condenser, reactivity control, reactor recirculation, etc. Certain disturbances in some of the support systems will also fall into this category. [29]

In Table 2.1 the OKG description of the transients and the relative IEs is reported [30]. This description is based on the EPRI list [29].

Table 2.1: OKG description of IEs for transients.

ID	Name	Description
TF	Loss of feed water system	Fast stop as the result of loss of feed water. Turbine condenser is additionally regarded as unavailable.
TT	Turbine scram with dump prohibition	Fast stop resulting from the turbine scram. The normal heat sink (the turbine condenser) is additionally unavailable which means dumping prohibition of steam.
TS	Other scrams	It includes all fast stop events where the operating system is initially available. Used for instances of expected scram signal and with access to the feed water and the turbine condenser.
TE	Loss of off-site power	Loss of substation switchyard and loss of grid or feeders.

2.6.2.3 Special common cause initiating events

Initiating events due to special common cause are events which, in addition to requiring reactor shutdown, simultaneously disable one or more of the mitigating/safety systems required to control the plant status following the initiator. Typically, they are unique to the plant being analyzed. [29]

2.6.2.4 Hazards

Hazards are covered in section 3.7.

2.6.3 EPRI list of IEs

The lists of IE categories for BWRs and PWRs provided in EPRI-NP-2230 [49] and NUREG/CR-3862 [29] reports were used as the starting point for IE selection in a large number of PSAs. The lists are derived by analyzing operating experience of a few hundred reactor-years in the USA. Therefore, the

lists can be considered as one of the best sources for providing a generic IE list for PSA of a new plant of similar design and reasonably operating practice. [29]

Since there is a considerable difference between IEs in PWR and BWR plants, EPRI developed a separate IE list based on operating experience of plants with BWRs. The data for BWRs include 903 events occurring over 101 reactor years. [29]

2.7 Grouping of initiating events for BWRs

For each of the initiating events defined, an event tree, depicting the spectrum of plant responses in terms of failures and successes, should be made. Some of the initiating events would induce the same or a reasonably similar plant response. In that respect, the different IEs are grouped in order to decrease the amount of analyses required for PSA. [29]

The grouping of initiating events shall be made in such way that all events in the group impose essentially the same success criteria on the frontline systems as well as the same special conditions (challenges to plant operators or to automatic plant responses) and shall result in the same core damage state. Thus the grouped events can be modelled using the same event/fault tree analysis. [29]

Sometimes the amount of subsequent analysis needed may be further reduced by grouping together IEs that evoke the same type of plant response but for which the frontline system success criteria are not identical. The success criteria applied to that group of events would then be most demanding (in terms of required systems) for any member of the group. The savings in effort must be weighed against the conservatism which this approach introduces. [29]

2.8 Analysis conditions

2.8.1 General analysis conditions

Events of the classes H2-H4 are assumed to occur at the conditions within planned normal operation (H1), and they render the most challenging impact with respect to the acceptance criteria. Planned normal operation means that all equipment is operational and that the operating point is within the allowed boundaries. [4]

All required safety functions should be ensured during events from classes H2-H4. One should also take into account the impact that the event itself might have on the safety functions. [4]

2.8.2 Specific analytical conditions

In the analysis of initiating events specific assumptions about single faults, secondary faults, planned maintenance, corrective maintenance, testing, grace time, safety- and operational-functions, and loss of off-site power must be taken into account. [4]

2.8.3 Conditions for probabilistic safety analysis

In addition to deterministic analysis under General analysis conditions and Specific analytical conditions the facility shall be analyzed with probabilistic methods so that a more comprehensive understanding of its safety can be provided. [4]

2.9 Acceptance criteria

An acceptance criterion is a limit value for a plant parameter that can describe the state of a fission product barrier. If the acceptance criterion is exceeded, then the relative fission product barrier will fail. These limits are established by the nuclear authority. In order to demonstrate the safety of the plant, analyses shall be performed and shall show that the plant parameters satisfy such acceptance criteria. In this process the different event classes need to be considered. [3] [4] [5]

2.9.1 Normal operation, H1

For H1 all operating parameters that, in case of deviation from normal operating values, requires automatically triggered actions at certain limit values, should be monitored and be contained with an acceptable margin to these limit values. [4]

2.9.2 Anticipated events, H2

An event within this class shall not trigger a more serious plant condition, which causes any of the barriers to lose their function. The consequence for this class should usually be a rapid stop, followed by a short period of warm or cold shutdown where corrective action is taken, and normal operations are then reached again. [4]

2.9.3 Unanticipated events, H3

An event within this class shall not trigger a more serious plant condition, such as loss of the reactor containment barrier if this is required during or after the event, or a substantial increase in mass loss from the reactor core such as loss of core cooling, in addition to what's the results of the primary event. The consequence of an event in class H3 where the reactor is involved can be automatically scrammed. An event of this group may represent a time of decommissioning of the station as well as parts of the fuel cannot be reused. [4]

2.9.4 Unlikely events, H4

An event within this class shall not result in impacts on the safety functions required during / after the event, such as loss of the reactor containment barrier or loss of core cooling function. The consequence of an event in the class H4 is the automatic scram of the reactor. In view of an event of this group the station cannot be put into operation within a short time, and a larger portion of the fuel elements would be damaged to such an extent that they could not be used any longer. [4]

2.9.5 Very unlikely events, H5, and beyond design basis events

An event within this class shall not result in impact on the irradiated fuel bundle cooling required during / after the event, this function protects the irradiated and exhausted fuel that is stored in the fuel pools. The consequence of an event in the class H5 is the automatic scram of the reactor. In view of an event of this group the station cannot be put back into operation, and the fuel elements would be damaged to such an extent that they could not be used any longer. The main concern are the consequences for the environment, this is quantified in PSA level 2 studies. [4]

2.9.6 Acceptance Criteria (PSA)

The probabilistic safety analysis (that consists of a level 1 and a level 2), in combination with the risk of the events under study, is used as a basis to identify and evaluate weaknesses of the plant. Hereby is the OKG methodology for reactor safety technical evaluation (based on IAEA CB-5 Revision 2 May 1996) utilized. Accordingly, acceptance criteria for the facility as a whole are defined as "GOOD" or

"ACCEPTABLE". Moreover, Acceptance criterion for identified weaknesses are given as "NEGLIGIBLE" with respect to the safety significance. [4]

2.10 PSA (Probabilistic Safety Analysis)

The probabilistic safety analysis is based on two levels, namely:

- **PSA level 1**: A model of the plant, executed with fault tree technique, which quantifies the frequency of core damage based on various initiating events.
- **PSA level 2:** A model of the plant, executed with fault tree technique, which quantifies the frequency of the release of radioactivity to the environment at reactor accident starting from different initial events in the PSA level 1.

To perform this kind of analysis **RiskSpectrum** can be used. This is a software for PSA modeling and quantification. [25]

2.10.1 Sequence analysis PSA level 1

Sequence analysis in PSA level 1 is aimed at identifying all relevant initiating events and modeling possible event sequences. Sequence analysis is an iterative process where the questions within the sequence analysis may affect the analysis of initiating events, and especially the grouping of these. [19]

2.10.1.1 Establishment of block diagram

In the block diagram, each block represents a function that can be credited for bringing the station to a safe state. The function refers to the system function itself, the systems that perform the function and relative auxiliary systems.

The block diagram is structured in chronological order, so that the functions to be utilized first are on the left-side of the diagram, while functions that affect the state of the facility in long-term course are on the right-side. This means that each record begins with an initiating event, followed by the function that is needed right after the initial event, and so on.

Figure 2.2 shows the principles of the block diagram used in the model. Successful function is illustrated with a line out to the right from the function block. Failed function is drawn with dash down. The block diagram is developed until a final state is reached. This means that the plant has either reached a safe end state; to the right in the diagram, or that the sequence ends in an unwanted end state with core damage. [19]

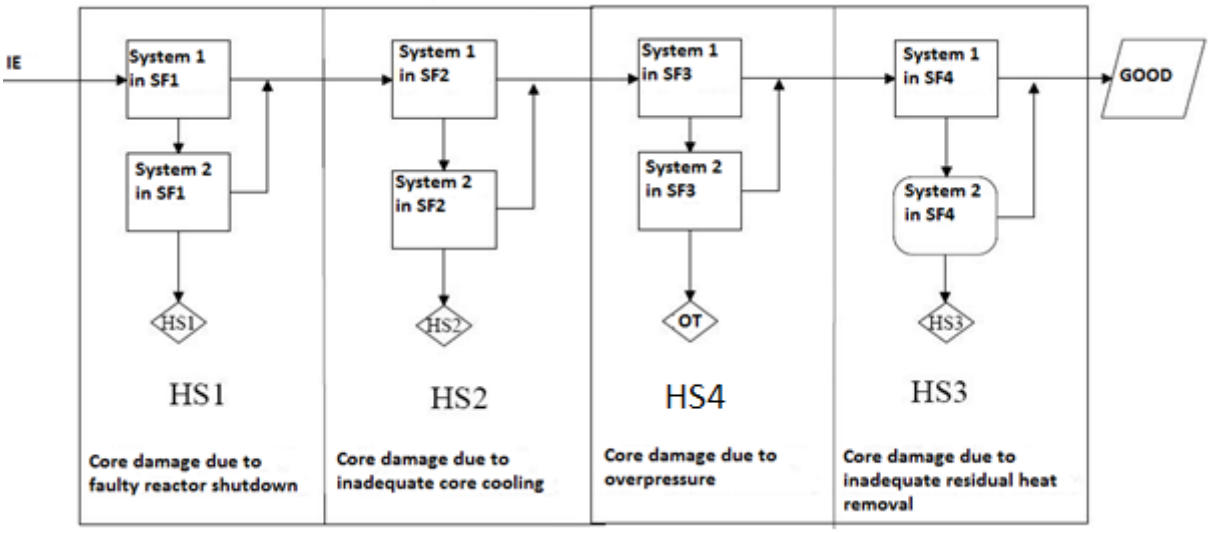


Figure 1.2: The principles of the block diagram used in the model.

2.10.1.2 Modelling of event tree

Block diagrams serves as basis for creating event trees. The various functional blocks correspond to nodes in the event tree. In the left is the initiating event. From each node there are two possible branches: the upper branch is followed when the function succeeds while the lower branch occurs when the function fails. To each branch a probability is associated. Branches (nodes) for pass/fail function are created for each function. The final state of each event sequence will be the final condition described in the block diagram. Figure 2.3 demonstrates the event tree for construction 2 with the initiating event Fire. Calculated frequency and set consequences can be seen on the right side. [19]

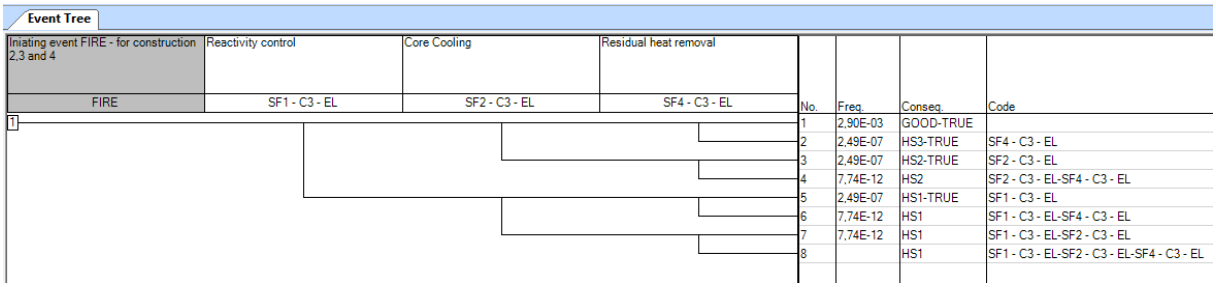


Figure 2.3: The principles of an event tree at level 1.

2.10.1.3 Safety level

The probabilistic safety target for the facility is established as lower than 10^{-4} year^{-1}. Four levels are defined for the total core damage frequency f_{GN}^{HS}.

- A **GOOD** safety level means that the calculated core damage frequency f_{GN}^{HS} is **significantly** lower than the safety target. The limit value to be applied depends on the uncertainty in the frequency estimation. The calculated frequency should be less than the safety goal by at least a factor of 10, i.e. $f_{GN}^{HS} < 10^{-5}$ year^{-1}.
- An **ACCEPTABLE** safety level means that the calculated core damage frequency f_{GN}^{HS} is **slightly lower** than the safety target, although not lower than the "significance threshold". $10^{-5} \leq f_{GN}^{HS} < 10^{-4}$ year^{-1}.

- A **QUESTIONABLE** safety level means that the calculated core damage frequency f_{GN}^{HS} is **slightly higher** than the safety target, but not higher than the limit for significant deviation. $10^{-4} \leq f_{GN}^{HS} < 10^{-3}$ year^{-1}.
- An **UNSATISFYING** safety level means that the calculated core damage frequency f_{GN}^{HS} is **significantly higher** than the safety objective. Which limit to be applied depends on the uncertainty in the frequency estimation. Typically this means that the calculated frequency exceeds the safety goal by at least a factor of 10, i.e. $f_{GN}^{HS} \geq 10^{-3}$ year^{-1}. [24]

2.10.2 Result evaluation

The PSA tool can be used directly to evaluate the question at issue effect on the defense in depth. Possible differences between the deterministic and probabilistic evaluation must be interpreted on a case by case basis. A few examples of possible reasons for the differences are presented below:

- Result: Deterministic evaluation indicate lower safety significance than probabilistic evaluation.
    - Possible interpretation: Failure in the safety concept has been identified with the help of PSA.
- Result: Probabilistic evaluation indicate lower safety significance than deterministic evaluation.
    - Possible interpretation: The PSA model is not detailed enough to describe all the relevant plant effects due to the question at issue.

Assuming that the plant PSA model is detailed enough and that the quality of input data is sufficiently high, this tool can be used to quantitatively evaluate the safety concept as such. [24]

2.10.3 CCF modeling

2.10.3.1 CCF groups

Common Cause Failure may affect identical trains/components. In practice, common cause failures are only interesting when such failure results in redundant trains becoming weakened or inaccessible.

CCF groups are generally based on identical components from different redundant trains that are part of one of the facility's identified system, for example System 1. [26]

2.10.3.2 CCF fault tree

CCF is implemented in the fault tree by creating a CCF fault tree consisting of gates and CCF-basic events. CCF-basic events are based on information about the original basic events that are included in the CCF groups, as well as the CCF model with corresponding parameters. [26]

2.10.3.3 CCF models

The α-factor model is the mainly used model in Swedish PSA studies for modeling and calculation of so-called low-redundant CCF (up to combinations of four simultaneous failures) and ECLM (Extended Common Load Model) for the so-called high-redundant CCF (combinations with more than four concurrent errors).

The method to calculate the probabilities for the various CCF basic incidents depends on the CCF model being used and the parameters that represents that model. This study will use the α-factor model, and the relative parameters are shown in Table 2.2. [26]

Table 2.2: α-factor model with associated parameters. [26]

CCF model	CCF parameters
α-factor model	$\alpha_1 = 1-(\alpha_2+ \alpha_3+ \alpha_4)$
	α_2
	α_3
	α_4

2.10.3.4 CCF data

CCF data is required to calculate the probability of the CCF basic events. Generic α-factors for group size 2 to 4 are obtained from NUREG/CR-5485 Table 5.11. These generic α-factors are displayed in Table 2.3. Values are obtained from Table 6 in the source [26]. One should be aware that NUREG has based the α-factors on a two train system, α (3, n) and α (4, n) has been calculated from these values. [26]

Table 2.3: The generic α-factors that are used in the α-factor model. [26]

Group size	α (1,n)	α (2,n)	α (3,n)	α (4,n)
4	0,950	0,021	0,010	0,019
3	0,950	0,024	0,026	-
2	0953	0,047	-	-

2.11 Delimitations

Following delimitations were done in order to get a list of initiating events as complete as possible. Support for completeness of IE lists is obtained from the large size of the IE lists. Most full scope PSAs use a list of over 40 IEs that cover LOCAs of all sizes, transients and CCIs of all relevant support systems. These IEs are then grouped into broad categories which are therefore less sensitive to the failure to include a particular IE. [29]

2.11.1 IE list for this study

The IE list for internal events was divided into three main categories. Each category was divided into more specific groups. All was done according to recommendation from IAEA-TECDOC-719[5] [29]. The IAEA-TECDOC-719 list of IE categories for BWRs is based on the EPRI list provided in EPRI-NP-2230. The lists in EPRI-NP-2230 can be considered as one of the best sources for providing a generic IE list for PSA of a new plant (if similar design and reasonably similar operating practice).

[5] The IAEA-TECDOC-719 defines initiating events for the purpose of probabilistic safety assessment. It provides information on different approaches for defining IEs. It includes a generic initiating event database that contains about 300 records taken from 30 plant specific PSAs.

2.11.1.1 LOCAs

LOCAs are grouped in different break size categories according to the different success criteria for the emergency core cooling system. [29]

The SUPER-ASAR Phase II Appendix A2 has pipe rupture frequencies from WASH 1400, adapted to the Swedish nuclear power plants. [32] Pipe rupture frequencies are obtained in Table 6 in [32] and will be used in this study.

The LOCA categories used in this study can be seen in table 2.4. ID, name and description were obtained from source [29]. The LOCA frequencies can be seen in table 6 in source [32].

Table 2.4: LOCA categories

ID	Name	Description	Mean value for LOCA frequencies
A	Large LOCA	Automatic depressurization of primary system is not required.	**$2.52 \cdot 10^{-4}$ [32]**
S_1	Medium LOCA	Automatic depressurization necessary in order to make it possible for low pressure ECCS injection.	**$9.00 \cdot 10^{-4}$ [32]**
S_2	Small LOCA	Low pressure ECCS injection not required.	**$3.00 \cdot 10^{-3}$ [32]**

2.11.1.2 Transients

In the Reactor Safety Study WASH-1400 the BWR transients were originally grouped into three major categories (see Table 2.5). [29]

Table 2.5: The transient categories used in this study.

ID	Name	Description
T1	Transients 1	Transients involving loss of off-site power
T2	Transients 2	Transients involving loss of the power conversion system (PCS) (MSIV closure, loss of condenser vacuum, etc.)
T3	Transients 3	Transients with the PCS initially available (turbine trip, etc)

T1 are analyzed through the initiating event “loss of off-site power”. T2 and T3 transients are analyzed through the event classes H2, H3 and H4 as initiating events.

2.11.1.3 Special common cause initiators (CCI)

This broad group of initiators includes relatively low frequency IEs that in addition to initiating fault cause failures of mitigating systems. They are very much plant specific and will not be specified in this study.

2.11.2 Grouping of initiating events for BWRs

Table 2.6 displays the comparison of OKGs and this study´s management of transients with the EPRI list in table 3.9 from source [29]. Definitions of transients affecting O1, O2 and O3 can be seen in table 2.1 in this report. Transient categories used in this study can be seen in table 2.5.

Table 2.6: Management of transients according to the approach of OKG and of this study, compared with the EPRI list.

Function	List of EPRIs BWR transient initiating events	Management of the transients in PSA for O1, O2, O3	Management of the transients in this study
Main turbine / generator	Electric load rejection	TE	T1
Main turbine / generator	Electric load rejection with turbine bypass valve failure	TE, TT	T1, T2
Main turbine / generator	Turbine trip	TS	T3
Main turbine / generator	Turbine trip with turbine bypass valve failure	TT	T2
Steam	Main steam isolation valve (MSIV) isolation	TT	T2
Steam	Inadvertent closure of one MSIV	TT	T2
Steam	Partial MSIV closure	TT	T2
Condenser vacuum	Loss of normal condenser vacuum	TT	T2
Reactor system pressure control	Pressure regulator fails open	TT	T2
Reactor system pressure control	Pressure regulator fails close	TT	T2
Steam	Inadvertent opening of a safety/relief valve (stuck)	CCI (TP, TT or S2t)	CCI (T2 or S_2)
Reactor system pressure control	Turbine bypass fails open	TT	T2
Reactor system pressure control	Turbine bypass fails or control valves cause increased pressure (closed)	TS	T3
Reactor system flow	Recirculation control failure-increasing flow	TS	T3
Reactor system flow	Recirculation control failure – decreasing flow	TS	T3
Reactor system flow	Trip of one recirculation pump	No transient	No transient
Reactor system flow	Trip of all recirculation pumps	TS	T3
Reactor system flow	Abnormal startup of idle recirculation pump	TS	T3
Reactor system flow	Recirculation pump seizure	TS	T3
Feedwater	Feedwater-increasing flow at power	TF	T3
Feedwater	Loss of feedwater heater	TS	T3
Feedwater	Loss of all feedwater flow	TT, TE	T2, T1
Feedwater	Trip of one feedwater pump (or condensate pump)	No transient	No transient
Feedwater	Feedwater - low flow	TF	T3

Feedwater	Low feedwater flow during startup or shutdown	Not analyzed	Not analyzed in this study
Feedwater	High feedwater flow during startup or shutdown	Not analyzed	Not analyzed in this study
Reactivity control	Rod withdrawal at power	TS	T3
Reactivity control	High flux due to rod withdrawal at startup	Not analyzed	Not analyzed in this study
Reactivity control	Inadvertent insertion of rod or rods	TS	T3
Miscellaneous	Detected fault in reactor protection system	TS	T3
Electrical power	Loss of offsite power	TE	T1
Electrical power	Loss of auxiliary power	CCI (TF)	CCI (T3, T1)
Safety injection	Inadvertent startup of HPCI/HPCS	TS	T3
Miscellaneous	Scram due to plant occurrences	TS	T3
Spurious trips	Spurious trip by way of instrumentation, RPS fault	TS	T3
Spurious trips	Manual scram – no out – of – tolerance condition	TS, TP	T3
Spurious trips	Cause unknown	TS	T3

2.11.2.1 Loss of offsite power

Loss of offsite power will be treated as an initiating event with the failure probability 100% on the basic event “electricity input”.

2.11.3 Hazards

When estimating the risks of nuclear power plants, contributions from both internal initiating events and external initiators (or hazards) need to be considered. Some of the PSA studies which include hazards have shown that these have a larger potential risk for the environment than internal initiators. [29]

2.11.3.1 Fire

There is 3 IEs of fire. Description about them and how they will be managed in this study is given in table 2.7.

Table 2.7: Different initiating events of fire.

Initiating event	Description	Managed in this study
H2-fire	H2-fire is only affecting the component where it is started.	H2-fire is covered in the parameter “free parameter” that represent the basic event “rest faults”. So H2-fire is not used as an initial event.
H3-fire	H3-fire that takes out the entire fire cell.	H3-fire represents a conservative analysis of fire as IE. Complete flashover is usually considered as an H4-event.

H4-fire	H4-fire that takes out the entire fire cell.	H4-fire represents a more realistic approach of fire as IE. A sensitivity analysis will be performed to verify this approach.

Hazards are covered in section 3.7.

3 A Swedish BWR according to SSMFS 2008:17

3.1 Safety functions

The nuclear reactor shall be designed so that the safety functions related to reactivity control, primary system integrity, emergency core cooling, residual heat removal and containment can be maintained, to an extent that depends on the operating mode, and that takes in account all the events up to improbable events. [3]

The safety functions “reactivity control” (SF1), “core cooling” (SF2) and “residual heat removal” (SF4) in Table 3.1 will be used at PSA level 1 analysis.

Table 3.1: Safety functions with selected nomenclature.

Safety function	Nomenclature	PSA Level analysis
Reactivity control	SF1	**Level 1**
Core cooling	SF2	**Level 1**
Pressure relief primary system	SF3	Level 2
Residual heat removal	SF4	**Level 1**
Containment integrity and protection	SF5	Level 2

3.1.1 Requirement for the construction and the safety functions

In the implementation of defense in depth in the reactor design shall the following design principles be applied to the extent that is possible and reasonable: simplicity and durability in the design of the safety systems. [3]

The safety functions shall be able to withstand single faults in all the events from the probable to the improbable ones, according to the classes mentioned in section 2.5. [3]

In the construction, manufacture, installation, commissioning, operation and maintenance of safety systems, proper technical and administrative measures must be taken to counteract the occurrence of common cause failures. [3]

To counter the simultaneous failure of redundant parts of the safety systems, the nuclear reactor shall be designed so that the redundant parts and support functions have sufficient physical and functional separation. [3]

The separation between different parts of the safety functions with regard to fire shall be such that the required capacity of the current safety functions can be maintained. The separation between equipment that does not withstand earthquakes shall be such that the required equipment are not compromised. [6]

Various realizations that meet these requirements shall be reviewed under "suggestions for designs."

3.2 Environmental durability and environmental impact

Nuclear reactor barriers and equipment belonging to the reactor's safety systems are designed to withstand the environmental conditions. The barriers and equipment are exposed in situations where their function is credited in the reactor safety analysis. Details are available in SSMFS 2008:17 § 17. [6]

The demands made on the required environmental qualification are specified in SAR and are not considered as part of this study.

3.3 Regulations for the control room

The nuclear reactor is designed according SSMFS 2008:17 18, 19 & 20 § requirements regarding regulations concerning the control room.

These requirements are not considered within the scope of this study.

3.4 Safety classification

The nuclear reactors structures, systems, components and devices are assumed to be divided into safety classes that meet the requirements of SSMFS 2008:17 § 21.

These requirements are not considered within the scope of this study.

3.5 Regulations for the reactor core

The nuclear reactor is constructed according to SSMFS 2008:17 23, 24, 25, 26 & 27 § requirements concerning regulations for the reactor core.

These requirements are not considered within the scope of this study.

3.6 LOCA

The nuclear reactor shall be resistant to global and local stress and other effects that can occur when a pipe breaks. The consequences of a pipe break as an initiating event, shall be analyzed and evaluated with respect to the barriers and the safety functions that are needed in such a case according SSMFS 2008:17 § 12. [3]

The frequency of spontaneous major rupture of the reactor vessel is estimated equal to $2.7 \cdot 10^{-7}$ per year. This means that the LOCA due to a large break of the reactor vessel is considered part of the residual risk in the PSA model. [4]

As mentioned above, LOCAs can be divided into Large LOCA (A), Medium LOCA (S1) and Small LOCA (S2) (see Table 2.4). In the current study, the same LOCA classification is used.

3.7 Hazards

The nuclear reactor shall be designed to withstand hazards and other events that arise outside or inside the plant and that could lead to an accident. The design limits must be established for such hazards and events. Hazards and events with such rapid sequences that no protective measures can be taken as they occur should also be sorted into an event class. There shall be an established action plan for those situations where the design limits might be exceeded. This must be done for each type of hazard that can lead to a nuclear accident according SSMFS 2008:17 § 14. [3]

Examples of hazards to be considered are shown in Table 3.2.

Table 3.2: Examples of hazards according to [3].

First paragraph		
Extreme temperature	**Extreme sea waves**	**Extreme algae growth**
Extreme water level	**Earthquake**	**Extreme wind**
Extreme rainfall	**Extreme icing**	**-**

Second paragraph		
Disturbance or Loss of offsite power	**Fire**	**Explosions**
Floods	**Airplane crash**	**-**

External events primarily affect the outer shell. Examples of them are wind and snow loads. External impact also refers to events such as various clogging processes of the cooling water intake and extreme sea levels. [8]

Safety classified buildings were originally *dimensioned and/or verified* against hazards from the "first paragraph" in the table 3.2. This means that extreme rainfall, extreme icing, extreme temperature, extreme sea waves, extreme algae growth, extreme water levels and extreme wind can be ignored in the model.

The methodology according to Standard Review Plan (SRP) 3.5.1.6 has been shown that the probability for airplane crash is so low that it does not need to be considered. Therefore this kind of accident is ignored and is placed in residual risks. [4]

3.7.1 Fire

In the analysis of fire in the plant, a fire that affects all the equipment in a fire compartment is assumed to occur. If it is proved by the analysis that the probability of failure of an entire fire cell is low, through the protective measures that have been implemented to prevent the spread of fire, then the burn up of the entire cell is not required to be assumed. Such fire analysis should include all the measures necessary until the fire is extinguished. The passive safety measures are prioritized and applied, such as room separation, enclosure or shielding of equipment, minimal fire load and distance separation between equipment.

If only the distance separation is included as protective measure between redundant equipment should this apply to spaces of sufficient size and under the assumption that fire analysis confirms that the separation is sufficient to prevent the spread of fire.

Furthermore, fire should be taken into consideration in the following way when analyzing initiating events:

- In the analysis of fire as initiating event, there is no need to suppose that an additional fire occurs in the plant.
- When analyzing initiating events other than fire, which in turn can cause a fire, a fire should be assumed to occur as possible secondary failure.

- When analyzing events other than fire, which in turn cannot create a fire, a fire should be assumed to occur no earlier than 12 hours after the initiating event. This sequence of events does not need to be combined with a single failure. This applies to the event class unanticipated events, apart from pipe breaks. According SSMFS 2008:17 Guidelines to § 14. [3]

All models are constructed with fire protection that takes into account the requirements above.

The result from [17] shows that the frequency of a fire occurrence under normal power operation is **$7.9 \cdot 10^{-3}$ per year**, and for the outage (refueling) period $2.1 \cdot 10^{-3}$ per year. The value **$7.9 \cdot 10^{-3}$ per year** will be used as conservative[6] fire frequency in this study.

3.7.1.1 Fire occurrence frequency

Fire frequency for complete flashover during normal power operation was calculated as follows:

The "number of events" and "conditional probability severe effect" were retrieved from Appendix D-3, figure 2, from the source [31].

- Number of events: 177
- Conditional probability for severe effects (p_E): 0.068 (is obtained from the sum of category 3-6 and 8 in the table 3.3)

Table 3.3 shows the different categories for fire occurrences. The table is taken from Appendix D-3, table 5 from source [31].

Table 3.3: Different categories for fire occurrences. [31].

Category	Consequence	Sum
0	None	0,226
1	Fire and damage contained to fire initiating object	0,54
2	Fire spread to at least one more object in room	0,118
3	Loss of one room	0,005
4	Impact on adjacent rooms in one fire compartment	0,016
5	Impact on more than one fire compartment	0,016
6	Structural damage	0,015
7	Impact is limited to only one safety train (partly double count, coincidence with 0,1,2)	0,20
8	Safety significant impact on safety trains (partly double count, coincidence with 3, 4, 5, or 6)	0,016

The formula for estimating fire occurrence frequency is given in section 3.3 of [17]. The calculated value **$2.9 \cdot 10^{-3}$** will be used in this study:

$$f_E^{Fire} = p_E \cdot \frac{events}{reactor\ years} \cdot \frac{time\ swedish\ operating\ year}{standard\ operating\ year} = 0.068 \cdot \frac{177.5}{4515} \cdot \frac{0.92}{0.85} = \mathbf{2.9 \cdot 10^{-3}/year} \quad (3.1)$$

[6] Conservative in the sense that the consequence is close to a H4-event while the frequency is more like H3-event.

3.7.1.2 Inadvertent actuation

Inadvertent actuation occurs when the cable insulation burns up and random cable connections can start various components. The phenomenon occurs during a short window of time because the fire quickly melts the cable after the insulation is burned up.

In this study it is assumed that the safety classified buildings have been *dimensioned and/or verified* against the phenomenon "inadvertent actuation" and is thereby not taken into consideration in the construction model.

3.7.2 Internal flooding

Structural design and layout is constructed so that, regardless of the rupture location and fracture size, the reactor safety systems will be able to perform the necessary tasks even after occurrence of flooding.

LOCA must consider room influence so flooding is covered by LOCA. Another room influence is inadvertent sprinkler actuation which is also covered by LOCA. The buildings has been *dimensioned and/or verified* against LOCAs, so internal flooding can be disregarded in the PSA model.

3.7.3 Earthquake

From a seismic point of view, Sweden is a stable area with shallow quakes that rarely has a magnitude above 4 on the Richter scale. Seismic areas in Sweden are in Västergötland, Värmland and along the Norrland coast. [28]

"The magnitude of earthquake chosen is primarily corresponding to 10^{-5} earthquake in SKI TR 92:3 [6]. Alternatively the magnitude of 0.15 g[7] based on Reg Guide 1.60 [6] can be used. For OKG site the specific seismic ground acceleration can also be used according to the interpretation and application of SSMFS 2008:17 § 14. [6]

Earthquake as H2 event has been assumed to be so small (<0.01g) that it does not need to be considered in the design of the facility. [7]

LOCA is not combined with a SSE (Safe Shutdown Earthquake) since a SSE is of such low probability and RCPB is designed to resist a SSE. This is the case because the frequency for this combination is very low (<10^{-7} per year). [15]

For frequencies exceeding about 10 Hz the agreement is rather good between the original design spectrum and the new spectrum for the level 10^{-5}. For low frequencies the original design spectra are associated with much lower probabilities, not to say that they are unrealistic, even for extreme events. Within the important range 2-5 Hz, (the range of fundamental frequencies of reactor buildings and containment) the original design spectrum appears to correspond to the probability range of 10^{-8} – 10^{-6} annual events per site. [33]

In this study the probability of **10^{-6}** [33] will be used for earthquakes as initiating event. This places them into the event class H5. Earthquake are not however analyzed in this study. Earthquake as initial event has been verified with deterministic methods and are not considered further.

---

[7] The gravitational constant 1g = 9.8 m/s^2

Deterministically it could be assumed that earthquakes knock out all the trains except the one that is earthquake-proof. This means that one train will be working and that meltdown of the core is prevented.

3.7.4 Explosion

The consequences of a detonation are: pressure wave, which can cause mechanical damage to the surrounding systems and buildings; heat wave, which can ignite surrounding materials; missiles that can be thrown and cause damage to surrounding materials e.g. buildings and systems; tremors by the ground or the atmosphere propagate and cause damage to, for example, electronic devices.

The above effects should be considered as ***extreme*** external impacts. [9]

All the equipment in safety class 1-3 shall be designed for ***extreme*** external impacts. [9]

It is assumed that the safety classified buildings have been *dimensioned and/or verified* against the hazard and "explosion", thus these issues are not considered in the construction model.

3.7.5 Disturbance or loss of off-site power

Disturbance or loss of off-site power are examples of events outside the facility which the nuclear reactor should be dimensioned to resist. [9]

The construction is protected from any phenomena that occur in the external grid, so that disturbance can be neglected. However the plant is not protected against loss of off-site power, which is classified to event class H2.

3.8 Initiating events and event classification

As regards subsection 2.5.1, the values of frequency that are associated to the event classification and that are used in this work are reported in table 3.4.

Table 3.4: Frequency for the event classes.

Event class	Mean number of events/year
Normal operation(H1)	Normal operation
Anticipated events (H2)	$\geq 10^{-2}$
Unanticipated events (H3)	$10^{-2} > F \geq 10^{-4}$
Unlikely events (H4)	$10^{-4} > F \geq 10^{-6}$
Very unlikely events (H5)	$10^{-7} \leq F < 10^{-6}$
Extremely unlikely events (rest risks)	$< 10^{-6}$

3.8.1 Management of event classes in this study

In the development of the current PSA model it is assumed 10 initiating events for each event class. The reason of this assumption is that, in the EPRI-list, there are 5 IEs in class T1, 10 IEs in class T2 and 19 IEs in class T3. Thereby 10 events for each class may be a reasonable choice. All 10 events are assumed to have a typical frequency within its event class. For example, H3 identify events with a frequency range $10^{-2} > F \geq 10^{-4}$, so a typical value is taken equal to 10^{-3}, and the 10 events with a typical value of 10^{-3} gives a total frequency 10^{-2} for event class H3.

Table 3.5: Frequency used in the PSA for the different event classes H2 to H5.

Event class	Typical number of events/year	Typical number of events for 10 IE/year/group
Normal operation (H1)	**Normal operation**	**Normal operation**
Anticipated events (H2)	**10^{-1}**	**1**
Unanticipated events (H3)	**10^{-3}**	**10^{-2}**
Unlikely events (H4)	**10^{-5}**	**10^{-4}**
Very unlikely events (H5)	**10^{-6}**	**10^{-5}**

Each event class is adjusted by subtracting the IE that has been analyzed separately:

3.8.1.1 Event class H2

Loss of off-site power has the frequency 10^{-1} and is located in the event class H2 resulting in the H2 frequency 1-0.1 = **0.9**. The total frequency of event class H2 can be seen in table 3.5. The frequency for loss of off-site power needs to be subtracted from event class H2 since it is investigated separately. Loss of offsite power is treated as an initiating event with the failure probability 100% on the basic event "electricity input". To be compared with all other initiating events in the event class H2 were electricity from the grid have a reasonable probability to be available.

3.8.1.2 Event class H3

- **Fire** has the frequency $2.9 \cdot 10^{-3}$ and is for that reason placed in the event class H3.
- **S2 Small LOCA** has the frequency $3.00 \cdot 10^{-3}$ and is for that reason placed in event class H3.
- **S1 Medium LOCA** has the frequency $9.00 \cdot 10^{-4}$ and is for that reason placed in event class H3.
- **A Large LOCA** has the frequency $2.52 \cdot 10^{-4}$ and is for that reason placed in event class H3.
- **The sum of Fire, S2, S1 and A** is subtracted from the event class H3 resulting in the H3 frequency **$2.95 \cdot 10^{-3}$.**

Table 3.6: Frequency used for each initiating event in this study.

Initiating event	Frequency/year
Normal operation (H1)	**Normal operation**
Anticipated events (H2)	**0.9**
Unanticipated events (H3)	**$2.95 \cdot 10^{-3}$**
Unlikely events (H4)	**10^{-4}**
Very unlikely events (H5)	**10^{-5}**
Fire	**$2.9 \cdot 10^{-3}$**
Loss of off-site power	**10^{-1}**
"A" Large LOCA	**$2.52 \cdot 10^{-4}$**
"S1" Medium LOCA	**$9.00 \cdot 10^{-4}$**
"S2" Small LOCA	**$3.00 \cdot 10^{-3}$**

3.9 Realization

The models developed in this work are driven by fire events. Since fire cells, i.e. the areas where a fire cannot spread over, are designed for each train, other requirements can be met with simple modifications of the models. The construction will be driven by fire where fire cells are designed for each train. Other requirements such as simplicity, robustness, redundancy, diversity and physical

separation can be met without any great complexity of the models. Different safety constructions will be used to analyze if the room analysis with fire protection has any significant effect on the "final" safety. Models are built with the goal of achieving a generic construction model for BWRs in Sweden.

3.9.1 Suggested constructions

An appropriate and reasonable diversification should be applied to the design of the safety functions according to § 3, with *realistic analysis assumptions and acceptance criteria* for the events up to the event class unanticipated events, where pipe break may be excluded. According to Swedish Radiation Safety Authority general guidelines regarding SSMFS 2008:17 § 10. [3]

The term "realistic analysis assumptions and acceptance criteria" are interpreted by Scandinavian nuclear power plants within BWR as follows.

Realistic analysis assumptions and acceptance criteria means, among other things, that the non-safety classed objects may be credited when demonstrating diversity. Furthermore, Single Fault tolerance is not required for the equipment that is credited. Principles for evaluation of diversification are reported in [Westinghouse Atomic Report SEP02-198]. This should be used when evaluating the need for diversification, but one must take into account that [Westinghouse Atomic Report SEP02-198] limits the need for diversification to CCF during the initial events in the event class H2 unless the sequence of events can lead to large emissions. Then initiating events in event class H3 should be considered. [16]

The construction models below assume that non-safety classed systems may be considered for managing fire in combination with CCF. Further, single faults are not applied when there is CCF.

CCF represents the dominant contribution to the frequency of core damage and radioactive release in nuclear power plants, especially in later generations of plants with high redundancy level. It is therefore important to properly prepare and use CCF data in the PSA studies. [26]

CCF is modeled in the PSA model by using the α-factor model in which the α-values are given in table 2.3.

3 different construction models were developed in this study. The 3 models are described and explained in subsection 3.9.1.1 to 3.9.1.3.

3.9.1.1 Construction 1 (SSMFS 2008:17 design)

Construction 1 reduces the fire frequency so that the simplest possible structure (2 systems and 3 trains) can be used. As shown in Figure 3.1, two systems (system 1 and system 2) with the same function (diversity) are taken in account. For system 1, two trains are included because of redundancy. For system 2 only one train is used.

The 3 trains are physically separated (one fire cell for each train). In the case of system 2, the fire cell is inert[8], i.e. the fire can be considered an H4 event and CCF does not need to be considered.

[8] Fire measures that can be introduced to reduce the fire frequency include e.g. additional extinguishing devices, fire trained and adequately equipped personal or lowering of oxygen levels.

Equipment in one of the train's fire cells are reinforced against earthquake. In case of earthquake that knocks out all the trains except the one that is earthquake-proof, there will be one train working and meltdown of the core is prevented.

Table 3.7 displays the construction choices for construction 1 and what they achieve.

Table 3.7: Construction choices with achieved requirement for construction 1.

Construction choice	Achieved requirement
3·100% train	Simplicity and robustness
Two train of system 1	Redundancy
Two different system (system 1 & system 2)	Diversity
One fire cell and flooding channel for each train	Physical separation
Fire cell for train 1 in system 2 is essentially inert	CCF-tolerant
One train is reinforced against earthquake	Earthquake-tolerant

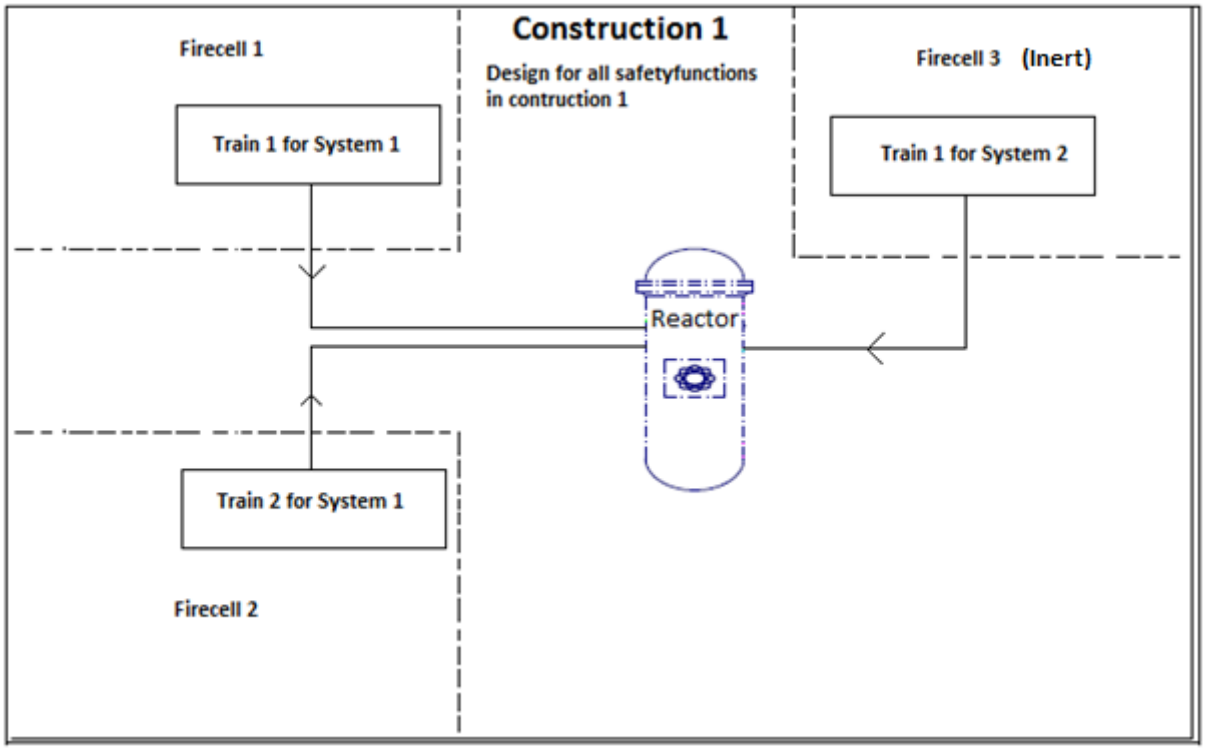


Figure 3.1: Construction 1.

3.9.1.2 Construction 2 (diversity design)

Construction 2 is purely based on the principle of diversification. As shown in Figure 3.2, three systems (system 1, system 2 and system 3) with the same function (diversity) are taken in account. Only one train is used in each system which gives a total of three trains. The 3 trains are physically separated (one fire cell for each train).

Two other types of systems still remain when one fire cell is taken out, this means that no additional fire measures against CCF are needed. Equipment in one of the train's fire cells are reinforced against

earthquake. In case of earthquake that knocks out all the trains except the one that is earthquake-proof, there will be one train working and meltdown of the core is prevented.

Table 3.8 displays the construction choices for construction 2 and what they achieve.

Table 3.8: Construction choices with achieved requirement for construction 2.

Construction choice	Achieved requirement
Three different system (system 1, system 2 & system 3)	Redundancy and diversity
3·100% train	Simplicity and robustness
One fire cell and flooding channel for each train	Physical separation
Two system still remain when one fire cell is taken out	CCF-tolerant
One train is reinforced against earthquake	Earthquake-tolerant

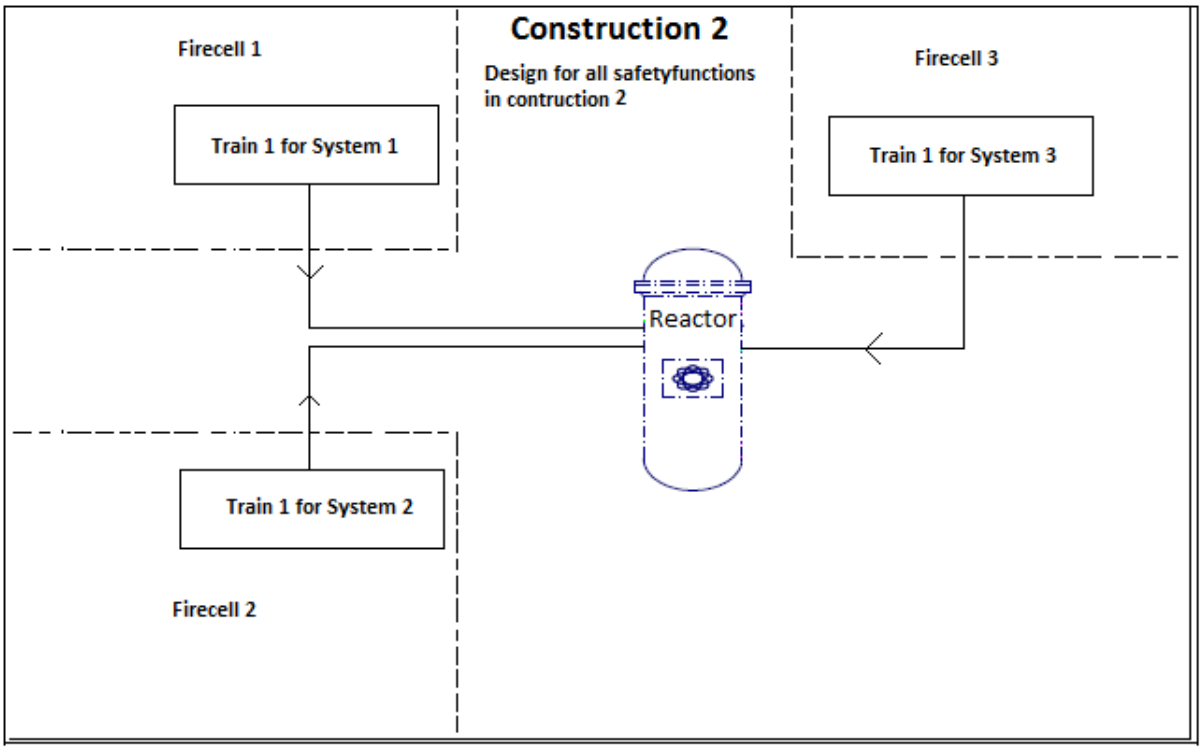


Figure 3.2: Construction 2.

3.9.1.3 Construction 3 (SSMFS 2008:17 design)

Construction 3 uses both diversification and redundancy. As shown in Figure 3.3, two systems (system 1 and system 2) with the same function (diversity) are taken in account. For both system 1 and system 2, two trains are included because of redundancy.

The 4 trains are physically separated (one fire cell and flooding channel for each train). Two other types of systems still remain when one fire cell is taken out, this means that no additional fire measures against CCF are needed. Equipment in one of the train's fire cells are reinforced against earthquake. In case of earthquake that knocks out all the trains except the one that is earthquake-proof, there will be one train working and meltdown of the core is prevented.

Table 3.9 displays the construction choices for construction 3 and what they achieve.

Table 3.9: Construction choices with achieved requirement for construction 3.

Construction choice	Achieved requirement
4·100% train	Robustness
Two train of each system (4 train in total)	Redundancy
Two different system (system 1 & system 2)	Diversity
One fire cell and flooding channel for each train	Physical separation
Two system and three trains still remain when one fire cell is taken out	CCF-tolerant
One train is reinforced against earthquake	Earthquake-tolerant

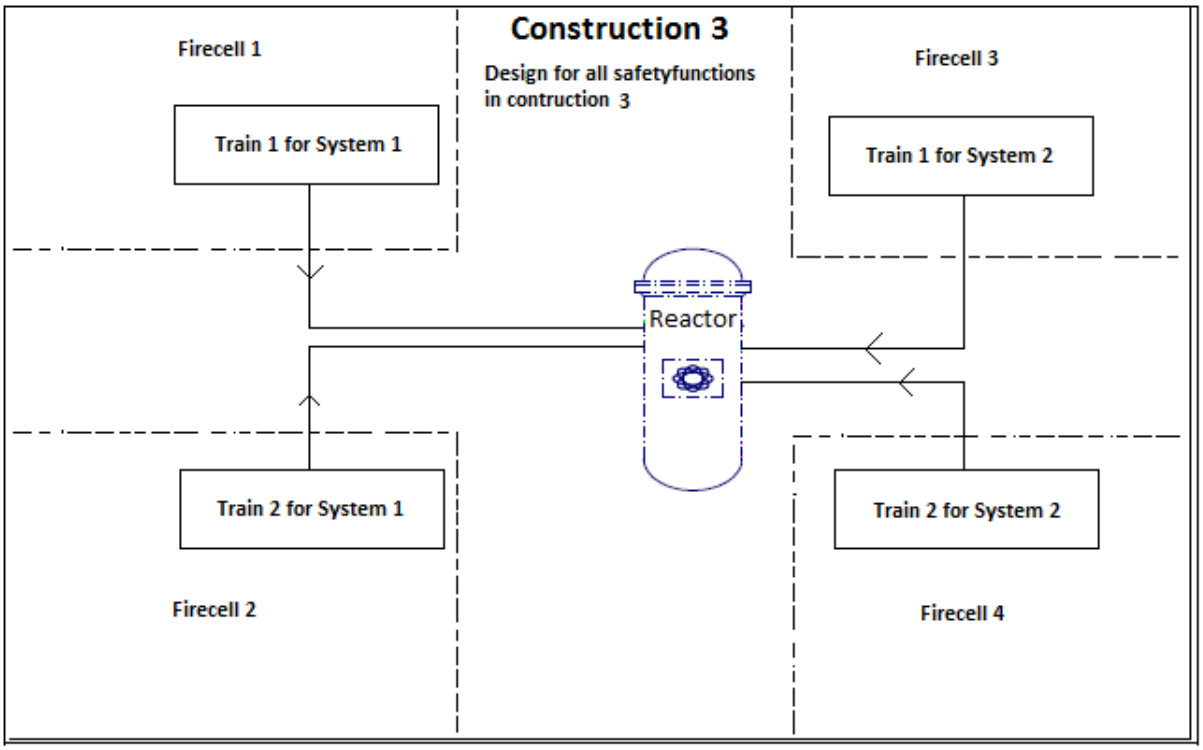


Figure 3.3: Construction 3.

3.10 PSA

3.10.1 Fault tree construction

Through the introduction of CCF in the PSA model one may distinguish between diversity and redundancy. This means that four event trees will be constructed and that one generic model that covers all the structures cannot be constructed. Two CCF groups were constructed for each safety function, CCF group 1 contains the basic event "auxillary power" and CCF group 2 contains the basic event "rest faults".

Each train can fail because of:

- ***Electrical faults***
  - ***Loss of offsite power*** - classed as one and the same basic event for all trains. Fault of the external grid will lead to failure at the basic event “electricity input” in all the

trains. This means that the CCF cannot be performed on this basic event. Generic value is obtained by the mean of event class H2 (10^{-1}) = **0.1**.[9]

- ***Auxillary power ("Backup power")*** - classed as a basic event. This study only includes diesel generators as Swedish BWRs are dependent on electricity. Two failure modes are defined "inadvertent stop" and "failure to start". "Backup power" failure is defined as failure through either one of these two failure modes.
  - ***Inadvertent stop*** – the mean value of inadvertent stop of diesel generators for all Swedish nuclear power plants is obtained from Table 7.1.1 in the T-book. [27]
  - ***Failure to start*** – the mean value of failure to start of diesel generators for all Swedish nuclear power plants is obtained from table 7.1.2 in the T-book. [27]

- ***Rest faults*** - classed as a basic event with a *free parameter*, this parameter is used to fine tune the PSA model.

3.10.1.1 Inadvertent stop

From the T-book [27] the following generic value was obtained: $\lambda_d = 16.5 \cdot 10^{-4}$ h^{-1}. The value for T1 is chosen equal to 0.5 h due to grace time[10], whereas manual actions can occur after 0.5 h. $< q_1 >$ is the term for inadvertent stop and it can be expressed as:

$$< q_1 > \approx \lambda_d * T_1 = 0.000825 \tag{3.2}$$

3.10.1.2 Failure to start

From the T-book [27] the following generic values were obtained: $\lambda_s = 12.6 \cdot 10^{-6}$ h^{-1} and $q_0 = 3.0 \cdot 10^{-4}$. A typical value for T_2 can be estimated equal to 4 weeks. $< q_2 >$ is the term for failure to start and it can be expressed as:

$$< q_2 > = q_0 + \lambda_s * \frac{T_2}{2} = 4.53 \cdot 10^{-3} \tag{3.3}$$

3.10.1.3 Generic value of auxiliary power

The total probability of failure of the auxiliary power is the sum between inadvertent stop and failure to start. q is the term for the generic value of auxiliary power and it can be expressed as:

$$q = < q_1 > + < q_2 > = 5.36 \cdot 10^{-3} \tag{3.4}$$

The calculated value **$5.36 \cdot 10^{-3}$** will therefore be used as a generic value for auxiliary power failure probability in the present analysis.

[9] Loss of offsite power is classified as an H2 event

[10] A postulated 30 minutes "Grace Time", where no manual actions are credited, is a design principle used in Swedish BWRs.

3.10.1.4 Fault Tree "RiskSpectrum" build

Figure 3.4 displays the Fault Tree for SF1 (reactivity control) in construction 1. SF1, SF2 (core cooling) and SF4 (residual heat removal) have analogous Fault Trees. Description and explanation of the Fault Tree can be seen in table 3.10.

Table 3.10: Description of the Fault Tree in figure 3.4.

Event	Terminology	Description
GATE SF1	Top event[11] and input to safety function 1 in construction 1 event tree.	Failure of safety function 1 (reactivity control).
Fault in System 1	AND-gate[12]: Intermediate system event 1.	Failure of safety system 1.
Train 1 for System 1	OR-gate[13]: Intermediate train event 1 for system 1.	Failure of train 1 in system 1.
Train 2 for System 1	OR-gate: Intermediate train event 2 for system 1.	Failure of train 2 in system 1.
Fault in System 2	AND-gate: Intermediate system event 2.	Failure of safety system 2
Train 1 for System 2	OR-gate: Intermediate train event 1 for system 2.	Represents failure of train 1 in system 2.
Rest faults	Basic event[14] and CCF-event[15] for system 1. CCF between the basic event rest faults in train 1 (system 1) and train 2 (system 1).	Rest faults failure probability is decided by iteration of its parameter which in this study has the nomenclature "free parameter".
Electricity fault	AND-gate: Intermediate event that have the same design in construction 1, 2 and 3 and safety function SF1, SF2 and SF4.	Failure of electricity input for each train.
Electricity input to all systems in construction 1, 2 and 3	Classed as one and the same basic event for all trains in all constructions.	Loss of offsite power (LOOP) which in this study has the failure probability 0.1. This basic event is also connected to the initiating event LOOP which triggers a 100% failure probability.
Reserve power	Basic event and CCF-event for system 1. CCF between the basic event reserve power in train 1 (system 1) and train 2 (system 1).	Auxiliary power from the diesel generators which in this study has the failure probability of $5.36 \cdot 10^{-3}$.

[11] Top event is the undesired event that is modelled in the Fault Tree. It can be used as an input to a function event.
[12] AND-gate means that the output event occurs if all of the input events occur.
[13] OR-gate means that the output event occurs if one or many of the input events occur.
[14] Basic event means that equipment failure requires no further breakdown into simpler failures. It contains information about failure probability or frequency.
[15] CCF-event means that common cause failure is taken into consideration. It contains information about which basic events that are connected. The generic α-factor (2,n) from table 2.3 is the input data required to calculate the probability of the CCF basic events.

Area phenomena – FIRE	Basic event. Placed in each train for construction 1. (for explanation see 3.10.4)	Fire that knock out an entire fire cell which in this study is one train. The basic event is connected to the initiating event fire which triggers a 100% failure probability. The failure probability is 0 for all other initiating events.

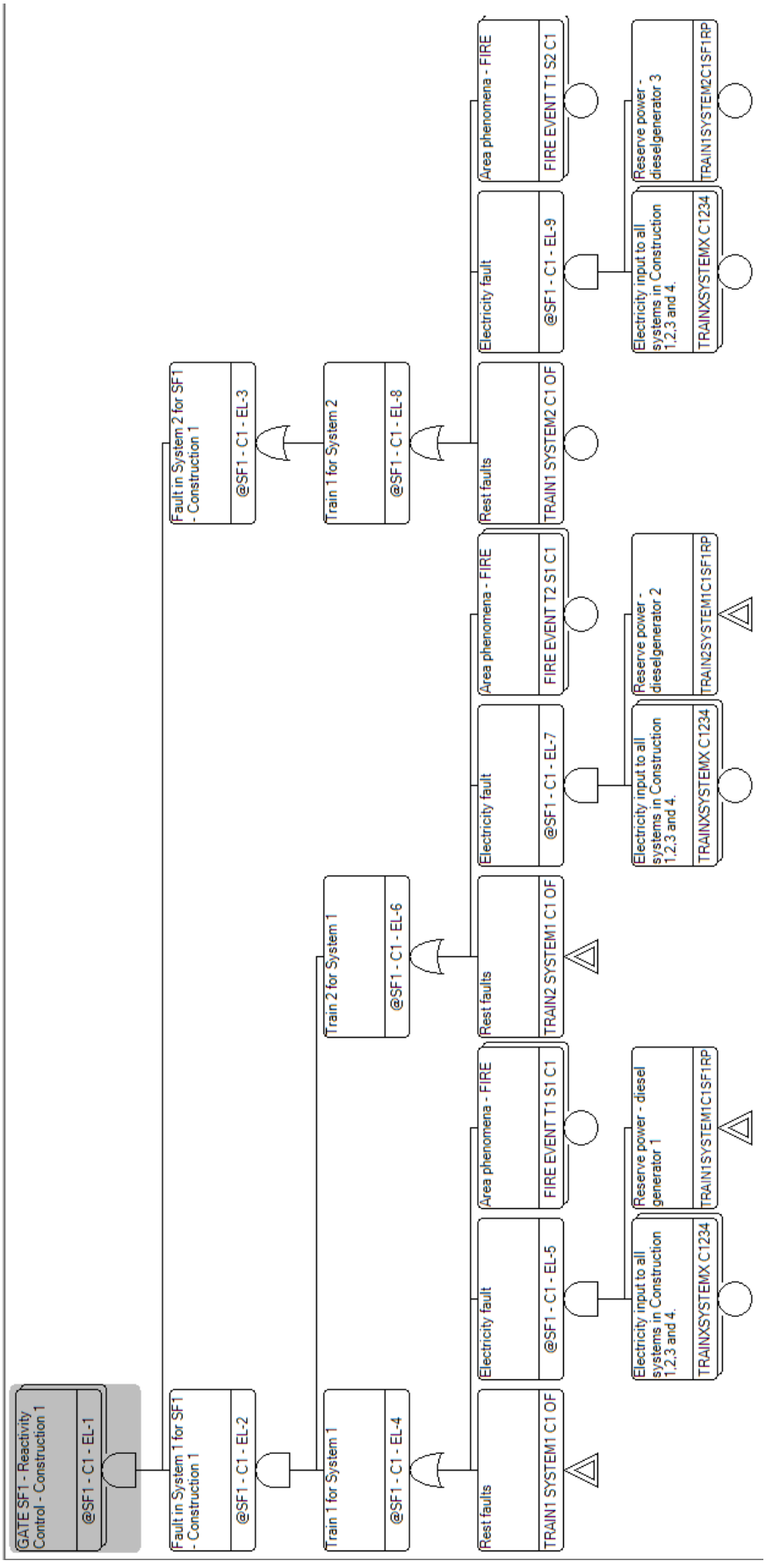


Figure 3.4: Fault tree for SF1 in construction 1.

Figure 3.5 displays the fault tree for SF1 in construction 2. SF1, SF2 (core cooling) and SF4 (residual heat removal) have analogous Fault Trees. Description and explanation of the Fault Tree can be seen in table 3.11.

Table 3.11: Description of the Fault Tree in figure 3.5.

Event	Terminology	Description
GATE SF1	Top event and input to safety function 1 in construction 2 event tree.	Failure of safety function 1 (reactivity control).
Fault in System 1	AND-gate: Intermediate system event 1.	Failure of safety system 1.
Train 1 for System 1	OR-gate: Intermediate train event 1 for system 1.	Failure of train 1 in system 1.
Fault in System 2	AND-gate: Intermediate system event 2.	Failure of safety system 2
Train 1 for System 2	OR-gate: Intermediate train event 1 for system 2.	Failure of train 1 in system 2.
Fault in System 3	AND-gate: Intermediate system event 3.	Failure of safety system 3
Train 1 for System 3	OR-gate: Intermediate train event 1 for system 3.	Failure of train 1 in system 3.
Rest faults	Basic event	Rest faults failure probability is decided by iteration of its parameter which in this study has the nomenclature “free parameter”.
Electricity fault	AND-gate: Intermediate event that has the same design in construction 1, 2 and 3 and safety function SF1, SF2 and SF4.	Failure of electricity input for each train.
Electricity input to all systems in construction 1, 2 and 3	Classed as one and the same basic event for all trains in all constructions.	Loss of offsite power (LOOP) which in this study has the failure probability 0.1. This basic event is also connected to the initiating event LOOP which triggers a 100% failure probability.
Reserve power	Basic event.	Auxiliary power from the diesel generators which in this study has the failure probability of $5.36 \cdot 10^{-3}$.
Area phenomena – FIRE	Basic event. Placed in train 1 (system 1) for construction 2. (for explanation see 3.10.4)	Fire that knock out an entire fire cell which in this study is one train. The basic event is connected to the initiating event fire which triggers a 100% failure probability. The failure probability is 0 for all other initiating events.

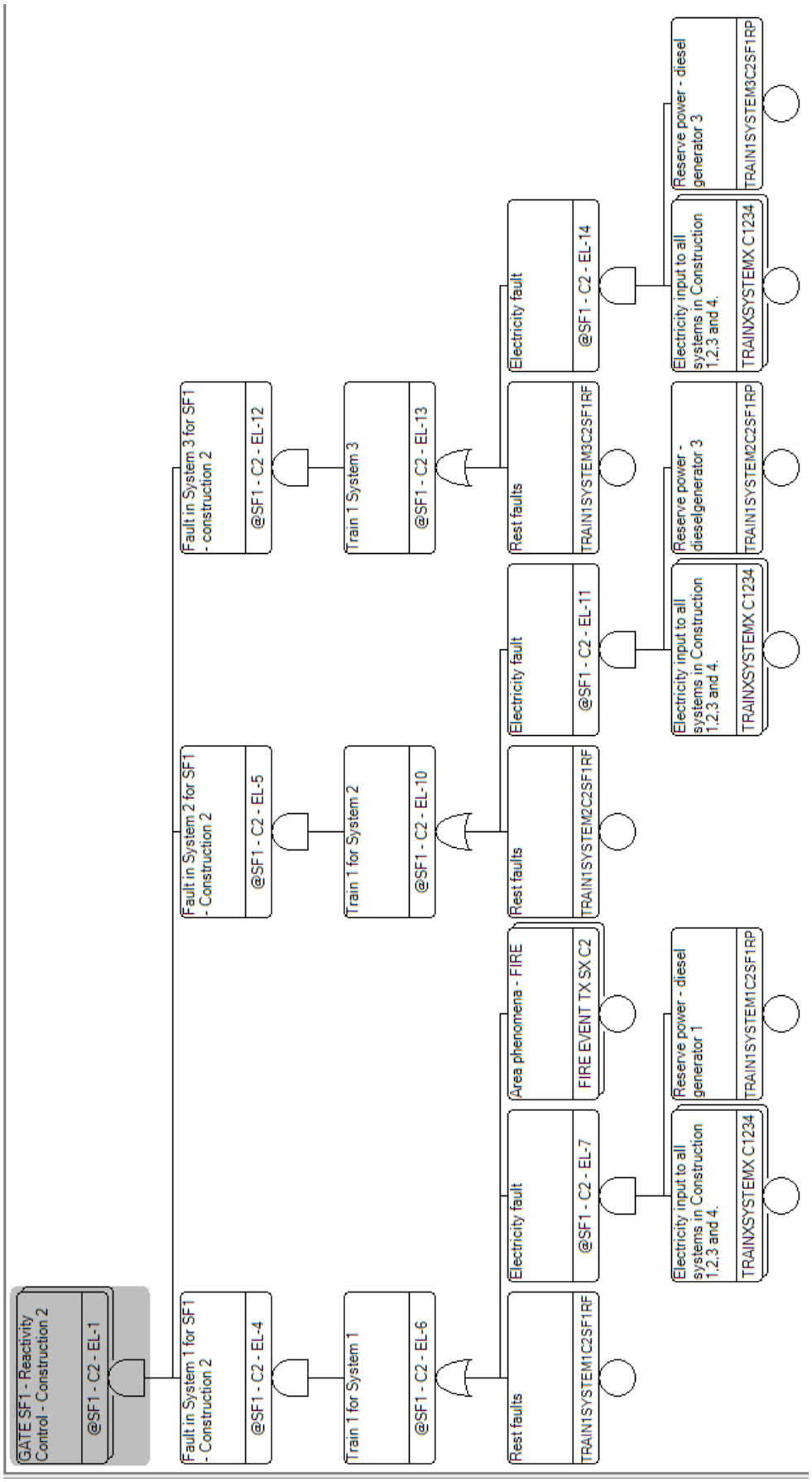


Figure 3.5: Fault tree for SF1 in construction 2.

Figure 3.6 displays the fault tree for SF1 in construction 3. SF1, SF2 (core cooling) and SF4 (residual heat removal) have analogous Fault Trees. Description and explanation of the Fault Tree can be seen in table 3.12.

Table 3.12: Description of the Fault Tree in figure 3.6.

Event	Terminology	Description
GATE SF1	Top event and input to safety function 1 in construction 3 event tree.	Failure of safety function 1 (reactivity control).
Fault in System 1	AND-gate: Intermediate system event 1.	Failure of safety system 1.
Train 1 for System 1	OR-gate: Intermediate train event 1 for system 1.	Failure of train 1 in system 1.
Train 2 for System 1	OR-gate: Intermediate train event 2 for system 1.	Failure of train 2 in system 1.
Fault in System 2	AND-gate: Intermediate system event 2.	Failure of safety system 2
Train 1 for System 2	OR-gate: Intermediate train event 1 for system 2.	Failure of train 1 in system 2.
Train 2 for System 2	OR-gate: Intermediate train event 2 for system 2.	Failure of train 2 in system 2.
Rest faults	Basic event and CCF-event for system 1 and system 2. CCF between the basic event rest faults in train 1 (system 1) and train 2 (system 1). CCF between the basic event rest faults in train 1 (system 2) and train 2 (system 2).	Rest faults failure probability is decided by iteration of its parameter which in this study has the nomenclature “free parameter”.
Electricity fault	AND-gate: Intermediate event that has the same design in construction 1, 2 and 3 and safety function SF1, SF2 and SF4.	Failure of electricity input for each train.
Electricity input to all systems in construction 1, 2 & 3	Classed as one and the same basic event for all trains in all constructions.	Loss of offsite power (LOOP) which in this study has the failure probability 0.1. This basic event is also connected to the initiating event LOOP which triggers a 100% failure probability.
Reserve power	Basic event and CCF-event for system 1 and system 2. CCF between the basic event reserve power in train 1 (system 1) and train 2 (system 1). CCF between the basic event reserve power in train 1 (system 2) and train 2 (system 2).	Auxiliary power from the diesel generators which in this study has the failure probability of $5.36 \cdot 10^{-3}$.
Area phenomena – FIRE	Basic event. Placed in train 1 (system 1) for construction 3. (for explanation see 3.10.4)	Fire that knock out an entire fire cell which in this study is one train. The basic event is connected to the initiating event fire which triggers a 100% failure probability. The failure probability is 0 for all other initiating events.

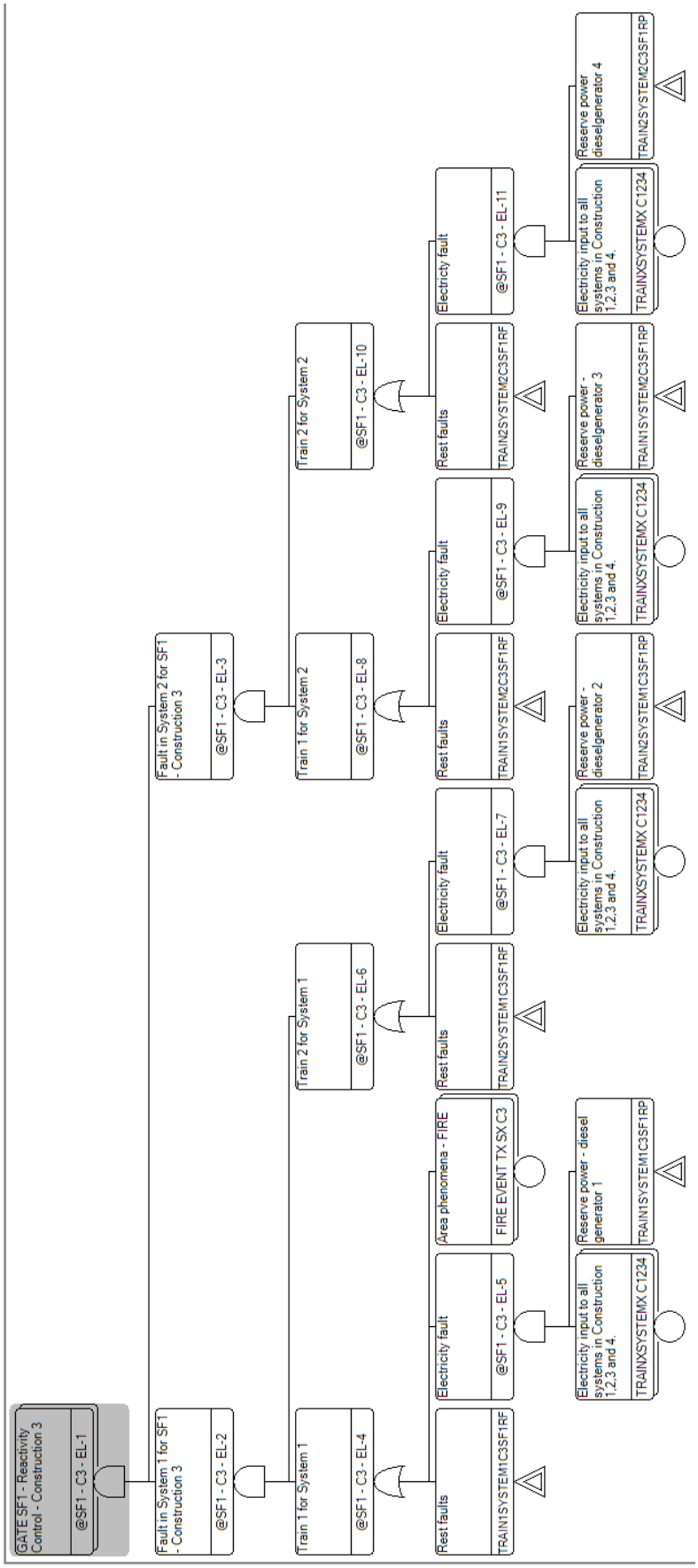
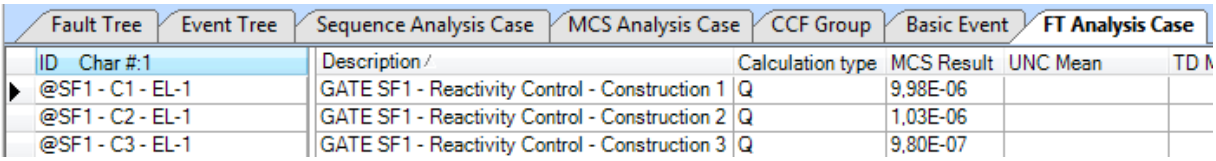


Figure 3.6: Fault tree for SF1 in construction 3.

Figure 3.7 displays the FT analysis performed on the three constructions. Results show that the probability at function level is different for all three constructions when the analysis is performed at train level with the same value on the “free parameter”.



ID Char #:1	Description	Calculation type	MCS Result	UNC Mean	TD M
@SF1 - C1 - EL-1	GATE SF1 - Reactivity Control - Construction 1	Q	9,98E-06		
@SF1 - C2 - EL-1	GATE SF1 - Reactivity Control - Construction 2	Q	1,03E-06		
@SF1 - C3 - EL-1	GATE SF1 - Reactivity Control - Construction 3	Q	9,80E-07		

Figure 3.7: FT analysis.

3.10.2 Generic model – event tree analysis

The three different PSA-models constructed represent a sufficient set of reasonable realizations. To meet SSMFS 2008:17 design requirements.

Event tree 1	**Generic for 3 Train BWRs with 2 diversified Systems**
Event tree 2	**Generic for 3 Train BWRs with 3 diversified Systems**
Event tree 3	**Generic for 4 Train BWRs with 2 diversified Systems**

3.10.3 Consequences

Boundary conditions for the Sequence Analysis Case were set to:

- Absolute Cutoff: 10^{-14}
- Relative Cutoff: 10^{-7}

The absolute cutoff is the minimal frequency that is taken into consideration in the sequence analysis calculation. Values lower than 10^{-14} are ignored since their contributions to the total core damage frequency are insignificant. Sequences below 10^{-14} events/year are considered extremely unlikely events.

The relative cutoff is the maximum frequency difference that is taken into consideration in the sequence analysis calculation. Sequences that are more than 10^{-7} away from the maximum sequence are ignored since their contributions to the total core damage frequency are insignificant.

The absolute cutoff and the relative cutoff are used to reduce the calculation time by reducing the number of sequences included in the simulation.

Consequences are defined in table 3.13.

Table 3.13: Consequences for different safety function failures.

Consequence	Description
GOOD-TRUE	*No core damage*
HS1-TRUE	*Loss of reactivity control* – fast event →core damage
HS1	*Loss of reactivity control combined with failure of other safety functions* – this leads to events that have negligible probabilities.
HS2-TRUE	*Loss of core cooling*; fast event when it is a big LOCA, slow event when it is a small LOCA. Both cases lead to core damage.
HS2	*Loss of core cooling combined with failure of other safety functions* – this leads to events that have negligible probabilities.
HS3-TRUE	*Loss of residual heat removal* – slow event →core damage
HS3	*Loss of residual heat removal combined with failure of other safety functions* – this leads to events that have negligible probabilities.
OT-TRUE	*Overpressure*; can be both fast- and slow-event, both cases lead to core damage.
OT	*Overpressure combined with failure of other safety functions* – this leads to events that have negligible probabilities.

3.10.4 Fire analysis

As explained above, each train is placed in a fire cell, i.e. a physical area where a potential fire cannot spread away. For the purpose of a fire analysis, the fault tree is used and it is supposed that a fire leads to the unavailability of one entire fire cell (so the unavailability of one train). When a construction are using 3 trains that are not symmetrical (construction 1) one has to divide the initial event "Fire" by 3, as follows:

$$\frac{2{,}9\cdot 10^{-3}}{3} = \mathbf{9{,}66 \cdot 10^{-4}}\ \textbf{/year} \tag{3.5}$$

Because a fire in fire cell 3 (figure 3.1) is an H4-event, a reduced IE-frequency is obtained and it is equal to 10^{-2}. In view of this, the calculated fire frequency is equal to **$9.66\cdot10^{-6}$/year.** Thereby (as a simplification) the frequency from fire cell 3 can be excluded and the fire frequency for construction 1 is:

$$\frac{2*(2{,}9\cdot 10^{-3})}{3} = \mathbf{1{,}93 \cdot 10^{-3}}\ \textbf{/year} \tag{3.6}$$

Construction 2 and 3 have symmetric systems, this means explicitly analyzing one train is enough, to get an overall picture of the core damage frequency with fire as initial event. The total fire frequency used for construction 2 and 3 are **$2.9\cdot10^{-3}$/year.**

Fire is applied to one fire cell in every analyze case. All analyzes are performed the same way except for construction 1 where 2 analyzes are performed, one for each system ("Train 1, System 1" and "Train 2, System 1" are identical). Each analysis knocks out a new train and the total frequency is calculated by adding together the three analytical results.

Construction 2 and 3 are analyzed by applying fire in one fire cell, the core damage frequency which is obtained covers all scenarios due to symmetrical structure of the fault trees.

4 Results

4.1 Frequency analysis

4.1.1 Introduction

It is important to assess the plant design and operation with respect to initiating events that could lead to core damage. To do so, frequency analysis is performed to identify those initiating events with the highest contributions to the risk. In addition, sensitivity studies complement this kind of an analysis. Identification of the main contributions to the core damage frequency highlights any weak points for which design and operation changes can be studied.

4.1.1.1 Analyzing conditions of the initiating events

The initiating event induced by fire may be excluded when considering the contribution from the possible initiating events. In fact if the conservative frequency for maximal fire spreading is postulated, it can be seen in table 4.1 that the fire sensitive construction 2 (C2) do not get a contribution above 51.98%, and that construction 1 (C1) and construction 3 (C3) are characterized by much smaller values.

If the "semi realistic" frequency for maximal fire spreading is postulated, it can be seen in table 4.1 that the fire sensitive construction 2 (compared to construction 1 and construction 3) do not get a contribution above 19.11%. This can be considered as a low risk contribution, since the probabilistic safety level would most unlikely change if the fire induced risks were included in the total risk. This is especially the case for construction 1 and 3 where the total core damage contribution in worst case scenario (conservative) is as low as 5.76% and 7.46% respectively. Thereby have IE Fire been excluded from the total core damage contribution that can be seen in Appendix 1 (table A1.1 to A1.19).

FIRE is treated as an initiating event and this would lead to a complete failure of the affected train (i.e., the failure probability is 100%). Such an event is named "Area phenomena - FIRE" and it is a basic event in the fault tree (see Figures 3.4, 3.5 and 3.6).

Table 4.1: Total core damage Contribution from IE Fire.

	C1	C2	C3	O1	O2	O3
Fire contribution (conservative, see 3.7.1) 7.9E-03/year	5.76%	51.98%	7.46%	31.1%	-	8.2%
Fire contribution ("semi realistic", see 3.7.1.1) 2.9E-03/year	2.16%	19.11%	2.47%	-	-	-

Initiating event class H2 includes the initiating event LOOP whose contribution has been implemented into H2 to obtain a clear picture when comparing construction 1, 2 and 3 to Oskarshamn 1, 2 and 3. LOOP is treated as an initiating event with the failure probability 100% on the basic event "electricity input". This means that the off-site power (basic event "TRAINXSYSTEMX C1234" in the fault tree) is assumed to be unavailable. Frequency of LOOP can be seen in 3.8.1.1 and basic event "TRAINXSYSTEMX C1234" can be seen in the fault tree diagrams described in 3.10.1.4.

In this study, initiating events related to S1 Medium LOCA (S1 ML) and S2 Small LOCA (S2 SL) are treated as separate in the management of event classes. S1 ML and S2 SL, however, are included in the initiating event class H3 to obtain a clear picture of the total core damage distribution. Frequency of S1 ML and S2 SL are discussed in subsection 3.8.1.2.

A Large LOCA (LL) is also treated as a separate initiating event. Nevertheless, A LL is included in the initiating event class H4 to obtain a complete picture of the total core damage distribution. Frequency of A LL can be seen in subsection 3.8.1.2.

The buildings have been dimensioned and/or verified against S1 ML, S2 SL and A LL. This means that all systems are assumed to be available. This results in no special system requirements in the fault tree diagrams illustrated in subsection 3.10.1.4, where all basic events are still available.

4.1.2 Construction Evaluations

4.1.2.1 Proposed constructions applied to Oskarshamn reactors

The 3 constructions presented in subsection 3.9.1 are applied to Oskarshamn 1, 2 and 3, in order to determine their performances. As reference, the PSA results included in the safety reports of the 3 Oskarshamn reactors are used. Figures 4.1 to 4.3 show the total core damage distribution for selected initiating events of class H2, H3, and H4. The results are qualitatively similar for the three reactors. No significant differences can be found between the developed construction 1, 2 and 3.

The three constructions give higher probability of core damage for H2 in comparison with O1, O2 and O3, while they predict a lower value for H3 and H4. The 3 constructions got close to 99% total core damage contribution from event class H2. However, the contribution from event class H3 would be larger if fire were included in the total core damage.

The plots show that there are variations between the references Oskarshamn 1, 2 and 3. Most similar total core damage contribution is estimated for Oskarshamn 3 with 82% from event class H2.

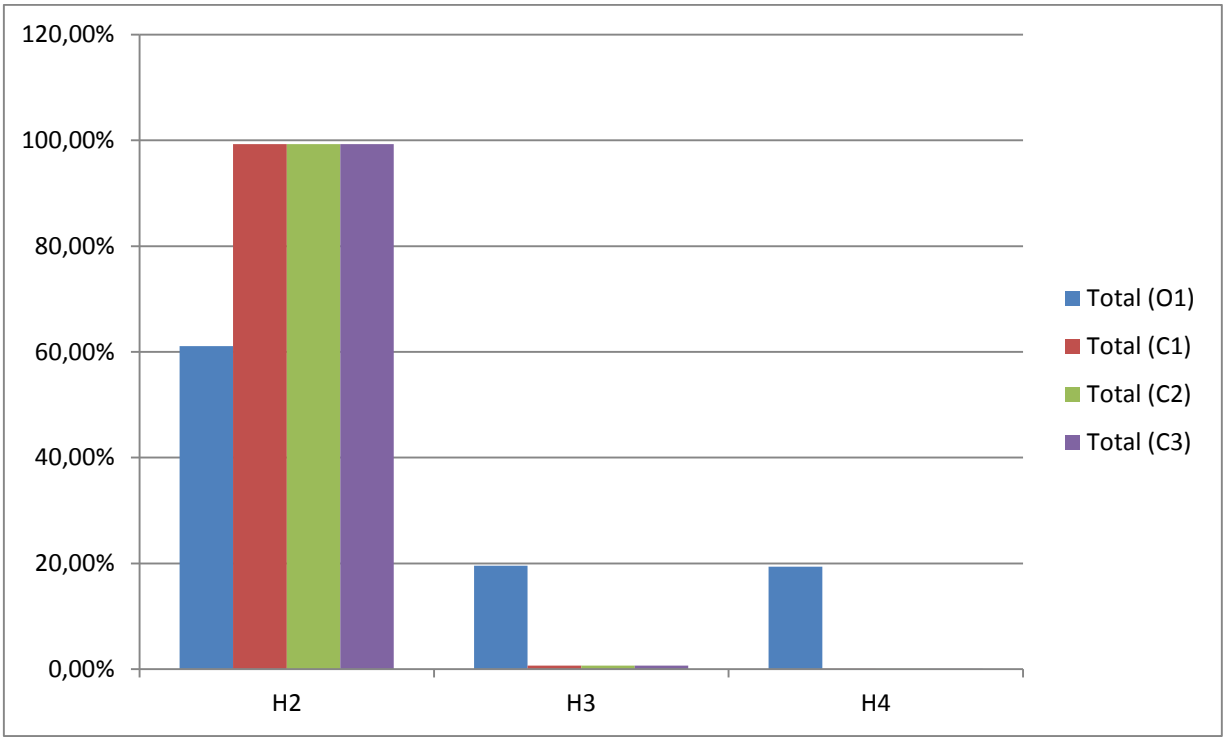


Figure 4.1: Comparison between construction 1, 2 and 3 and reference Oskarshamn 1.

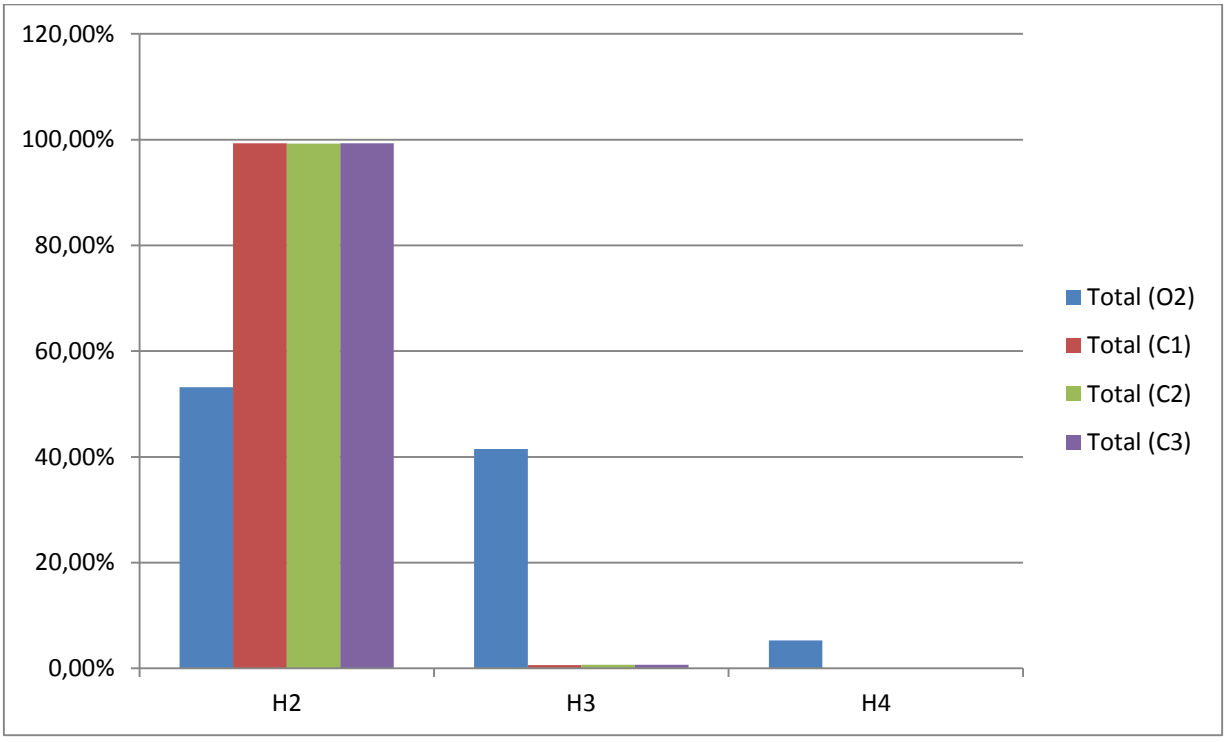


Figure 4.2: Comparison between construction 1, 2 and 3 and reference Oskarshamn 2.

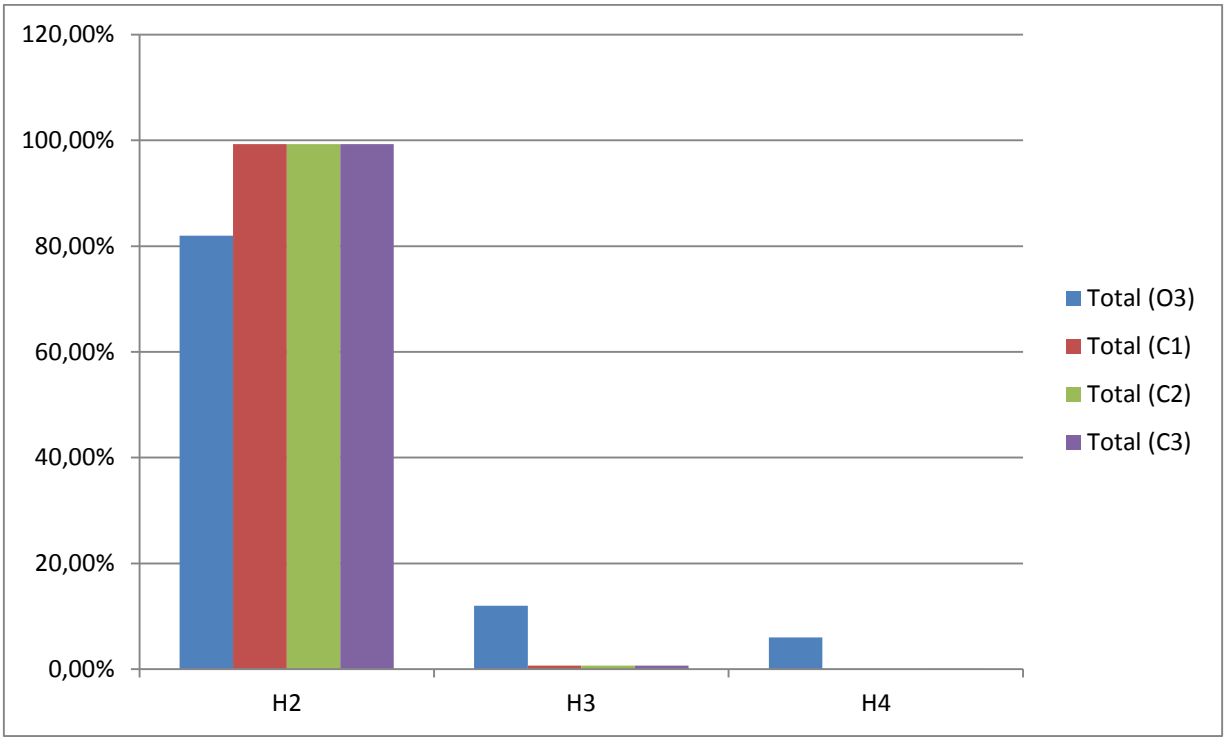


Figure 4.3: Comparison between construction 1, 2 and 3 and reference Oskarshamn 3.

4.1.2.2 Construction 1vs Oskarshamn 2

A more detailed investigation of construction 1 was conducted, because this model resembles the 'three train' construction principle of O2 in a better way.

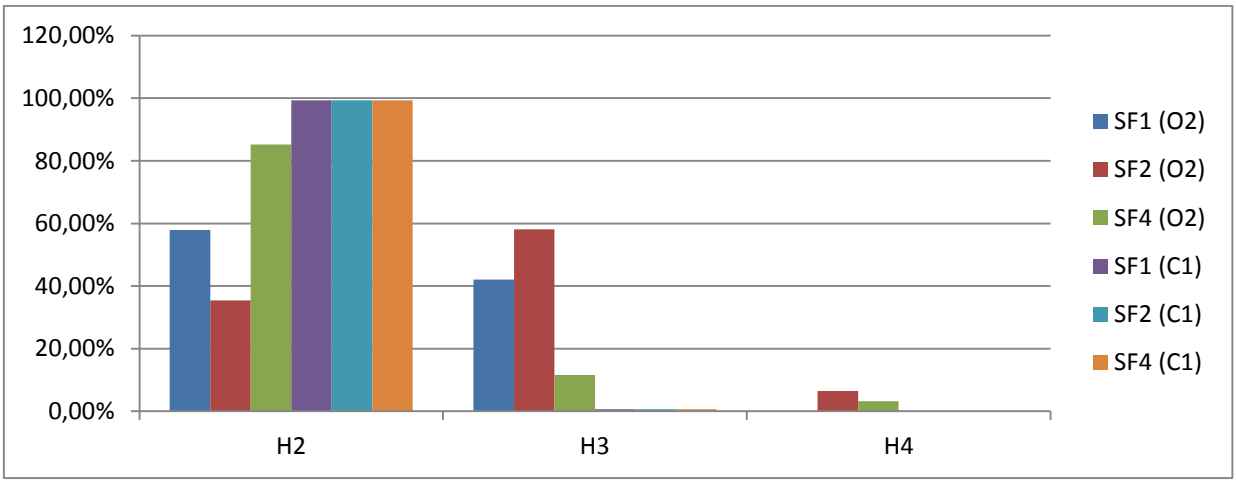


Figure 4.4: Comparison between construction 1 and reference Oskarshamn 2 with respect of the safety functions.

Figure 4.4 shows the relative core damage distribution with respect of the safety functions. SF1 is reactivity control, SF2 is core cooling and SF4 is residual heat removal. The model developed for the safety report of Oskarshamn 2 gives variations between the three safety functions. On the other hand construction 1 got an even distribution. This is due to the fact that construction 1 is very generic, so the event tree is not detailed enough to capture possible variations at the level of different safety functions. Event class H3 and H4 are not visible for construction 1 due to its low contribution (less than 1%). The main difference between Oskarshamn 2 and Construction 1 seems to

be at event class H3, for all safety functions. This appears to be one of the significant differences between a SSMFS 2008:17 reactor and an old reactor.

4.1.2.3 Construction 2vs Oskarshamn 1

Construction 2 takes in account the principle of diversity. Therefore it is further studied in the case of Oskarshamn 1 where diversity plays a relevant role.

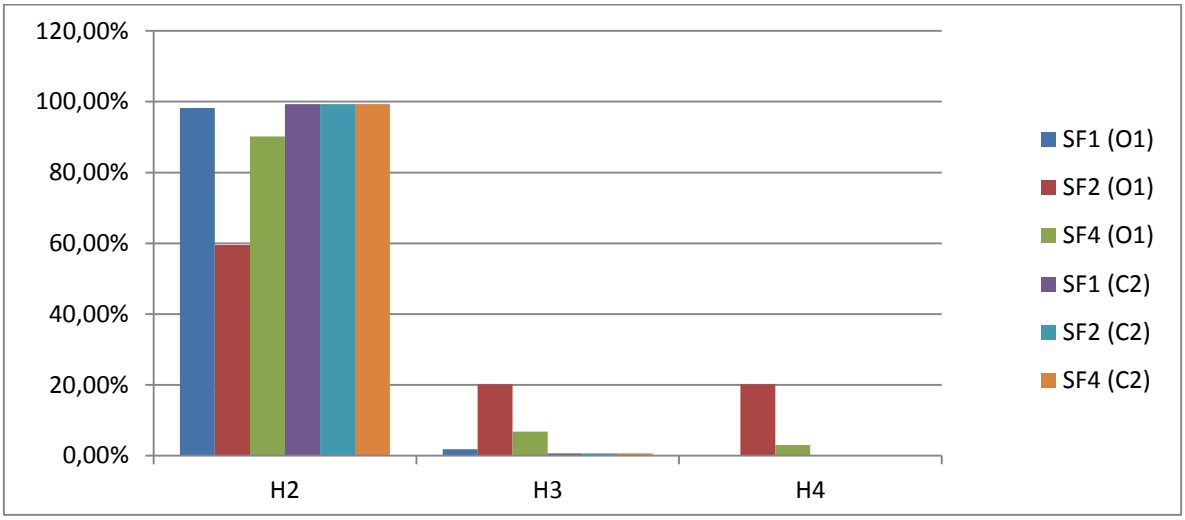


Figure 4.5: Comparison between construction 2 and reference Oskarshamn 1 with respect of the safety functions.

The following can be seen in figure 4.5: the event class H2 give a similar result when SF1 is considered. SF4 also provides a similar result for event class H2, still there is a noticeable difference. Event class H2 has a key difference when SF2 is considered. This difference suggests that Oskarshamn 1 weakness occurs in core cooling (SF2) for event class H3 and H4. Construction 2 event tree is not detailed enough to capture possible variations at the level of different safety functions.

4.1.2.4 Construction 3vs Oskarshamn 3

The model C3 and the reference model of O3 have been built by making use of a similar strategy, i.e. taking in account 'four train'.

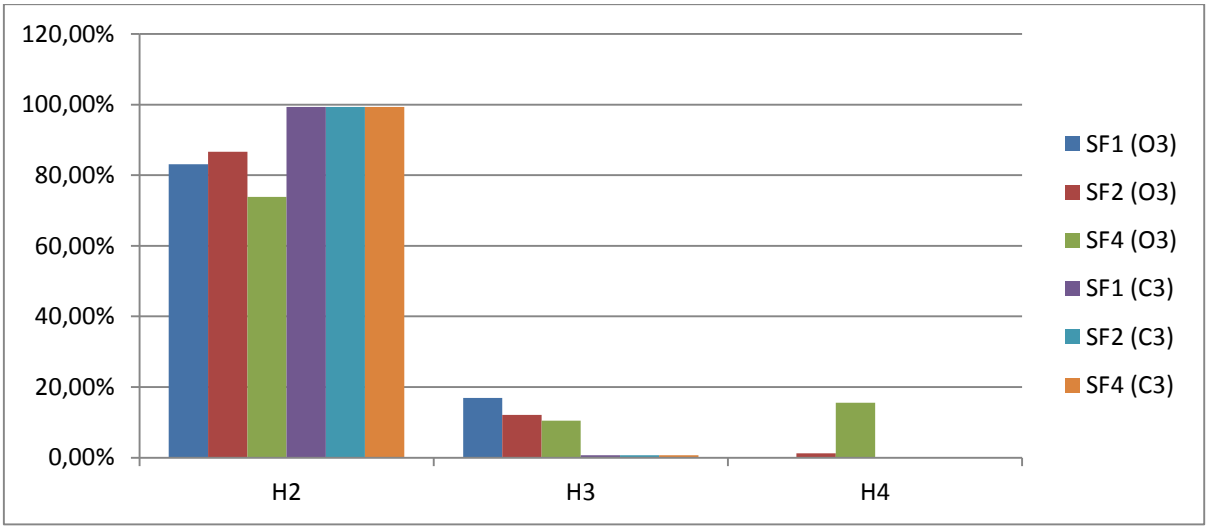


Figure 4.6: Comparison between construction 3 and reference Oskarshamn 3 with respect of the safety functions.

Figure 4.6 shows that the reference model got a rather even core damage distribution over the different safety functions (with the exception of SF4 in event class H4). Main differences between construction 3 and Oskarshamn 3 is the contribution from H3 and H4 events that is close to non-existent in the designs developed in this study.

4.1.3 Conclusion

The three generic PSA models estimate a nearly identical total core damage frequency contribution from different initiating events. Percentage contribution from the initiating events is determined by the frequency of the initiating event and the design of the event tree. The frequency of the initiating event is a set value that does not change between the models. On the other hand the design of the fault tree depends on the specific model. However, it seems that the variation of the fault tree design does not affect the total core damage frequency percentage distribution (between different initiating events - fire excluded) to the extent that clear differences cannot be seen. This indicates that the SSMFS 2008:17 design requirements lead to a specific core damage frequency percentage distribution.

The generic PSA models that have been designed in this work are based on the requirements provided in SSMFS 2008:17 but they do not include several initiating events that may be of great importance in the case of Oskarshamn reactors. The generic models are highly dependent on H2 initiating events. O1 and O2 are the oldest reactors and designed according to regulations of that period, and a generic model may not be suitable for describing such plants (see Figures 4.4 and 4.5). Conversely, O3 is built on a more modern design and a generic PSA model can lead to better results (see Figure 4.6). Therefore a modern reactor that is constructed according to SSMFS 2008:17 would behave and show similar total core damage frequency percentage distribution as the generic models give.

4.1.3.1 FREE PARAMETER

The probabilistic modeling of the plant depends on a free parameter. This free parameter is the probability of failure for the basic event rest faults that is located in all trains for construction 1, 2 and 3 (see figure 3.4 to 3.6). Table 4.2 shows the estimated probability of the free parameter to be equal to the maximum total core damage frequency that can be allowed ($\approx 10^{-5}$), for the three constructions. The free parameter is tuned by iteration in RiskSpectrum so that the total core damage frequency for the different construction models are as close to 10^{-5} as possible.

Table 4.2: Free parameter for the developed models.

Construction model	[Probability] "free parameter"
Construction 1	$5.47 \cdot 10^{-3}$
Construction 2	$1.48 \cdot 10^{-2}$
Construction 3	$1.77 \cdot 10^{-2}$

From the probabilities for construction 1, 2 and 3, it can be noticed that construction 1 requires higher level of quality of its components. In fact the basic event rest faults are all other faults that are not taken into consideration in the probabilistic models developed in this study. Hence comparing the rest fault ratio between the constructions provides an indication of the level of quality required of their components:

$$\frac{Construction\ 2}{Construction\ 1} = \frac{Free\ parameter\ (C2)}{Free\ parameter\ (C1)} = \frac{14.8}{5.47} = 2.7 \tag{4.1}$$

$$\frac{Construction\ 3}{Construction\ 1} = \frac{Free\ parameter\ (C3)}{Free\ parameter\ (C1)} = \frac{17.7}{5.47} = 3.2 \tag{4.2}$$

4.2 System Barrier analysis

4.2.1 Introduction

The aim of a system barrier analysis is to assess the reliability of safety functions and systems which preserve the barriers intact. The two criteria used in system barrier analysis are the core damage frequency and the initiating event frequency. There are target values that the system barriers need to achieve for each event class, and they are reported in Table 4.3.

4.2.2 Construction evaluations

The concept of system barrier analysis is similar to the so-called conditional core damage probability[16]. It can be explained as the probability of core damage any time a particular initiating event may occur. It is given by the ratio between the core damage frequency contribution for an initiating event divided by the initiating event frequency:

$$\frac{Core\ damage\ frequency\ (calculated\ in\ PSA)}{Initiating\ event\ frequency} = barrier \tag{4.3}$$

Table 4.3: Target value on the system barrier for the different event classes. Obtained from table 2 in source [38].

Event class	Target value for the system barrier
H1, H2	1.00E-05
H3	3.00E-04
H4, H5	1.00E-02

Following nomenclature is used in Table 4.4 to 4.6: SF1 (HS1) = reactivity control, SF2 (HS2) = core cooling, SF4 (HS3) = residual heat removal. Oskarshamn 1, 2 and 3 results are omitted in this report due to confidentiality. Complete results are available in [44].

[16] Conditional core damage probability is the probability of core damage. The element of time is incorporated into the calculation allowing the analyst to estimate the risk magnitude for an event at a certain point of time (e.g. at the time of an initiating event). [50]

4.2.2.1 Construction 1 for the case of Oskarshamn 2

From the results summarized in table 4.4, construction 1 shows that no significant weakness affects the plant. In fact the values calculated for the reactivity control system (SF1) are satisfactory. However, comparing the calculated results between the safety functions makes no difference for construction 1. This is due to the fact that construction 1 is very generic, so the event tree is not detailed enough to capture possible variations at the level of different safety functions.

Table 4.4: Calculated barrier for Oskarshamn 2 and construction 1.

	H2	H3	H4	LOOP (H2)	A LL (H4)	S_1 ML (H3)	S_2 SL (H3)
SF1 (HS1) O2	-	-	-	-	-	-	-
SF1 (HS1) C1	3.22E-06	3.22E-06	3.23E-06	4.13E-06	3.23E-06	3.22E-06	3.22E-06
SF2 (HS2) O2	-	-	-	-	-	-	-
SF2 (HS2) C1	3.22E-06	3.22E-06	3.23E-06	4.13E-06	3.23E-06	3.22E-06	3.22E-06
SF4 (HS3) O2	-	-	-	-	-	-	-
SF4 (HS3) C1	3.22E-06	3.22E-06	3.23E-06	4.13E-06	3.23E-06	3.22E-06	3.22E-06

The comparison between table 4.3 and table 4.4 shows that event class H2 is close to the target value and consequently the weakest barrier in construction 1. The calculated barrier values for event class H3 and H4 are at least 100 times better than the target value. Basically, low probability of core damage provides a greater safety margin.

Oskarshamn 2 reference values are missing due to confidentiality. Consequently, there will be no comments about its calculated barrier values.

4.2.2.2 Construction 2 for the case of Oskarshamn 1

From the results summarized in table 4.5, construction 2 shows that no significant weakness affects the plant. In fact the values calculated for all safety functions (SF1, SF2 and SF3) are satisfactory. However, comparing the calculated results between the safety functions makes no difference for construction 2. This is due to the fact that construction 2 is very generic, so the event tree is not detailed enough to capture possible variations at the level of different safety functions.

Table 4.5: Calculated barrier for Oskarshamn 1 and construction 2.

	H2	H3	H4	LOOP (H2)	A LL (H4)	S_1 ML (H3)	S_2 SL (H3)
SF1 (HS1) O1	-	-	-	-	-	-	-
SF1 (HS1) C2	3.3E-06	3.3E-06	3.3E-06	3.8E-06	3.3E-06	3.3E-06	3.3E-06
SF2 (HS2) O1	-	-	-	-	-	-	-
SF2 (HS2) C2	3.3E-06	3.3E-06	3.3E-06	3.8E-06	3.3E-06	3.3E-06	3.3E-06
SF4 (HS3) O1	-	-	-	-	-	-	-
SF4 (HS3) C2	3.3E-06	3.3E-06	3.3E-06	3.8E-06	3.3E-06	3.3E-06	3.3E-06

The comparison between table 4.3 and table 4.5 shows that event class H2 is close to the target value and consequently the weakest barrier in construction 2. The calculated barrier values for event

class H3 and H4 are at least 100 times better than the target value. Basically, low probability of core damage provides a greater safety margin.

Oskarshamn 1 reference values are missing due to confidentiality. Consequently, there will be no comments about its calculated barrier values.

4.2.2.3 Construction 3 for the case of Oskarshamn 3

From the results summarized in table 4.6, construction 3 shows that no significant weakness affects the plant. In fact the values calculated for all safety functions (SF1, SF2 and SF3) are satisfactory. However, comparing the calculated results between the safety functions makes no difference for construction 3. This is due to the fact that construction 3 is very generic, so the event tree is not detailed enough to capture possible variations at the level of different safety functions.

Table 4.6: Calculated barrier for Oskarshamn 3 and construction 3.

	H2	H3	H4	LOOP (H2)	A LL (H4)	S_1 ML (H3)	S_2 SL (H3)
SF1 (HS1) O3	-	-	-	-	-	-	-
SF1 (HS1) C3	3.28E-06	3.28E-06	3.28E-06	3.60E-06	3.28E-06	3.28E-06	3.28E-06
SF2 (HS2) O3	-	-	-	-	-	-	-
SF2 (HS2) C3	3.28E-06	3.28E-06	3.28E-06	3.60E-06	3.28E-06	3.28E-06	3.28E-06
SF4 (HS3) O3	-	-	-	-	-	-	-
SF4 (HS3) C3	3.28E-06	3.28E-06	3.28E-06	3.60E-06	3.28E-06	3.28E-06	3.28E-06

The comparison between table 4.3 and table 4.6 shows that event class H2 is close to the target value and consequently the weakest barrier in construction 3. The calculated barrier values for event class H3 and H4 are at least 100 times better than the target value. Basically, low probability of core damage provides a greater safety margin.

Oskarshamn 3 reference values are missing due to confidentiality. Consequently, there will be no comments about its calculated barrier values.

4.2.3 Conclusion

The three generic PSA models lead to a similar probability in terms of barrier protection, and all the calculated values do not exceed the acceptance criteria based on the free parameter boundary condition, and they ensure that the total core damage frequency is equal to about 10^{-5}/year. This means that barrier safety criteria are fulfilled according to the predictions of all the PSA models and no relevant weaknesses could be observed.

When comparing the results between the O-reactors one can see that there is a large variation between the reactors when considering barrier values at different safety functions. As already mentioned, O1 and O2 are the oldest reactors, while O3 is a more modern BWR-type reactor. The system barrier analysis also confirms that a generic PSA model suits better the more advanced case of O3.

4.3 Sensitivity analysis

4.3.1 Introduction

Sensitivity analysis determines the impact of the input data on the model output. In the current context, the objective of this kind of analysis is to identify the parameters that play the major role in the risk and to reduce the risk by acting on the dominant contributors. The sensitivity analysis in this study is performed by varying one variable while the others are kept constant and equal to their expected (deterministic) values. To do so, RiskSpectrum was used since it has the capability for sensitivity analysis so that sensitivity measures can be obtained for all variables used in the probabilistic safety model. The corresponding results can be valuable information for: plant design, operation, maintenance and tests, human factor and component reliability.

It can be seen from the tables in appendix 1 that the initiating events H2 and LOOP are the ones that contribute the most to the total core damage frequency. Initiating event fire is excluded from the total core damage frequency, but the possible contribution has been evaluated by dividing “core damage frequency due to fire” with total core damage frequency. Sensitivity analysis will consequently be carried out with respect to these 3 IEs. To obtain graphs with clear trends, one may neglect the basic events that have low fraction contribution.

4.3.2 Results

4.3.2.1 Construction 1

4.3.2.1.1 Initiating event “Fire”

Figure 4.7 shows the outcome of the sensitivity analysis with respect to the initiating event “Fire” for construction 1. The nomenclature is explained in Table 4.7. In the graph the basic events are sorted by the magnitude of their Fraction Contribution (FC), where the one with the highest FC is on the left. The largest contributors are from the basic event “rest faults” (32%) in system 1 for safety function SF1, SF2 and SF4. TRAINXSYSTEMX C1234 is the electricity supply from the external power grid, which has a smaller fraction contribution (4.5%). The other basic events can be ignored because their insignificant fraction contribution.

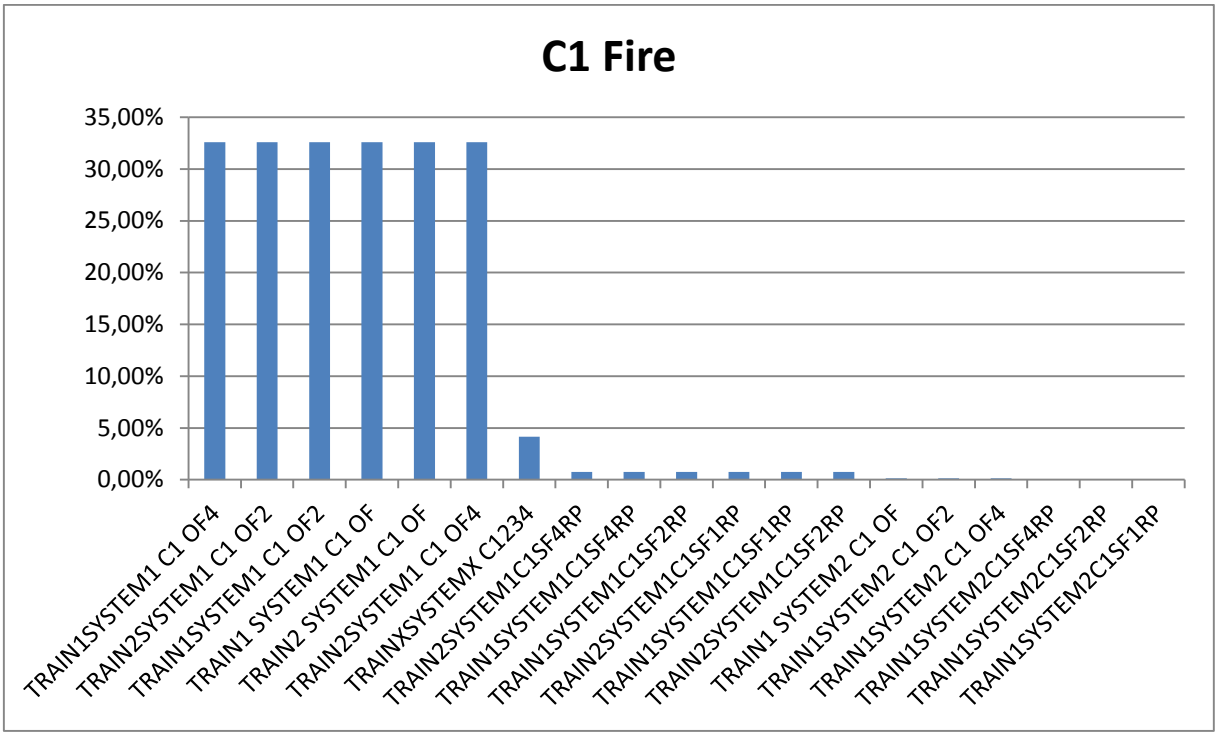


Figure 4.7: Sensitivity analysis with respect to the initiating event "Fire" for construction 1.

Table 4.7: Definition of the nomenclature used in figure 4.7.

Nomenclature	Definition
TRAIN1SYSTEM1 C1 OF4	Basic event "rest faults" in system 1, train 1, residual heat removal (SF4).
TRAIN2SYSTEM1 C1 OF2	Basic event "rest faults" in system 1, train 2, core cooling (SF2).
TRAIN1SYSTEM1 C1 OF2	Basic event "rest faults" in system 1, train 1, core cooling (SF2).
TRAIN1 SYSTEM1 C1 OF	Basic event "rest faults" in system 1, train 1, reactivity control (SF1).
TRAIN2 SYSTEM1 C1 OF	Basic event "rest faults" in system 1, train 2, reactivity control (SF1).
TRAIN2SYSTEM1 C1 OF4	Basic event "rest faults" in system 1, train 2, residual heat removal (SF4).
TRAINXSYSTEMX C1234	Basic event "electricity input" from the external power grid. Used in all systems, trains and constructions.

4.3.2.1.2 Initiating event H2

Figure 4.8 shows the outcome of the sensitivity analysis with respect to the initiating event class "H2" for construction 1. The nomenclature is described in Table 4.8. In the graph the basic events are sorted by the magnitude of their FC (fraction contribution), where the one with the highest FC is on the left. TRAIN1 SYSTEM2 C1 OF, TRAIN1 SYSTEM2 C1 OF2, TRAIN1 SYSTEM2 C1 OF4 are the basic event "rest faults" related to system 2 for the safety functions SF1, SF2 and SF4, respectively, and they give the largest fraction contributors (32.60%) for an H2 IE. These are followed by CCF for the basic event "rest faults" (31.30%) that involves system 1 for the safety functions SF1, SF2 and SF4. Then TRAINXSYSTEMX C1234, which is the electricity supply from the external power grid, has a

contribution of 4.24%. The other basic events can be ignored because their insignificant fraction contribution.

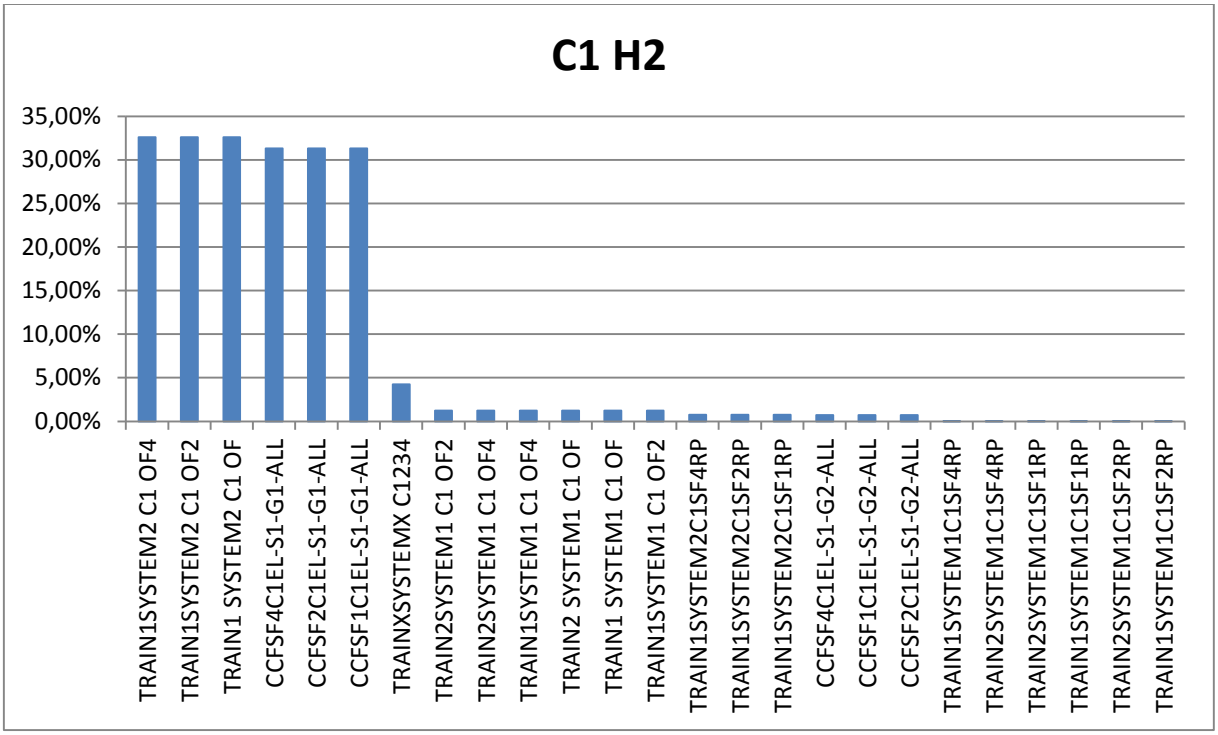


Figure 4.8: Sensitivity analysis with respect to the initiating event class "H2" for construction 1.

Table 4.8: Definition of the nomenclature used in figure 4.8.

Nomenclature	Definition
TRAIN1SYSTEM2 C1 OF4	Basic event "rest faults" in system 2, train 1, residual heat removal (SF4).
TRAIN1SYSTEM2 C1 OF2	Basic event "rest faults" in system 2, train 1, core cooling (SF2).
TRAIN1 SYSTEM2 C1 OF	Basic event "rest faults" in system 2, train 1, reactivity control (SF1).
CCFSF4C1EL-S1-G1-ALL	Common cause failure for the basic event "rest faults" in system 1, safety function residual heat removal (SF4).
CCFSF2C1EL-S1-G1-ALL	Common cause failure for the basic event "rest faults" in system 1, safety function core cooling (SF2).
CCFSF1C1EL-S1-G1-ALL	Common cause failure for the basic event "rest faults" in system 1, safety function reactivity control (SF1).

4.3.2.1.3 Initiating event LOOP

Figure 4.9 shows the sensitivity analysis on the initiating event "LOOP" for construction 1. In Table 4.9 explanation of the nomenclature is reported. In the graph the basic events are ordered from left to right with respect to the magnitude of their FCs. LOOP 100 is the event that knocks out off site power. LOOP100 concerns the basic event "electricity input" that affects all systems (S1 and S2) and all safety functions (SF1, SF2 and SF4). This has the highest fraction contribution to the core damage frequency (30.70%). TRAIN1 SYSTEM2 C1 OF, TRAIN1 SYSTEM2 C1 OF2, TRAIN1 SYSTEM2 C1 OF4, i.e. the basic event "rest faults" of system 2 for safety functions SF1, SF2 and SF4, respectively, have the

second biggest impact (27.90%). CCF on the basic event “rest faults” of system 1 for safety function SF1, SF2 and SF4 also play an important role (26.60%). The basic event “reserve power – diesel generator” for train 1 in system 2 has, as expected, large fraction contribution as the plant lost off-site power (5.48%). Same thing can be said for CCF on the basic event “reserve power” for system 1 in all safety functions (SF1, SF2 and SF4) (5.24%). The other basic events have negligible contributions.

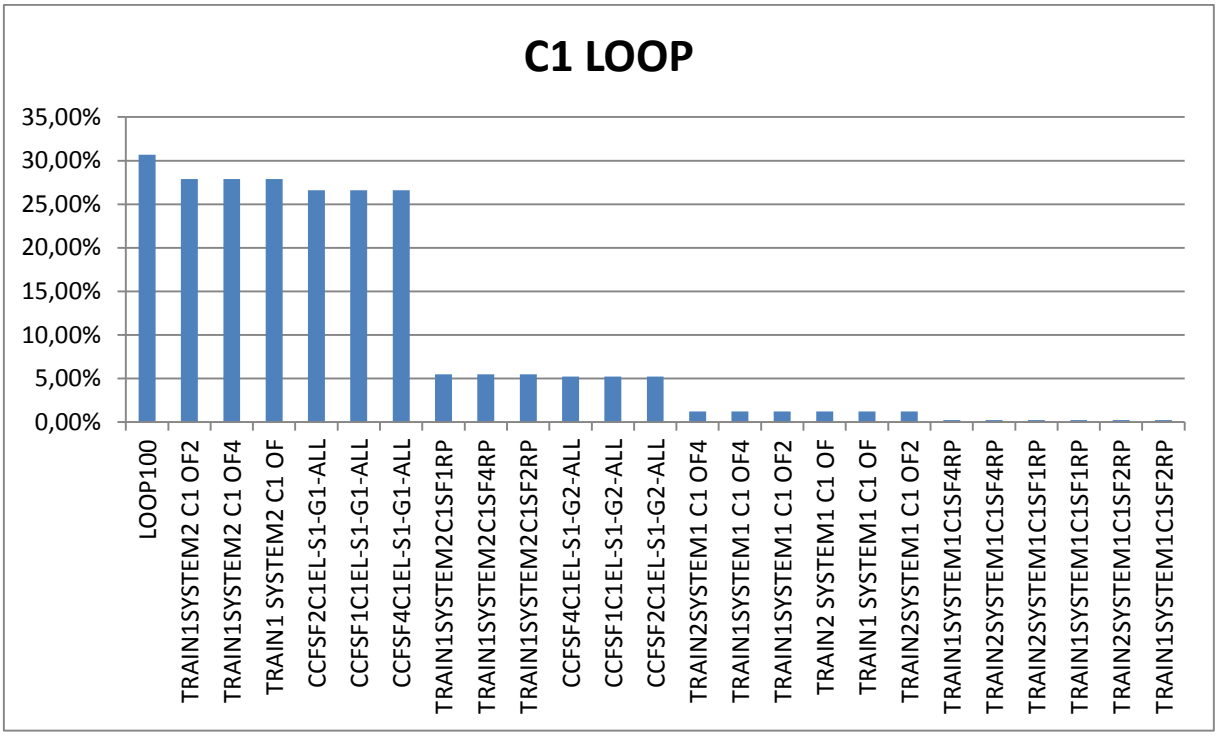


Figure 4.9: Sensitivity analysis with respect to the initiating event “LOOP” for construction 1.

Table 4.9: Definition of the nomenclature used in figure 4.9.

Nomenclature	Definition
LOOP100	Initiating event that gives basic event "electricity input" a failure probability of 100%. Affects all systems, trains and safety functions.
TRAIN1SYSTEM2 C1 OF2	Basic event "rest faults" in system 2, train 1, core cooling (SF2).
TRAIN1 SYSTEM2 C1 OF	Basic event "rest faults" in system 2, train 1, reactivity control (SF1).
TRAIN1SYSTEM2 C1 OF4	Basic event "rest faults" in system 2, train 1, residual heat removal (SF4).
CCFSF4C1EL-S1-G1-ALL	Common cause failure for the basic event "rest faults" in system 1, safety function residual heat removal (SF4).
CCFSF2C1EL-S1-G1-ALL	Common cause failure for the basic event "rest faults" in system 1, safety function core cooling (SF2).
CCFSF1C1EL-S1-G1-ALL	Common cause failure for the basic event "rest faults" in system 1, safety function reactivity control (SF1).
TRAIN1SYSTEM2C1SF1RP	Basic event "auxiliary power" in system 2, train 1, reactivity control (SF1).
TRAIN1SYSTEM2C1SF4RP	Basic event "auxiliary power" in system 2, train 1, residual heat removal (SF4).
TRAIN1SYSTEM2C1SF2RP	Basic event "auxiliary power" in system 2, train 1, core cooling (SF2).
CCFSF4C1EL-S1-G2-ALL	Common cause failure for the basic event "auxiliary power" in system 1, safety function residual heat removal (SF4).
CCFSF1C1EL-S1-G2-ALL	Common cause failure for the basic event "auxiliary power" in system 1, safety function reactivity control (SF1).
CCFSF2C1EL-S1-G2-ALL	Common cause failure for the basic event "auxiliary power" in system 1, safety function core cooling (SF2).

4.3.2.2 Construction 2

4.3.2.2.1 Initiating event "Fire"

Figure 4.10 shows the sensitivity analysis on the initiating event "Fire" for construction 2. In the graph the basic events are sorted by the magnitude of their Fraction Contribution (FC), where the basic event with the highest FC is on the left. The basic events "rest faults" in system 2 and 3 for safety function SF1, SF2 and SF4 have the highest fraction contributions to the core damage frequency (33.10%). The reason that system 1 is not in this category is that the IE FIRE takes out system 1 in this simulation. TRAINXSYSTEMX C1234 is the power supply from the external power grid, which has a marginal fraction contribution (1.53%). The other basic events can be ignored because their insignificant fraction contribution.

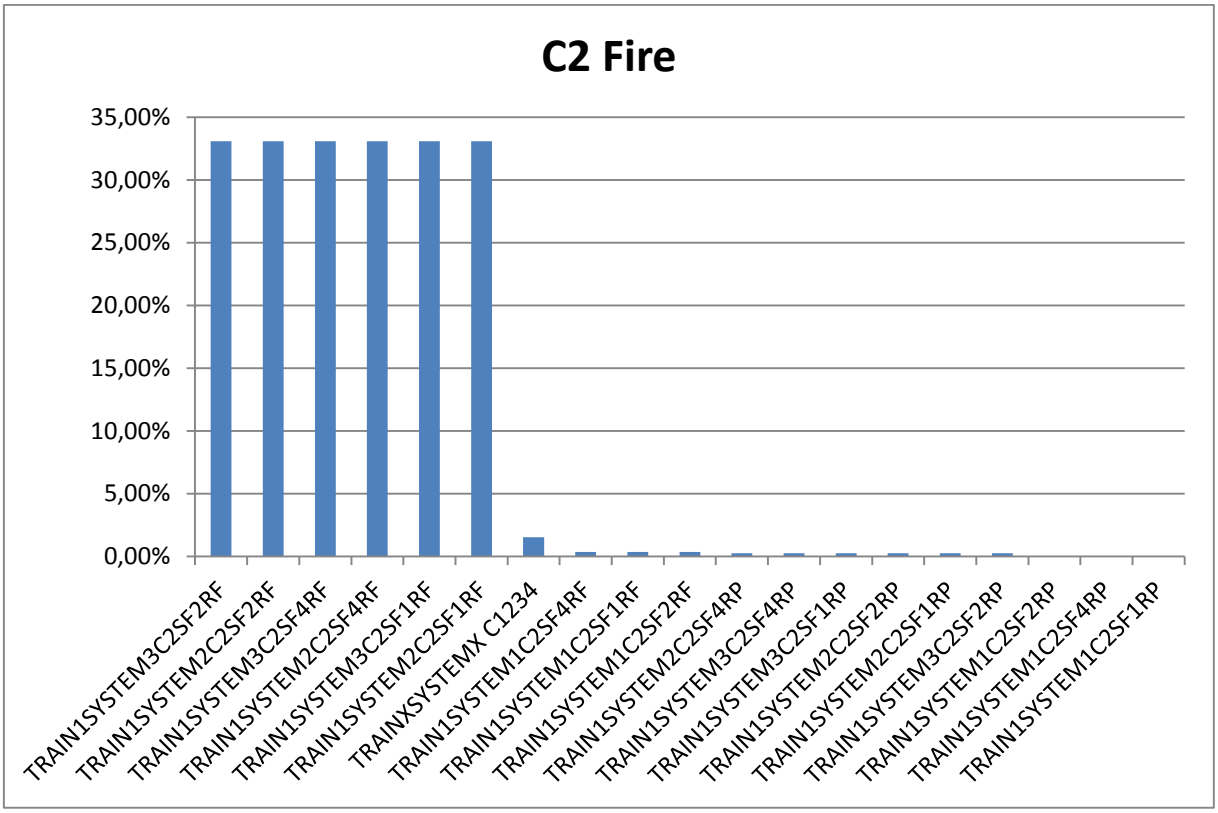


Figure 4.10: Sensitivity analysis with respect to the initiating event "FIRE" for construction 2.

Table 4.10: Definition of the nomenclature used in figure 4.10.

Nomenclature	Definition
TRAIN1SYSTEM3C2SF2RF	Basic event "rest faults" in system 3, train 1, core cooling (SF2).
TRAIN1SYSTEM2C2SF2RF	Basic event "rest faults" in system 2, train 1, core cooling (SF2).
TRAIN1SYSTEM3C2SF4RF	Basic event "rest faults" in system 3, train 1, residual heat removal (SF4).
TRAIN1SYSTEM2C2SF4RF	Basic event "rest faults" in system 2, train 1, residual heat removal (SF4).
TRAIN1SYSTEM3C2SF1RF	Basic event "rest faults" in system 3, train 1, reactivity control (SF1).
TRAIN1SYSTEM2C2SF1RF	Basic event "rest faults" in system 2, train 1, reactivity control (SF1).

4.3.2.2.2 Initiating event "H2"

Figure 4.11 shows the sensitivity analysis on the initiating event class "H2" for construction 2. The details of the nomenclature are summarized in Table 4.11. In the graph the basic events are sorted by the magnitude of their FC, where the basic event with the largest FC is on the left. The dominating contributions come from the basic events "rest faults" (33.10%) in all trains, and for all safety functions (SF1, SF2 and SF4). TRAINXSYSTEMX C1234 is the electrical power supply from the external power grid, and it has a small influence (2.35%). The other basic events can be ignored because their insignificant fraction contribution.

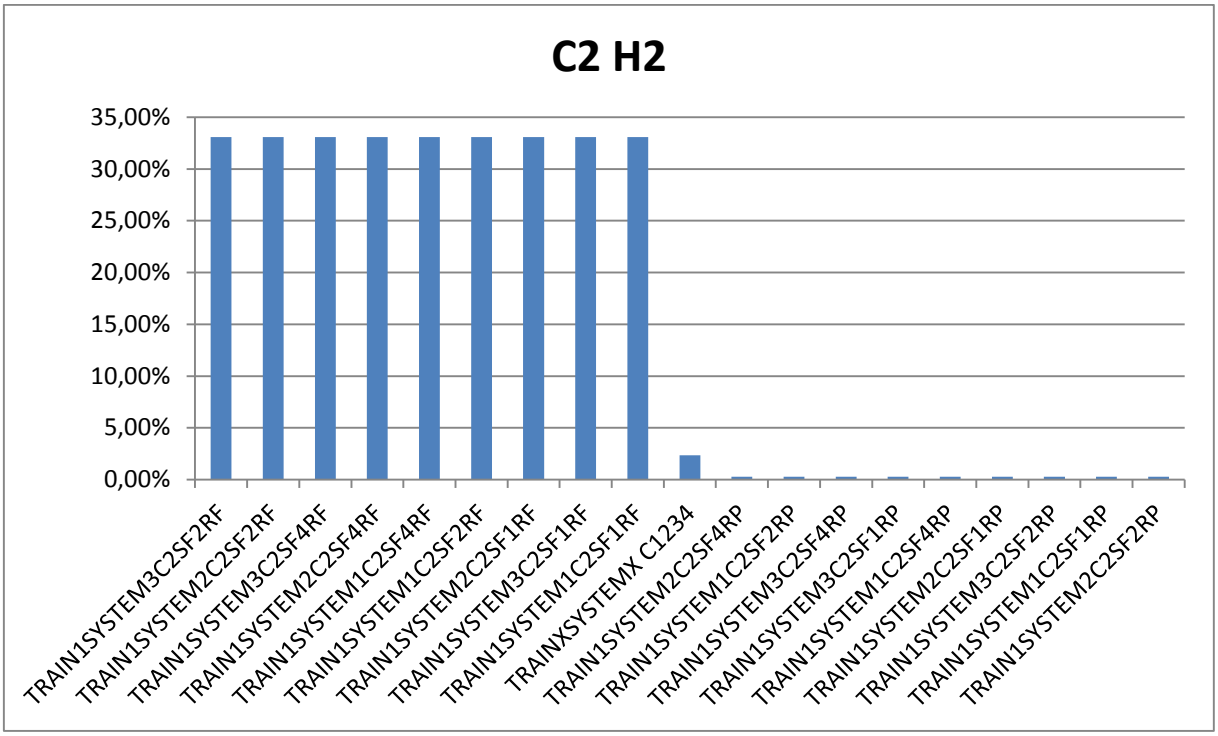


Figure 4.11: Sensitivity analysis with respect to the initiating event class "H2" for construction 2.

Table 4.11: Definition of the nomenclature used in figure 4.11.

Nomenclature	Definition
TRAIN1SYSTEM3C2SF2RF	Basic event "rest faults" in system 3, train 1, core cooling (SF2).
TRAIN1SYSTEM2C2SF2RF	Basic event "rest faults" in system 2, train 1, core cooling (SF2).
TRAIN1SYSTEM3C2SF4RF	Basic event "rest faults" in system 3, train 1, residual heat removal (SF4).
TRAIN1SYSTEM2C2SF4RF	Basic event "rest faults" in system 2, train 1, residual heat removal (SF4).
TRAIN1SYSTEM3C2SF1RF	Basic event "rest faults" in system 3, train 1, reactivity control (SF1).
TRAIN1SYSTEM2C2SF1RF	Basic event "rest faults" in system 2, train 1, reactivity control (SF1).
TRAIN1SYSTEM1C2SF2RF	Basic event "rest faults" in system 1, train 1, core cooling (SF2).
TRAIN1SYSTEM1C2SF4RF	Basic event "rest faults" in system 1, train 1, residual heat removal (SF4).
TRAIN1SYSTEM1C2SF1RF	Basic event "rest faults" in system 1, train 1, reactivity control (SF1).
TRAINXSYSTEMX C1234	Basic event "electricity input" from the external power grid. Used in all systems, trains and constructions.

4.3.2.2.3 Initiating event "LOOP"

Figure 4.12 shows the sensitivity analysis on the initiating event "LOOP" for construction 2. Table 4.12 provides the description of the nomenclature. In the graph the basic events are sorted by the magnitude of their FC, where the basic event with the largest FC is on the left. The major contributions come from the basic events "rest faults" (31%) in all trains and for all safety functions (SF1, SF2 and SF4). The fraction contributions are even larger than for LOOP100 (19.4%) which leads to a failure of the electricity supply to all trains. This is the only initiating event where one can notice

the basic event “auxiliary power” (2.31%) from the diesel generators in all trains for all safety functions. The other basic events can be ignored because their insignificant fraction contribution.

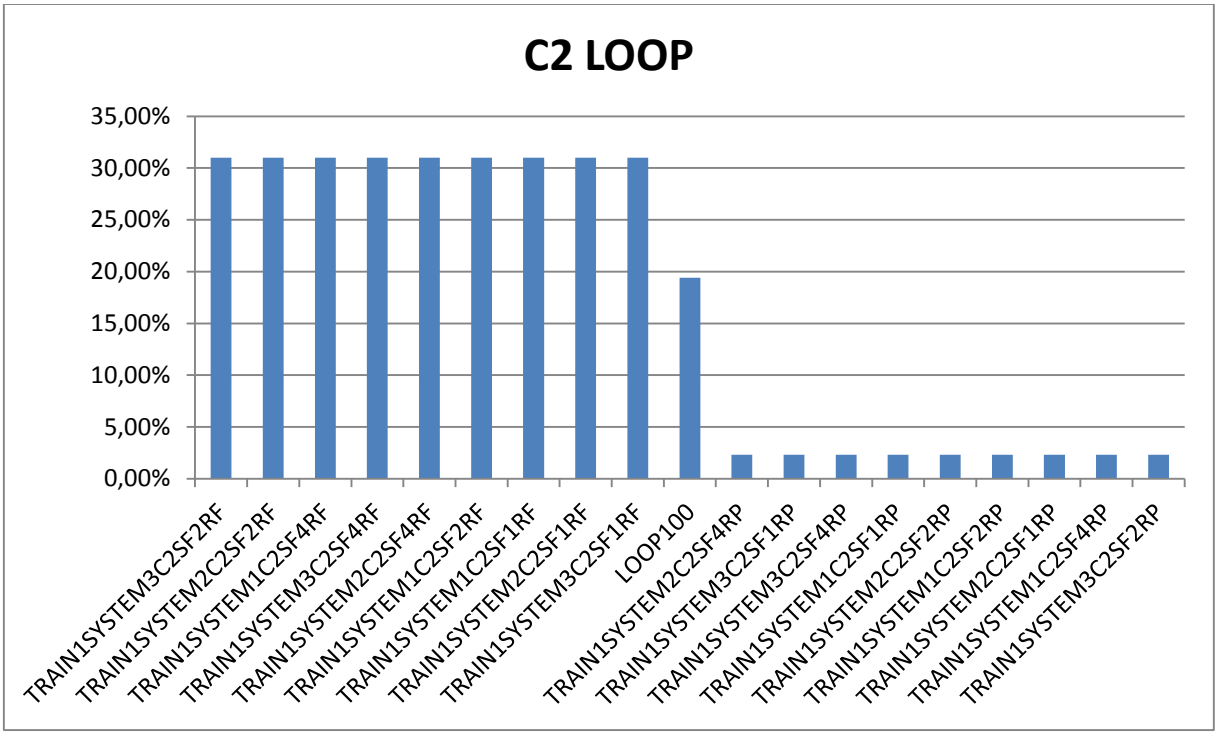


Figure 4.12: Sensitivity analysis with respect to the initiating event “LOOP” for construction 2.

Table 4.12: Definition of the nomenclature used in figure 4.12.

Nomenclature	Definition
LOOP100	Initiating event that gives basic event "electricity input" a failure probability of 100%. Affects all systems, trains and safety functions.
TRAIN1SYSTEM3C2SF2RF	Basic event "rest faults" in system 3, train 1, core cooling (SF2).
TRAIN1SYSTEM2C2SF2RF	Basic event "rest faults" in system 2, train 1, core cooling (SF2).
TRAIN1SYSTEM3C2SF4RF	Basic event "rest faults" in system 3, train 1, residual heat removal (SF4).
TRAIN1SYSTEM2C2SF4RF	Basic event "rest faults" in system 2, train 1, residual heat removal (SF4).
TRAIN1SYSTEM3C2SF1RF	Basic event "rest faults" in system 3, train 1, reactivity control (SF1).
TRAIN1SYSTEM2C2SF1RF	Basic event "rest faults" in system 2, train 1, reactivity control (SF1).
TRAIN1SYSTEM1C2SF2RF	Basic event "rest faults" in system 1, train 1, core cooling (SF2).
TRAIN1SYSTEM1C2SF4RF	Basic event "rest faults" in system 1, train 1, residual heat removal (SF4).
TRAIN1SYSTEM1C2SF1RF	Basic event "rest faults" in system 1, train 1, reactivity control (SF1).
TRAIN1SYSTEM3C2SF2RP	Basic event "auxiliary power" in system 3, train 1, core cooling (SF2).
TRAIN1SYSTEM2C2SF2RP	Basic event "auxiliary power" in system 2, train 1, core cooling (SF2).
TRAIN1SYSTEM3C2SF4RP	Basic event "auxiliary power" in system 3, train 1, residual heat removal (SF4).
TRAIN1SYSTEM2C2SF4RP	Basic event "auxiliary power" in system 2, train 1, residual heat removal (SF4).
TRAIN1SYSTEM3C2SF1RP	Basic event "auxiliary power" in system 3, train 1, reactivity control (SF1).
TRAIN1SYSTEM2C2SF1RP	Basic event "auxiliary power" in system 2, train 1, reactivity control (SF1).
TRAIN1SYSTEM1C2SF2RP	Basic event "auxiliary power" in system 1, train 1, core cooling (SF2).
TRAIN1SYSTEM1C2SF4RP	Basic event "auxiliary power" in system 1, train 1, residual heat removal (SF4).
TRAIN1SYSTEM1C2SF1RP	Basic event "auxiliary power" in system 1, train 1, reactivity control (SF1).

4.3.2.3 Construction 3

4.3.2.3.1 Initiating event "Fire"

Figure 4.13 shows the sensitivity analysis of construction 3, given as initiating event "Fire". The explanation of the nomenclature is given in Table 4.13. In the graph the basic events are sorted by the magnitude of their FCs, where the basic event with the highest FC is on the left. FIRE is the initiating event so this basic event will be ignored in the sensitivity analysis. The FIRE was assumed to occur in the area where train 1 of system 1 is placed and causes the entire train to fail. This increases the contribution (30.20%) from the basic events "rest faults" in train 2 of system 1, for safety functions SF1, SF2 and SF4. There is also a high contribution (29.50%) from CCF for the basic events "rest faults" in system 2 for all safety functions SF1, SF2 and SF4. The other basic events can be ignored because their insignificant contribution.

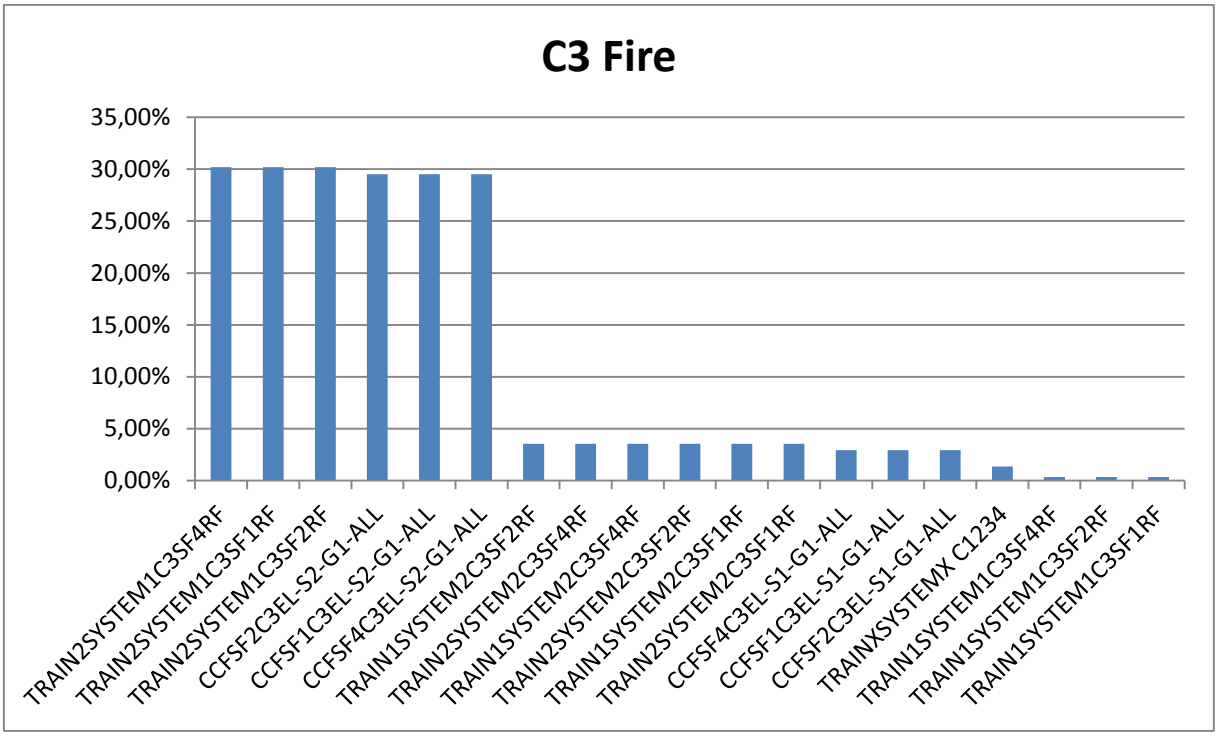


Figure 4.13: Sensitivity analysis with respect to the initiating event "FIRE" for construction 3.

Table 4.13: Definition of the nomenclature used in figure 4.13.

Nomenclature	Definition
TRAIN2SYSTEM1C3SF4RF	Basic event "rest faults" in system 1, train 2, residual heat removal (SF4).
TRAIN2SYSTEM1C3SF1RF	Basic event "rest faults" in system 1, train 2, reactivity control (SF1).
TRAIN2SYSTEM1C3SF2RF	Basic event "rest faults" in system 1, train 2, core cooling (SF2).
CCFSF2C3EL-S2-G1-ALL	Common cause failure for the basic event "rest faults" in system 2, safety function core cooling (SF2).
CCFSF1C3EL-S2-G1-ALL	Common cause failure for the basic event "rest faults" in system 2, safety function reactivity control (SF1).
CCFSF4C3EL-S2-G1-ALL	Common cause failure for the basic event "rest faults" in system 2, safety function residual heat removal (SF4).

4.3.2.3.2 Initiating event "H2"

Figure 4.14 shows the sensitivity analysis on the initiating event "H2" for construction 3. The explanation of the nomenclature is given in Table 4.14. In the graph the basic events are sorted by their FC values, where the basic event with the highest FC is on the left. H2 is the initiating event so this basic event will be ignored in the sensitivity analysis. The dominating contributors (29.50%) are CCF on the basic event "rest faults" for both systems (system 1 and 2) and for all safety functions (SF1, SF2 and SF4). The basic events "rest faults" in all trains and for all safety functions give a somewhat of a small fraction of the risk, i.e. 3.57%. The other basic events can be ignored because their insignificant fraction contribution.

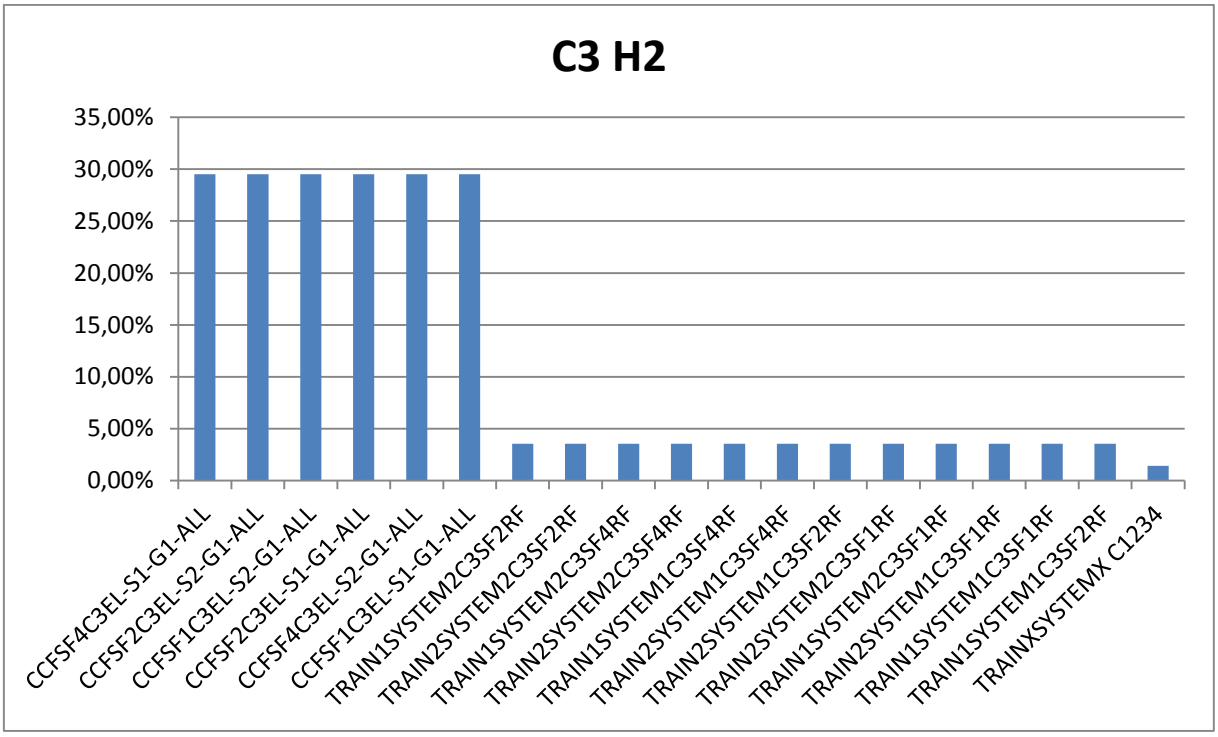


Figure 4.14: Sensitivity analysis with respect to the initiating event class "H2" for construction 3.

Table 4.14: Definition of the nomenclature used in figure 4.14.

Nomenclature	Definition
CCFSF2C3EL-S1-G1-ALL	Common cause failure for the basic event "rest faults" in system 1, safety function core cooling (SF2).
CCFSF1C3EL-S1-G1-ALL	Common cause failure for the basic event "rest faults" in system 1, safety function reactivity control (SF1).
CCFSF4C3EL-S1-G1-ALL	Common cause failure for the basic event "rest faults" in system 1, safety function residual heat removal (SF4).
CCFSF2C3EL-S2-G1-ALL	Common cause failure for the basic event "rest faults" in system 2, safety function core cooling (SF2).
CCFSF1C3EL-S2-G1-ALL	Common cause failure for the basic event "rest faults" in system 2, safety function reactivity control (SF1).
CCFSF4C3EL-S2-G1-ALL	Common cause failure for the basic event "rest faults" in system 2, safety function residual heat removal (SF4).

4.3.2.3.3 Initiating event "LOOP"

Figure 4.15 shows the sensitivity analysis on the initiating event "LOOP" for construction 3. The nomenclature is described in Table 4.15. In the graph the basic events are sorted by their FC values, where the basic event with the highest FC is on the left. The most important factor is once again the contribution from CCF on the basic events "rest faults" for both systems (system 1 and 2) and for all safety functions (SF1, SF2 and SF4), that is evaluated equal to 27.8%. Such a contribution is even larger than LOOP100 (12.8%) which knocks out electricity input for all trains. The contributions from "rest faults" in all trains for all safety functions are smaller (3.55%). CCF of the auxiliary power from the diesel generators has a contribution of 1.7% and is not displayed in this graph. The other basic events can be ignored because their insignificant fraction contribution.

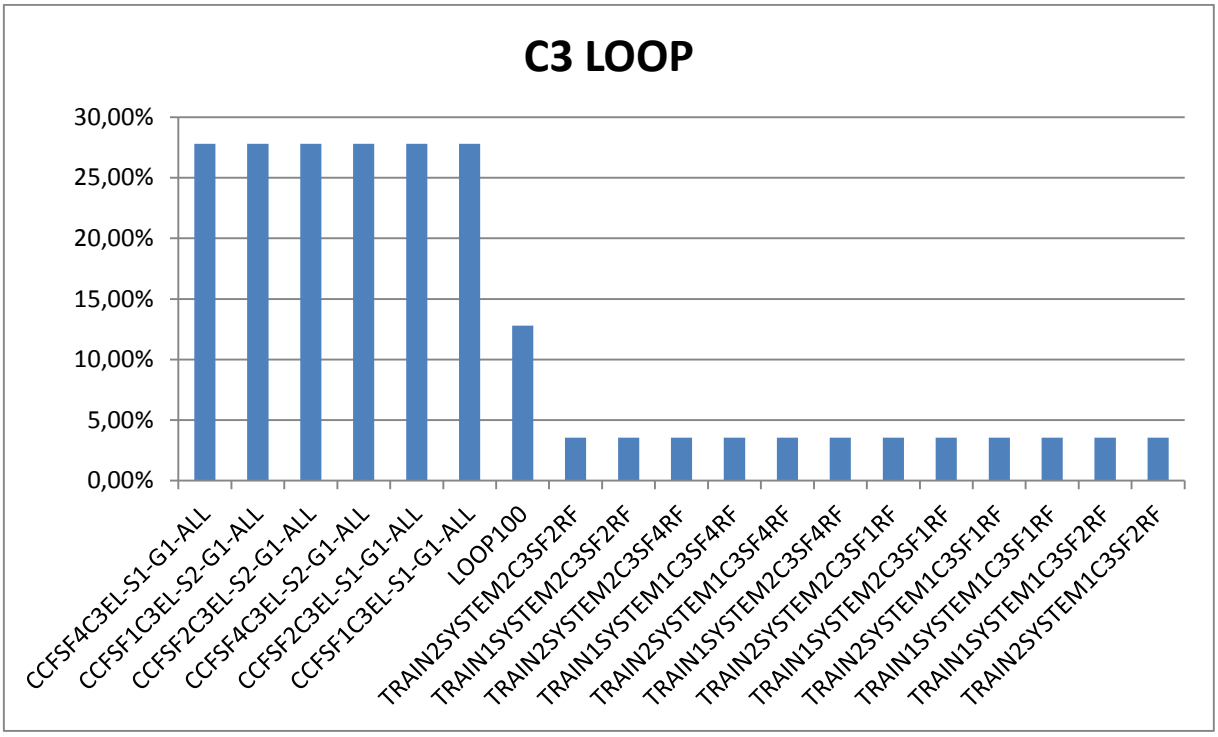


Figure 4.15: Sensitivity analysis with respect to the initiating event "LOOP" for construction 3.

Table 4.15: Definition of the nomenclature used in figure 4.15.

Nomenclature	Definition
CCFSF2C3EL-S1-G1-ALL	Common cause failure for the basic event "rest faults" in system 1, safety function core cooling (SF2).
CCFSF1C3EL-S1-G1-ALL	Common cause failure for the basic event "rest faults" in system 1, safety function reactivity control (SF1).
CCFSF4C3EL-S1-G1-ALL	Common cause failure for the basic event "rest faults" in system 1, safety function residual heat removal (SF4).
CCFSF2C3EL-S2-G1-ALL	Common cause failure for the basic event "rest faults" in system 2, safety function core cooling (SF2).
CCFSF1C3EL-S2-G1-ALL	Common cause failure for the basic event "rest faults" in system 2, safety function reactivity control (SF1).
CCFSF4C3EL-S2-G1-ALL	Common cause failure for the basic event "rest faults" in system 2, safety function residual heat removal (SF4).
LOOP100	Initiating event that gives basic event "electricity input" a failure probability of 100%. Affects all systems, trains and safety functions.

4.3.3 Conclusion

Generic models that are constructed according to SSMFS 2008:17 are sensitive to H2 events. However, no weakness towards Initiating event class H3 and H4 is found. To be able to get a more specific PSA model one must further develop the basic event "rest faults" into appropriate sub-system.

The result of construction 2 clearly shows that fire mitigating measures are required. In addition, according to the calculations based on constructions 1 and 3, SSMFS 2008:17 design requirements

leads to a design that is fire resistant. In view of this, fire can be excluded from the total core damage frequency calculations in PSA level 1 studies for construction 1 and 3. Finally, construction 3 is the simplest design in which measures for the reduction of the fire frequency are not needed.

The sensitivity study summarized in table 4.16 compares the case of fire as initiating event with a semi-realistic fire frequency and the case with a conservative fire frequency. It can be seen that measures to reduce the fire frequency[17] are crucial for reactors whose safety systems consist of 3 trains (construction 1 and 2). Construction 2 fulfills SSMFS 2008:17 design requirements but it would have its fire contribution drastically lowered (close to construction 3).). In the case of construction 1, the system 2 fire cell is inert, i.e. measures to reduce the fire frequency has already been applied to construction 1 in table 4.16 results. (Where % in table 4.16 means contribution to the total core damage frequency)

Table 4.16: Semi realistic fire frequency compared with conservative fire frequency for construction 1, 2 and 3.

IE	IF FIRE (semi-realistic fire frequency)	IE FIRE (conservative fire frequency)
Construction 1	2.16%	5.70%
Construction 2	19.01%	51.98%
Construction 3	2.47%	7.46%

The results in the section LOOP shows that loss of off-site power has a noticeable effect on the total core damage on SSMFS 2008:17 reactors. The contribution can be lowered by implementing one more diesel generator per train so the basic event “reserve power” (auxiliary power) acquires redundancy.

The results from the basic events shows that the dominating risk contribution for C1 and C3 is CCF on the basic event “rest fault”. The dominating risk contribution for construction 2 is the basic event “rest faults”, CCF cannot occur due to C2’s diversification design. This displays that generic models that are constructed according to Swedish radiation authority are sensitive to the basic event “rest faults”.

4.4 Validation

4.4.1 Introduction

The validation method used in this section is based on the safety evaluation study that was conducted on Oskarshamn 1, 2 and 3.

OKG method for nuclear safety is based on both deterministic and probabilistic approaches and details can be found in [42]. Probabilistic and deterministic results are expected to be consistent with each other. A safety evaluation of construction 1, 2 and 3 was performed according to the evaluation method developed in [42].

[17] Fire measures that can be introduced to reduce the fire frequency include e.g. additional extinguishing devices, fire trained and adequately equipped personal or lowering of oxygen levels.

The deterministic evaluation focuses on specific event sequences and the goal is to predict in a deterministic fashion the actual state of the system with respect to the event sequence under study. Therefore plant parameters that are connected to the integrity of the barriers and to the performance of the safety systems are estimated. Finally, the potential consequences of the events are evaluated. This information is used as coordinates in a decision matrix (table 4.17) where the safety significance of the issue at hand is decided. Four risk categories are used: Negligible, Low, Moderate or High safety significance. [42]

Table 4.17: Deterministic decision matrix used to determine the impact on the reactor safety. It is obtained from Table 2 [43]

Potential consequences		Moderate			Significant			Considerable	
Robustness of the safety concept	Robust	Acceptable	Insufficient	Robust	Acceptable	Insufficient	Robust	Acceptable	Insufficient
Event frequency									
H1, H2	LOW	LOW	MODERATE	MODERATE	HIGH	HIGH	HIGH	HIGH	HIGH
H3	NEGLIGIBLE	NEGLIGIBLE	LOW	LOW	MODERATE	HIGH	MODERATE	MODERATE	HIGH
H4	NEGLIGIBLE	NEGLIGIBLE	NEGLIGIBLE	NEGLIGIBLE	LOW	LOW	LOW	LOW	MODERATE
H5	NEGLIGIBLE	NEGLIGIBLE	NEGLIGIBLE	NEGLIGIBLE	NEGLIGIBLE	NEGLIGIBLE	NEGLIGIBLE	LOW	LOW

The probabilistic evaluation is such that the contributions to the core damage frequency are quantified by considering all the possible event sequences that can start from a certain safety issue. The values for each contribution are normalized with respect to the plant total core damage frequency, and the ratio is called “relative risk contribution”. The plant total core damage frequency is the basis for determining the “probabilistic safety level”. Probabilistic safety level and relative risk contribution are used in a decision matrix where the safety significance of the question at issue can be identified (see table 4.18). Similar to Table 4.17, four different risk categories are implemented, namely negligible, low, moderate or high safety significance. [42]

Table 4.18: Probabilistic decision matrix used to determine the impact on the reactor safety. It is obtained from Table 3 [43]

The relative safety significance of	SAFETY LEVEL OF THE NUCLEAR PLANT			
the question at issue	GOOD	ACCEPTABLE	UNCERTAIN	INSUFFICIENT
S≥100	HIGH	HIGH	HIGH	HIGH
100>S≥30	MODERATE	HIGH	HIGH	HIGH
30>S≥10	MODERATE	MODERATE	HIGH	HIGH
10>S≥3	LOW	MODERATE	HIGH	HIGH
3>S≥1	LOW	LOW	MODERATE	HIGH
1>S≥0.3	NEGLIGIBLE	LOW	MODERATE	MODERATE
0.3>S≥0.1	NEGLIGIBLE	NEGLIGIBLE	LOW	MODERATE
0.1>S≥0.03	NEGLIGIBLE	NEGLIGIBLE	LOW	LOW
0.03>S≥0.01	NEGLIGIBLE	NEGLIGIBLE	NEGLIGIBLE	LOW
0.01>S	NEGLIGIBLE	NEGLIGIBLE	NEGLIGIBLE	NEGLIGIBLE

For the nuclear safety evaluation in this work, the OKG methodology has been applied [42].

“Hypothetical” safety-related cases have been implemented in order to investigate whether it is reasonable to assume that the deterministic and probabilistic approaches give equivalent results. The evaluations were partly deterministic and partly probabilistic and they were based on the PSA

models for construction 1, construction 2 and construction 3. The facility is supposed to be under the operating mode 'power operation'[18].

The safety issues that were considered are of two types: F and S. The safety issues F are related to individual initiating events that have an actual or potential impact on the frequency of the initiating events. The ones labeled with S impact the availability of the safety functions.

In the category **F**, two groups can be identified:

(**Fa**) If the IE-frequency is only marginally affected, then it is assumed that the event class as well as IE-frequency remains unchanged.

(**Fb**) If the IE-frequency is significantly increased, then it is assumed that the event class is moved one or several steps and the IE-frequency is increased by 100 times per step. Events in H2-H5 is concerned.

Category **S** consists of:

(**Sa**) If the availability of safety functions is only marginally affected, the safety concept is presumed to be "Robust" and the probability for loss of function remain unchanged. Events in H2-H5 are concerned.

(**Sb**) If the safety function is not CCF-tolerant, it is assumed that the safety concept is "Adequate" and the probability of loss of function of the affected "diversification items" is 100%. H2 and H3 events are affected from deterministic point of view. All initial events are evaluated from a probabilistic point of view.

(**Sc**) If a safety function is not single failure tolerant, it is assumed that the safety concept is "Adequate" and the probability of failure to function concerned "redundant items" is 100%. H2 to H5 events are affected from the deterministic point of view. All initial events are evaluated from a probabilistic point of view.

(**Sd**) If a safety function is unavailable, it is assumed that the safety concept is "Inadequate" and the consequences are assumed to be conservatively "Serious". The probability of failure for the function is set to 100%. Events in H2-H5 are affected." [42]

Simulation and changes to the models were performed in RiskSpectrum. The cases that actually had to be checked are as follows.

- For **Fa**, the selected initiating events are 4: LOOP (Loss of off-site power) for H2; S1 ML (Medium LOCA) for H3, initiating event A LL (Large LOCA) for H4 and initiating event class H5 (event class H5) for H5.

[18] Power operation is normal operation at full power as initial condition.

- In the case of **Fb** elevated frequencies were investigated according to the following scheme: H3 → H2; H4 → H3; H4 → H2; H5 → H4; H5 → H3, H5 → H2. These scenarios are analyzed by increasing the initiating event frequency by 100 per step.

For example the H3 → H2 scenario; chosen event in event class H3 is S1 ML (medium LOCA) which have the frequency $9.00 \cdot 10^{-4}$. S1 ML acts as a H2 event by increasing the frequency by 100: $9.00 \cdot 10^{-4} \cdot 100 = 9.00 \cdot 10^{-2}$. The consequence is an increased initiating event frequency that causes an increased total core damage frequency. The impact is evaluated by both deterministic and probabilistic approach in section **Fb**.

As regards category **S**, different degrees of impact were analyzed by choosing a safety function that is credited with all event classes. In particular, this part of the investigation focuses on:

- For **Sa,** the probability to fail (factor 1) for the basic event "failure to start diesel generator" was increased.
- For type **Sb**, one system was considered inaccessible in construction 1 and construction 3, and two systems were assumed inaccessible for construction 2.
- In the case of the safety issues **Sc**, two trains are inaccessible for construction 1, two systems are inaccessible for construction 2, and 3 trains are inaccessible for construction 3.
- **Sd**: One safety function is inaccessible. A total of 3 cases where safety function core cooling (SF2) is inaccessible for construction 1, construction 2 and construction 3.

See figure A5.1 in appendix 5 for the hypothetical safety-related cases used in the validation study.

If the check concludes that deterministic and probabilistic evaluation give the same result, or differ by a maximum of one level (Negligible/Low, Low/Moderate or Moderate/High), the assumption of consistency between the two approaches can be thus considered reasonable. For results that differ with two or three levels, a deviation has been identified, which then need to be explained and justified. [42]

4.4.2 Results

4.4.2.1 Construction 1

Table 4.19 shows that there are six deviations for construction 1, namely **Fb (H3 → H2), Fb (H4 → H2), Fb (H5 → H3), Fb (H5 → H2), Sb** and **Sc**.

For **Fb (H3 → H2), Fb (H4 → H2), Fb (H5 → H3)** and **Fb (H5 → H2)** construction 1 has a strong protection against core damage associated with the selected initiating event. The deterministic evaluation assumes that the safety functions are challenged about the same amount by events that are in the same event class. This is a relatively conservative hypothesis and can lead to some deviations as shown by the cases of medium and large break. The probabilistic evaluation instead provides a more realistic evaluation of the safety significance in this case. [42]

For **Sb** and **Sc** deviations between deterministic and probabilistic approach are found and it ***may*** be due to the fact that OKG applied a somewhat conservative interpretation of the CB-5 (see [45]). The analysis suggests that the maximum consequences that are allowed for class H3 can fall in the same consequence category of H1 and H2, and this requires further considerations. In the present interpretation H3 and H4 consequences belong to the same category. If the Sb and Sc cases are

changed to have “Low” safety significance from the deterministic point of view, the deviations would thus be eliminated. [42]

Table 4.19: Comparison between probabilistic and deterministic evaluation for construction 1.

Safety evaluation	IE/Conditions	Probabilistic	Deterministic	Deviation
Fa (H2)	LOOP	Negligible	Low	No
Fa (H3)	S1 ML	Negligible	Low	No
Fa (H4)	A LL	Negligible	Negligible	No
Fa (H5)	H5	Negligible	Negligible	No
Fb (H3→H2)	**S1 ML**	**Negligible**	**Moderate**	**Yes**
Fb (H4→H3)	A LL	Negligible	Low	No
Fb (H4→H2)	**A LL**	**Negligible**	**Moderate**	**Yes**
Fb (H5→H4)	H5	Negligible	Low	No
Fb (H5→H3)	**H5**	**Negligible**	**Moderate**	**Yes**
Fb (H5→H2)	**H5**	**Low**	**High**	**Yes**
Sa	Increased probability (factor 1) ”failure to start diesel generator”	Negligible	Low	No
Sb	**One system is inaccessible**	**Negligible**	**Moderate**	**Yes**
Sc	**Two trains are inaccessible**	**Negligible**	**Moderate**	**Yes**
Sd	One safety function is inaccessible	High	High	No

4.4.2.2 Construction 2

Table 4.20 shows that there are five deviations for construction 2, namely **Fb (H3 → H2), Fb (H5 → H3)**, **Fb (H5 → H2), Sb** and **Sc**.

For the case **Fb (H3 → H2), Fb (H5 → H3)** and **Fb (H5 → H2)** construction 2 gives discrepancies between deterministic and probabilistic approaches. This can be explained by the conservative assumptions for the deterministic calculations. In fact the deterministic evaluation assumes that the safety functions are challenged about the same amount by events that are in the same event class, and this is not always the case. The probabilistic evaluation provides a more realistic evaluation of the safety significance in this case. [42]

For **Sb** and **Sc** deviations between deterministic and probabilistic approach are found and it ***may*** be due to the fact that OKG applied a somewhat conservative interpretation of the CB-5 (see [45]). The analysis suggests that the maximum consequences that are allowed for class H3 can fall in the same consequence category of H1 and H2, and this requires further considerations. In the present interpretation H3 and H4 consequences belong to the same category. If the Sb and Sc cases are changed to have “Low” safety significance from the deterministic point of view, the deviations would thus be eliminated. [42]

Table 4.20: Comparison between probabilistic and deterministic evaluation for construction 2.

Safety evaluation	IE/Conditions	Probabilistic	Deterministic	Deviation
Fa (H2)	LOOP	Negligible	Low	No
Fa (H3)	S1 ML	Negligible	Low	No
Fa (H4)	A LL	Negligible	Negligible	No
Fa (H5)	H5	Negligible	Negligible	No
Fb (H3→H2)	**S1 ML**	**Negligible**	**Moderate**	**Yes**
Fb (H4→H3)	A LL	Negligible	Low	No
Fb (H4→H2)	A LL	Low	Moderate	No
Fb (H5→H4)	H5	Negligible	Low	No
Fb (H5→H3)	**H5**	**Negligible**	**Moderate**	**Yes**
Fb (H5→H2)	**H5**	**Low**	**High**	**Yes**
Sa	Increased probability (factor 1) ”failure to start diesel generator”	Negligible	Low	No
Sb	**Two systems are inaccessible**	**Negligible**	**Moderate**	**Yes**
Sc	**Two systems are inaccessible**	**Negligible**	**Moderate**	**Yes**
Sd	One safety function is inaccessible	High	High	No

4.4.2.3 Construction 3

Table 4.21 shows that there are six deviations for construction 3, namely **Fb (H3 → H2)**, **Fb (H4 → H2), (H5 → H3)**, **Fb (H5 → H2), Sb** and **Sc**.

Cases **Fb (H3 → H2)**, **Fb (H4 → H2), (H5 → H3)** and **Fb (H5 → H2)** show deviations between the deterministic and the probabilistic results. This is due to the conservative assumptions related to the deterministic simulations. In fact the deterministic evaluation assumes that the safety functions are challenged about the same amount by events that are in the same event class, and this is not always the case. The probabilistic evaluation provides a more realistic evaluation of the safety significance in this case. [42]

For **Sb** and **Sc** deviations between deterministic and probabilistic approach are found and it ***may*** be due to the fact that OKG applied a somewhat conservative interpretation of the CB-5 (see [45]). The analysis suggests that the maximum consequences that are allowed for class H3 can fall in the same consequence category of H1 and H2, and this requires further considerations. In the present interpretation H3 and H4 consequences belong to the same category. If the Sb and Sc cases are changed to have “Low” safety significance from the deterministic point of view, the deviations would thus be eliminated. [42]

Table 4.21: Comparison between probabilistic and deterministic evaluation for construction 3.

Safety evaluation	IE/Conditions	Probabilistic	Deterministic	Deviation
Fa (H2)	LOOP	Negligible	Low	No
Fa (H3)	S1 ML	Negligible	Low	No
Fa (H4)	A LL	Negligible	Negligible	No
Fa (H5)	H5	Negligible	Negligible	No
Fb (H3→H2)	**S1 ML**	**Negligible**	**Moderate**	**Yes**
Fb (H4→H3)	A LL	Negligible	Low	No
Fb (H4→H2)	**A LL**	**Negligible**	**Moderate**	**Yes**
Fb (H5→H4)	H5	Negligible	Low	No
Fb (H5→H3)	**H5**	**Negligible**	**Moderate**	**Yes**
Fb (H5→H2)	**H5**	**Low**	**High**	**Yes**
Sa	Increased probability (factor 1) ”failure to start diesel generator”	Negligible	Low	No
Sb	**One system is inaccessible**	**Negligible**	**Moderate**	**Yes**
Sc	**Three trains are inaccessible**	**Negligible**	**Moderate**	**Yes**
Sd	One safety function is inaccessible	High	High	No

4.4.3 Conclusion

The results in Table 4.19, 4.20, 4.21 display that construction 1, 2 and 3 have been validated by OKGs safety evaluation.

It can be concluded that there are deviations between deterministic and probabilistic evaluation results. The study, conducted in [42] suggests that these deviations can be managed through a good knowledge of the specific strengths and weaknesses of the plant.

The study involved $3 \cdot 14 = 42$ "hypothetical" safety evaluations. Of these, it was found deviations in 17 cases. The results show consistency between construction 1, 2 and 3 with the exception H4 → H2. Construction 2 safety concept is based on diversity; this means that the plant may be more sensitive to increased IE-frequency when compared with safety concepts which include redundancy.

5 Conclusions and Future work

5.1 Summary and outcomes of the thesis

In the current master thesis project PSA models were developed for different generic constructions, namely construction 1, construction 2, construction 3. These models were based on different principles that are described in table 5.1. The main difference between the models is the amount of systems and trains used to achieve the design requirements.

Table 5.1: Construction choices with achieved requirement for construction 1, construction 2 and construction 3.

Construction choice for construction 1	Achieved requirement
3·100% train	Simplicity and robustness
Two train of system 1	Redundancy
Two different system (system 1 & system 2)	Diversity
One fire cell and flooding channel for each train	Physical separation
Fire cell for train 1 in system 2 is essentially inert	CCF-tolerant
One train is reinforced against earthquake	Earthquake-tolerant
Construction choice for construction 2	Achieved requirement
Three different system (system 1, system 2 & system 3)	Redundancy and diversity
3·100% train	Simplicity and robustness
One fire cell and flooding channel for each train	Physical separation
Two system still remain when one fire cell is taken out	CCF-tolerant
One train is reinforced against earthquake	Earthquake-tolerant
Construction choice for construction 3	Achieved requirement
4·100% train	Robustness
Two train of each system (4 train in total)	Redundancy
Two different system (system 1 & system 2)	Diversity
One fire cell and flooding channel for each train	Physical separation
Two system and three trains still remain when one fire cell is taken out	CCF-tolerant
One train is reinforced against earthquake	Earthquake-tolerant

The PSA models were used for frequency analysis, barrier analysis and sensitivity analysis. It was found that the performances of the different constructions have clear resemblances. This suggests that one single generic model could be built and applied over a wide spectrum of possible cases.

First, a frequency analysis was performed. The main outcomes of this analysis were that constructions 1, 2 and 3 estimates similar core damage distributions. In particular, they display most resemblances with Oskarshamn 3 (see Figure 4.3). This could be due to the fact that Oskarshamn 3 is a more modern reactor. Older reactors as O1 (see Figure 4.1) and O2 (see Figure 4.2) do not demonstrate any clear resemblances when compared to construction 1, 2 and 3.

Then, an investigation of the barriers with the three models was carried out. This part of the work showed that barrier safety criteria are fulfilled according to the predictions of all the PSA models and no relevant weaknesses could be observed. The system barrier analysis also confirms that a generic PSA model suits better the more advanced case of O3.

The sensitivity analysis demonstrated that the generic models are sensitive to the basic event "rest faults". CCF on the basic event "rest faults" is the dominating risk contribution for construction 1 and 3. Construction 3 is the simplest design in which no fire measure is needed. The sensitivity study distinctly shows that constructions with multiple trains for a system, i.e. construction 1 (see Figure 3.1) and construction 3 (see Figure 3.3), have a reduced contribution to the core damage frequency due to fire. (see Table 4.16).

In the validation study, validation of the probabilistic results (see table 4.19, 4.20 and 4.21) show that the PSA models construction 1, 2 and 3 are **robust** because the margin to the next safety level is large compared to the reasonable estimates of the uncertainty in the input data. Assuming that the plant PSA model is detailed enough and that the quality of input data is sufficiently high, this benchmark tool can be used to quantitatively evaluate the safety concept as such.

General conclusions and remarks can be summarized as:

- Construction 1 is the simplest possible structure solution that can be used but it requires fire dampening and high level of quality of its components.
- Construction 3 is the simplest possible structure solution that does not require extraordinary systems for fire mitigation and allows to relax the requirements on the quality of its components.
- A construction based on the design requirement of SSMFS 2008:17 and with multiple trains for a system, as construction 1 and 3, leads to a design that is fire resistant (see table 4.16).
- Analysis of the free parameter[19] indicates that construction 1 requires higher level of quality of its components with respect to, for instance, construction 3 (see eq. 4.2). This assumption is based on the simple fact that the probability of the free parameter (representing all other faults) is three times higher for construction 3. This means that the quality of the components represented by the free parameter for construction 3 can be of lower quality but still achieve desired total core damage frequency ($f<10^{-5}$).
- Construction 3 is recommended to be used as the one generic PSA model and thereby as benchmark tool for all Swedish BWRs. The main reason is that further development of the PSA model will be easier when extraordinary fire mitigation measures do not need to be taken into consideration.

5.2 Future studies

The scope of the current thesis was a first investigation on the possible development of a generic model for PSA. This involved the first level of the probabilistic analysis (core damage risk assessment). To fully assess the validity of such an approach, the next step is to address the second level of PSA (risk assessment regarding large radioactive releases). For this purpose the RiskSpectrum model built in this project can be used.

[19] The free parameter is the probability of failure for the basic event rest faults that is located in all trains for construction 1, 2 and 3 (see figure 3.4 - 3.6). The free parameter is tuned by iteration in RiskSpectrum so that the total core damage frequency for the different construction models are as close to 10^{-5} as possible.

The results could also be further supported by data from Swedish BWRs other than O1, O2 and O3. Moreover, it would be valuable to expand the capability of the generic PSA model by taking in account the details of the basic event called “Rest faults”.

Appendix

Appendix 1

A1.1 Total core damage frequency

Analysis of construction 1, construction 2 and construction 3 displayed different core damage frequencies. The sum of HS frequencies should be $<10^{-5}$. To attain this one need the probability for fault on the basic event "rest faults" fine-tuned for each construction model. By adjusting the parameter called “free parameter” the following values were obtained:

Table A1.1: Shows the estimated probability of maximum allowable value of the “free parameter” in the basic event "rest faults" for the various constructions. The sum of the frequencies is $<10^{-5}$ and the “free parameter” is tuned so that the sums of the different construction models are as close together as possible. The probability for the “free parameter” was obtained by iteration in RiskSpectrum.

Construction model	[Probability] “free parameter”	The sum of the HS frequencies (fire excluded) per year
Construction 1	$5.47 \cdot 10^{-3}$	$1.00 \cdot 10^{-5}$
Construction 2	$1.48 \cdot 10^{-2}$	$1.00 \cdot 10^{-5}$
Construction 3	$1.77 \cdot 10^{-2}$	$1.00 \cdot 10^{-5}$

A1.2 O1

A1.2.1 Initiating events

Table A1.2: Shows the contributions from events belonging to different event classes with different end states (HS-frequencies). Values were calculated from index 3 in source [37]. Calculations can be seen in index 3 in this rapport. The total frequency from IE Fire was obtained from index 1 in source [39] (conservative IE Fire: 7.9E-03/year). Results omitted in this report. Complete results are available in [44].

	H1-H2	H3	H4-H5	LOOP (H2)	A LL (H4)	S_1 ML (H3)	S_2 SL (H3)	Total	Fire (H3) Excluded
SF1 (HS1)	-	-	-	-	-	-	-	-	-
SF2 (HS2)	-	-	-	-	-	-	-	-	-
SF4 (HS3)	-	-	-	-	-	-	-	-	-
Total	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**-**

Table A1.3: Shows the percentage distribution between different event classes with different end states (based on HS-frequencies). Values were calculated from index 3 in source [37]. Calculations can be seen in index 3 in this rapport.

	H1-H2	H3	H4-H5	LOOP (H2)	A LL (H4)	S_1 ML (H3)	S_2 SL (H3)	Total	Fire (H3) Excluded
SF1 (HS1)	59.62%	-	-	38.63%	-	-	1.82%	**1.3%**	-

SF2 (HS2)	2.48%	-	-	57.07%	20.15%	12.74%	7.49%	**95.6%**	-
SF4 (HS3)	3.07%	2.31%	-	87.15%	3.00%	3.17%	1.37%	**2.7%**	-
Total	**3.6%**	**0.07%**	**-**	**57.5%**	**19.4%**	**12.3%**	**7.2%**	**100%**	**31.1%**

A1.2.2 Barrier analysis

Table A1.4: Shows the contributions from events belonging to different event classes with different end states (barrier-probabilities). Values were calculated from index 3 in source [37]. Calculations can be seen in index 3 in this rapport. Results omitted in this report. Complete results are available in [44].

	H1-H2	H3	H4-H5	LOOP (H2)	A LL (H4)	S_1 ML (H3)	S_2 SL (H3)	Fire (H3) Excluded
SF1 (HS1)	-	-	-	-	-	-	-	-
SF2 (HS2)	-	-	-	-	-	-	-	-
SF4 (HS3)	-	-	-	-	-	-	-	-
Total	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**-**

A1.3 O2

A1.3.1 Initiating events

Table A1.5: Shows the contributions from events belonging to different event classes with different end states (HS-frequencies). Values were calculated from Index 1 in source [38]. Calculations can be seen in index 2 in this rapport. The total frequency from IE Fire was obtained from source [40] (conservative IE Fire: 7.9E-03/year). Results omitted in this report. Complete results are available in [44].

	H1-H2	H3	H4-H5	LOOP (H2)	A LL (H4)	S_1 ML (H3)	S_2 SL (H3)	Total	Fire (H3) Excluded
SF1 (HS1)	-	-	-	-	-	-	-	-	-
SF2 (HS2)	-	-	-	-	-	-	-	-	-
SF4 (HS3)	-	-	-	-	-	-	-	-	-
Total	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**-**

Table A1.6: Shows the percentage distribution between different event classes with different end states (HS-frequencies). Values were calculated from Index 1 in source [38]. Calculations can be seen in index 2 in this rapport.

	H1-H2	H3	H4-H5	LOOP (H2)	A LL (H4)	S_1 ML (H3)	S_2 SL (H3)	Total	Fire (H3) Excluded
SF1 (HS1)	45.50%	42.05%	-	12.45%	-	-	-	**<0.01%**	-
SF2 (HS2)	5.56%	13.85%	2.44%	29.91%	4.01%	13.34%	30.89%	**64.3%**	-
SF4 (HS3)	45.39%	11.58%	3.20%	39.82%	-	-	-	**35.7%**	-
Total	**19.8%**	**13.0%**	**2.7%**	**33.4%**	**2.6%**	**8.6%**	**19.9%**	**100%**	**-**

A1.3.2 Barrier analysis

Table A1.7: Shows the contributions from events belonging to different event classes with different end states (barrier-probabilities). Values were calculated from index 1 in source [38]. Calculations can be seen in index 2 in this rapport. Results omitted in this report. Complete results are available in [44].

	H1-H2	H3	H4-H5	LOOP (H2)	A LL (H4)	S_1 ML (H3)	S_2 SL (H3)	Fire (H3) Excluded
SF1 (HS1)	-	-	-	-	-	-	-	-
SF2 (HS2)	-	-	-	-	-	-	-	-
SF4 (HS3)	-	-	-	-	-	-	-	-
Total	-	-	-	-	-	-	-	-

A1.4 O3

A1.4.1 Initiating events

Table A1.8: Shows the contributions from events belonging to different event classes with different end states (HS-frequencies). Values were calculated from Index 1 in source [35]. Calculations can be seen in index 4 in this rapport. The total frequency from IE Fire was obtained from source [41] (conservative IE Fire: 7.9E-03/year). Results omitted in this report. Complete results are available in [44].

	H1-H2	H3	H4-H5	LOOP (H2)	A LL (H4)	S_1 ML (H3)	S_2 SL (H3)	Total	Fire (H3) Excluded
SF1 (HS1)	-	-	-	-	-	-	-	-	-
SF2 (HS2)	-	-	-	-	-	-	-	-	-
SF4 (HS3)	-	-	-	-	-	-	-	-	-
Total	-	-	-	-	-	-	-	-	-

Table A1.9: Shows the percentage distribution between different event classes with different end states (HS-frequencies). Values were calculated from Index 1 in source [35]. Calculations can be seen in index 4 in this rapport.

	H1-H2	H3	H4-H5	LOOP (H2)	A LL (H4)	S_1 ML (H3)	S_2 SL (H3)	Total	Fire (H3) Excluded
SF1 (HS1)	22%	16.74%	-	61.12%	-	0.14%	-	**7.5%**	-
SF2 (HS2)	18.27%	5.56%	1.24%	68.33%	-	6.60%	-	**58.2%**	-
SF4 (HS3)	69.28%	10.53%	15.55%	4.60%	0.05%	-	-	**34.2%**	-
Total	**36.1%**	**8.1%**	**6.0%**	**45.9%**	**0.01%**	**3.9%**	-	**100%**	**8.2%**

A1.4.2 Barrier analysis

Table A1.10: Shows the contributions from events belonging to different event classes with different end states (barrier-probabilities). Values were calculated from index 1 in source [35]. Calculations can be seen in index 4 in this rapport. Results omitted in this report. Complete results are available in [44].

	H1-H2	H3	H4-H5	LOOP (H2)	A LL (H4)	S_1 ML (H3)	S_2 SL (H3)	Fire (H3) Excluded
SF1 (HS1)	-	-	-	-	-	-	-	-

SF2 (HS2)	-	-	-	-	-	-	-	-
SF4 (HS3)	-	-	-	-	-	-	-	-
Total	-	-	-	-	-	-	-	-

A1.5 C1

A1.5.1 Initiating events

Table A1.11: Shows the contributions from events belonging to different event classes with different end states (HS-frequencies). Values were calculated from the model (construction 1) in RiskSpectrum. Fire is excluded in the total core damage frequency. Conservative IE fire value 7.9E-03/year was used in the PSA model.

	H2	H3	H4	LOOP (H2)	A LL (H4)	S_1 ML (H3)	S_2 SL (H3)	Total	Fire (H4) Excluded
SF1 (HS1)	2.90E-06	9.50E-09	3.23E-10	4.13E-07	8.13E-10	2.90E-09	9.66E-09	**3.33E-06**	1.92E-07
SF2 (HS2)	2.90E-06	9.50E-09	3.23E-10	4.13E-07	8.13E-10	2.90E-09	9.66E-09	**3.33E-06**	1.92E-07
SF4 (HS3)	2.90E-06	9.50E-09	3.23E-10	4.13E-07	8.13E-10	2.90E-09	9.66E-09	**3.33E-06**	1.92E-07
Total	**8.71E-06**	**2.85E-08**	**9.68E-10**	**1.24E-06**	**2.44E-09**	**8.71E-09**	**2.90E-08**	**1.00E-05**	**5.76E-07**

Table A1.12: Shows the percentage distribution between different event classes with different end states (HS-frequencies). Values were calculated from the model (construction 1) in RiskSpectrum. Fire percentages are obtained by dividing the fire frequency with the total core damage frequency (fire excluded).

	H2	H3	H4	LOOP (H2)	A LL (H4)	S_1 ML (H3)	S_2 SL (H3)	Total	Fire (H4) Excluded
SF1 (HS1)	87.10%	0.28%	0.01%	12.38%	0.02%	0.09%	0.29%	**33.33%**	5.76%
SF2 (HS2)	87.10%	0.28%	0.01%	12.38%	0.02%	0.09%	0.29%	**33.33%**	5.76%
SF4 (HS3)	87.10%	0.28%	0.01%	12.38%	0.02%	0.09%	0.29%	**33.33%**	5.76%
Total	**87.10%**	**0.28%**	**0.01%**	**12.38%**	**0.02%**	**0.09%**	**0.29%**	**100%**	**5.76%**

A1.5.2 Barrier analysis

Table A1.13: Shows the contributions from events belonging to different event classes with different end states (barrier-probabilities). Values were calculated from the model (construction 1) in RiskSpectrum.

	H2	H3	H4	LOOP (H2)	A LL (H4)	S_1 ML (H3)	S_2 SL (H3)	Fire (H4) Excluded
SF1 (HS1)	3.22E-06	3.22E-06	3.23E-06	4.13E-06	3.23E-06	3.22E-06	3.22E-06	2.43E-05
SF2 (HS2)	3.22E-06	3.22E-06	3.23E-06	4.13E-06	3.23E-06	3.22E-06	3.22E-06	2.43E-05
SF4 (HS3)	3.22E-06	3.22E-06	3.23E-06	4.13E-06	3.23E-06	3.22E-06	3.22E-06	2.43E-05
Total	**9.67E-06**	**9.67E-06**	**9.68E-06**	**1.24E-05**	**9.68E-06**	**9.67E-06**	**9.67E-06**	**7.29E-05**

A1.6 C2

A1.6.1 Initiating events

Table A1.14: Shows the contributions from events belonging to different event classes with different end states (HS-frequencies). Values were calculated from the model (construction 2) in RiskSpectrum. Fire is excluded in the total core damage frequency. Conservative IE fire value 7.9E-03/year was used in the PSA model.

	H2	H3	H4	LOOP (H2)	A LL (H4)	S_1 ML (H3)	S_2 SL (H3)	Total	Fire (H3) Excluded
SF1 (HS1)	2.97E-06	9.73E-09	3.30E-10	3.80E-07	8.30E-10	2.97E-09	9.9E-09	**3.36E-06**	1.75E-06
SF2 (HS2)	2.97E-06	9.73E-09	3.30E-10	3.80E-07	8.30E-10	2.97E-09	9.9E-09	**3.36E-06**	1.75E-06
SF4 (HS3)	2.97E-06	9.73E-09	3.30E-10	3.80E-07	8.30E-10	2.97E-09	9.9E-09	**3.36E-06**	1.75E-06
Total	**8.91E-06**	**2.92E-08**	**9.90E-10**	**1.14E-06**	**2.49E-09**	**8.91E-09**	**2.97E-08**	**1.01E-05**	**5.25E-06**

Table A1.15: Shows the percentage distribution between different event classes with different end states (HS-frequencies). Values were calculated from the model (construction 2) in RiskSpectrum. Fire percentages are obtained by dividing the fire frequency with the total core damage frequency (fire excluded).

	H2	H3	H4	LOOP (H2)	A LL (H4)	S_1 ML (H3)	S_2 SL (H3)	Total	Fire (H3) Excluded
SF1 (HS1)	88.03%	0.29%	0.01%	11.26%	0.02%	0.09%	0.29%	**33%**	51.98%
SF2 (HS2)	88.03%	0.29%	0.01%	11.26%	0.02%	0.09%	0.29%	**33%**	51.98%
SF4 (HS3)	88.03%	0.29%	0.01%	11.26%	0.02%	0.09%	0.29%	**33%**	51.98%
Total	**88.03%**	**0.29%**	**0.01%**	**11.26%**	**0.02%**	**0.09%**	**0.29%**	**100%**	**51.98%**

A1.6.2 Barrier analysis

Table A1.16: Shows the contributions from events belonging to different event classes with different end states (barrier-probabilities). Values were calculated from the model (construction 2) in RiskSpectrum.

	H2	H3	H4	LOOP (H2)	A LL (H4)	S_1 ML (H3)	S_2 SL (H3)	Fire (H3) Excluded
SF1 (HS1)	3.3E-06	3.3E-06	3.3E-06	3.8E-06	3.3E-06	3.3E-06	3.3E-06	1.25E-04
SF2 (HS2)	3.3E-06	3.3E-06	3.3E-06	3.8E-06	3.3E-06	3.3E-06	3.3E-06	1.25E-04
SF4 (HS3)	3.3E-06	3.3E-06	3.3E-06	3.8E-06	3.3E-06	3.3E-06	3.3E-06	1.25E-04
Total	**9.9E-06**	**9.9E-06**	**9.9E-06**	**1.14E-05**	**9.9E-06**	**9.9E-06**	**9.9E-06**	**6.64E-04**

A1.7 C3

A1.7.1 Initiating events

Table A1.17: Shows the contributions from events belonging to different event classes with different end states (HS-frequencies). Values were calculated from the model (construction 3) in RiskSpectrum. Fire is excluded in the total core damage frequency. Conservative IE fire value 7.9E-03/year was used in the PSA model.

	H2	H3	H4	LOOP (H2)	A LL (H4)	S_1 ML (H3)	S_2 SL (H3)	Total	Fire (H3) Excluded

SF1 (HS1)	2.95E-06	9.66E-09	3.28E-10	3.60E-07	8.26E-10	2.95E-09	9.83E-09	**3.33E-06**	2.48E-07
SF2 (HS2)	2.95E-06	9.66E-09	3.28E-10	3.60E-07	8.26E-10	2.95E-09	9.83E-09	**3.33E-06**	2.48E-07
SF4 (HS3)	2.95E-06	9.66E-09	3.28E-10	3.60E-07	8.26E-10	2.95E-09	9.83E-09	**3.33E-06**	2.48E-07
Total	**8.86E-06**	**2.90E-08**	**9.84E-10**	**1.08E-06**	**2.48E-09**	**8.86E-09**	**2.95E-08**	**1.00E-05**	**7.46E-07**

Table A1.18: Shows the percentage distribution between different event classes with different end states (HS-frequencies). Values were calculated from the model (construction 3) in RiskSpectrum. Fire percentages are obtained by dividing the fire frequency with the total core damage frequency (fire excluded).

	H2	H3	H4	LOOP (H2)	A LL (H4)	S_1 ML (H3)	S_2 SL (H3)	Total	Fire (H3) Excluded
SF1 (HS1)	88.5%	0.29%	0.01%	10.79%	0.02%	0.09%	0.29%	**33%**	7.46%
SF2 (HS2)	88.5%	0.29%	0.01%	10.79%	0.02%	0.09%	0.29%	**33%**	7.46%
SF4 (HS3)	88.5%	0.29%	0.01%	10.79%	0.02%	0.09%	0.29%	**33%**	7.46%
Total	**88.5%**	**0.29%**	**0.01%**	**10.79%**	**0.02%**	**0.09%**	**0.29%**	**100%**	**7.46%**

A1.7.2 Barrier analysis

Table A1.19: Shows the contributions from events belonging to different event classes with different end states (barrier-probabilities). Values were calculated from the model (construction 3) in RiskSpectrum.

	H2	H3	H4	LOOP (H2)	A LL (H4)	S_1 ML (H3)	S_2 SL (H3)	Fire (H3) Excluded
SF1 (HS1)	3.28E-06	3.28E-06	3.28E-06	3.60E-06	3.28E-06	3.28E-06	3.28E-06	3.14E-05
SF2 (HS2)	3.28E-06	3.28E-06	3.28E-06	3.60E-06	3.28E-06	3.28E-06	3.28E-06	3.14E-05
SF4 (HS3)	3.28E-06	3.28E-06	3.28E-06	3.60E-06	3.28E-06	3.28E-06	3.28E-06	3.14E-05
Total	**9.84E-06**	**9.84E-06**	**9.84E-06**	**1.08E-05**	**9.84E-06**	**9.84E-06**	**9.84E-06**	**9.44E-05**

Appendix 2

The tables in appendix 2 display the calculations that were done for O2. Values were taken from index 1 in source [38]. Results omitted in this report. Complete results are available in [44].

HS1	HS1-Frequency	Relative contribution	Event class	IE	Barrier Probability
TS	-	-	H2	-	-
C663F04	-	-	H3	-	-
C663E04	-	-	H3	-	-
TT	-	-	H2	-	-
TE	-	-	LOOP	-	-
C733	-	-	H3	-	-
TA	-	-	H2	-	-
TF	-	-	H2	-	-
TI	-	-	H2	-	-
TY	-	-	H2	-	-
C665C02	-	-	H3	-	-
C665D02	-	-	H3	-	-
C642A04	-	-	H3	-	-
C642B04	-	-	H3	-	-
C642C04	-	-	H3	-	-
C641G6	-	-	H3	-	-
C642L04	-	-	H3	-	-
C641D6	-	-	H3	-	-
C642K04	-	-	H3	-	-
C642D04	-	-	H3	-	-
Total LOOP	-	-		-	-
Total H2	-	-		-	-
Total H3	-	-		-	-
Total A					
Total S1					
Total S2					
Total HS1	-	-			

HS2	HS2-Frequency	Relative contribution	Event class	IE	Barrier Probability
TE	-	-	LOOP	-	-
C733	-	-	H3	-	-
C712	-	-	H3	-	-
C721	-	-	H3	-	-
S1B.1	-	-	S1	-	-
C711	-	-	H4	-	-
S2.01	-	-	S2	-	-
S2.16	-	-	S2	-	-
S2.11	-	-	S2	-	-

S2.06	-	-	S2	-	-
S2.05	-	-	S2	-	-
S2.08	-	-	S2	-	-
S2.15	-	-	S2	-	-
S2.14	-	-	S2	-	-
S2.09	-	-	S2	-	-
S1T.S2.2	-	-	S1	-	-
C675Al1:2	-	-	H2	-	-
S2.12	-	-	S2	-	-
S2.17	-	-	S2	-	-
S2.04	-	-	S2	-	-
S2.13	-	-	S2	-	-
S2.10	-	-	S2	-	-
S2.02	-	-	S2	-	-
S1T.S2.1	-	-	S1	-	-
S2.07	-	-	S2	-	-
S2.03	-	-	S2	-	-
AT.S2.2	-	-	A	-	-
AT.S2.1	-	-	A	-	-
TS	-	-	H2	-	-
AB.1	-	-	A	-	-
S2.19	-	-	S2	-	-
TT	-	-	H2	-	-
S1B.S2.05	-	-	S1	-	-
C675DL1:2	-	-	H2	-	-
S1T.3	-	-	S1	-	-
C675CL1:2	-	-	H2	-	-
C675BL1:2	-	-	H2	-	-
S1B.S2.01	-	-	S1	-	-
S1B.S2.14	-	-	S1	-	-
S1B.S2.06	-	-	S1	-	-
S1B.S2.08	-	-	S1	-	-
S1B.S2.15	-	-	S1	-	-
S1B.S2.10	-	-	S1	-	-
S1B.S2.12	-	-	S1	-	-
S1B.S2.02	-	-	S1	-	-
S1B.S2.17	-	-	S1	-	-
S1B.S2.04	-	-	S1	-	-
S1B.S2.13	-	-	S1	-	-
S1B.S2.07	-	-	S1	-	-
S1B.S2.11	-	-	S1	-	-
S1B.S2.09	-	-	S1	-	-
TA	-	-	H2	-	-
S1B.S2.16	-	-	S1	-	-

TF	-	-	H2	-	-
AT.3	-	-	A	-	-
Total LOOP	-	-		-	-
Total H2	-	-		-	-
Total H3	-	-		-	-
Total H4	-	-		-	-
Total A	-	-		-	-
Total S1	-	-		-	-
Total S2	-	-		-	-
Total HS2	-	-			
HS3	**HS3-Frequency**	**Relative contribution**	**Event class**	**IE**	**Barrier Probability**
TE	-	-	LOOP	-	-
C675AL1:2	-	-	H2	-	-
C675BL1:2	-	-	H2	-	-
C721	-	-	H3	-	-
C712	-	-	H3	-	-
C711	-	-	H4	-	-
TS	-	-	H2	-	-
C664G04	-	-	H3	-	-
C675AL1:2	-	-	H3	-	-
TT	-	-	H2	-	-
TA	-	-	H2	-	-
TY	-	-	H2	-	-
TI	-	-	H2	-	-
C665C02	-	-	H3	-	-
C675DL1:2	-	-	H2	-	-
C642A04	-	-	H3	-	-
C641A6	-	-	H3	-	-
Total LOOP	-	-		-	-
Total H2	-	-		-	-
Total H3	-	-		-	-
Total H4	-	-		-	-
Total A	-	-			
Total S1	-	-			
Total S2	-	-			
Total HS3	-	-			
OT2	**OT2-Frequency**	**Relative contribution**	**Event class**	**IE**	**Barrier Probability**
TT	-	-	H2	-	-
TE	-	-	LOOP	-	-
C675AL1:2	-	-	H2	-	-
C675BL1:2	-	-	H2	-	-

TS	-	-	H2	-	-
C675CL1:2	-	-	H2	-	-
C675DL1:2	-	-	H2	-	-
TA	-	-	H2	-	-
TF	-	-	H2	-	-
TI	-	-	H2	-	-
TY	-	-	H2	-	-
Total LOOP	-	-		-	-
Total H2	-	-		-	-
Total H3					
Total A					
Total S1					
Total S2					
Total OT2	-	-			

HS1 to OT2	**HS1-OT2-Freq**	**Relative contribution**			**Barrier probability**	**Rel. barrier contr.**
Total H2 ALL	-	-			-	-
Total H3 ALL	-	-			-	-
Total H4 ALL	-	-			-	-
Total LOOP	-	-			-	-
Total A	-	-			-	-
Total S1	-	-			-	-
Total S2	-	-			-	-
					-	-

Totaltotal	-	-	-
O2 index	-		
Tot Left out	-		

Appendix 3

The tables in appendix 3 display the calculations that were done for O1. Values were taken from index 1 in source [39]. Results omitted in this report. Complete results are available in [44].

HS1	HS1-Frequency	Relative contribution	Event class	IE	Barrier Probability	HS1 total HS-freq
TE	-	-	LOOP	-	-	-
TT/TIS	-	-	H2	-	-	-
TS	-	-	H2	-	-	-
TIH	-	-	H2	-	-	-
LS2.2	-	-	S2	-	-	-
TII	-	-	H2	-	-	-
TF	-	-	H2	-	-	-
TIY	-	-	H2	-	-	
Total LOOP	-	-		-	-	
Total H2	-	-		-	-	
Total H3	-	-		-	-	
Total A	-	-		-	-	
Total S1	-	-		-	-	
Total S2	-	-		-	-	
Total HS1	-	-				

HS2	HS2-Frequency	Relative contribution	Event class	IE	Barrier Probability	HS2 total HS-freq
TE	-	-	LOOP	-	-	-
LS1B	-	-	S1	-	-	-
LAB.1	-	-	A	-	-	-
LS2.1	-	-	S2	-	-	-
LS1T.2	-	-	S1	-	-	-
LAT.1	-	-	A	-	-	-
LAB.4	-	-	A	-	-	-
LAB.6	-	-	A	-	-	
LAB.3	-	-	A	-	-	
LAB.2	-	-	A	-	-	
TIH	-	-	H2	-	-	
TT/TIS	-	-	H2	-	-	
LS2.7	-	-	S2	-	-	
LS2.8	-	-	S2	-	-	
Total LOOP	-	-		-	-	
Total H2	-	-		-	-	
Total H3						
Total H4						
Total A	-	-			-	
Total S1	-	-			-	
Total S2	-	-			-	
Total HS2	-	-				

HS3	HS3-Frequency	Relative contribution	Event class	IE	Barrier Probability	HS3 total HS-freq
TE	-	-	LOOP	-	-	-
LS1B	-	-	S1	-	-	-
LAB.1	-	-	A	-	-	-
CCI-733	-	-	H3	-	-	-
TIH	-	-	H2	-	-	-
LS2.1	-	-	S2	-	-	-
TT/TIS	-	-	H2	-	-	-
LS1T.2	-	-	S1	-	-	
TS	-	-	H2	-	-	
LAT.1	-	-	A	-	-	
Total LOOP	-	-			-	
Total H2	-	-			-	
Total H3	-	-			-	
Total H4					-	
Total A	-	-			-	
Total S1	-	-			-	
Total S2	-	-			-	
Total HS3	-	-				

OT2	OT2-Frequency	Relative contribution	Event class	IE	Barrier Probability	OT2 total HS-freq
TT/TIS	-	-	H2	-	-	-
TE	-	-	LOOP	-	-	-
TS	-	-	H2	-	-	-
IL2	-	-	H3	-	-	-
TIH	-	-	H2	-	-	-
TF	-	-	H2	-	-	-
TII	-	-	H2	-	-	-
TIY	-	-	H2	-	-	
LS2.2	-	-	S2	-	-	
C643.B04	-	-	H3	-	-	
C643.C04	-	-	H3	-	-	
Total LOOP	-	-			-	
Total H2	-	-			-	
Total H3	-	-			-	
Total A					-	
Total S1					-	
Total S2	-	-			-	
Total OT2	-	-				

HS1 to OT2	HS1-OT2-Freq	Relative contribution			Barrier probability	Rel. barrier contr.

Total H2 ALL	-	-			-	-
Total H3 ALL	-	-			-	-
Total H4 ALL	-	-			-	-
Total LOOP	-	-			-	-
Total A	-	-			-	-
Total S1	-	-			-	-
Total S2	-	-			-	-

Totaltotal	-	-	-
O1 index	-		
Tot Left out	-		

Appendix 4

The tables in appendix 4 display the calculations that were done for O3. Values were taken from index 1 in source [35]. Results omitted in this report. Complete results are available in [44].

HS1	HS1-Frequency	Relative contribution	Event class	IE	Barrier Probability	Total freq HS1
TE	-	-	LOOP	-	-	**1,09E-06**
CCI-672WA1	-	-	H3	-	-	
CCI-672WC1	-	-	H3	-	-	
TF	-	-	H2	-	-	
TIM	-	-	H2	-	-	
TT/TIS	-	-	H2	-	-	
CCI-673WA2	-	-	H2	-	-	
CCI-673WB2	-	-	H2	-	-	
CCI-673WC2	-	-	H2	-	-	
CCI-673WD2	-	-	H2	-	-	
TII	-	-	H2	-	-	
TS	-	-	H2	-	-	
CCI-677WB1	-	-	H3	-	-	
CCI-672WB1	-	-	H3	-	-	
CCI-672WD1	-	-	H3	-	-	
LS1T.9	-	-	S1	-	-	**Rel. Barrier Contr.**
Total LOOP	-	-			-	-
Total H2	-	-			-	-
Total H3	-	-			-	-
Total A						-
Total S1	-	-			-	-
Total S2					-	
Total HS1	-	-			-	

HS2	HS2-Frequency	Relative contribution	Event class	IE	Barrier Probability
TE	-	-	LOOP	-	-
TF	-	-	H2	-	-
TIM	-	-	H2	-	-
CCI-672WA1	-	-	H3	-	-
CCI-672WC1	-	-	H3	-	-
CCI-112/711	-	-	H4	-	-
LS1T.1	-	-	S1	-	-
TT/TIS	-	-	H2	-	-
CCI-673WA2	-	-	H2	-	-
CCI-673WB2	-	-	H2	-	-
CCI-673WC2	-	-	H2	-	-
CCI-673WD2	-	-	H2	-	-

CCI-672WB1	-	-	H2	-	-	
LS1B.14	-	-	S1	-	-	
LS1B.2	-	-	S1	-	-	
LS1B.4	-	-	S1	-	-	
CCI-677WB1	-	-	H3	-	-	
LS1B.10	-	-	S1	-	-	
LS1B.12	-	-	S1	-	-	
LS1B.13	-	-	S1	-	-	
LS1B.16	-	-	S1	-	-	
LS1B.17	-	-	S1	-	-	
LS1B.3	-	-	S1	-	-	
LS1B.5	-	-	S1	-	-	
LS1B.8	-	-	S1	-	-	
LS1B.9	-	-	S1	-	-	
LS1B.7	-	-	S1	-	-	
TS	-	-	H2	-	-	
LS1B.18	-	-	S1	-	-	
TII	-	-	H2	-	-	
LS1B.1	-	-	S1	-	-	
LS1B.11	-	-	S1	-	-	
LS1B.15	-	-	S1	-	-	
LS1B.6	-	-	S1	-	-	
CCI-672WD1	-	-	H3	-	-	
LS1T.4	-	-	S1	-	-	**Rel. Barrier Contr.**
Total LOOP	-	-			-	-
Total H2	-	-			-	-
Total H3	-	-			-	-
Total H4	-	-			-	-
Total A					-	-
Total S1	-	-			-	-
Total S2					-	-
Total HS2	-	-			-	-

HS3	**HS3-Frequency**	**Relative contribution**	**Event class**	**IE**	**Barrier Probability**
TIM	-	-	H2	-	-
CCI-112/711	-	-	H4	-	-
TF	-	-	H2	-	-
TE	-	-	LOOP	-	-
CCI-672WA1	-	-	H3	-	-
CCI-672WB1	-	-	H3	-	-
CCI-672WD1	-	-	H3	-	-
CCI-677WB1	-	-	H3	-	-
CCI-673WA2	-	-	H2	-	-

TT/TIS	-	-	H2	-	-	
CCI-673WB2	-	-	H2	-	-	
CCI-673WC2	-	-	H2	-	-	
CCI-673WD2	-	-	H2	-	-	
TS	-	-	H2	-	-	
CCI-672WC1	-	-	H3	-	-	
CCI-672WB2	-	-	H3	-	-	
CCI-672WD2	-	-	H3	-	-	
CCI-672WC2	-	-	H3	-	-	
CCI-672WA2	-	-	H3	-	-	
TII	-	-	H2	-	-	
LAT.6	-	-	A	-	-	**Rel. Barrier Contr.**
Total LOOP	-	-			-	-
Total H2	-	-			-	-
Total H3	-	-			-	-
Total H4	-	-			-	-
Total A	-	-			-	-
Total S1					-	-
Total S2					-	-
Total HS3	-	-			-	-

OT2	**OT2-Frequency**	**Relative contribution**	**Event class**	**IE**	**Barrier Probability**	
TE	-	-	LOOP	-	-	
TF	-	-	H2	-	-	
TIM	-	-	H2	-	-	
CCI-677WB1	-	-	H3	-	-	
TT/TIS	-	-	H2	-	-	
CCI-672WC1	-	-	H3	-	-	
CCI-673WC2	-	-	H2	-	-	
CCI-673WD2	-	-	H2	-	-	
TII	-	-	H2	-	-	**Rel. Barrier Contr.**
Total LOOP	-	-			-	-
Total H2	-	-			-	-
Total H3	-	-			-	-
Total A						
Total S1						
Total S2						
Total OT2	-	-			-	-

HS1 to OT2	**HS1-OT2-Freq**	**Relative contribution**			**Barrier probability**	**Rel. barrier contr.**

Total H2 ALL	-	-			-	-
Total H3 ALL	-	-			-	-
Total H4 ALL	-	-			-	-
Total LOOP	-	-			-	-
Total A	-	-			-	-
Total S1	-	-			-	-
Total S2						

Totaltotal	-
O3 index	-
Tot Left out	-

-	-

Appendix 5

A5.1 Validation – hypothetical safety-related cases

Figure A5.1 displays the "hypothetical" safety-related cases that have been implemented in order to investigate whether it is reasonable to assume that the deterministic and probabilistic approaches give equivalent results.

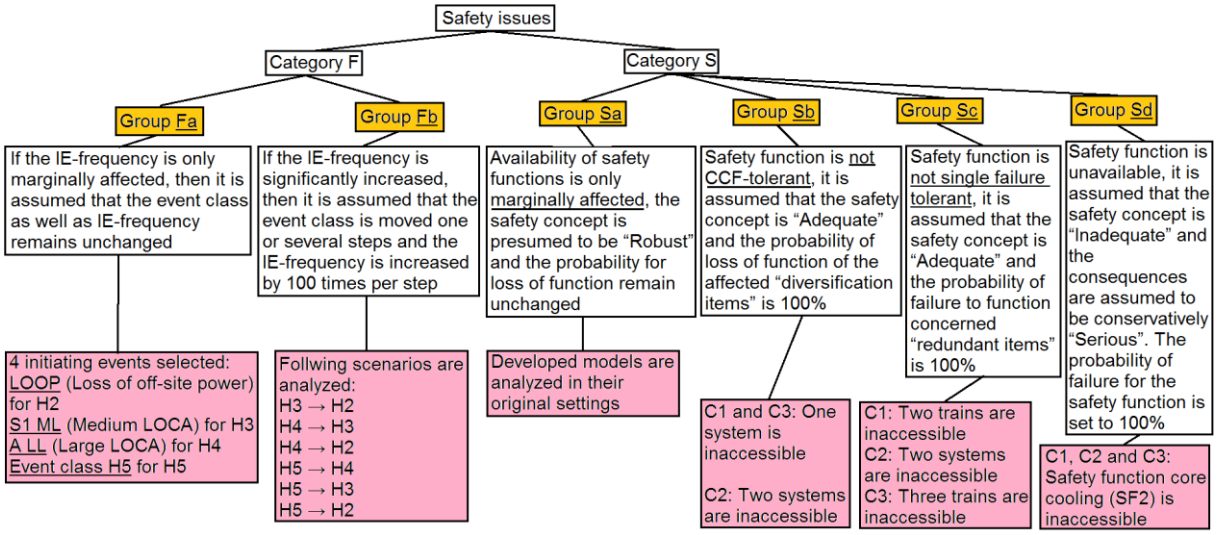


Figure A5.1: Displays the hypothetical safety-related cases used in the validation study.

References

[1] A1 Säkerhetsrapport – Allmän del, reg nr 2005-15169, 2012-05-29 OKG Oskarshamn.

[2] BWR Säkerhetsprinciper och funktioner, KraftAkademin 2003.

[3] Swedish Radiation Safety Authority Författningssamling, SSMFS 2008:17, ISSN 2000-0987, Johan Strandberg.

[4] A1 Säkerhetsrapport – Allmän del, O3 - Konstruktionsstyrande händelseförlopp och acceptanskriterier, reg nr 2003-09231, 2013-11-20 OKG Oskarshamn.

[5] Swedish Radiation Safety Authority Författningssamling, SSMFS 2008:1, ISSN 2000-0987, Ulf Yngvesson.

[6] A4 Säkerhetsrapport referensdel, Tolkning och tillämpning av SSMFS 2008:17, reg nr 2005-12584, 2012-12-19 OKG Oskarshamn.

[7] A1 Säkerhetsrapport – Allmän del, reg nr 2003-09285, 2009-02-16 OKG Oskarshamn.

[8] A1 Säkerhetsrapport – Allmän del, Yttre påverkan, reg nr 2006-06747, 2012-10-29 OKG Oskarshamn.

[9] A1 Säkerhetsrapport – Allmän del, Skydd mot yttre påverkan, reg nr 2003-09307, 2012-06-27 OKG Oskarshamn.

[10] A1 Säkerhetsrapport – Allmän del, O2 – Beskrivning av anläggningens säkerhetsfunktioner, reg nr 2007-23163, 2007-12-15 OKG Oskarshamn.

[11] A2 Systembeskrivning, O3 – System 314 – Avblåsningssystem, reg nr 2007-13844, 2009-03-31 OKG Oskarshamn.

[12] A2 Systembeskrivning, O3 – System 316 – Kondensationssystem, reg nr 2007-13830, 2012-04-27 OKG Oskarshamn.

[13] A2 Systembeskrivning, O3 – System 321 – Kylsystem för avställd reaktor, reg nr 2007-20372, 2014-01-09 OKG Oskarshamn.

[14] A2 Systembeskrivning, O3 – System 322 – Sprinklersystem för reaktorinneslutningen, reg nr 2007-21534, 2014-01-03 OKG Oskarshamn.

[15] A1 Säkerhetsrapport, Seismisk konstruktion, reg nr 2003-09285, 2009-02-16 OKG Oskarshamn.

[16] A4 Säkerhetsrapport referensdel – Tolkning och tillämpning av SSMFS 2008:17, reg nr 2005-12584, 2012-12-19 OKG Oskarshamn.

[17] 3.1 Rapport – Allmän, Oskarshamn 1, 2 och 3 – framtagning av generiska branduppkomstfrekvenser för användning inom PSA, reg nr 2010-33307, 2010-12-23 OKG Oskarshamn.

[18] G5 Teknisk rapport, Oskarshamn 1, 2 och 3 – Frekvenser för transienter i PSA uppdaterad tom 2010, reg nr 32800049-22-A-R-004, 2011-04-01 OKG Oskarshamn.

[19] 21.1 Beskrivning – Allmän, Oskarshamn 1,2 och 3 – PSA Metodbeskrivning D1 – Sekvensanalys nivå 1, reg nr 2011-02998, 2012-01-13 OKG Oskarshamn.

[20] 21.1 Beskrivning – Allmän, Oskarshamn 1, 2 och 3 – PSA Metodbeskrivning D2 – Sekvensanalys PSA nivå 2, reg nr 2011-02999, 2012-01-13 OKG Oskarshamn.

[21] Beskrivning av TRs analysverksamhet med MAAP, reg nr 2006-02058, 2006-02-14 OKG Oskarshamn.

[22] 21.1 Beskrivning Allmän, Oskarshamn 1, 2 och 3 – PSA Metodbeskrivning B1 – Översikt, fastställande av omfattning och faser, reg nr 2011-02987, 2012-04-26 OKG Oskarshamn.

[23] SKI Rapport 99:53, Kommentarer från SKI:s granskning av Oskarshamn 3 PSA, ISSN 1104-1374, 1999-12 Safetech Engineering AB Västerås.

[24] TRs anvisning för reaktorsäkerhetsteknisk värdering, reg nr 2004-08419, 2005-09-13 OKG Oskarshamn.

[25] 21.1 Beskrivning – Allmän, PSA-verksamhet, reg nr 2007-27456, 2012-11-21 OKG Oskarshamn.

[26] SKI Rapport 2006:19, Hantering av CCF vid beräkningar i PSA och PSA-tillämpningar, ISSN 1104-1374, 2006-03 SSM.

[27] T-boken – Version 7, Tillförlitlighetsdata för komponenter i nordiska kraftreaktorer, ISBN 978-91-633-6143-2, TUD-kansliet Vattenfall Power Consultant AB, 2010 Stockholm.

[28] Handbok för riskanalys, sidan 30-31, ISBN 91-7253-178-9, Räddningsverket 2003.

[29] IAEA-TECDOC-719, Defining initiating events for purposes of probabilistic safety assessment, ISSN 1011-4289, 1993 IAEA Vienna.

[30] A3 PSA-rapport, Oskarshamn 1 – Inre händelser vid effektdrift, reg nr 2012-06266, 2012-08-06 OKG Oskarshamn.

[31] 3.1 Rapport – Allmän, Fire Project Report: ”Collection and Analysis of Fire Events (2002-2008) – First Applications and Expected Further Developments”, reg nr 2010-23588, 2010-09-16 OKG Oskarshamn

[32] A3 PSA-rapport, Oskarshamn 1 – PSA Kapitel 6.2.1 – Frekvenser för inre händelser vid effektdrift, reg nr 2012-06356, 2012-08-06 OKG Oskarshamn.

[33] SKI Technical Report 92:3, Project SEISMIC SAFETY – Characterization of seismic ground motions for probabilistic safety analyses of nuclear facilities in Sweden, reg nr 2007-27563, 1992 VBBconsulting Ltd Stockholm.

[34] 21.1 Beskrivning – Allmänn, PSA Metodbeskrivning A4 – Förkortningar, beteckningar och definitioner, reg nr 2011-02986, 2012-08-16 OKG Oskarshamn.

[35] 3.1 Rapport – Allmän, Oskarshamn 3 – PSA Nivå 1 – Resultatredovisning effektdrift, reg nr 2006-08716, 2011-07-11 OKG Oskarshamn.

[36] A1 Säkerhetsrapport – Allmän del, Oskarshamn 1 – Säkerhetsrapport – Kapitel 6 Avsnitt 6.18, reg nr 2002-11555, 2012-11-14 OKG Oskarshamn.

[37] A3 PSA-rapport, Oskarshamn 1 – PSA Kapitel 8.2.1 – Resultat Nivå 1 effektdrift – Inre händelser, reg nr 2012-06374, 2012-09-18 OKG Oskarshamn.

[38] 3.1 Rapport – Allmän, Oskarshamn 2 – PSA Nivå 1 – Effektdrift – Resultatredovisning, reg nr 2007-03673, 2007-10-25 OKG Oskarshamn.

[39] A3 PSA-rapport, Oskarshamn 1 – PSA Kapitel 8.4.1 – Resultat brand, reg nr 2012-06380, 2012-10-19 OKG Oskarshamn.

[40] Oskarshamn 2 – Resultat brand, reg nr 2007-03687, OKG Oskarshamn.

[41] Oskarshamn 3 – Resultat brand, reg nr 2006-05125, OKG Oskarshamn.

[42] 2014-02656, Utvärdering av OKGs metod för säkerhetsvärdering – samstämmighet mellan deterministisk och probabilistisk utvärdering.

[43] 2004-08419 utgåva 3, Genomförande av reaktorsäkerhetsteknisk värdering.

[44] R.Hurtig, Resultat hörande till Roger Hurtigs examensarbete på TR, OKG meddelande.

[45] 2012-28779 utgåva 1. Förslag till utveckling av rutiner och metod för reaktorsäkerhetsteknisk värdering.

[46] Lloyd's Register Consulting (2015), RiskSpectrum PSA. Available at: http://www.riskspectrum.com/en/risk/Meny_2/RiskSpectrum_PSA/ (Accessed 10 Mars 2015).

[47] United States Nuclear Regulatory Commission (15 January 2015), Boling Water Reactors. Available at: http://www.nrc.gov/reactors/bwrs.html (Accessed 11 Mars 2015).

[48] Vattenfall (1 October 2013), Nuclear power – how it works. Available at: http://corporate.vattenfall.com/about-energy/electricity-and-heat-production/nuclear-power/how-it-works/ (Accessed 11 Mars 2015).

[49] NP-2230, Frequency of Anticipated Transients, 1982 Electric Power Research Institute, Palo Alto California.

[50] Idaho National Engineering and Environmental Laboratory, Calculating Conditional Core Damage Probabilities for Nuclear Power Plant Operations, Idaho Falls, Idaho 83201.