

Master's programme in Automation and Electrical Engineering

Application of System-Theoretic Process Analysis (STPA) in Nuclear Instrumentation and Control systems

Hiruni Kothalawala

Copyright © 2023 Hiruni Kothalawala

Author Hiruni Kothalawala

Title Application of System-Theoretic Process Analysis (STPA) in Nuclear Instrumentation and Control systems

Degree programme Automation and Electrical Engineering

Major Control, Robotics and Autonomous Systems

Supervisor Prof. Valeriy Vyatkin

Advisors Polina Ovsiannikova (MSc), Eetu Heikkilä (MSc)

Date 25 July 2023

Number of pages 58+30

Language English

Abstract

This thesis evaluates the application of System-Theoretic Process Analysis (STPA) in analyzing the Instrumentation and Control (I&C) systems within Nuclear Power Plants (NPPs). Ensuring the safety of I&C systems is crucial, as they play an important role in NPPs' operations. Most I&C systems in NPPs are reaching their end of life and require upgrades. These upgrades will replace the older analog electromechanical systems with newer software-intensive digital I&C systems.

Traditional hazard analysis methods, such as Fault Tree Analysis (FTA) and Failure Modes and Effects Analysis (FMEA) are more suitable to be used when analyzing older analog electromechanical systems and they have limitations when applied to these newer digital I&C systems. System-Theoretic Accident Model and Processes (STAMP) is a new accident model based on the System Theory. STPA is a tool based on STAMP that can be used to analyze complex systems that consist of software.

This thesis uses a case study of a feedwater control system that is used to control the feedwater level inside the reactor pressure vessel of an NPP. The provided case study is analyzed using STPA and the results are presented in this thesis. In addition to the results of the STPA, the observations, and challenges throughout the process are discussed. The thesis also discusses the impact of the level of information used in conducting STPA.

Keywords STPA, STAMP, Hazard Analysis, Safety Critical Systems, Instrumentation and Control Systems, Nuclear power generation, Nuclear power plants, Nuclear Safety

Preface

I am honored to present this master's thesis, which represents the culmination of my academic journey and research efforts. Undertaking this study has been an enlightening experience, and it would not have been possible without the support and guidance of numerous individuals and organizations.

First and foremost, I would like to express my deepest gratitude to my supervisor Professor Valeriy Vyatkin. His unwavering dedication, insightful guidance, and invaluable expertise have been instrumental in shaping this research work.

I would also like to extend my heartfelt appreciation to my advisors Polina Ovsianikova (Aalto University) and Eetu Heikkilä. Their expertise, scholarly insights, and constructive feedback have significantly contributed to the development and refinement of this thesis.

Furthermore, I would like to express my sincere appreciation to VTT Technical Research Centre of Finland and TVO (Teollisuuden Voima Oyj), for their collaboration and support throughout this research endeavor. The access provided to their resources and expertise has been pivotal in conducting a comprehensive analysis and achieving meaningful results. Their commitment to fostering research and innovation in the nuclear power industry is commendable, and I am grateful for the opportunity to collaborate with such esteemed organizations.

I would like to acknowledge the invaluable contribution of the project manager Antti Pakonen (VTT), whose diligent coordination and oversight ensured the smooth progress of this research. In addition, I would like to express my sincere gratitude to Risto Tiisanen (VTT) and Josepha Berger (VTT) who have provided expertise on STPA (Systems-Theoretic Process Analysis). Their contributions have been vital in understanding the intricacies of this analysis technique, its application to my research, and the interpretation of the analysis results.

Furthermore, I would like to express my deepest gratitude to Lauri Tuominen and Pekka Nuutinen from TVO. Their willingness to share their extensive knowledge, provide clarifications, and answer my numerous questions has been instrumental in shaping the research outcomes.

Finally, I would like to express my heartfelt thanks to my family, friends, and loved ones for their unwavering support and encouragement throughout this journey. Their belief in my abilities and their constant motivation has been a source of strength.

Otaniemi, 25 July 2023

Hiruni A. Kothalawala

Contents

Abstract	3
Preface	4
Contents	5
Abbreviations	7
1 Introduction	8
2 Literature review	10
2.1 Systems and Safety-Critical systems	10
2.2 Nuclear energy for power generation	10
2.2.1 Olkiluoto NPP	12
2.2.2 Boiling Water Reactor (BWR)	12
2.2.3 Power states of an NPP	13
2.2.4 Nuclear I&C Systems	14
2.2.5 Nuclear Safety	15
2.3 Hazard Analysis	17
2.3.1 Traditional Hazard Analysis Methods	18
2.4 System-Theoretic Process Analysis (STPA)	18
2.4.1 System-Theoretic Accident Model and Process (STAMP) . .	19
2.4.2 Step 1: Defining the objective of the analysis	20
2.4.3 Step 2: Creating a model of the system as a Control Structure	21
2.4.4 Step 3: Identifying Unsafe Control Actions	21
2.4.5 Step 4: Identifying Loss Scenarios	23
2.4.6 Output of STPA	23
2.5 Tools for STPA	24
3 Case-study: Feedwater Control System	26
3.1 Introduction: Feedwater Control System	26
3.1.1 Inputs to the feedwater control system	26
3.1.2 Outputs from the feedwater control system	28
3.1.3 Controllers in the system	29
3.2 Operation	32
3.2.1 Valve behavior during Normal operation	32
3.2.2 Valve behavior during Low-power operation	32
3.2.3 Pump behavior	33
3.2.4 Reactor Scram	33
3.2.5 Operator interactions with the system	33

4	Case Study: Application of STPA on the Feedwater control system	35
4.1	Initial preparations	35
4.2	STPA Step 1: Define the purpose of the analysis	35
4.2.1	Identifying Losses	36
4.2.2	Identifying System-Level Hazards	36
4.3	STPA Step 2: Model the control structure	37
4.4	STPA Step 3: Identifying the unsafe control actions	38
4.5	STPA Step 4: Identifying loss scenarios	46
4.5.1	Identification of scenarios that leads to UCAs	46
4.5.2	Identification of scenarios with improper execution of control actions	48
5	Discussion and Conclusion	54
5.1	Application of STPA	54
5.2	Results of the STPA	55
5.3	Future work	55
	References	56
	59appendix.A	
	60appendix.B	
	66appendix.C	

Abbreviations

BWR	Boiling Water Reactor
CA	Control Action
CAST	Causal Analysis based on System Theory
EPR	European Pressurized Reactor
FMEA	Failure Modes and Effects Analysis
FTA	Fault Tree Analysis
HAZOP	Hazard & Operability Analysis
HWR	Heavy-Water Reactors
IAEA	International Atomic Energy Agency
I&C	Instrumentation and Control
NPP	Nuclear Power Plant
PRA	Probabilistic Risk Assessment
PWR	Pressurized Water Reactor
STAMP	System-Theoretic Accident Model and Processes
STPA	System-Theoretic Process Analysis
STUK	Radiation and Nuclear Safety Authority
TVO	Teollisuuden Voima Oyj
UCA	Unsafe Control Action

1 Introduction

Nuclear power has been in use for decades in many countries. Similar to any other system, when nuclear systems became a part of the modern world, the hazards, and risks that come with them have become a part of the modern world as well. However, due to their sensitive nature, the public still has safety concerns about Nuclear Power Plants (NPP). Despite these concerns, nuclear power seems to gain popularity due to its low carbon footprint and high efficiency. Nuclear systems are categorized as safety-critical systems similar to domains such as aviation, military applications, and medical devices since the consequences of failure of such systems would be simply unacceptable [1].

The systems that perform control functions, service functions, and monitoring functions related to the operation of an NPP, are the Instrumentation and Control (I&C) systems, and they are often seen as the central neural system of an NPP [2, 3]. Hence, they are playing an essential role in the safety of the plants, and it is important to have safe practices integrated into their standard operation.

Ericson et al. [4] describe hazard as a potential condition existing within a system that could result in an accident, causing damages, loss, injury, and even death. Hazard analysis is a usual practice for any system, and it is the main step in ensuring the safety of a system. In the Nuclear context, the hazard analysis of the I&C systems is crucial to ensure the safety of the NPP and is required by the relevant authorities. The traditional hazard analysis methods such as Fault Tree Analysis (FTA) and Failure Modes and Effects Analysis (FMEA), are mostly based on traditional analytical decomposition theory. They assume that the system can be broken into components that are independent of each other and that they only interact with each other in known ways [5, 6]. It is also assumed that the accidents in the systems are only due to failures in one or more components. These assumptions were almost accurate for most of the analog electromechanical systems in the NPPs.

However, I&C systems in most NPPs are reaching the end of their lifetime and are in need of upgrades. Most upgrades will move these systems from electromechanical systems to digital systems. These digital systems are far more complex and raise different issues related to safety, human factors, and security, compared to the previous electromechanical, analog systems [3]. With this complexity in digital systems, accidents can occur not only due to component failures but also due to flaws in the system [5, 6]. These flaws could be the system being driven into an unsafe state or being unable to issue the required commands. Hence, the traditional hazard analysis methods as well as the assumptions associated with them become limited when applied to these newer systems. This problem creates the requirement for a new analysis.

System-Theoretic Process Analysis (STPA) is a relatively new system analysis technique based on the System Theory that perceives the system as a whole rather than as a collection of sub-components [5]. Even though most of the applications use STPA for system safety analysis, it can also be used for analyzing other emergent properties in the system such as reliability and security. STPA can be applied at the first stage of the system design instead of waiting till the system design is completed so that safety becomes an inherent property of the system [5].

Despite STPA being already applied in many industries such as aviation and automobiles, little work has been focused on its applicability in the Nuclear domain. Thus, the aim of this thesis is to evaluate the use of STPA in the Nuclear energy domain and to identify possible challenges. The level of information required about the system under investigation, for conducting STPA will be also discussed. In order to achieve these goals, a case study will be conducted by analyzing a sample I&C system from an NPP using STPA. The selected I&C system is the feedwater control system of an NPP and an example will be provided from the industry. The STPA will be conducted using resources from the industry, discussions with experts, and collaborative workshops. Based on the observations throughout the analysis process, the thesis will present the conclusions about the use of STPA in the nuclear industry. This thesis is a part of the SEAMLES project, funded by the National Nuclear Safety and Waste Management Research Programme 2023-2028 (SAFER2028).

The remainder of this thesis is organized as follows. Chapter 2 reviews the literature on the relevant concepts including Nuclear energy operations and background to the STPA process. Chapter 3 provides the structure and the operation of the feedwater control system from the case study. Chapter 4 presents the process of applying the STPA to the case study, the observations and the result. Finally, in Chapter 5, summarizes the observations from the study, faced challenges and possible future work.

2 Literature review

This chapter presents the relevant background for the thesis, including details on Nuclear Power Plants (NPP), I&C systems, and hazard analysis methods. Also, the method used in this case study, STPA, and its steps are described.

2.1 Systems and Safety-Critical systems

For most of our lives, we interact with different systems and they have become a part of the modern world. This means we also have the hazards and risks that come with the systems, in our lives. Ericson et al. [4] describe hazard as a potential condition existing within a system when actuated becomes an actual mishap event causing damages, loss, injury, and even death.

A system is safety-critical if the consequences of a failure in the said system are unacceptable [1]. Some examples of applications of safety-critical systems are medical devices such as heart-lung machines, air traffic controls in aviation, military applications, weapons, and also nuclear reactors. The use of the software is now has become popular in each of those domains. Even though some claim that the use of software contributes positively to the safety of the system, their reliability is not measurable in applications, due to their unpredictability and complexity [7].

The highest priority of a safety-critical system should be given to avoiding injuries or loss of human life, even at the cost of the availability of the system. Hence the development of such a system requires not just technical skills but also ethical considerations since most of the decisions related to software are made considering economic impacts rather than safety [7].

2.2 Nuclear energy for power generation

The primary operation of an NPP is the electrical power generation for the electric grid using nuclear reactions. Even though it was possible to use nuclear fission and nuclear decay reactions for power generation, the most common choice in NPPs is using nuclear fission of uranium and plutonium. There are different reactor types used for nuclear power generation. Out of these different types, the most common reactor types are Pressurized Water Reactor (PWR) and Boiling Water Reactor (BWR). More than 60% of the world's nuclear reactors are of PWR type. PWR and BWR are mostly light-water reactors, which means they use light water as their coolant and moderator [8]. The function of the coolant is to transfer heat and the function of the moderator is to slow down the neutron inside the reactor. Light water refers to the ordinary water (H_2O) that is commonly found in nature. Some reactors use heavy water as the coolant and heavy water (D_2O) is a chemically different type of water that consists of a heavier Hydrogen isotope. PWR has two separate water circuits to transfer heat from the reactor core to generate steam, while the BWR has only one circuit to create steam from the heat inside the reactor core. The operation of a BWR is described in detail below.

There are also less popular reactor types such as Heavy-water reactors (HWR), Gas-cooled reactors, and Fast breeder reactors [8].

Currently, more than 30 countries utilize nuclear power to cater to the country's electricity demand and there are more than 400 operable reactors scattered around the world [9]. As shown in Figure 1, out of the total electricity generation of the world about 10% is from nuclear power. The United States, France, China, Russia, and South Korea are among the top five countries that utilize nuclear power [9].

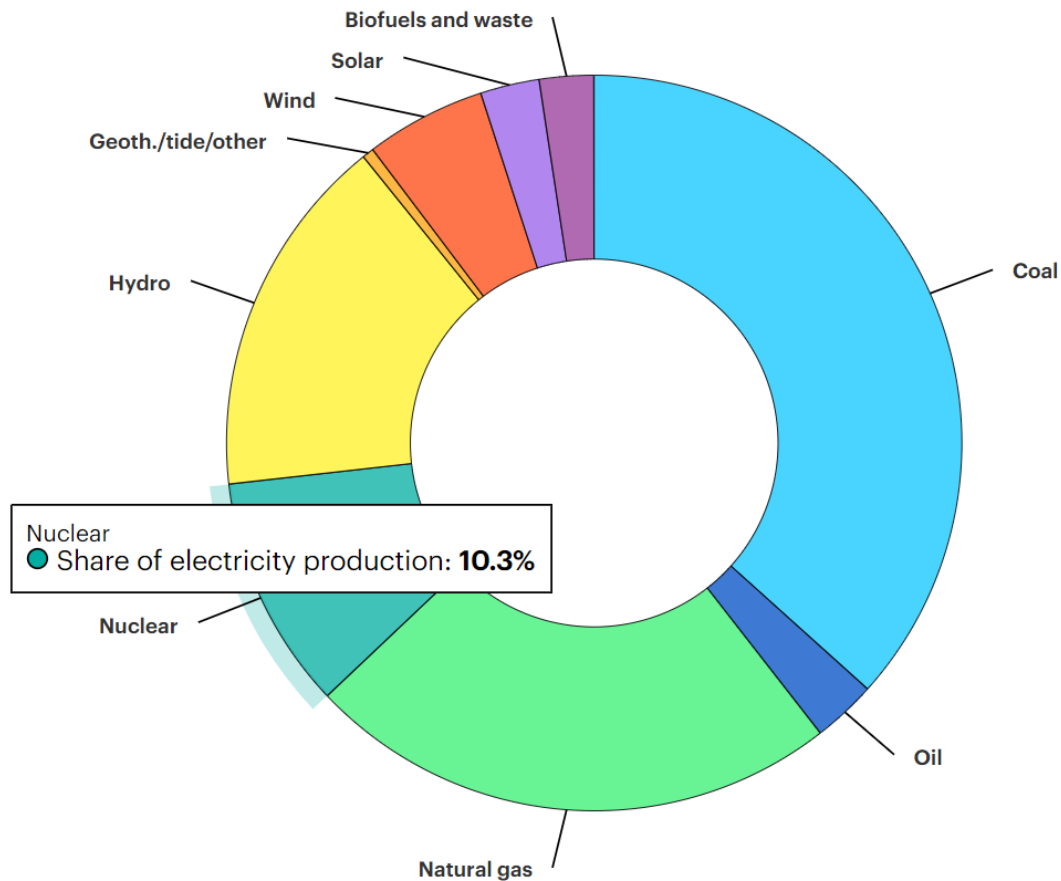


Figure 1: World gross electricity production by source, 2019 [9].

When it comes to Europe, there are 13 countries that use nuclear power generation including Finland. Of the total electricity generation in Europe, 25% was from nuclear power in 2021.

As shown in Table 1, there are five reactors in operation in Finland, providing a net capacity of about 4.4 GW. OL3 in Olkiluoto NPP is the newest addition to the mix. In the year 2021, 32.8% of the country's total electricity generation was obtained from nuclear power [10].

Site	Plant	Capacity
Loviisa NPP	LO1	507 MW
Loviisa NPP	LO2	507 MW
Olkiluoto NPP	OL1	890 MW
Olkiluoto NPP	OL2	890 MW
Olkiluoto NPP	OL3	1600 MW

Table 1: Operable nuclear power plants in Finland.

2.2.1 Olkiluoto NPP

In this thesis, we are considering a case study from the NPP located on Olkiluoto island in Finland. The plant belongs to and is also operated by Teollisuuden Voima Oyj (TVO). The plant has two identical power plant units with Boiling Water Reactors (BWR); OL1 and OL2. OL1 and OL2 were first connected to the national grid in 1978 and 1980 respectively. Both reactors use Uranium Dioxide (UO_2) as the fuel and each reactor core has 500 fuel assemblies. These two were able to supply 20% of Finland's electricity demand in 2022. The newest addition to the NPP is OL3, a European Pressurized Reactor (EPR). It is forecasted that 30% of Finland's electricity requirements will be fulfilled by these three reactors together [11].

We are only focusing on the two BWR in this case study, OL1, and OL2. Each of these plants can produce 890MW of electricity. A cross-section of the OL1 and OL2 plants is shown in Figure 2.

The operations in the power plant are highly automated so that the Normal operation only requires minimal manual interactions with the operators in the control room.

2.2.2 Boiling Water Reactor (BWR)

Reactor types are defined based on the moderator and the coolant used in the reactor. Of the seven main types of nuclear reactors used in the world, the second most common type is the Boiling water reactor with 20% reactors being this type [11]. The Boiling Water Reactor (BWR) is a type of light-water reactor, where both the moderator and the coolant are light water.

As illustrated in Figure 3, Feedwater enters the reactor vessel, and the heat generated inside the BWR by the fuel rods (1) produces steam from the feedwater. The steam-water mixture is then sent through moisture separation and steam is separated. The steam is then directed through the high-pressure turbine (4), a reheater (5), and then a low-pressure turbine (6). The steam turns the turbines and subsequently, the turbine turns the generator (7) attached to it. The generator generates and provides electricity to the national grid. The steam then goes into the condenser (8) where it condensed back into water and is pumped back into the reactor vessel by the feedwater pumps (10). The control rods (2) and the recirculation pumps (3) are used to control the power output of the reactor. The recirculation pumps are used to circulate the water inside the reactor pressure vessel for better cooling of the core.

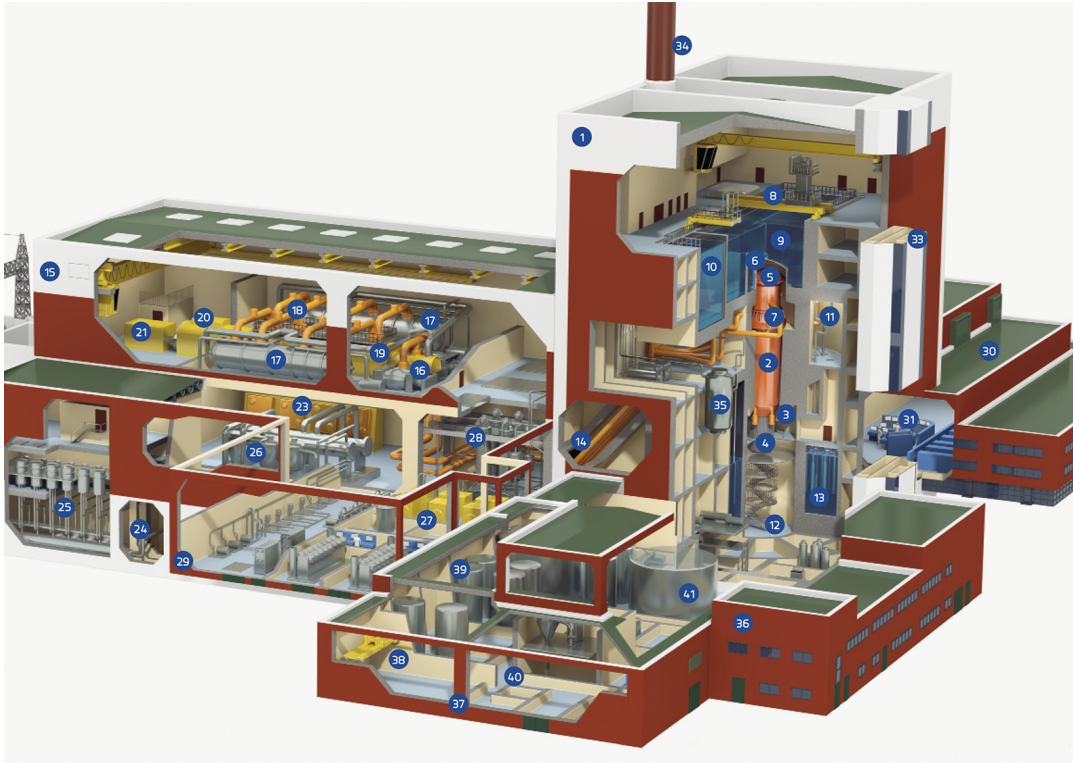


Figure 2: Crosssection of OL1 and OL2 reactors in Olkiluoto NPP [11].

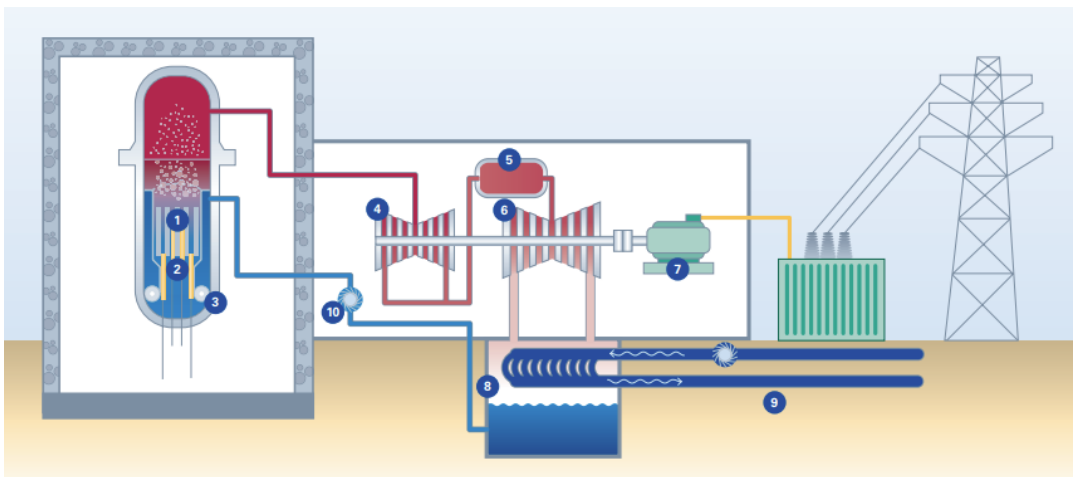


Figure 3: Operation of a Boiling Water Reactor [12].

In a BWR the steam and the feedwater might contain radioactive material due to its structure [13]. The feedwater system regulates the feedwater flow into the reactor.

2.2.3 Power states of an NPP

The NPP can operate continuously with a power output between 100% to 20% of the nominal output. When the power level is below 20% such as during the start-ups and

shutdowns, the plant is operated manually. The most common power states of an NPP are:

Normal operation During Normal operation, the power generation is around the nominal power of the output. Hence, the feedwater flow is also around the nominal value.

Low power operation During Low power operation the reactor generates a reduced output using a reduced feedwater flow. The margin between the normal operation and the Low power operation is based on the capability of different plant equipment such as feedwater pumps and turbines.

Hot shutdown Hot shutdown is required for some maintenance tasks that cannot be performed when the reactor is in operation.

Cold shutdown Cold shutdown is required for refueling and also for maintenance tasks on the primary system.

Reactor Scram Scram is an emergency shutdown of the reactor by cutting off the nuclear reaction. This is done by the rapid insertion of the control rods causing the reactor power to drop fast. During a Scram, the turbine is soon disconnected from the grid.

2.2.4 Nuclear I&C Systems

I&C systems are perceived as the “controlling system” and are often considered the central neural system of a facility. The components or systems being controlled become the “controlled system” [3]. The I&C systems can either facilitate manual control of a system by acting as an interface between the operators and the plant or provide automatic control based on the situation [14].

The main functions of an I&C system can be categorized as Information functions and Control functions. Information functions are tasks related to acquiring, processing, and displaying information. These include Monitoring, Displaying, Alarms, Data recording, and Archiving. Control functions of an I&C include functions for various tasks such as Protection, Limitation, Regulation, Interlocking, Discrete Control, and Remote Control. I&C systems could be either overall I&C systems that monitor and control all technological components at the NPP or individual I&C systems that work together [2].

There are different operational requirements for I&C systems including the instrument specifications as well as environmental conditions. These requirements are generated by analyzing the steady state, transient and accident conditions of the system under the regulatory requirements. Even though the I&C systems are placed in protected areas with good environmental conditions, it is important that they can perform in worse conditions as well. This is because accidents could create different environmental conditions and systems shouldn't fail in such cases. But in general, most of the I&C systems except sensors, are placed in better environmental conditions [15].

Due to the functions of an NPP, I&C systems are an integral component to ensuring the safety and security of the plant. It is common for I&C systems at an NPP to have safety in-built into their normal operation. An accident at an NPP could cause damage to the general public, the environment, personnel, and the plant itself. One of the main tasks of the I&C systems is to participate in functions to avoid such accidents [2, 14].

Most of the new or upgraded plants have digital I&C systems. Plants that are reaching their end of life are now looking at upgrading their analog system to digital systems. Transitioning from analog I&C systems to digital systems is expected to improve the safety as well as the performance, reliability, and availability of the NPPs. However, there are some concerns regarding this transition due to the uncertainty, lack of experience, and technical issues associated with the new technologies used in digital I&C systems. Digital systems are complex and they raise different issues related to factors such as safety, human factors, and security, compared to the previous analog systems. This possibility of new hazards is one major issue highlighted and it can greatly affect the safety of the system. Another concern is selecting suitable safety assessment techniques for the digital I&C systems [3, 15].

2.2.5 Nuclear Safety

In a global scope, the International Atomic Energy Agency (IAEA) provides safety standards to achieve nuclear safety. Even though each country is responsible for the regulation of its own nuclear operations, the impact of a nuclear accident would not be limited to the country's borders. Hence, cooperation between countries and knowledge-sharing is important to prevent disasters [16]. The safety standards from IAEA consist of Safety Fundamentals, Safety Requirements, and Safety Guides.

The Nuclear Energy Act (990/1987) is the governing legislation for the use of Nuclear Energy in Finland. This highlights the general principles of using Nuclear Energy, nuclear waste management, licensing, and competent authorities [17]. According to the Nuclear Energy Act, a license is required to operate an NPP and the responsibility of ensuring the safety of the NPP falls on the license holder [18].

The governing body for Nuclear safety in Finland is the Radiation and Nuclear Safety Authority (STUK). STUK has two main responsibilities regarding the NPPs in Finland; Supervising Nuclear Safety and Participating in the licensing process. The supervision is conducted from the design phase of the nuclear facilities until their end-of-life decommissioning [19]. STUK provides regulations as well as guides on nuclear energy and radiation application. The YVL guides composed by the STUK, based on the Nuclear Energy Act (990/1987), provide guidance on nuclear safety and security. These regulations came into effect in December 2013 and cover all operations related to an NPP [19]. The basis for the YVL guides is taken from the Nuclear Energy Act (990/1987), which states that *"the safety of nuclear energy use shall be maintained at as high a level as practically possible"* [20].

STUK's contribution during the licensing process of an NPP is to provide a safety assessment of the proposed plant and to provide guidance to the license candidate. Apart from the STUK, there are several parties involved in the licensing process. However, the final decision will be made by the Finnish Council of State [21]. STUK

also possesses the authority to intervene in the NPP operations when it is necessary to maintain safety. The license for an NPP is periodic and the period is decided based on various factors. However, in case of periods more than 10 years, STUK carries out intermediate safety assessments [21].



Figure 4: Global and local authorities for Nuclear governing.

The fundamental principle in the safety of an NPP is avoiding the radioactive material being released into the environment. The safety of the power plant is ensured by three conditions.

- Controlling of the chain reaction and the generated power
- Fuel cooling during normal operation and after shutdown
- Isolation of the radioactive substances from the environment

The safety approaches that provide the basis for nuclear safety are Defense-in-depth and Multiple barriers [22]. With these principles, an accident or a hazardous situation can occur only if several issues arise simultaneously. In other words, one error somewhere in the plant cannot drive the plant to an unsafe situation. With these approaches, the safety of the NPP is ensured by utilizing a good design, high quality, and careful operations to ensure safety [22].

In the Defense-in-depth approach, the goal is to prevent damage to the reactor and undesired radiation through several layers of safety that strengthen each other. These layers are; Preventive, Protective, and Mitigating. At the Preventive level, the focus is to prevent deviations from the desired behavior of the plant by conducting the design and operations of the plant to higher standards. The second level, the Protective level aims to identify problems and avoid them from progressing into an accident through safety systems. At the Mitigating level, there are safety systems implemented to mitigate the impact during an accident, especially to ensure that the containment is not compromised. These safety measures can be either physical measures or otherwise and they address both functional and structural systems.

The Multiple barriers principle is about placing many barriers between the radioactive materials and the environment [22]. These are physical safety measures in order to protect the environment against radioactive leakages. The typical barriers are a nuclear fuel rod that contains radioactive fuel, a cooling circuit wall, a containment

building that is pressure-resistant and gas-tight, and another building surrounding the containment building.

There are several other principles that are taken into account such as the principle of redundancy, the principle of separation, and the principle of diversity to improve the safety and the reliability of the NPP [22]. The redundancy requirement for an NPP in Finland is that the most important safety systems should be able to function at least with one non-functioning component and one damaged component in the system. Usually, this means having three devices working in parallel. By the principle of separation, redundant subsystems are placed in different locations inside the plant to avoid simultaneous failures. The principle of diversity focuses on implementing redundant systems using different operating technologies. Another principle is a 30-minute rule, which states that the operations that are required within a 30-minute period after an accident should be automated.

2.3 Hazard Analysis

It is understood one cannot completely get rid of hazards and risks, rather they should be mitigated by integrating safety into the system design. Hazard analysis is the main step in the process of ensuring system safety and it can help to identify the hazards, the effects of the hazards, and their causal factors [4].

While there are more than 100 hazard analysis techniques present [4], some mostly used techniques in digital I&C systems are:

- Design Failure Modes and Effects Analysis (DFMEA)
- Functional Failure Modes and Effects Analysis (FFMEA)
- Hazard & Operability Analysis (HAZOP)
- Fault Tree Analysis (FTA)
- System-Theoretic Process Analysis (STPA)

Out of these different methods, one can select one or more based on the scope and objectives of the analysis. For example, STPA, HAZOP, and FFMEA methods are most effective in plant-level analysis and the interactions of the plant with its environment. In contrast to this, DFMEA is most effective in a device-level analysis. When analyzing failures and behaviors of a system, STPA, and HAZOP become the most effective in identifying both expected and unexpected behaviors [4]. On the other hand, DFMEA and FTA are most effective in identifying expected behaviors. Another factor is that these techniques are most effective in different phases of the system development life cycle.

Even with their differences, these Hazard analysis techniques become highly effective in analyzing digital systems when taken to their extremes. However, it could be an expensive, time-consuming process that might deliver complex results.

The most common hazard analysis method in the nuclear industry is the Probabilistic Risk Assessment (PRA) method. In PRA, the risk of an incident is quantified using

two parameters: the severity of the accidents that can occur and the probability of occurrence. The PRA could be either qualitative or quantitative based on how these two parameters are expressed. The PRA process requires knowledge about possible accidents, their severity, and how likely they are to occur as inputs to the process. Hence, the accuracy of the results is dependent on the knowledge available on the probability of failures [23].

However, in this study, our focus is on the use of STPA. There are several differences between the traditional hazard analysis methods and STPA, based on their underlying concepts and assumptions.

2.3.1 Traditional Hazard Analysis Methods

Most of the traditional hazard analysis techniques such as FMEA (Failure Mode and Effects Analysis) make use of the Analytical Decomposition Theory [5]. In this approach, the system is broken down into smaller components and analyzed separately for their possible failures. The combination of these results is used to calculate the probability of different failures in the complete system. In the Analytical decomposition and therefore in the traditional hazard analysis methods, it is assumed that the sub-components are independent of each other and that the accidents are caused solely by failures of these components [5]. These assumptions were mostly true for the analog electromechanical systems that were used earlier.

However, the inclusion of software components in the systems, makes them more complex and more unpredictable. Accidents in these complex systems can occur not just from individual component failures anymore but also from flaws in the system, making it much more difficult to calculate the probability of incidents in these complex systems. These flaws could be the system being driven into an unsafe state or the system being unable to issue the required commands [5, 6]. In other words, safety is no longer related to the failures in individual components, but also to the unsafe interactions between the component that has not failed. Hence, the assumptions as well as the traditional hazard analysis methods become limited when applied to these complex, software-intensive systems.

2.4 System-Theoretic Process Analysis (STPA)

STPA is a fairly new analysis method based on the System Theory, where the system is treated as a whole. System Theory was introduced after World War II since the complexity of the systems started to increase since then. System theory differs from the traditional way of perceiving systems in several aspects. The main idea behind this is "the whole is more than the sum of its parts" [5]. In other words, the system theory acknowledges that the interactions between the components of a system cannot be always predicted and that the analysis by decomposition could provide an incomplete result.

Another unique feature of the system theory is the emergent properties. Emergent properties are properties that are absent in the collection of the system components but are arising when the system components interact with each other. Some examples

of these emergent properties are safety, security, maintainability, and operability [5]. Hence, to control these emergent properties, the controlling of individual components is insufficient. STPA can be applied for analyzing any emergent property other than safety and can be used to analyze different systems with different levels of technology and human involvement, even organizational systems.

In most cases, safety aspects are excluded from the system engineering process even though safety should be a top-most priority in system requirements. This makes some safety issues to be hidden until it is too late and they are often found when there are no easy solutions. Using STPA along with the system engineering process helps to avoid this issue by creating the safety requirements of the system before the system is implemented [5]. Furthermore, STPA is very easy to integrate with the system engineering process so that safety is ensured at all stages of the process. STPA can begin at the same time as the early stages of the system engineering process. STPA is now becoming a popular tool and plenty of research is being conducted in many industries such as aviation, robotics [24], defense [25], automotive [26, 27], and maritime [28].

Since STPA is a worst-case analysis method, when analyzing already existing systems, the safety features that are in place are not taken into consideration. One reason is in a worst-case scenario, the safety features might behave unpredictably and another is that STPA aims to prevent hazards irrespective of these safety features [5].

2.4.1 System-Theoretic Accident Model and Process (STAMP)

The theoretical foundation for the STPA is provided by System-Theoretic Accident Model and Processes (STAMP). STAMP is a new accident causation model based on System theory. STAMP improves the traditional model of causality which is based on chain-of-failure events, to suit more complex systems by considering unsafe interactions between components. STAMP perceives safety as a control problem rather than preventing failures and argues that accidents occur due to insufficient control. It makes it easier to analyze complex systems due to its top-down approach. STAMP takes the software, human and organizational components into consideration as causal factors. STPA is one of the analysis methods presented based on the STAMP framework. Another tool is Causal Analysis based on System Theory (CAST). CAST is used to investigate the analysis that has already happened while STPA is a proactive analysis method.

STPA follows four basic steps to conduct the Analysis as described in Leveson and Thomas (2018) [5].

1. Defining the objective of the analysis
2. Creating a model of the system as a Control Structure
3. Identifying Unsafe Control Actions
4. Identifying Loss Scenarios

2.4.2 Step 1: Defining the objective of the analysis

The first step of the STPA analysis is to define the objective of the analysis as well as the system under investigation. The objective of the analysis is important because STPA can be used for not just safety analysis, but also to investigate other aspects such as security and performance. There are four parts to be defined when going through the first step:

1. Define Losses

In STPA, a *loss* is defined as "a loss of something of value to the stakeholders". Also, a loss is not always safety-related but also could be related to other properties of the system such as security, privacy, and performance. Losses are unacceptable to the stakeholders and the target of conducting STPA is to prevent losses. Losses can be easily identified by first identifying the stakeholders of the system and then evaluating what they value in the system. However, losses are not components or states in the system. Some examples are loss of life, injuries, damages to the properties or environment, loss of production, and loss of confidential data.

2. Define System-level hazards

Hazards are defined in STPA as states or conditions of a system that could lead to loss when combined with external conditions. At this stage, we do not investigate the causes of these hazards. Before identifying the system-level hazards, it is important to identify the system under consideration and its boundary. Then we can identify the system states or conditions that can lead to one or more losses that were identified earlier in Part 1. It is important to note that we do not include external factors that are out of the control of the designer. Also, these hazards are not component-level failures, but rather system-level states. It is important to note that the hazards do not always lead to losses, but also depend on some external impacts. There are useful formats provided in the STPA Handbook [5] that can be used to record findings of the STPA process without missing important details and also without losing context. The below format can be used to specify hazards [5]. :

$$\langle \text{Hazard} \rangle = \langle \text{System} \rangle \ \& \ \langle \text{Unsafe Action} \rangle \ \& \ \langle \text{Link to Losses} \rangle$$

3. Define System-level constraints

System-level constraints are conditions for the system either to avoid hazards before they occur or to minimize losses in case a hazard occurs. System-level constraints can be directly derived from the system-level hazards identified in Part 2 above. One or more system-level constraints can be derived from a system-level hazard. In the same way, one system-level constraint could be connected to more than one hazard. Even though these constraints specify which conditions to avoid, they should not provide solutions at this stage.

The system-level constraints can be specified in the below format [5]:

<Constraint> = <System> & <Condition to ensure> & <Link to Hazard>

4. Refine Hazards (Optional)

This final and optional part is to create sub-hazards by refining the identified hazards, based on the complexity of the analysis to reduce the effort. Then the sub-hazards can be used as in Part 3 to specify more system constraints.

2.4.3 Step 2: Creating a model of the system as a Control Structure

In step 2 of the STPA, a model of the system is created depicting the functional relationships and interactions in the system using control loops. This hierarchical model is called a Control Structure. Creating the Control Structure is an iterative process that can begin at an abstract level and work through to redefine it with more details. The control structure is created vertically, depicting the authority each component has over the components below in the system.

A control structure diagram depicts *Controlling Units* and *Controlled processes*, while the arrows are representing the interactions between them. Interactions are *Control actions* depicted by downward direction arrows and then *Feedback* represented in upward direction arrows [29]. Controlling Units issue control actions to the controlled process to control their behaviors. The *Control algorithm* is the controlling unit's method of decision-making. The feedback is to communicate the current status of the component to the controlling unit. This feedback is used to educate the *Process Model* in the Controlling Unit about the Controlled Process. The controlled process is usually placed at the bottom of the control structure.

Figure 5 depicts a hierarchical control structure that can be used to represent systems with several different control loops. It is important to understand that this diagram is not limited to the hardware components of the system, but also should include personnel and software interacting with the system. For example, the Controllers in the Control Structure can be either automated controllers or humans [5]. However, the control structure is neither a physical model nor a simulation model.

When creating the control structure, each component can have its responsibilities defined. The responsibility of each component is their contribution to ensure system-level constraints. These responsibilities can be used to further refine the control structure as suitable for the analysis. Despite all the control actions and feedback being shown in the control structure, it is not assumed that they are obedient so that they are always executed perfectly.

2.4.4 Step 3: Identifying Unsafe Control Actions

STPA defines *Unsafe Control Actions* as control actions that in a particular context and in a worst-case situation can lead to a hazard [5]. In the STPA Step 3, the control actions from the Control Structure created in Step 2 earlier, are then analyzed to identify how they could become Unsafe Control Actions (UCA) contributing to the losses identified in Step 1.

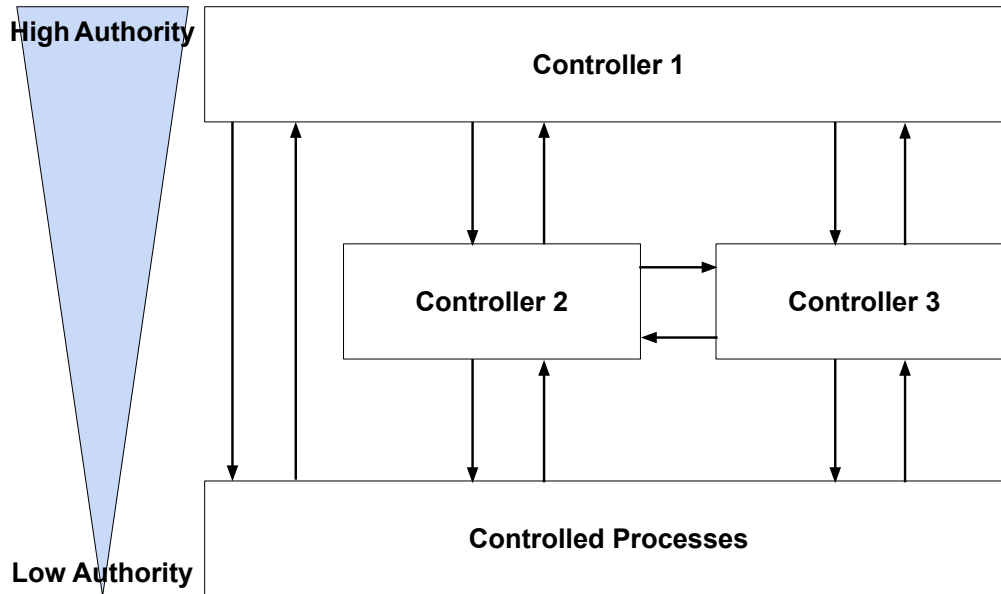


Figure 5: Generic Hierarchical Control Structure adopted from [5].

The STPA framework provides four behaviors of a control action that can lead to an unsafe state:

1. Not providing the control action
2. Providing the control action
3. Providing the control action at an inappropriate time (e.g. too soon, too late, or in the wrong order)
4. Providing the control action for an inappropriate duration (e.g. Stops too soon or stops too late)

The control actions of the system are not always unsafe but rather depend on the state of the system. Hence it is important to provide context about when or what makes the control action unsafe. The UCA can be specified in the following format [5]:

$\langle \text{UCA} \rangle = \langle \text{Source} \rangle \& \langle \text{Type} \rangle \& \langle \text{Control Action} \rangle \& \langle \text{Context} \rangle \& \langle \text{Link to Hazard} \rangle$

Then we can specify the controller constraints for each controller usually by inverting the UCAs. These are the conditions for the controller in order to avoid UCAs from happening.

2.4.5 Step 4: Identifying Loss Scenarios

In the final step of the STPA, different scenarios are identified as causal factors for unsafe control actions and consequently hazards. Loss scenarios can be either related to a UCA or not related to any UCA and then can be further classified based on the types of causal factors, as shown in Figure 6.

- **Scenarios related to UCA**

When looking for this type of scenario, the UCAs identified in the previous Step of the STPA are considered and the causes for a UCA to occur are analyzed. Below two cases should be considered when generating loss scenarios related to the UCAs.

1. **Unsafe controller behavior**

Some example scenario types that are related to the controller would be failures in the controller hardware, errors in the control algorithm, and unsafe inputs from another controller. The insufficient process model is another type of scenario that leads to UCAs. The process model of the controller is the beliefs formed in the controller using the feedback and information that the controller receives. Therefore, when defining scenarios caused by an insufficient process model, it is important to also provide the root cause that created this insufficient process model.

2. **Insufficient feedback and information to the controller**

When a scenario is caused by an insufficient process model, it needs to be further analyzed to identify the reason that causes this flawed process model. The root cause could be either the controller not receiving a piece of information/feedback or the controller receiving incorrect information/feedback.

- **Scenarios related to improper execution of control actions**

Even though the control action is correct and adequate, hazards can still occur by the wrong execution of the signals. These errors in executions could be either in the path of the control action or in the controlled process. The path of the control action could consist of components such as actuators and communication equipment. Unpredictable behavior in such components could affect the control signal or even delay the signal. Unpredictable behavior from the controlled process such as unexpected responses to the control actions and not responding to the control actions could also create scenarios that could lead to hazards.

2.4.6 Output of STPA

All the information and results from each step of the STPA can be summarized in Figure 7. This shows how these results are connected to each other and also the top-to-bottom approach in the STPA method. There are many ways these outputs can

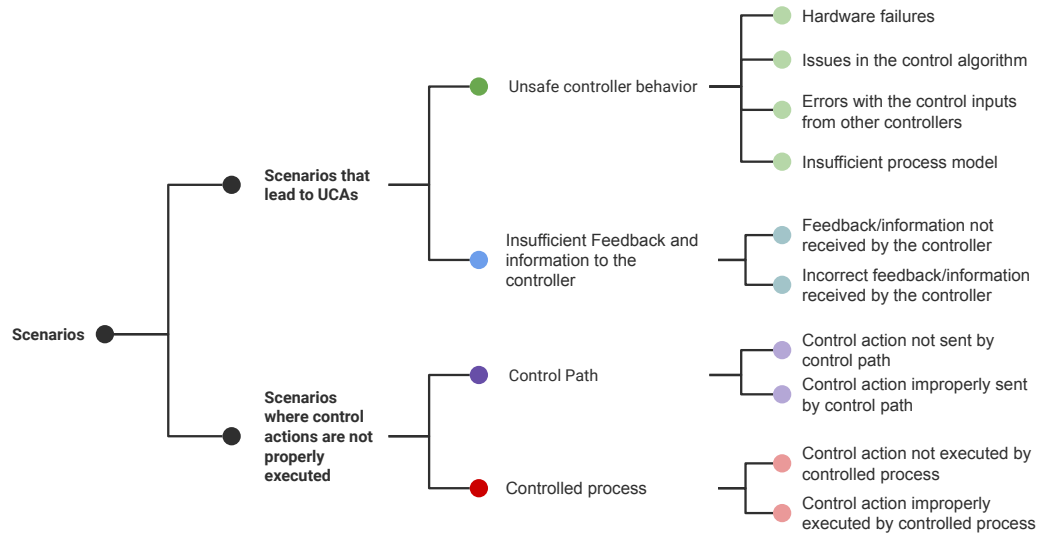


Figure 6: Different types of loss scenarios that lead to UCAs, summarized from [5].

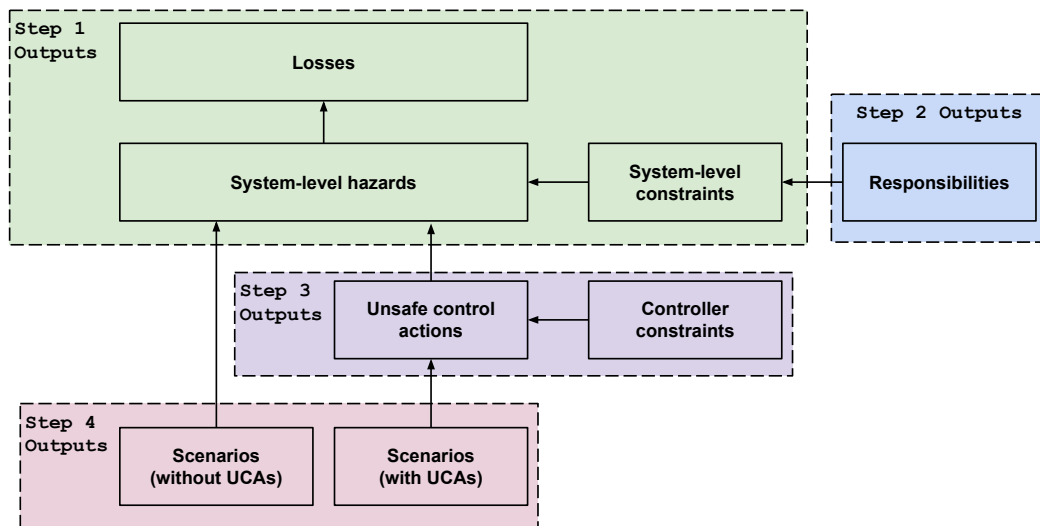


Figure 7: Information from each step of the STPA adopted from [5].

be used such as to create system requirements and to provide recommendations for the system design [5].

These requirements can be used to take subsequent actions such as defining additional requirements to ensure system safety.

2.5 Tools for STPA

STPA is a relatively new technique with limited tool support. Hence, it is common to use pen and paper or other general tools like Office Packages and drawing software. However, there are a few experimental tools that promote and support the use of STPA.

Some of these tools are freely available while some are commercial.

One such tool is A-STPA, implemented using Java to support the STPA. This tool provides different functionalities to automate the STPA steps of establishing fundamentals, defining safety constraints, creating control structure diagrams, and then editing the different analysis tables [30].

Then SafetyHAT is another tool proposed for conducting STPA. In this tool, the main 4 steps of the STPA are broken down into 8 steps to simplify the process for the user. SafetyHAT has the capability to store, manage, and organize data, document the analysis, and create a mapping between causal factors to system-level losses. SafetyHAT includes a customized guide for transportation systems [31].

SAHRA (STPA-based Hazard and Risk Analysis) is another tool supporting STPA. This tool provides unique methods to capture the details in a visual mind map during the first two steps of the STPA process. SAHRA was proven to be a success when used in R&D projects in the industry as well as in academia [32].

The STPA case study in this thesis was conducted manually using conventional tools since many of the above tools are based on older versions of STPA.

3 Case-study: Feedwater Control System

The selected I&C system is the feedwater level control system that controls the feedwater level inside the reactor pressure vessel in OL1 and OL2 of the Olkiluoto NPP. Since OL1 and OL2 are identical, the feedwater control systems are also of the same structure.

In order to analyze the feedwater control system, it is important to understand the structure and operation of the system. This chapter provides an overview of the feedwater control system to be analyzed and its components. The documentation and guidance required for studying the system were provided by TVO.

3.1 Introduction: Feedwater Control System

The main goal of the feedwater level control system is to maintain the water level inside the reactor pressure vessel within the desired range, in different operational scenarios. Hence the main functions of the feedwater control system are:

- To maintain the water level inside the reactor pressure vessel within the desired range, during all power states (i.e. Normal operation, Low power operation).
- To maintain the water level inside the reactor pressure vessel within the desired range, during a hot shutdown.
- To limit the feedwater flow into the reactor pressure vessel to an acceptable value during a Scram event.

This is done by controlling the speeds of the feedwater pumps and the opening of the control valves in the feedwater system. The feedwater is received from the condenser and then pumped into the reactor pressure vessel using the feedwater pumps. Figure 8 shows the complete cycle of water flow required for the NPP operations, from feedwater being converted into steam and then later condensate in the condenser.

An overview of the feedwater system is shown in Figure 9, where there are two water flow circuits; feedwater flow which goes into the reactor vessel, and the recirculation flow which goes back into the condenser. The feedwater flow is the main flow supplying the feedwater to the reactor pressure vessel. The recirculation circuit is used during the start-up, shutdown, and Low power operation of the plant and sends a portion of the feedwater back to the condenser when required. The requirement for recirculation is to control the feedwater flow into the reactor vessel easier and faster. Feedwater flow is the summation of the feedwater flow that goes into the reactor pressure vessel and the recirculation flow. By maintaining a recirculation flow, the feedwater flow to the reactor can be easily increased or decreased when required.

3.1.1 Inputs to the feedwater control system

The components that provide input signals to the feedwater control system are transducers, monitors, and the safety systems of the plant. These signals provide

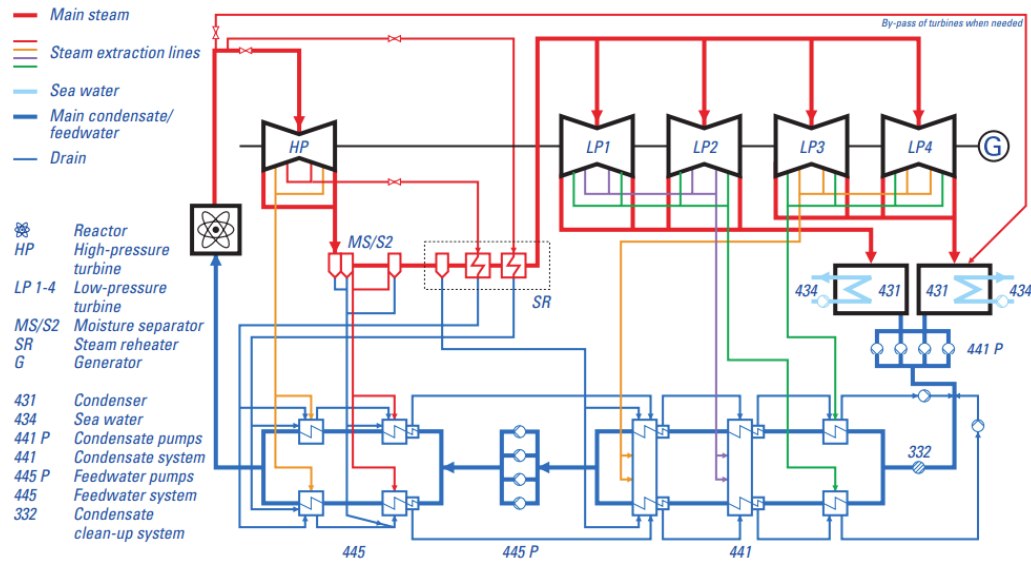


Figure 8: Steam, Condensate and Feedwater flow [12].

different information regarding the feedwater system and overall plant behavior. The measurements of the process variables are obtained using different transducers installed in the feedwater circuit. Below is a list of main input measurements to the feedwater control system.

Reactor water level This measurement is provided by four identical sensors that are mounted symmetrically. The pressure difference is measured using a Barton Cell and then used to convert the water level using a measurement converter. The output signal from the converter is an analog signal between 4-20 mA that converts. The average value from the four sensors is used in the feedwater control system algorithm.

Total steam flow The steam flow is measured using a Venturi [33] and a differential pressure measurement which provides an analog output signal of 4-20 mA. There are four measurements of the steam flow and the total steam flow is calculated as their summation.

Feedwater flow A throttle flange and a differential pressure measurement is used to obtain the feedwater flow. This also provides an output signal of 4-20 mA. However, this feedwater flow measurement is the total feedwater flow that flows into the reactor vessel as well as the recirculation. Therefore when the recirculation circuit is used, this feedwater flow measurement does not provide the feedwater flow that actually goes into the reactor vessel. In that case, the actual flow into the reactor pressure vessel is measured using the valve positions of the two valves in the feedwater path.

Feedwater pump speed measurements Each of the feedwater pumps is equipped with a tachometer to measure their speeds.

Control valve positions Positions of the control valves indicate how much they are open in a value between 0% and 100%. They are measured using the position of the actuators that are used to open and close the control valves. The actuators are equipped with position sensors that provide information about the control valve positions.

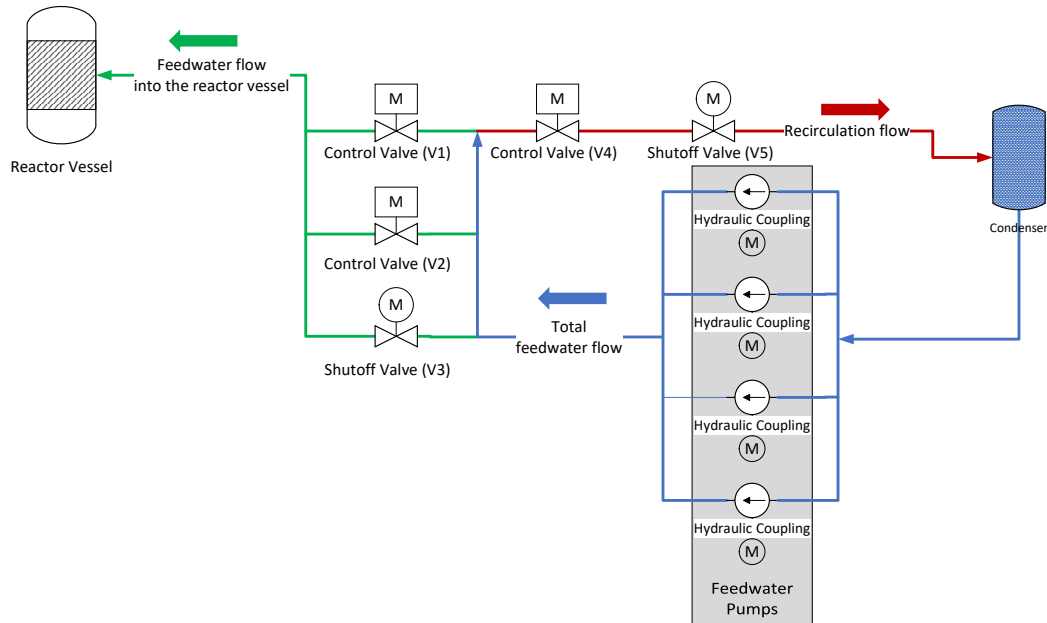


Figure 9: Feedwater system.

3.1.2 Outputs from the feedwater control system

The output signals from the feedwater control system are sent to different actuators in the feedwater system. The main actuators are the feedwater pumps and valves in feedwater lines. The main actuators can be observed in Figure 9.

Feedwater pumps There are four feedwater pumps coupled parallelly. Each pump is driven using a constant-speed, squirrel cage induction motor. A hydraulic coupling between the motor and the pump is used to achieve the variable speed in the pumps by varying the amount of oil in the coupling using an electric actuator.

Control Valves The control valves are used in the feedwater system to eliminate the non-linear behaviors in the system. The control valves are also actuated using means of electric actuators. The feedwater flow circuit has two parallel coupled control valves (V1, V2) to control the feedwater flow into the reactor vessel and the recirculation circuit has another control valve (V4) for the control of recirculation flow.

Shutoff valves There are two shutoff valves in the feedwater system. One shutoff valve is located in the feedwater flow circuit (V3) and the other is in the recirculation circuit (V5). The shut-off valve ensures there are no leakages through the closed control valves.

3.1.3 Controllers in the system

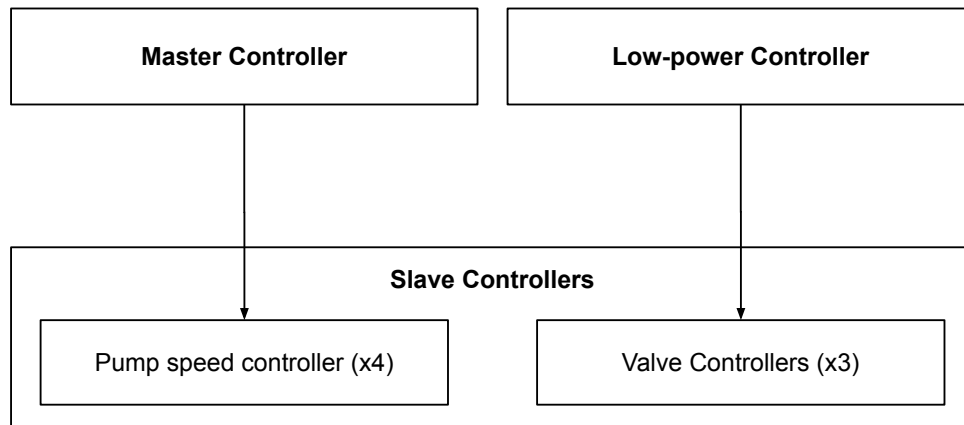
The feedwater control system has one Master controller, seven slave controllers, and a Low power controller that are installed inside control cubicles. The highest level of control is from the Master controller and the Low power controller. The slave controllers are controlled by the Master controller and the Low power controller based on the operational state of the reactor. Figure 10 shows an overview of the controller behavior of the feedwater control system based on the operational state of the NPP.

Master controller The Master controller of the feedwater control system controls the feedwater pumps during Normal power operation of the NPP and during an event of a SCRAM as shown in Figure 10. It consists of a three-point level controller unit and a flow controller unit. The water level inside the reactor pressure vessel is maintained by combining these two units in an algorithm. The preset value for the water level of the reactor pressure vessel is 4.2 m above the core and can be set using the potentiometers in the controller cubicles. The main inputs to the Master controller are the water level measurement inside the reactor, feedwater flow, and the total steam flow. Another important component in the Master controller is the SCRAM unit that controls the feedwater to the reactor pressure vessel after a SCRAM is triggered. The most important components of the Master controller are tripled to achieve redundancy in the controller. The Master controller generates three output signals that are sent to the slave controllers of the feedwater pumps as the pump speed set point. Figure 11 provides an overview of the structure of the Master controller.

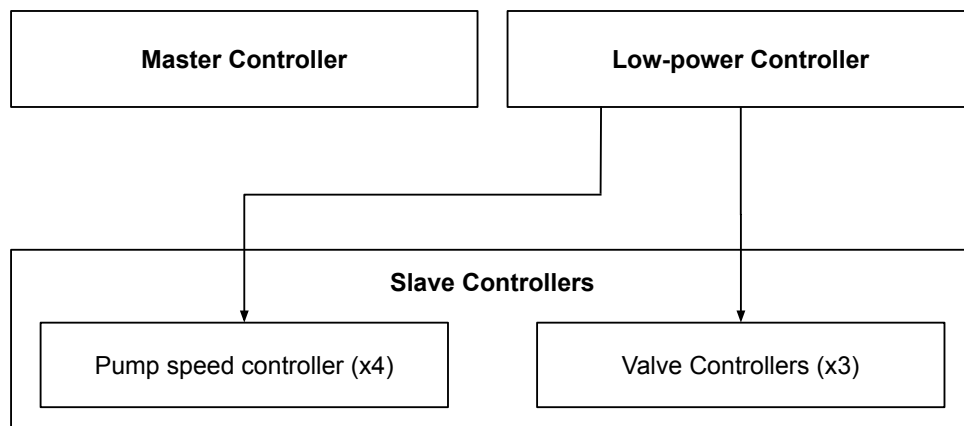
Low power controllers As the name suggests the Low power controller is intended only for the control operations during low-power states of the NPP. This also contains a level controller, a flow controller, and a few slave controllers for the control valves. The Low power controller also contains a differential pressure controller. As indicated in Figure 10, the Low power controller controls the feedwater pumps during Low power operation and also all the valves in the feedwater system during all operational states.

The main components of both the Master controller and the Low power controller are a Level controller and a Flow controller.

Level Controller There are level controllers in the system as parts of the Master controller as well as the Low power controller. The level controller of the Master controller takes four water level measurements inside the reactor pressure vessel using four redundant transducers and the steam flow rate to calculate the actual value of the water level by averaging. However, this measured water level is



(a) During Normal Operations and Scram



(b) During Low-power Operations

Figure 10: Overview of the controller behavior of the feedwater Control system during different operation modes.

different from the actual water level and the deviation from the actual value is calculated based on the steam flow rate. Therefore, in addition, the steam flow rate is taken as another input to the level controller. The output from the level controller is combined with the output from the flow controller to compensate for the steam flow. The set value can be set using a potentiometer in the Master controller. The level controller has a PIP control characteristic. The level controller in of Low power controller also receives the water level inside the reactor pressure vessel and its set point is adjusted programmatically. This level controller also has a PIP characteristic.

Flow Controller The set point for the flow controller is calculated using the total steam flow and the feedwater flow rate in the system. The steam flow is

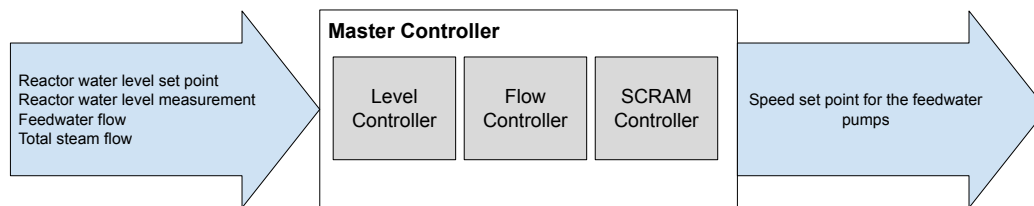


Figure 11: Structure of the Master controller.

calculated by taking the summation of the four steam flow measurements from four transducers. The flow controller takes the measurements of the steam flow and the feedwater flow to create an output signal proportional to the difference between them. This is to change the feedwater flow rapidly based on the changes in the steam flow. The flow controller also has a PIP controller characteristic.

The second level of control in the feedwater control system after the Master controller and the Low power controller are the slave controllers.

Slave Controllers The seven slave controllers in the feedwater control system are for the four feedwater pumps and three control valves. The slave controllers for the feedwater pumps can be operated by either the Master controller or the Low power controller based on the operation conditions of the NPP as shown in Figure 10. However, the slave controllers for the control valves are controlled only by the Low power controller. Despite the controllers available in the feedwater control system, it is also possible to manually control all the pumps and valves if required.

There are two types of slave controllers present in the feedwater control system.

Slave controllers for feedwater pumps The goal of the Pump controller is to maintain the feedwater pump speed at the point provided. The set point for each Pump controller is calculated by averaging the three signals received from the Master controller. Each pump has a tachometer measuring the pump speed and providing feedback to the respective Pump controller. These slave controllers operate independently from each other by maintaining an equal load. There is another tachometer measuring the speed of the electric actuator and providing feedback to the Pump controller. The slave controllers for the feedwater pumps have no redundant units. However, using multiple pumps gives a certain level of redundancy to the system.

Slave controllers for the control valves There are two slave controllers for the two control valves in the feedwater circuit and one slave controller for the control valve in the recirculation circuit. At Low power operation, the control valves are operated by the Low power controller by providing them with a set point. The set points for the valves are calculated by the flow and level controllers in the

Low power controller unit. During Normal operation, the valves are either fully open or fully closed and do not require variable set points.

The two control valves for the feedwater flow are considered as one by the controller. The set point calculated by the controller is then divided by two and applied to both control valves to achieve the total flow.

3.2 Operation

The feedwater control system has three control modes based on the different operational states of the NPP. The three control modes are:

- Normal operation
- Low power operation
- Reactor Scram

The feedwater system control during these three modes is automated. However, When the feedwater flow is below 3 kg/s the feedwater into the reactor is controlled manually by the operator. This is usually during the start-up and shutdown of the reactor.

3.2.1 Valve behavior during Normal operation

In normal operating conditions, the Control valves (V1, V2) and the shutoff valve (V3) in the feedwater circuit are fully open. The recirculation circuit is not used and hence valves V4 and V5 are closed. All the valves are either fully opened or fully closed by the Low power controller.

3.2.2 Valve behavior during Low-power operation

Low-power operation calls for a lower feedwater supply than in Normal operation and the feedwater control system goes into a “low-flow” operation. When either the steam flow or the feedwater flow is below 300 kg/s for about 30 seconds (24% of the full flow), the system goes into Low power operation. The shutoff valve (V3) is closed and the recirculation shutoff valve (V5) is opened. During the Low power operation, the feedwater flow is controlled by varying the level of the two control valves; V1 and V2 from the feedwater circuit and V4 from the recirculation circuit. However, when the feedwater flow into the reactor is decreasing, one target of the Low power operation is to avoid the total feedwater flow being below 200 kg/s by adjusting the recirculation flow. In other words, when the feedwater flow into the reactor falls below 200 kg/s, the total feedwater flow will remain constant at 200 kg/s by varying the recirculation flow.

When the feedwater flow increases and exceeds 350 kg/s for about 30 seconds (28% of the full flow) and the recirculation shutoff valve (V5) is closed and the shutoff valve (V3) is opened again.

3.2.3 Pump behavior

The pump speeds are varied by the Master controller during the Normal operation, to maintain the water level at the desired level inside the reactor pressure vessel. They are controlled by the Low power controller during the Low power operation. This approach with two controllers for different operation modes is required since the feedwater pumps need to be controlled in two different control methods in high feedwater flow and in low feedwater flow.

However, the transition of control of feedwater pumps from the Master controller to the Low power controller can be either Automatic or Manual. In Automatic mode, the controllers handle the transition when the plant operation transfers from the Low power operation to Normal operation. If the operator sets this transfer mode to manual, the feedwater control will remain with the Low power controller, even if the plant operation is in Normal mode until the pumps are manually transferred over to the Master controller by the operator.

3.2.4 Reactor Scram

The feedwater supply during the reactor Scram is also controlled by the Master controller. During a Scram, the reactor power reduces rapidly and consequently, the steam flow also falls down to about 30% of the nominal value in about 2 seconds. At the same time, the water level inside the reactor will also reduce. Under normal circumstances, these situations would drive the feedwater system to pump more water into the system to compensate for the reduction. Since the preheaters are no longer active, the feedwater will have a lower temperature than usual. This heavy flow of colder feedwater flow into the reactor creates thermal transients inside the reactor, and hence this should be handled differently compared to Normal operation.

The Master controller contains a Scram controller that limits the feedwater flow during a Scram, to avoid these thermal transients. In a Scram event, the feedwater flow is reduced to 21% of the full flow in 6s and maintained at that level.

3.2.5 Operator interactions with the system

When the feedwater flow is below 3 kg/s the feedwater into the reactor is controlled manually. The operator can interact and control the system to an extent from the Central control room. However, it is not possible to actuate the Master controller manually from there.

It is possible to manually operate the slave controllers from the central control room through a M/A (Manual/Automatic) unit. This unit allows the switching between manual and automatic operations for the slave controllers and provides indicators for the status. Changing from the automatic mode to the manual mode is easier than changing from manual to automatic since it requires the operator to balance the pumps manually.

During the start-up process of the plant, the feedwater flow and the reactor water level are first controlled by manually controlling the valves and one feedwater pump.

Once the feedwater flow is stable and exceeds 3 kg/s, the valves are moved to Auto mode. When the pressure difference between the reactor and the feedwater pumps is at the desired level, the feedwater pump can be moved to Auto mode. When the feedwater flow increases, the other feedwater pumps will be activated by the Master controller.

Similarly, when the feedwater flow is decreased, the feedwater pumps will shut down one after the other. During a shutdown, when the feedwater flow is decreased and reaches 3kg/s with one feedwater pump in operation, the feedwater system is taken into manual control. The operator decides the next control steps for the valves and the feedwater pump based on the type of shutdown. A Hot shutdown is initiated for service activities that cannot be done with the reactor in operation. Cold shutdown is usually performed for the refueling of the reactor and maintenance work on the primary system.

It is also possible for the operator to manually transfer the control of feedwater pumps to the Master control or remain in the Low power controller based on the requirements.

4 Case Study: Application of STPA on the Feedwater control system

In this chapter, first, the methodology for conducting the STPA is described. Next, the STPA is applied to the feedwater control system, and the results of each STPA step are presented.

4.1 Initial preparations

In this thesis, the system being analyzed is the feedwater control system of the OL1 and OL2 reactors of the Olkiluoto NPP in Finland. This case study was provided by TVO, which is the primary stakeholder in the analysis. The proposed system is the feedwater control system that controls the water level inside the reactor pressure vessel. The documentation regarding the system and its operation was provided by TVO along with guidance to understand the system better. It was evident that this type of study requires expertise in both technical aspects of the system as well as the STPA process. The knowledge and guidance on performing STPA were provided by STPA experts from VTT Technical Research Centre of Finland Ltd (VTT).

Upon receiving the technical documentation from TVO, they were thoroughly studied to understand the overall NPP operation and the feedwater control system structure. It was also important to understand the feedwater control system's role with respect to the complete reactor operation under different conditions. This initial phase of gathering information was a combination of studying technical documents on the feedwater control system, studying STPA, and plenty of discussions to clarify related details. The findings related to the feedwater control system were then documented and presented comprehensively in Chapter 3. Once a better understanding of the system is gained, the next step was to proceed with STPA steps.

4.2 STPA Step 1: Define the purpose of the analysis

Step 1 of the STPA began by identifying the objective of this analysis and the system being analyzed. Discussions were held with the stakeholders of the analysis to understand their interests and goals from the analysis. In this case, they were interested in the nuclear safety aspect, and their goal was to study the safety losses of the system. Hence, the emergent property targeted in this thesis is Safety and the objective of the analysis is to identify scenarios that compromise the system's safety.

To define the system components and the system boundary, the information gathered in the preparation phase was used. A challenge faced when conducting the STPA is isolating the feedwater control system's operation from the rest of the plant's operations. Even though the documentation provides clear system boundaries, in real-world operations the feedwater control system interacts with many other systems in a complex manner, which made it difficult to disregard other systems when conducting the analysis. To overcome this challenge, it was agreed with the stakeholders how

these interactions were handled, in order to make the analysis accurate while making it reasonably simple.

Once the system and the boundary are clearly understood, the next step was to proceed with the identification of system losses and system hazards. The information gathered during the initial stage and discussions with the stakeholders was necessary for this step to identify these losses and hazards.

4.2.1 Identifying Losses

In this stage, system losses that were related to the objective of the analysis were identified. Table 2 shows the identified safety losses of the Feedwater control system. Since the analysis is focusing on the safety losses of the system, the losses that are irrelevant to the safety of the system such as loss of electrical power generation, are disregarded in this analysis.

- L-1 Injuries to humans
- L-2 Exposure to radiation
- L-3 Damages to the plant equipment and components

Table 2: Safety losses in the system.

4.2.2 Identifying System-Level Hazards

Since the feedwater control system is being used to control the water level inside the reactor pressure vessel, the undesired states of the system are mainly related to the water level being at an incorrect level, which could be either too low or too high. Based on that, both cases with too low water levels and too high water levels were studied separately to see if they would lead to any losses.

Discussions to some extent with TVO were required to understand how these two conditions impact the plant operation and how they could lead to losses. The findings were that when the reactor water level falls below the minimum required level, the temperature inside the reactor pressure vessel is not properly regulated within the desired range. The high temperature inside the Reactor pressure vessel causes the fuel rods to melt and settle at the bottom of the vessel leading to the L-3. Also, the high temperature can result in different damages to the containment. These could lead to radioactive material being released into the environment, leading to L-2. Both these instances can lead to injuries to humans, hence L-1.

On the other hand, if the water level exceeds the maximum allowed water level, the water can enter the steam lines, compromising the isolation valves. Having water in the very hot steam lines could rupture the steam lines, allowing leakage of radioactive material. This again leads to all L-1, L-2, and L-3.

Once it was clear that both cases can lead to losses, the system-level hazards were defined as shown in Table 3 along with the loss they can lead to. However, it is understood that all these hazards could lead to any of the losses from Table 2.

Next, the identified hazards are used to derive the system-level constraints as shown in Table 4.

H-1	Reactor Water level falls below the minimum required level	[L-1],[L-2],[L-3]
H-2	Reactor Water level exceeding the maximum allowed level	[L-1],[L-2],[L-3]

Table 3: System-level hazards in the system.

SC-1	Reactor vessel Water level should be maintained above the minimum required level
SC-2	Reactor water level should be maintained below the maximum allowed level

Table 4: System-level constraints.

4.3 STPA Step 2: Model the control structure

The second step of the STPA process is to create the control structure for the selected system. The operation of the feedwater control system was represented in a hierarchical order to create the control structure. The information gathered in the initial stages was again used in this step for generating the control structure. First, an initial control structure was created to show the operations of the feedwater control system as shown in Figure 12.

This initial simple control structure and the operations of the feedwater control system were then used to identify the responsibilities of the main components of the control structure and the findings are shown in Table 5.

Then the control structure was further refined to include all required details regarding the feedwater control system. This was a repetitive and time-consuming task that required a bit of back-and-forth communication, in order to get a final control structure with accurate details. In this step as well, it was agreed on to which level the control structure needs to be refined so that the rest of the STPA steps can rely on its accuracy, meanwhile not over-complicating the diagram with too many details. Once the final version was ready, it was agreed through discussions that it represents the actual system to a satisfactory level and that it can be used in the next steps.

Apart from the horizontal architecture, currently, the STPA guidelines do not provide rules on modeling the control structure. Hence a general tool was used with a few defined colors and patterns that made the diagram clearer to understand. The complete control structure created using Microsoft Visio can be found in Appendix A. This final version includes all the system elements, control actions, feedback signals, and external inputs that are considered in the next steps of this process. Figure 13 shows an extract from the complete control structure that shows the Pump control system in detail.

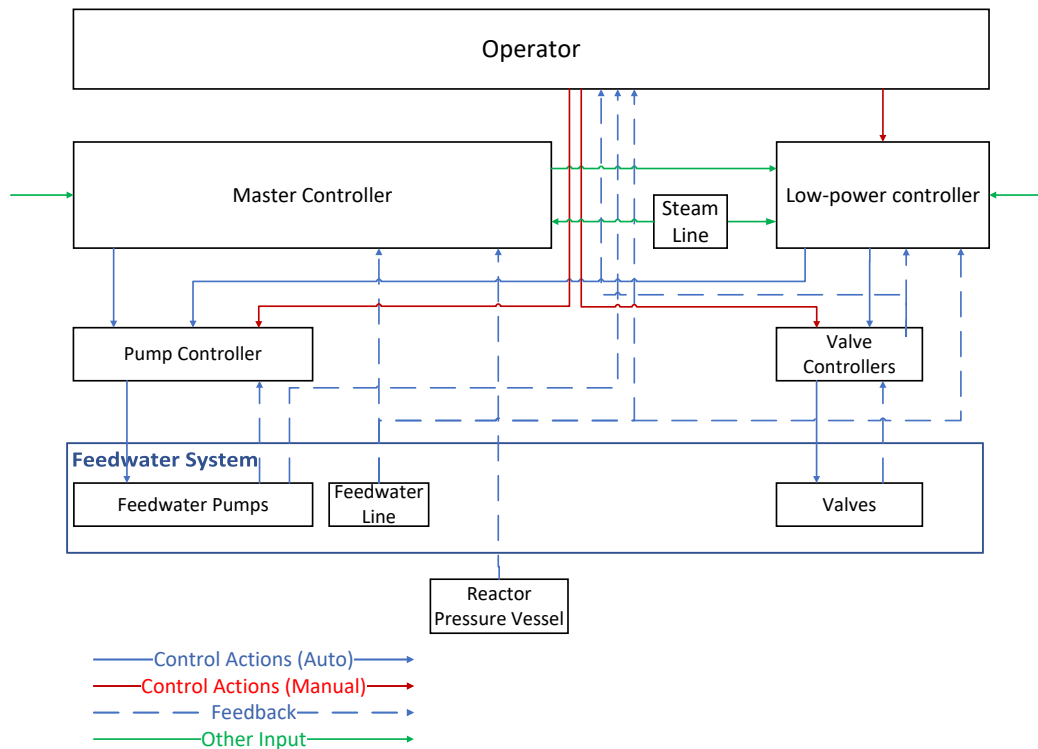


Figure 12: Control structure of the feedwater control system.

4.4 STPA Step 3: Identifying the unsafe control actions

The next step of the STPA is to identify the Unsafe Control Actions (UCA) using the control structure developed in Step 2. As a start, a list was compiled containing all the control actions depicted in the control structure created in Step 2. As an example, Table 6 lists the control actions from Figure 13, their respective origins, and their destinations.

Then this list of control actions was analyzed to see which control actions can lead to UCAs and under which conditions. In summary, a control action might become unsafe and lead to hazards when it is:

- Provided
- Not provided
- Provided, but at the wrong time (too early, too late, or in the wrong order)
- Provided for an inappropriate duration (for too long or for too short)

However, it is important to note that a UCA does not always end up creating a hazard but has the potential to end up creating one or more. Hence, when defining the UCA, the hazards that can occur should also be indicated. Another conflict is that when analyzing existing systems, the current safety constraints in place could avoid UCAs or provide protection against them. In most cases, these safety measures are

Operator

- R-1 Provide reactor water level set points to the Master controller and the Low power controller
- R-2 Manually control the feedwater pumps during the start-up, shutdown, and if required.
- R-3 Manually control the valves during the start-up, shutdown, and if required.

Master controller

- R-4 Monitor water level inside the reactor vessel
- R-5 Calculate pump speed set point based on the reactor water level, feedwater flow, and steam flow during the Normal operation
- R-6 Calculate pump speed set point based on the reactor water level, feedwater flow, and steam flow during a Scram event

Low power controller

- R-7 Calculate pump speed set point based on the reactor water level, feedwater flow, and steam flow during the Low power operation
- R-8 Calculate the required valve position set points during all operational states based on the required feedwater flow
- R-9 Control all shutoff valves based on the operational state of the reactor

Pump controller

- R-10 Adjust the feedwater pump speed to match the set point provided
- R-11 Monitor the actual speed of the feedwater pumps

Valve Controllers - Control Valves

- R-12 Adjust the control valve positions to match the provided valve position set points
- R-13 Monitor the actual positions of the control valves

Valve Controllers - Shutoff Valves

- R-14 Open or Close the shutoff valves to match the input from the Low power controller
- R-15 Monitor the actual states of the shutoff valves

Table 5: Responsibilities of the main components of the control structure.

mostly reactive controls to accidents. STPA perceives safety as a control problem and promotes proactive safety controls that will try to avoid accidents. Also, STPA targets the worst-case scenarios in the system, where the safety systems could fail. Hence, as suggested in the STPA method, the worst-case scenarios are considered and the existing safety measures were disregarded in this analysis.

Once the UCAs were identified and the results were ready, they were presented to the stakeholders. Then the necessary adjustments were done based on their feedback

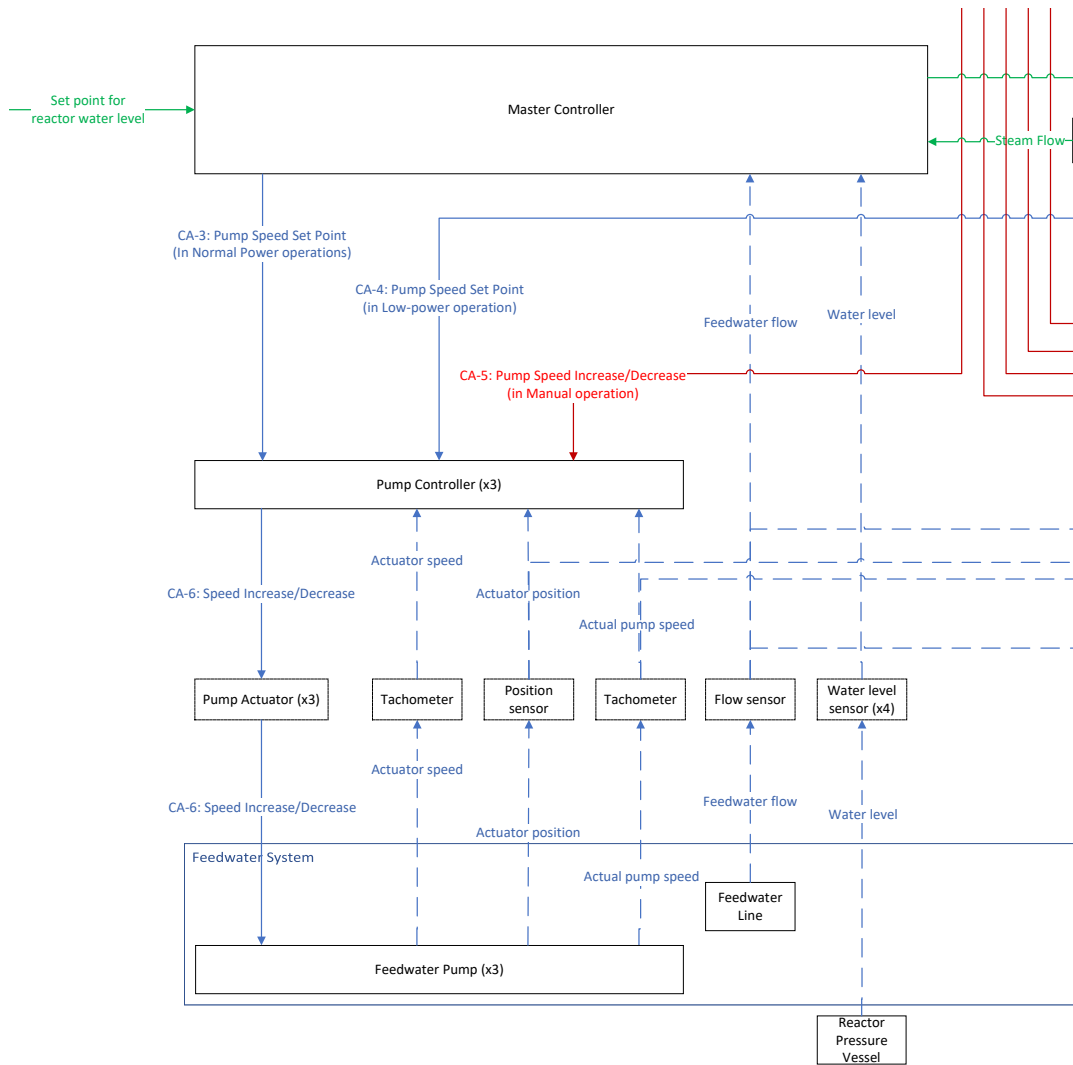


Figure 13: Extract from the control structure: Pump controller.

and agreed that these results can be used in the final step of the STPA. The final result of step 3 consists of 144 UCAs that can originate from 18 control actions. and the complete result is provided in Appendix B.

A few examples based on the control actions from Table 6 will be discussed here as examples.

Let us consider the control action CA-6, where the Speed Increase or decrease signal is sent from the Pump controller to the feedwater pump as mentioned in Table 6. The result of analyzing this control action under the four situations above is listed in Table 7.

The operation of the Pump controller is to receive the speed set point and maintain the speed of the pumps at the set point. The Pump controller takes a few different measurements from the feedwater pumps and their actuators in order to control the speed of the pumps appropriately. Providing the CA-6 can cause hazards in the system

	Control Action	From	To
CA-3	Pump speed set point (In Normal Power operations and Scram events)	Master controller	Pump controller
CA-4	Pump speed set point (in Low power operation)	Low power controller	Pump controller
CA-5	Pump speed increase/decrease (in manual operations)	Operator	Pump controller
CA-6	Speed Increase/Decrease	Pump controller	Feedwater pumps

Table 6: Example: Control Actions.

if the speed of the pumps is increased or decreased when it is not desired to do so. Specifically, if the actual pump speed is at the set point, increasing or decreasing the speed could lead to a hazard. Similarly, not providing the signal to increase the speed when it needs to be increased or not providing the decrease signal when it needs to be decreased can also lead to a hazard. Even if the correct signal is applied to the pump, it can still lead to a hazardous situation, if it is applied at an inappropriate time, too soon, or too late. For example, if the pump speed goes over the set point and the signal to decrease speed is not applied on time, the high speed of the feedwater pump can lead to a hazard. Finally, providing the correct signal for too long or too short a duration could lead to a hazard, such as continuously applying the signal to increase the speed, way past the set point. Under these circumstances, there are 12 Unsafe Control Actions (UCA) identified as shown in Table 7.

Let us consider another example using CA-3, the feedwater pump speed set point sent to the Pump controller from the Master controller. The Master controller's intended operation is to provide a speed set point to the Pump controller during Normal operation and during a Scram event. Therefore, the Master controller providing a set point during low-power operation is undesired and could lead to a hazard. Even during Normal operation or during a Scram event, if the Master controller provides an incorrect set point to the Pump controller, it could cause a hazard. On the other hand, not providing a set point during Normal operation, and during a Scram event could lead to hazards. Even if the set point is provided, if it is not delivered on time to the Pump controller, a hazard can occur, especially during a time-sensitive event such as a Scram. Under these situations, six UCAs were identified related to the CA-3 and they are shown in Table 8.

In addition to the automatic control by the controllers, it is also possible for the operator to control the feedwater pumps manually. CA-5 is the control action of the operator providing the signal to Increase or Decrease the speed of the feedwater pumps. When analyzing this manual control action 12 UCAs were identified as shown in the Table 9. Similarly to the above examples, all four cases can lead to hazards in manual operation as well. One challenge faced in defining UCAs for manual control actions was the difficulty in defining the exact context in which these control actions could become unsafe since the manual operation has a broader range of applications

compared to the automatic control actions from the controllers.

It is important to note that even though the examples related to the pump control function are discussed, similar examples can be provided for the valve control function of the system.

CA-6 Speed Increase/Decrease

Provided	Not provided
UCA-6-1: The Pump controller provides the signal to increase the pump speed when the speed needs to be decreased (when above the set point). [H-2]	UCA-6-5: Pump controller not providing the Increase signal to the pump actuator when speed falls below the set point and needs to be increased. [H-1]
UCA-6-2: The Pump controller provides the signal to decrease the pump speed when the speed needs to be increased (when below the set point). [H-1]	UCA-6-6: Pump controller not providing the Decrease signal to the pump actuator when speed goes above the set point and needs to be decreased. [H-2]
UCA-6-3: The Pump controller provides the signal to increase the pump speed when the speed does not need to be increased (at the set point). [H-2]	
UCA-6-4: The Pump controller provides the signal to decrease the pump speed when the speed does not need to be decreased (at the set point). [H-1]	
Provided at wrong time	Provided for an incorrect duration
UCA-6-7: The Pump controller applies the signal to increase the pump speed too late after the pump speed falls below the set point. [H-1]	UCA-6-9: Pump controller applying the signal to increase pump speed for too long after reaching the set point. [H-2]
UCA-6-8: The Pump controller applies the signal to decrease the pump speed too late after the pump speed goes above the set point. [H-2]	UCA-6-10: Pump controller applying the signal to decrease pump speed for too long after reaching the set point. [H-1]
	UCA-6-11: Pump controller stopping the signal to increase pump speed too soon before reaching the set point. [H-1]
	UCA-6-12: Pump controller stopping the signal to decrease pump speed too soon before reaching the set point. [H-2]

Table 7: Example: Unsafe Control Actions of control action CA-6 - Speed Increase/Decrease from Pump controller to the feedwater pump.

CA-3 Speed set point

Provided	Not provided
UCA-3-1: The master controller provides the pump speed set point to the Pump controller during the Low power operation. [H-1, H-2]	UCA-3-4: Master controller does not provide the pump speed set point to the Pump controller point during Normal operation. [H-1, H-2]
UCA-3-2: The Master controller provides an incorrect pump speed set point to the Pump controller during Normal operation. [H-1, H-2]	UCA-3-5: Master controller does not provide the pump speed set point to the Pump controller point during a Scram event. [H-2]
UCA-3-3: The Master controller provides an incorrect pump speed set point to the Pump controller during a Scram event. [H-2]	
Provided at wrong time	Provided for an incorrect duration
UCA-3-6: The Master controller provides the pump speed set point to the Pump controller too late after a Scram event is initialized. [H-2]	N/A

Table 8: Example: Unsafe Control Actions of control action CA-3 - Pump speed set point from the Master controller to the Pump controller.

CA-5 Pump Speed Increase/Decrease (in Manual operation)

Provided	Not provided
UCA-5-1: The operator increases the pump speed in manual operations when the speed needs to be decreased. [H-2]	UCA-5-5: Operator does not increase the pump speed when the speed needs to be increased. [H-1]
UCA-5-2: The operator increases the pump speed in manual operations when the speed does not need to be changed. [H-2]	UCA-5-6: Operator does not decrease the pump speed when the speed needs to be decreased. [H-2]
UCA-5-3: The operator decreases the pump speed in manual operations when the speed needs to be increased. [H-1]	
UCA-5-4: The operator decreases the pump speed in manual operations when the speed does not need to be changed. [H-1]	
Provided at wrong time	Provided for an incorrect duration
UCA-5-7: The operator increases the pump speed, too late after the speed needs to be increased. [H-1]	UCA-5-9: Operator applying the signal to increase the pump speed, for too long after reaching the desired speed level. [H-2]
UCA-5-8: The operator decreases the pump speed, too late after the speed needs to be decreased. [H-2]	UCA-5-10: Operator applying the signal to decrease the pump speed, for too long after reaching the desired speed level. [H-1]
	UCA-5-11: The operator stops the signal to increase the pump speed too soon, before reaching the desired speed level.[H-1]
	UCA-5-12: The operator stops the signal to decrease the pump speed too soon, before reaching the desired speed level. [H-2]

Table 9: Example: Unsafe Control Actions of control action CA-5 - Pump Speed Increase/Decrease (in Manual operation)

4.5 STPA Step 4: Identifying loss scenarios

The final step of the STPA is to identify loss scenarios for the feedwater control system. As described in Chapter 2, these scenarios will provide the causes that could lead to hazards.

This step of the STPA was the most time-consuming and complex step due to its explorative nature. Following the guidelines provided in the STPA Handbook [5], a classification of scenarios was first created to simplify the identification process. This classification is shown in Figure 6. Next, based on these classifications, two different approaches were defined to systematically identify the two different types of loss scenarios and to avoid missing possible scenarios.

The identification of different possible scenarios in the feedwater control system requires expertise in the system function as well as STPA knowledge. Therefore, a workshop session was conducted as an initiation to the final step of the STPA with the participation of the experts of the nuclear industry with knowledge about the feedwater control system from TVO as well as the experts on using STPA from VTT. During this workshop, a few example scenarios and different possible incidents that could happen in the system were discussed in detail. Issues that can occur in system hardware were also discussed to clearly define the scenarios.

Following the workshop, utilizing the shared knowledge, this final step was completed. The insights and knowledge shared during the workshop provided the basis for continuing the scenario identification, especially when it comes to the physical components of the system. The procedures followed for identifying the different types of scenarios are described next.

4.5.1 Identification of scenarios that leads to UCAs

The first approach was defined to identify the scenarios that could lead to UCAs. The flow of this approach is illustrated in Figure 14. Each identified UCA from the Step 3 was analyzed using this approach to identify scenarios along with the hazard that they can cause.

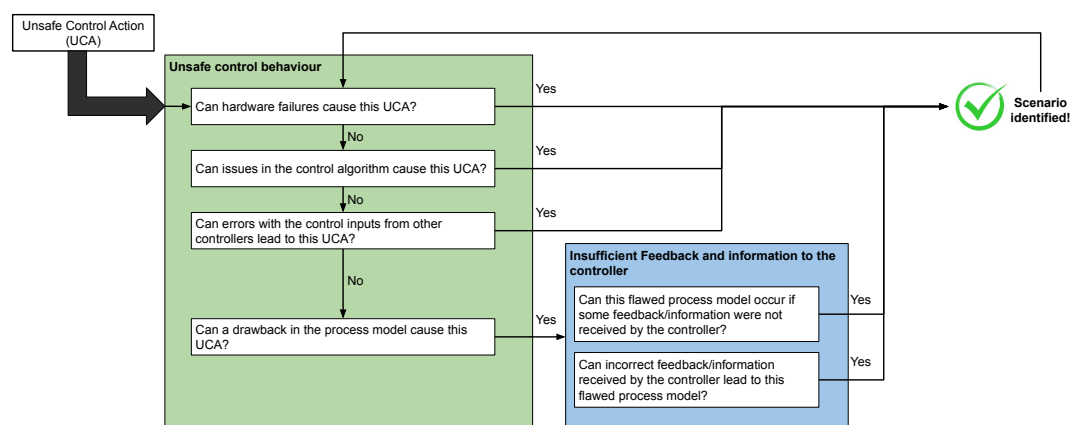


Figure 14: Identification of loss scenarios that lead to UCAs.

It is important to note that there could be more than one scenario leading to a single UCA and also one scenario could lead to more than one UCA. Therefore each UCA needs to be analyzed repetitively to identify all possible scenarios.

As an example, Let us consider the UCA-6-1, which is related to the CA-6 from Table 7. UCA-6-1 is providing the signal to increase the speed of the feedwater pumps when it needs to be decreased. Then using the process shown in Figure 14, scenarios that would lead to the UCA-6-1 can be identified. The scenarios that were identified are listed in Table 10.

CA-6-1 The Pump controller provides the signal to increase the pump speed when the speed needs to be decreased (when above the set point). [H-2]

Scenario	Component
1 The physical Pump controller malfunctions and provides the signal to Increase the speed continuously [UCA-6-1, UCA-6-3, UCA-6-9], causing the pumps to go over the speed set point. As a result, the water level in the reactor may be too high [H-2].	
2 The Pump controller incorrectly believes that the Actual pump speed is lower than the speed set point and increases the speed further [UCA-6-1, UCA-6-3, UCA-6-9]. As a result, the pump speed could go over the set point and the water level in the reactor may be too high [H-2]. This flawed process model can be caused due to the Pump controller receiving incorrect feedback/information regarding the Actual pump speed.	Actual pump speed (Feed-back)
3 The pump controller increases the pump speed incorrectly past the set point due to incorrect feedback [UCA-6-1, UCA-6-3, UCA-6-9]. As a result, the pump speed could go over the set point and the water level in the reactor may be too high [H-2]. This flawed process model can be caused due to: - insufficient Actuator position feedback. - insufficient Actuator speed feedback.	Actuator position (Feedback) Actuator speed (feedback)

Table 10: Example: Scenarios that can lead to UCA-6-1.

Looking at the scenarios where the UCA-6-1 is caused due to controller hardware failure, Scenario 1 can be identified. Scenario 1 is the feedwater pump speed being increased continuously due to a malfunction in the Pump controller. It can be observed that this scenario can lead to not just UCA-6-1, but also to UCA-6-3 and to UCA-6-9. Scenario 2, which belongs to the scenario type with an insufficient process model, describes the Pump controller incorrectly believing that the Actual pump speed is lower than the set point and reacts to increase the speed further. This is because the Pump

controller is a set point controller trying to match the provided speed set point and the actual speed. Scenario 3 also belongs to the same type of scenario with an insufficient process model caused by incorrect feedback on Actuator speed and position. As observed in Table 10, the scenarios are defined along with the system-level hazards they could lead to. Here, Scenario 1 of the UCA-6-1 could lead to H-2, which is the hazard of having too much water in the reactor vessel.

In this type of scenario where the controller has an insufficient model by believing incorrect information, the scenario should be further specified to provide details on why this insufficient process model is created. For instance, in this case, the Pump controller believes an incorrect actual speed which is from the Actual pump speed feedback and it should be analyzed to identify the causes that can make this feedback incorrect. To make the documentation easy and avoid repetition, the feedback elements were analyzed separately. From Table 11 which contains an analysis of feedback signals, it can be observed how insufficient feedback regarding the Actual pump speed, Actuator position, and Actuator speed might be provided to the Pump controller.

One obvious scenario is a failure in the sensor that measures the feedback, which in this case the tachometers and position sensor. Hence, they are analyzed next, to identify the scenarios of how the sensors can cause the feedback to be incorrect or missing. The result of this is presented in Table 12 where the analysis results of the system elements are presented. These scenarios from Tables 10, 11 and 12 together show how the process illustrated in Figure 14 is applied to the identified UCAs.

Let us consider another example that involves a manual operation. UCA-5-9 is derived from the control action CA-5, where the operator increases the feedwater pump speed for too long even after reaching the desired speed level. Analyzing UCA-5-9 using the process from Figure 14 several scenarios were identified as shown in Table 13.

Out of these scenarios, the first one is related to the operation being manual and the operator making a mistake. The second scenario is due to an insufficient process model, or in other words, the operator incorrectly believing something. The operator controls the pump speed with the help of three feedback signals same as the Pump controller. Hence, it is important to identify how those three pieces of feedback can become incorrect or not reach the operator at all. One possibility is a failure in the control panel that indicates the feedback information. However, the feedback signals need to be analyzed further to see how else they can be insufficient. These can be again found in Table 11 where the analysis of feedback signals is presented. Furthermore, the tachometers and the position sensor which are system elements related to these feedback signals, are analyzed and the results are in Table 12.

4.5.2 Identification of scenarios with improper execution of control actions

The other type of scenario shown in Figure 6 is where the correct control action is provided but not executed as expected. To define these scenarios, all identified control actions from the Step 2 were analyzed to recognize the ways these control actions can be improperly executed. This analysis was done following the steps shown in Figure 15. These could be either an issue with the control path or an issue in the

Feedback: Actual pump speed		
	Scenario	Component
1	The Pump controller does not receive the Actual pump speed feedback due to a failure in the speed sensor (tachometer).	Tachometer
2	The Pump controller does not receive the Actual pump speed feedback due to a failure in the connection between the Pump controller and the speed sensor (tachometer).	
3	The sensor provides an invalid or out-of-range input to the Pump controller and the Pump controller fails to recognize that the input is invalid.	
Feedback: Actuator position		
	Scenario	Component
1	The Pump controller does not receive the Actuator position feedback due to a failure in the position sensor.	Position sensor
2	The Pump controller does not receive the Actuator position feedback due to a failure in the connection between the Pump controller and the position sensor.	
3	The position sensor provides an invalid or out-of-range input to the Pump controller and the Pump controller fails to recognize that the input is invalid.	
Feedback: Actuator speed		
	Scenario	Component
1	The Pump controller does not receive the Actuator speed feedback due to a failure in the speed sensor (tachometer).	Tachometer
2	The Pump controller does not receive the Actuator speed feedback due to a failure in the connection between the Pump controller and the speed sensor (tachometer).	
3	The sensor provides an invalid or out-of-range input to the Pump controller and the Pump controller fails to recognize that the input is invalid.	

Table 11: Example: Insufficient feedback/information that can lead to flawed process models.

controlled process.

Let us consider the control action CA-6 as an example. CA-6 is the signal to increase or decrease pump speed that comes from the Pump controller to the feedwater pumps. In this second type of scenario, it is assumed that the control action is correctly issued. By analyzing the CA-6 using the control structure together to identify how this correct control action can result in an undesired outcome, several scenarios can be identified as shown in Table 14. One possibility is that something in the control path between the Pump controller and the feedwater pumps is interfering with the signal

System element: Tachometer	
1	A failure occurs in the physical tachometer.
2	A failure occurs in the power supply to the tachometer.
3	The tachometer is calibrated incorrectly, causing the measurement to be incorrect.
4	The tachometer is unintentionally tampered with during maintenance and repair tasks.
5	The tachometer is misaligned or installed in an inappropriate location.
6	A tachometer of an incorrect model is installed during replacement and goes unnoticed during calibration and tuning.

System element: Position sensor	
1	A failure occurs in the physical position sensor.
2	A failure occurs in the power supply to the position sensor.
3	The position sensor is calibrated incorrectly, causing the measurement to be incorrect.
4	The position sensor is unintentionally tampered with during maintenance and repair tasks.
5	The position sensor is misaligned or installed in an inappropriate location.
6	A position sensor of an incorrect model is installed during replacement and goes unnoticed during calibration and tuning.

Table 12: Example: Analysis of system elements that can lead to insufficient information/feedback

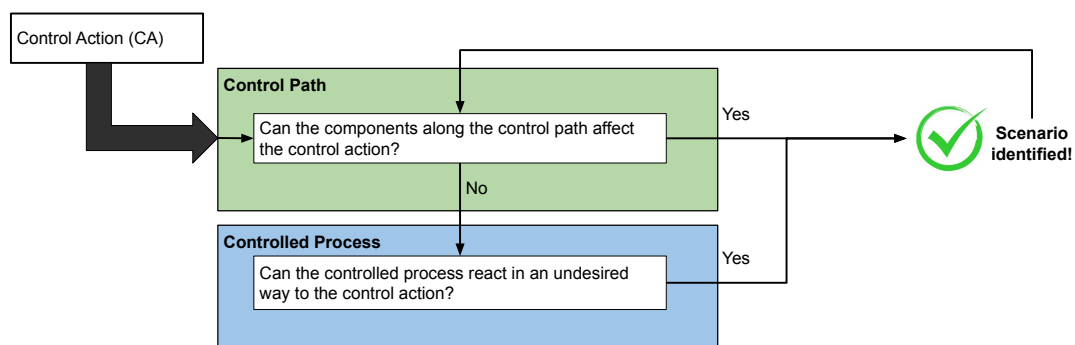


Figure 15: Identification of loss scenarios that interfere with the control actions.

and the first three scenarios in Table 14 relate to this case. The other possibility is that even if the signal reaches the feedwater pumps correctly, the pumps do not respond as expected. The last scenario from Table 14 relates to this case.

Let us consider CA-5, a manual control action where the pump speed is changed by the operator. In this type of scenario, since it is assumed that the issued control action is correct, the identified scenarios do not differ based on whether they are manual or

CA-5-9 The operator applying the signal to increase the pump speed, for too long after reaching the desired speed level. [H-2]

Scenario	Component
1 The pumps are being controlled manually and the operator accidentally applies the signal to increase the pump speed for too long [UCA-5-9], causing the pumps to go beyond the desired speed level. As a result, the reactor water level could be too high [H-2].	
2 The pumps are being controlled manually and the operator applies the signal to increase/decrease the pump speed for an incorrect duration based on insufficient feedback/information [UCA-5-9, UCA-5-10, UCA-5-11, UCA-5-12], causing the pump speed to be different from the desired speed. As a result, the reactor water level could be either too low or too high [H-1, H-2]. This flawed process model can occur due to: <ul style="list-style-type: none"> - insufficient Actual pump speed feedback. - insufficient Actuator position feedback. - insufficient Actuator speed feedback. - a failure in the control panel indicators 	<p>Actual pump speed (Feedback)</p> <p>Actuator position (Feedback)</p> <p>Actuator speed (feedback)</p>

Table 13: Example: Scenarios that can lead to UCA-5-9.

automatic. This can be observed in Table 15.

Finally, at the end of step 4 of the STPA, there were more than 300 possible scenarios identified and the full list can be found in Appendix C.

CA-6 Speed Increase/Decrease

Index	Scenario
1	Pump controller provides the appropriate speed increase/decrease signal to the Feedwater pumps. However, failures in the physical pump actuators cause the pumps to not have the desired speed. As a result, the water level in the reactor may be too low or too high [H-1, H-2].
2	Pump controller provides the appropriate speed increase/decrease signal to the Feedwater pumps. However, failures in the connection between the Pump controller and the Pump actuators cause the Pump actuators to receive an incorrect signal or not receive the signal at all. As a result, the water level in the reactor may be too low or too high [H-1, H-2].
3	Pump controller provides the appropriate speed increase/decrease signal to the Feedwater pumps. However, failures in the mechanical coupling between the Pump actuators and the pumps can cause the pumps to not have the desired speed. As a result, the water level in the reactor may be too low or too high [H-1, H-2].
4	Pump controller provides the appropriate speed increase/decrease signal to the Feedwater pumps. However, one or more feedwater pumps fail. As a result, the water level in the reactor may be too low [H-1].

Table 14: Example: Scenarios related to improper execution of CA-6: Speed increase/decrease.

CA-5 Speed Increase/Decrease (Manual operation)

Index	Scenario
1	The pump speed is controlled manually by the operator. However, it is not received by the Pump controller due to a failure in the connection between the operator and the Pump controller. As a result, the water level in the reactor may be too low or too high [H-1, H-2].
2	The pump speed is controlled manually by the operator. However, it is not sent correctly to the Pump controller due to a failure in the physical control panel. As a result, the water level in the reactor may be too low or too high [H-1, H-2].
3	The pump speed is controlled manually by the operator. However, it is misinterpreted by the Pump controller due to a malfunction in the Pump controller. As a result, the water level in the reactor may be too low or too high [H-1, H-2].
4	The pump speed is controlled manually by the operator. However, it is misinterpreted by the Pump controller due to a software error in the Pump controller. As a result, the water level in the reactor may be too low or too high [H-1, H-2].

Table 15: Example: Scenarios related to improper execution of CA-5: Speed increase/decrease (Manual operation).

5 Discussion and Conclusion

In this thesis, a case study was conducted to evaluate the application of STPA in the I&C systems in the Nuclear domain. Overall, it was clear that the STPA provides a comprehensive result that contains many possible failure scenarios for the feedwater control system in the NPP.

5.1 Application of STPA

The process of understanding the STPA and its application is well-guided in the STPA Handbook [5]. The handbook provides many examples and clear instructions on the application as well as documentation of analysis results.

One objective of the analysis was to study the level of information necessary to perform STPA on a given system. For this case study, the system was defined and the scope was agreed upon in the initial stages of the process. However, some minor details were added based on requirements at several stages. Considering that STPA is an iterative process, it is always possible to refine previous steps as needed. Using finer details about the system, especially when modeling the system using a control structure in STPA step 2, will lead to more detailed results at the end stages of the STPA. While these highly accurate, finer results would be useful in practical applications such as commissioning and consulting, the research projects such as this case study often do not require such fine results. Furthermore, it was also observed that the level of information considered in the study can greatly affect the consumption of resources, especially time. It also could make the analysis more complex for a beginner. Based on these observations, the best course of action would be to agree on the level of information to be used, based on the objective of the study, availability of resources including time, and the expertise of the contributors.

One major challenge highlighted from the beginning of the case study is that the STPA requires both knowledge of STPA fundamentals as well as field knowledge about the system under investigation. In our case, the required support and knowledge were provided by several experts from the nuclear industry. However, for this reason, conducting the STPA as a collaborative task could be more beneficial and efficient rather than being conducted as a one-man job.

In this study, the conducting STPA and the documentation of the results from each step were done using Microsoft Excel, which is a general office tool. This approach was found to be easier for a beginner due to its simplicity and familiarity. Also, the manual approach made it possible to understand how STPA works and clearly see the traceability of its results. During the early stages of the process, freely available tools were also tried to see their behavior and usability. Even though these tools provide support during the STPA process, the accuracy and reliability of the results depend greatly on the user's knowledge of STPA as well as the system being analyzed, which makes it more suitable for users that are more experienced with STPA. Also, their limited customization is another disadvantage.

5.2 Results of the STPA

One important advantage of the STPA results is their traceability from the loss scenarios to the system-level losses. This traceability with the top-down approach made it easier to understand all possible end results of an incident including the worst-case scenario. Looking at the final result of the STPA, and the identified loss scenarios, it can be identified which system-level hazards are reached through a given scenario and how. They also provide more context about the possible incidents such as the conditions they could occur, which is another important advantage of the results. Consider Scenario-197 from Appendix C shown in Table 16 below. Unlike the previous examples, this Scenario is related to the Valve controlling function of the system. From this scenario definition, the reader can understand the context of the loss scenario, the UCAs it can cause, and the hazardous situation it can create.

Scenario-197	The feedwater control valves are being controlled manually and the operator increases the feedwater control valve opening when not desired [UCA-11-1, UCA-11-2], based on incorrect information. As a result, the reactor water level could be too high [H-2]. This flawed process model can occur due to errors in the Actual valve position feedback.
--------------	---

Table 16: Scenario-197.

However, STPA being a qualitative analysis, it could be difficult to filter and prioritize the final results, unlike other quantitative analysis methods such as PRA. Considering these different advantages and disadvantages, the best approach to hazard analysis could be to use a combination of methods.

5.3 Future work

As this thesis is completed under the SEAMLES project funded by the National Nuclear Safety and Waste Management Research Programme 2023-2028 (SAFER2028), the results of this study will be further utilized in the SEAMLES project by VTT Technical Research Centre of Finland Ltd (VTT). One objective of this future research would be to investigate how these results from STPA can be utilized when upgrading the old I&C systems to digital I&C systems in NPPs. This possibly could include research on filtering and prioritization of the final results, considering the parameters such as the probability of events. Also, the results can be utilized in identifying loss scenarios that are not handled by current safety measures in the system. The findings from these could be utilized to make safety design changes and improvements when redesigning and upgrading NPPs.

On the other hand, a future improvement for the STPA process could be to introduce the prioritization of the final results so that the results can be addressed and used in an effective way.

References

- [1] J. C. Knight, “Safety critical systems: challenges and directions,” in *Proceedings of the 24th international conference on software engineering*, pp. 547–550, 2002.
- [2] M. Yastrebenetsky, *Nuclear power plant instrumentation and control systems for safety and security*. IGI Global, 2014.
- [3] *Introduction to Systems Engineering for the Instrumentation and Control of Nuclear Facilities*. No. NR-T-2.14 in Nuclear Energy Series, Vienna: INTERNATIONAL ATOMIC ENERGY AGENCY, 2022.
- [4] C. A. Ericson *et al.*, *Hazard analysis techniques for system safety*. John Wiley & Sons, 2015.
- [5] N. Leveson and J. Thomas, “Stpa handbook - massachusetts institute of technology.”
- [6] T. Ishimatsu, N. G. Leveson, J. Thomas, M. Katahira, Y. Miyamoto, and H. Nakao, “Modeling and hazard analysis using stpa,” 2010.
- [7] J. Bowen, “The ethics of safety-critical systems,” *Commun. ACM*, vol. 43, p. 91–97, apr 2000.
- [8] “Reactor types.” <https://www.tvo.fi/en/index/production/basicinformationaboutnuclearpower/reactortypes.html>. [Accessed 16-May-2023].
- [9] IEA, “World gross electricity production by source, 2019 –charts – data & statistics.”
- [10] “IAEA - country nuclear power profiles 2022 edition - finland.” <https://cnpp.iaea.org/countryprofiles/Finland/Finland.htm>.
- [11] “Cross section.” <https://www.tvo.fi/tuotanto/laitosyksikot/olijaol2/halkileikkaus.html>.
- [12] “Nuclear power plant units Olkiluoto 1 and Olkiluoto 2.” <https://www.tvo.fi/uploads/File/nuclear-power-plant-units.pdf>.
- [13] *Boiling Water Reactor (BWR) Systems*. USNRC Technical Training Center.
- [14] B. Wahlström, “Safety principles and i&c design,” in *9th International Topical Meeting on Nuclear Plant Instrumentation, Control, and Human-Machine Interface Technologies, NPIC and HMIT 2015*, vol. 2, (United States), pp. 1171–1180, American Nuclear Society, 2015. International Topical Meeting on Nuclear Plant Instrumentation, Control, and Human-Machine Interface Technologies, NPIC and HMIT ; Conference date: 22-02-2015 Through 26-02-2015.

- [15] N. R. Council *et al.*, *Digital instrumentation and control systems in nuclear power plants: safety and reliability issues*. National Academies Press, 1997.
- [16] “Safety standards | IAEA — iaea.org.” <https://www.iaea.org/resources/safety-standards>. [Accessed 16-May-2023].
- [17] “Finland - Nuclear Energy Act (990/1987). — ilo.org.” http://www.ilo.org/dyn/natlex/natlex4.detail?p_lang=&p_isn=85507&p_classification=14.01. [Accessed 28-Mar-2023].
- [18] “Nuclear Energy Act 11.12.1987/990 | Regulation | Stuklex — stuklex.fi.” <https://www.stuklex.fi/en/ls/19870990>. [Accessed 16-May-2023].
- [19] “STUK’s duties in the supervision of nuclear safety - stuk-en — stuk.fi.” <https://stuk.fi/en/regulatory-oversight>. [Accessed 16-May-2023].
- [20] “Regulatory Guides on nuclear safety and security (YVL) - stuk-en — stuk.fi.” <https://www.stuklex.fi/en/yvl-ohje>. [Accessed 16-May-2023].
- [21] “STUK participates in the licensing of nuclear facilities - stuk-en — stuk.fi.” <https://www.stuk.fi/web/en/stuk-supervises/nuclear-safety/stuk-participates-in-the-licensing-of-nuclear-facilities>. [Accessed 16-May-2023].
- [22] “Safety principles - stuk-en — stuk.fi.” <https://stuk.fi/en/safety-principles>. [Accessed 16-May-2023].
- [23] M. Stamatelatos, “Probabilistic risk assessment: what is it and why is it worth performing it,” *NASA Office of Safety and Mission Assurance*, vol. 4, no. 05, p. 00, 2000.
- [24] A. Adriaensen, L. Pintelon, F. Costantino, G. D. Gravio, and R. Patriarca, “An stpa safety analysis case study of a collaborative robot application,” *IFAC-PapersOnLine*, vol. 54, no. 1, pp. 534–539, 2021. 17th IFAC Symposium on Information Control Problems in Manufacturing INCOM 2021.
- [25] S. Chiesi, “STPA application for safety assessment of generic missile systems,” pp. 1–7, 01 2016.
- [26] E. Acar Celik, C. Cârlan, A. Abdulkhaleq, F. Bauer, M. Schels, and H. J. Putzer, “Application of stpa for the elicitation of safety requirements for a machine learning-based perception component in automotive,” in *Computer Safety, Reliability, and Security* (M. Trapp, F. Saglietti, M. Spisländer, and F. Bitsch, eds.), (Cham), pp. 319–332, Springer International Publishing, 2022.
- [27] B. Li, S. Shang, and Y. Fu, “The application of stpa in the development of autonomous vehicle functional safety,” in *2021 International Conference on Intelligent Computing, Automation and Applications (ICAA)*, pp. 863–868, 2021.

- [28] M. Chaal, O. Valdez Banda, S. Basnet, J. A. Glomsrud, S. Hirdaris, and P. Kujala, "A framework to model the STPA hierarchical control structure of an autonomous ship," *Safety Science*, vol. Volume 132, p. 15, 2020.
- [29] M. Rejzek and C. Hilbes, "Use of stpa as a diverse analysis method for optimization and design verification of digital instrumentation and control systems in nuclear power plants," *Nuclear Engineering and Design*, vol. 331, pp. 125–135, 2018.
- [30] A. Abdulkhaleq and S. Wagner, "Open tool support for system-theoretic process analysis," 2014.
- [31] Q. Hommes, "Safetyhat a transportation systems safety hazard analysis tool," in *STAMP 2014 Conference at MIT*, 2014.
- [32] S. S. Krauss, M. Rejzek, C. Senn, and C. Hilbes, "Sahra-an integrated software tool for stpa," in *4th European STAMP Workshop, Zurich, 13-15 September 2016*, ZHAW Zürcher Hochschule für Angewandte Wissenschaften, 2016.
- [33] B. G. Liptak, *Flow measurement*. CRC Press, 1993.

A STPA Step 2: Control Structure of the feedwater control system ¹

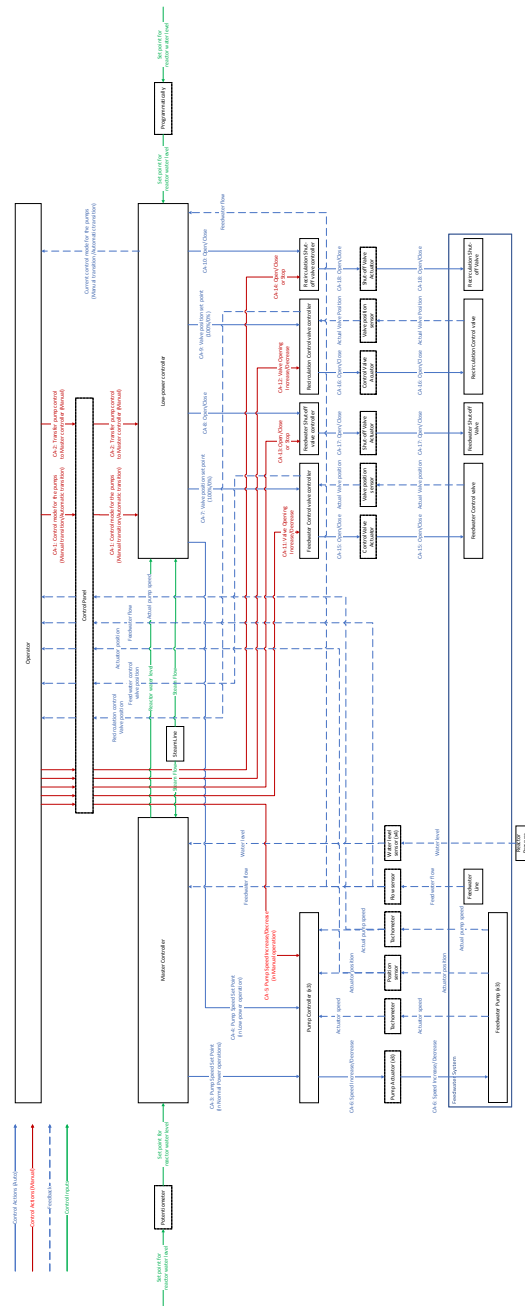


Figure A1: Control structure of the feedwater control system.

¹Refer to the digital version of the thesis for a clear view of drawings and tables.

B STPA Step 3: Identified Unsafe Control Actions ²

	Control action	From	To	Providing causes hazard	Not providing causes hazard	Providing too soon / too late / in wrong order causes hazard	Stopping too soon / applying too long causes hazard
CA-1	Control mode for the pumps (Manual transition/Automatic transition)	Operator	Low-power controller	<p>UCA-1-1: Operator sets the pump transition to Manual when the pumps need to be transitioned Automatically.</p> <p>UCA-1-2: Operator sets the pump transition to Manual when the pumps need to be transitioned Automatically.</p>	<p>UCA-1-3: Operator does not set the control to Low-power controller when the pumps control needs to be changed to the Low-power controller.</p> <p>UCA-1-4: Operator does not set the control to Master controller when the pumps control needs to be changed to the Master controller.</p>	NA	NA
CA-2	Transfer pump control to Master controller (Manual)	Operator	Low-power controller	<p>UCA-2-1: Operator transfers the pump control over to the Master controller when it needs to be controlled by the Low power controller [H-1,H-2].</p>	<p>UCA-2-2: Operator does not change the pump control over to the Master controller when required to do so [H-1,H-2].</p>	<p>UCA-2-3: Operator transfers the pump control over to the Master controller too soon [H-1,H-2].</p> <p>UCA-2-4: Operator transfers the pump control over to the Master controller too late [H-1,H-2].</p>	NA
CA-3	Pump Speed Set point (In Normal Power operations and Scram events)	Master Controller	Pump Controller	<p>UCA-3-1: Master Controller provides the pump speed set point to the Pump controller during the low-power operations. [H-1,H-2]</p> <p>UCA-3-2: Master controller provides an incorrect pump speed set point to the Pump controller during normal operations. [H-1,H-2]</p> <p>UCA-3-3: Master controller provides an incorrect pump speed set point to the Pump controller during a Scram event. [H-2]</p>	<p>UCA-3-4: Master Controller does not provide the pump speed set point to the Pump controller point during the normal operations. [H-1,H-2]</p> <p>UCA-3-5: Master Controller does not provide the pump speed set point to the Pump controller point during a Scram event. [H-2]</p>	<p>UCA-3-6: Master controller provides the pump speed set point to the Pump controller too late after a Scram event is initialized. [H-2]</p>	NA
CA-4	Pump Speed Set point (In Low Power operations)	Low-power controller	Pump Controller	<p>UCA-4-1: Low power Controller provides the pump speed set point to the Pump controller during the normal operations. [H-1,H-2]</p> <p>UCA-4-2: Low power Controller provides the pump speed set point to the Pump controller during a Scram event. [H-1,H-2]</p> <p>UCA-4-3: Low-power controller provides an incorrect pump speed set point to the Pump controller during low-power operations. [H-1,H-2]</p>	<p>UCA-4-4: Low-power Controller does not provide the pump speed set point to the Pump controller during the low-power operations. [H-1,H-2]</p>	<p>UCA-4-5: Low-power controller provides the pump speed set point to the Pump controller too late after Low-power mode is initialized. [H-2]</p>	NA

²Refer to the digital version of the thesis for a clear view of drawings and tables.

CA-5	Pump Speed Increase/Decrease (in Manual operation)	Operator	Pump Controller	<p>UCA-5-1: Operator increases the pump speed in the manual operations when the speed needs to be decreased. [H-2]</p> <p>UCA-5-2: Operator increases the pump speed in the manual operations when the speed does not need to be changes. [H-2]</p> <p>UCA-5-3: Operator decreases the pump speed in the manual operations when the speed needs to be increased. [H-1]</p> <p>UCA-5-4: Operator decreases the pump speed in the manual operations when the speed does not need to be changed. [H-1]</p>	<p>UCA-5-5: Operator does not increase the pump speed when the speed needs to be increased. [H-1]</p> <p>UCA-5-6: Operator does not decrease the pump speed when the speed needs to be decreased. [H-2]</p>	<p>UCA-5-7: Operator increases the pump speed, too late after the speed needs to be increased. [H-1]</p> <p>UCA-5-8: Operator decreases the pump speed, too late after the speed needs to be decreased. [H-2]</p>	<p>UCA-5-9: Operator applying the signal to increase the pump speed, for too long after reaching the desired speed level. [H-2]</p> <p>UCA-5-10: Operator applying the signal to decrease the pump speed, for too long after reaching the desired speed level. [H-1]</p> <p>UCA-5-11: Operator stopping the signal to increase the pump speed too soon, before reaching the desired speed level.[H-1]</p> <p>UCA-5-12: Operator stopping the signal to decrease the pump speed too soon, before reaching the desired speed level. [H-2]</p>
CA-6	Speed Increase/Decrease	Pump Controller	Feedwater pump	<p>UCA-6-1: Pump controller provides the signal to increase the pump speed when speed needs to be decreased (when above the set point). [H-2]</p> <p>UCA-6-2: Pump controller provides the signal to decrease the pump speed when speed needs to be increased (when below the set point). [H-1]</p> <p>UCA-6-3: Pump controller provides the signal to increase the pump speed when speed does not need to be increased (at the set point). [H-2]</p> <p>UCA-6-4: Pump controller provides the signal to decrease the pump speed when speed does not need to be decreased (at the set point). [H-1]</p>	<p>UCA-6-5: Pump controller not providing the Increase signal to the pump actuator when speed falls below the set point and needs to be increased. [H-1]</p> <p>UCA-6-6: Pump controller not providing the Decrease signal to the pump actuator when speed goes above the set point and needs to be decreased. [H-2]</p>	<p>UCA-6-7: Pump controller applying the signal to increase pump speed too late after the pump speed falls below the set point. [H-1]</p> <p>UCA-6-8: Pump controller applying the signal to decrease pump speed too late after the pump speed goes above the set point. [H-2]</p>	<p>UCA-6-9: Pump controller applying the signal to increase pump speed for too long after reaching the set point. [H-2]</p> <p>UCA-6-10: Pump controller applying the signal to decrease pump speed for too long after reaching the set point. [H-1]</p> <p>UCA-6-11: Pump controller stopping the signal to increase pump speed too soon before reaching the set point. [H-1]</p> <p>UCA-6-12: Pump controller stopping the signal to decrease pump speed too soon before reaching the set point. [H-2]</p>
CA-7	Valve Position Set point - Feedwater Control Valve	Low-power controller	Feedwater control valve controller	<p>UCA-7-1: Low power controller provides an incorrect valve position set point to the Feedwater control valve controller during low-power operation. [H-1,H-2]</p> <p>UCA-7-2: Low power controller provides a lower valve position set point (than 100% open) to the Feedwater control valve controller during normal operations. [H-1]</p>	<p>UCA-7-3 Low power controller does not provide the maximum set point (100% open) to the feedwater control valve controller during normal operations. [H-1]</p> <p>UCA-7-4: Low power controller does not provide a valve position set point to the feedwater control valve controller during low-power operations. [H-2]</p>	<p>UCA-7-5: Low-power controller provides a valve position set point to the feed water control valve controller too late after Low-power mode is initialized. [H-2]</p> <p>UCA-7-6: Low-power controller provides the maximum valve position set point (100% open) to the feedwater control valve controller too late after normal operations are initialized. [H-1]</p>	NA
CA-8	Valve position Set point - Recirculation Control Valve	Low-power controller	Recirculation control valve controller	<p>UCA-8-1: Low power controller provides an incorrect valve position set point to the recirculation control valve controller during low-power operation. [H-1,H-2]</p> <p>UCA-8-2: Low power controller provides a higher valve position set point (than 0% open) to the recirculation control valve controller during normal operation. [H-1]</p>	<p>UCA-8-3: Low power controller does not provide the minimum set point (0% open) to the recirculation control valve controller during normal operations. [H-1]</p> <p>UCA-8-4: Low power controller does not provide a valve position set point to the recirculation control valve controller during low-power operations. [H-2]</p>	<p>UCA-8-5: Low-power controller provides a valve position set point to the recirculation control valve controller too late after Low-power mode is initialized. [H-2]</p> <p>UCA-8-6: Low-power controller provides the minimum valve position set point (0% open) to the recirculation control valve controller too late after normal operations are initialized. [H-1]</p>	NA

CA-9	Open/Close - Feedwater Shutoff Valve	Low-power controller	Feedwater shutoff valve controller	<p>UCS-9-1: Low power controller provides Open signal to the feedwater shutoff valve controller during low-power operations. [H-2]</p> <p>UCS-9-2: Low power controller provides Open signal to the feedwater shutoff valve controller after a Scram is initiated. [H-2]</p> <p>UCS-9-3: Low power controller provides Close signal to the feedwater shutoff valve controller during normal operations. [H-1]</p>	<p>UCS-9-4: Low power controller does not provide Open signal to the feedwater shutoff valve controller when entering normal operations. [H-1]</p> <p>UCS-9-5: Low power controller does not provide Close signal to the feedwater shutoff valve controller when entering low-power operations. [H-2]</p>	<p>UCS-9-6: Low power controller provides the Close signal to the feedwater shutoff valve controller too late (>TBD seconds) after entering the low-power operations.[H-2]</p> <p>UCS-9-7: Low power controller provides the Open signal to the feedwater shutoff valve controller too late (>TBD seconds) after entering the normal operations. [H-1]</p>	NA
CA-10	Open/Close - Recirculation Shutoff Valve	Low-power controller	Recirculation shutoff valve controller	<p>UCS-10-1: Low power controller provides Open signal to the recirculation shutoff valve controller during normal operations. [H-1]</p> <p>UCS-10-2: Low power controller provides Close signal to the recirculation shutoff valve controller during low-power operations. [H-2]</p>	<p>UCS-10-3: Low power controller does not provide Open signal to the recirculation shutoff valve controller when entering low-power operations. [H-2]</p> <p>UCS-10-4: Low power controller does not provide Close signal to the recirculation shutoff valve controller when entering normal operations. [H-1]</p>	<p>UCS-10-5: Low power controller provides the Close signal to the recirculation shutoff valve controller too late (>TBD seconds) after entering the normal operations.[H-1]</p> <p>UCS-10-6: Low power controller provides the Open signal to the recirculation shutoff valve controller too late (>TBD seconds) after entering the low-power operations. [H-2]</p>	NA
CA-11	Valve opening Increase/Decrease - Feedwater control valve (Manual Control)	Operator	Feedwater control valve controller	<p>UCA-11-1: Operator increases the feedwater control valve opening when the valve opening needs to be reduced. [H-2]</p> <p>UCA-11-2: Operator increases the feedwater control valve opening when the valve opening does not need to be opened. [H-2]</p> <p>UCA-11-3: Operator decreases the feedwater control valve opening when the valve opening needs to be further opened. [H-1]</p> <p>UCA-11-4: Operator decreases the feedwater control valve opening when the valve opening does not need to be reduced. [H-1]</p>	<p>UCA-11-5: Operator does not increase the feedwater control valve opening when the valve opening needs to be further opened. [H-1]</p> <p>UCA-11-6: Operator does not decrease the feedwater control valve opening when the valve opening needs to be reduced. [H-2]</p>	<p>UCA-11-7: Operator increases the feedwater control valve opening, too late after the valve opening needs to be opened. [H-1]</p> <p>UCA-11-8: Operator decreases the feedwater control valve opening, too late after the valve opening needs to be reduced. [H-2]</p>	<p>UCA-11-9: Operator applying the signal to increase the feedwater control valve opening, for too long after reaching the desired level. [H-2]</p> <p>UCA-11-10: Operator applying the signal to decrease the feedwater control valve opening, for too long after reaching the desired level. [H-1]</p> <p>UCA-11-11: Operator stopping the signal to increase the feedwater control valve opening too soon, before reaching the desired level.[H-1]</p> <p>UCA-11-12: Operator stopping the signal to decrease the feedwater control valve opening too soon, before reaching the desired level. [H-2]</p>

CA-12	Valve opening Increase/Decrease - Recirculation control valve (Manual Control)	Operator	Recirculation control valve controller	<p>UCA-12-1: Operator increases the recirculation control valve opening when the valve opening needs to be reduced. [H-1]</p> <p>UCA-12-2: Operator increases the recirculation control valve opening when the valve opening does not need to be opened. [H-1]</p> <p>UCA-12-3: Operator decreases the recirculation control valve opening when the valve opening needs to be further opened. [H-2]</p> <p>UCA-12-4: Operator decreases the recirculation control valve opening when the valve opening does not need to be reduced. [H-2]</p>	<p>UCA-12-5: Operator does not increase the recirculation control valve opening when the valve opening needs to be further opened. [H-2]</p> <p>UCA-12-6: Operator does not decrease the recirculation control valve opening when the valve opening needs to be reduced. [H-1]</p>	<p>UCA-12-7: Operator increases the recirculation control valve opening, too late after the valve opening needs to be opened. [H-2]</p> <p>UCA-12-8: Operator decreases the recirculation control valve opening, too late after the valve opening needs to be reduced. [H-1]</p>	<p>UCA-12-9: Operator applying the signal to increase the recirculation control valve opening, for too long after reaching the desired level. [H-1]</p> <p>UCA-12-10: Operator applying the signal to decrease the recirculation control valve opening, for too long after reaching the desired level. [H-2]</p> <p>UCA-12-11: Operator stopping the signal to increase the recirculation control valve opening too soon, before reaching the desired level. [H-2]</p> <p>UCA-12-12: Operator stopping the signal to decrease the recirculation control valve opening too soon, before reaching the desired level. [H-1]</p>
CA-13	Open/Close or Stop (Manual control)	Operator	Feedwater shutoff valve controller	<p>UCA-13-1: Operator providing the Open signal to the feedwater shutoff valve, when opening is required. [H-2]</p> <p>UCA-13-2: Operator providing the Close signal to the feedwater shutoff valve, when opening is required. [H-1]</p> <p>UCA-13-3: Operator providing the Stop signal to the feedwater shutoff valve, when not in emergency situations. [H-1,H-2]</p>	<p>UCA-13-4: Operator not providing the Open signal to the feedwater shutoff valve, when opening is required. [H-1]</p> <p>UCA-13-5: Operator not providing the Close signal to the feedwater shutoff valve, when closing is required. [H-2]</p> <p>UCA-13-6: Operator not providing the Stop signal to the feedwater shutoff valve, when stopping is required during an emergency. [H-1,H-2]</p>	<p>UCA-13-7: Operator opens the feedwater shutoff valve, too late after the valve needs to be opened. [H-1]</p> <p>UCA-13-8: Operator closes the feedwater shutoff valve, too late after the valve needs to be closed. [H-2]</p> <p>UCA-13-9: Operator stops the feedwater shutoff valve, too late after an emergency has occurred. [H-1,H-2]</p>	NA
CA-14	Open/Close or Stop (Manual control)	Operator	Recirculation shutoff valve controller	<p>UCA-14-1: Operator providing the Open signal to the recirculation shutoff valve, when closing is required. [H-1]</p> <p>UCA-14-2: Operator providing the Close signal to the recirculation shutoff valve, when opening is required. [H-2]</p> <p>UCA-14-3: Operator providing the Stop signal to the recirculation shutoff valve, when not in emergency situations. [H-1,H-2]</p>	<p>UCA-14-4: Operator not providing the Open signal to the recirculation shutoff valve, when opening is required. [H-2]</p> <p>UCA-14-5: Operator not providing the Close signal to the recirculation shutoff valve, when closing is required. [H-1]</p> <p>UCA-14-6: Operator not providing the Stop signal to the recirculation shutoff valve, when stopping is required during an emergency. [H-1,H-2]</p>	<p>UCA-14-7: Operator opens the recirculation shutoff valve, too late after the valve needs to be opened. [H-2]</p> <p>UCA-14-8: Operator closes the recirculation shutoff valve, too late after the valve needs to be closed. [H-1]</p> <p>UCA-14-9: Operator stops the recirculation shutoff valve, too late after an emergency has occurred. [H-1,H-2]</p>	

CA-15	Open/Close - Feedwater Control Valve	Feedwater control valve controller	Feedwater Control valve	<p>UCA-15-1: Feedwater control valve controller provides the signal to increase the feedwater control valve opening, when valve needs to be closed (when opened above the set point). [H-2]</p> <p>UCA-15-2: Feedwater control valve controller provides the signal to decrease the feedwater control valve opening, when valve needs to be opened (when opened below the set point). [H-1]</p> <p>UCA-15-3: Feedwater control valve controller provides the signal to increase the feedwater control valve opening, when valve does not need to be opened (at the set point). [H-2]</p> <p>UCA-15-4: Feedwater control valve controller provides the signal to decrease the feedwater control valve opening, when valve does not need to be closed (at the set point). [H-1]</p>	<p>UCA-15-5: Feedwater control valve controller not providing the increase signal to the feedwater control valve, when the valve position is below the set point. [H-1]</p> <p>UCA-15-6: Feedwater control valve controller not providing the decrease signal to the feedwater control valve, when the valve position is above the set point. [H-2]</p>	<p>UCA-15-7: Feedwater control valve controller applying the signal to increase the feedwater control valve opening, too late after the valve position falls below the set point. [H-1]</p> <p>UCA-15-8: Feedwater control valve controller applying the signal to decrease the feedwater control valve opening, too late after the pump speed goes above the set point. [H-2]</p>	<p>UCA-15-9: Feedwater control valve controller applying the signal to open the feedwater control valve, for too long after reaching the set point. [H-2]</p> <p>UCA-15-10: Feedwater control valve controller applying the signal to close the feedwater control valve, for too long after reaching the set point. [H-1]</p> <p>UCA-15-11: Feedwater control valve controller stopping the signal to open the feedwater control valve, too soon, before reaching the set point. [H-1]</p> <p>UCA-15-12: Feedwater control valve controller stopping the signal to close the feedwater control valve, too soon, before reaching the set point. [H-2]</p>
CA-16	Open/Close - Recirculation Control Valve	Recirculation control valve controller	Recirculation control valve	<p>UCA-16-1: Recirculation control valve controller provides the signal to increase the recirculation control valve opening, when valve needs to be closed (when opened above the set point). [H-1]</p> <p>UCA-16-2: Recirculation control valve controller provides the signal to decrease the recirculation control valve opening, when valve needs to be opened (when opened below the set point). [H-2]</p> <p>UCA-16-3: Recirculation control valve controller provides the signal to increase the recirculation control valve opening, when valve does not need to be opened (at the set point). [H-1]</p> <p>UCA-16-4: Recirculation control valve controller provides the signal to decrease the recirculation control valve opening, when valve does not need to be closed (at the set point). [H-2]</p>	<p>UCA-16-5: Recirculation control valve controller not providing the increase signal to the recirculation control valve, when the valve position is below the set point. [H-2]</p> <p>UCA-16-6: Recirculation control valve controller not providing the decrease signal to the recirculation control valve, when the valve position is above the set point. [H-1]</p>	<p>UCA-16-7: Recirculation control valve controller applying the signal to increase the recirculation control valve opening, too late after the valve position falls below the set point. [H-2]</p> <p>UCA-16-8: Recirculation control valve controller applying the signal to decrease the recirculation control valve opening, too late after the pump speed goes above the set point. [H-1]</p>	<p>UCA-16-9: Recirculation control valve controller applying the signal to open the recirculation control valve, for too long after reaching the set point. [H-1]</p> <p>UCA-16-10: Recirculation control valve controller applying the signal to close the recirculation control valve, for too long after reaching the set point. [H-2]</p> <p>UCA-16-11: Recirculation control valve controller stopping the signal to open the recirculation control valve, too soon, before reaching the set point. [H-2]</p> <p>UCA-16-12: Recirculation control valve controller stopping the signal to close the recirculation control valve, too soon, before reaching the set point. [H-1]</p>
CA-17	Open/Close - Feedwater Shutoff Valve	Feedwater shutoff valve controller	Feedwater shutoff valve	<p>UCA-17-1: Feedwater shutoff valve controller providing the Open signal to the feedwater shutoff valve, when closing is required. [H-2]</p> <p>UCA-17-2: Feedwater shutoff valve controller providing the Close signal to the feedwater shutoff valve, when opening is required. [H-1]</p>	<p>UCA-17-3: Feedwater shutoff valve controller not providing the Open signal to the feedwater shutoff valve, when opening is required. [H-1]</p> <p>UCA-17-4: Feedwater shutoff valve controller not providing the Close signal to the feedwater shutoff valve, when closing is required. [H-2]</p>	<p>UCA-17-5: Feedwater shutoff valve controller Closes the feedwater shutoff valve too late after the closing is required. [H-2]</p> <p>UCA-17-5: Feedwater shutoff valve controller Opens the feedwater shutoff valve too late after the opening is required. [H-1]</p>	

CA-18	Open/Close - Recirculation Shutoff Valve	Recirculation shutoff valve controller	Recirculation shutoff valve	<p>UCA-18-1: Recirculation shutoff valve controller providing the Open signal to the recirculation shutoff valve, when closing required. [H-1]</p> <p>UCA-18-2: Recirculation shutoff valve controller providing the Close signal to the recirculation shutoff valve, when opening required. [H-2]</p>	<p>UCA-18-3: Recirculation shutoff valve controller not providing the Open signal to the recirculation shutoff valve, when opening required. [H-2]</p> <p>UCA-18-4: Recirculation shutoff valve controller not providing the Close signal to the recirculation shutoff valve, when closing required. [H-1]</p>	<p>UCA-18-7: Recirculation shutoff valve controller Closes the recirculation shutoff valve too late after the closing is required. [H-1]</p> <p>UCA-18-5: Recirculation shutoff valve controller Opens the recirculation shutoff valve too late after the opening is required. [H-2]</p>	
-------	--	--	-----------------------------	--	--	--	--

C STPA Step 4: Identified Loss Scenarios ³

Scenario No.			Associated Feedback/Component
Scenario-1	UCA-1-1	The operator accidentally sets the pump control transfer mode to be Manual, when it should be Automatic [UCA-1-1], causing the pump control transfer to not happen without operator intervention. As a result the water level of the reactor could be either too high or too low [H-1,H-2].	
Scenario-2	UCA-1-2	The operator accidentally sets the pump control transfer mode to be Automatic, when it should be Manual [UCA-1-2], causing the pump control transfer to happen unexpectedly without operator intervention. As a result the water level of the reactor could be either too high or too low [H-1,H-2].	
Scenario-3	UCA-1-1, UCA-1-2	The operator sets the pump control transfer mode to be the wrong option [UCA-1-1,UCA-1-2] following an incorrect procedure, causing the pump control transfer to be unpredictable. As a result the water level of the reactor could be either too high or too low [H-1,H-2]. This flawed process model can be due to: - Operator following an inappropriate procedure mistakenly - the process not being updated accordingly - procedure being updated and not being communicated properly	
Scenario-4	UCA-1-1, UCA-1-2	The operator sets the pump control transfer mode to be the wrong option [UCA-1-1,UCA-1-2] based on incorrect information/feedback, causing the pump control transfer to be unpredictable. As a result the water level of the reactor could be either too high or too low [H-1,H-2]. This flawed process model can be due to insufficient feedback on the Actual pump speed.	Actual pump speed (Feedback)
Scenario-5	UCA-1-1, UCA-1-2	The operator sets the pump control transfer mode to be the wrong option [UCA-1-1,UCA-1-2] based on incorrect information/feedback, causing the pump control transfer to be unpredictable. As a result the water level of the reactor could be either too high or too low [H-1,H-2]. This flawed process model can be due to insufficient feedback on the Actuator position.	Actuator position (Feedback)
Scenario-6	UCA-1-1, UCA-1-2	The operator sets the pump control transfer mode to be the wrong option [UCA-1-1,UCA-1-2] based on incorrect information/feedback, causing the pump control transfer to be unpredictable. As a result the water level of the reactor could be either too high or too low [H-1,H-2]. This flawed process model can be due to insufficient feedback on the Actuator speed.	Actuator speed (Feedback)
Scenario-7	UCA-1-1, UCA-1-2	The operator sets the pump control transfer mode to be the wrong option [UCA-1-1,UCA-1-2] based on incorrect information/feedback, causing the pump control transfer to be unpredictable. As a result the water level of the reactor could be either too high or too low [H-1,H-2]. This flawed process model can be due to insufficient feedback on the Steam flow.	Steam flow (External)
Scenario-8	UCA-1-1, UCA-1-2	The operator sets the pump control transfer mode to be the wrong option [UCA-1-1,UCA-1-2] based on incorrect information/feedback, causing the pump control transfer to be unpredictable. As a result the water level of the reactor could be either too high or too low [H-1,H-2]. This flawed process model can be due to insufficient feedback on the feedwater flow.	Feedwater flow (Feedback)
Scenario-9	UCA-1-3	The operator does not change the pump control transfer mode to Automatic [UCA-1-3], incorrectly believing that the mode is already set to Automatic, causing the pump control transfer to not happen. As a result the water level of the reactor could be either too high or too low [H-1,H-2].	
Scenario-10	UCA-1-4	The operator does not change the pump control transfer mode to Manual [UCA-1-4], incorrectly believing that the mode is already set to Manual, causing the pump control transfer unexpectedly. As a result the water level of the reactor could be either too high or too low [H-1,H-2].	
Scenario-11	UCA-1-3	The operator does not change the pump control transfer mode to Automatic [UCA-1-3], due to insufficient feedback information, causing the pump control transfer to not happen. As a result the water level of the reactor could be either too high or too low [H-1,H-2]. This flawed process model can be due to insufficient feedback on Current control mode of the pumps.	
Scenario-12	UCA-1-4	The operator does not change the pump control transfer mode to Manual [UCA-1-4], due to insufficient feedback information, causing the pump control transfer unexpectedly. As a result the water level of the reactor could be either too high or too low [H-1,H-2]. This flawed process model can be due to insufficient feedback on Current control mode of the pumps.	
Scenario-13	UCA-1-3, UCA-1-4	The operator does not set the pump control transfer mode to the appropriate option [UCA-1-3,UCA-1-4] following an incorrect procedure, causing the pump control transfer to be unpredictable. As a result the water level of the reactor could be either too high or too low [H-1,H-2]. This flawed process model can be due to: - Operator following an inappropriate procedure mistakenly - the process not being updated accordingly - procedure being updated and not being communicated properly	
Scenario-14	UCA-1-3, UCA-1-4	The operator does not set the correct pump control transfer mode [UCA-1-3,UCA-1-4] based on incorrect information/feedback, causing the pump control transfer to be unpredictable. As a result the water level of the reactor could be either too high or too low [H-1,H-2]. This flawed process model can be due to insufficient feedback on the Actual pump speed.	Actual pump speed (Feedback)
Scenario-15	UCA-1-3, UCA-1-4	The operator does not set the correct pump control transfer mode [UCA-1-3,UCA-1-4] based on incorrect information/feedback, causing the pump control transfer to be unpredictable. As a result the water level of the reactor could be either too high or too low [H-1,H-2]. This flawed process model can be due to insufficient feedback on the Actuator position.	Actuator position (Feedback)
Scenario-16	UCA-1-3, UCA-1-4	The operator does not set the correct pump control transfer mode [UCA-1-3,UCA-1-4] based on incorrect information/feedback, causing the pump control transfer to be unpredictable. As a result the water level of the reactor could be either too high or too low [H-1,H-2]. This flawed process model can be due to insufficient feedback on the Actuator speed.	Actuator speed (Feedback)

³Refer to the digital version of the thesis for a clear view of drawings and tables.

Scenario-17	UCA-1-3, UCA-1-4	The operator does not set the correct pump control transfer mode [UCA-1-3,UCA-1-4] based on incorrect information/feedback, causing the pump control transfer to be unpredictable. As a result the water level of the reactor could be either too high or too low [H-1,H-2]. This flawed process model can be due to insufficient feedback on the Steam flow.	Steam flow (External)
Scenario-18	UCA-1-3, UCA-1-4	The operator does not set the correct pump control transfer mode [UCA-1-3,UCA-1-4] based on incorrect information/feedback, causing the pump control transfer to be unpredictable. As a result the water level of the reactor could be either too high or too low [H-1,H-2]. This flawed process model can be due to insufficient feedback on the feedwater flow.	Feedwater flow (Feedback)
Scenario-19	UCA-2-1	The transfer of pump control is set to Manual mode and the operator accidentally transfer the pump control over to the Master controller at an undesired time [UCA-2-1]. This will cause unexpected behavior in the feedwater pumps. As a result the water level of the reactor could be either too high or too low [H-1,H-2].	
Scenario-20	UCA-2-1	The transfer of pump control is set to Manual mode and the operator transfer the pump control over to the Master controller at an undesired time [UCA-2-1], based on incorrect feedback/information due to a failure in the control panel. This will cause unexpected behavior in the feedwater pumps. As a result the water level of the reactor could be either too high or too low [H-1,H-2].	
Scenario-21	UCA-2-1	The transfer of pump control is set to Manual mode and the operator transfer the pump control over to the Master controller at an undesired time [UCA-2-1], based on incorrect feedback/information. This will cause unexpected behavior in the feedwater pumps. As a result the water level of the reactor could be either too high or too low [H-1,H-2]. This flawed process model can be due to insufficient feedback on the Actual pump speed.	Actual pump speed (Feedback)
Scenario-22	UCA-2-1	The transfer of pump control is set to Manual mode and the operator transfer the pump control over to the Master controller at an undesired time [UCA-2-1], based on incorrect feedback/information. This will cause unexpected behavior in the feedwater pumps. As a result the water level of the reactor could be either too high or too low [H-1,H-2]. This flawed process model can be due to insufficient feedback on the Actuator position.	Actuator position (Feedback)
Scenario-23	UCA-2-1	The transfer of pump control is set to Manual mode and the operator transfer the pump control over to the Master controller at an undesired time [UCA-2-2], based on incorrect feedback/information. This will cause unexpected behavior in the feedwater pumps. As a result the water level of the reactor could be either too high or too low [H-1,H-2]. This flawed process model can be due to insufficient feedback on the Actuator speed.	Actuator speed (Feedback)
Scenario-24	UCA-2-2	The transfer of pump control is set to Manual mode and the operator does not transfer the pump control over to the Master controller [UCA-2-2], incorrectly believing that the transfer mode is set to Automatic. This will cause unexpected behavior in the feedwater pumps. As a result the water level of the reactor could be either too high or too low [H-1,H-2]. This flawed process model can be due to insufficient feedback on the current transfer mode due a failure in the control panel.	
Scenario-25	UCA-2-2	The transfer of pump control is set to Manual mode and the operator mistakenly does not transfer the pump control over to the Master controller [UCA-2-2]. This will cause unexpected behavior in the feedwater pumps. As a result the water level of the reactor could be either too high or too low [H-1,H-2].	
Scenario-26	UCA-2-2	The transfer of pump control is set to Manual mode and the operator does not transfer the pump control over to the Master controller when required [UCA-2-2], based on incorrect feedback/information. This will cause unexpected behavior in the feedwater pumps. As a result the water level of the reactor could be either too high or too low [H-1,H-2]. This flawed process model can be due to insufficient feedback on the Actual pump speed.	Actual pump speed (Feedback)
Scenario-27	UCA-2-2	The transfer of pump control is set to Manual mode and the operator does not transfer the pump control over to the Master controller when required [UCA-2-2], based on incorrect feedback/information. This will cause unexpected behavior in the feedwater pumps. As a result the water level of the reactor could be either too high or too low [H-1,H-2]. This flawed process model can be due to insufficient feedback on the Actuator position.	Actuator position (Feedback)
Scenario-28	UCA-2-2	The transfer of pump control is set to Manual mode and the operator does not transfer the pump control over to the Master controller when required [UCA-2-2], based on incorrect feedback/information. This will cause unexpected behavior in the feedwater pumps. As a result the water level of the reactor could be either too high or too low [H-1,H-2]. This flawed process model can be due to insufficient feedback on the Actuator speed.	Actuator speed (Feedback)
Scenario-29	UCA-2-3, UCA-2-4	The transfer of pump control is set to Manual mode and the operator accidentally transfers the pump control over to the Master controller too late or too soon [UCA-2-3,UCA-2-4]. This will cause unexpected behavior in the feedwater pumps. As a result the water level of the reactor could be either too high or too low [H-1,H-2].	
Scenario-30	UCA-2-3, UCA-2-4	The transfer of pump control is set to Manual mode and the operator transfers the pump control over to the Master controller too late or too soon [UCA-2-3,UCA-2-4], based on incorrect feedback/information. This will cause unexpected behavior in the feedwater pumps. As a result the water level of the reactor could be either too high or too low [H-1,H-2]. This flawed process model can be due to a failure in the control panel.	
Scenario-31	UCA-2-3, UCA-2-4	The transfer of pump control is set to Manual mode and the operator transfers the pump control over to the Master controller too late or too soon [UCA-2-3,UCA-2-4], based on incorrect feedback/information. This will cause unexpected behavior in the feedwater pumps. As a result the water level of the reactor could be either too high or too low [H-1,H-2]. This flawed process model can be due to insufficient feedback on the Actual pump speed.	Actual pump speed (Feedback)
Scenario-32	UCA-2-3, UCA-2-4	The transfer of pump control is set to Manual mode and the operator transfers the pump control over to the Master controller too late or too soon [UCA-2-3,UCA-2-4], based on incorrect feedback/information. This will cause unexpected behavior in the feedwater pumps. As a result the water level of the reactor could be either too high or too low [H-1,H-2]. This flawed process model can be due to insufficient feedback on the Actuator position.	Actuator position (Feedback)
Scenario-33	UCA-2-3, UCA-2-4	The transfer of pump control is set to Manual mode and the operator transfers the pump control over to the Master controller too late or too soon [UCA-2-3,UCA-2-4], based on incorrect feedback/information. This will cause unexpected behavior in the feedwater pumps. As a result the water level of the reactor could be either too high or too low [H-1,H-2]. This flawed process model can be due to insufficient feedback on the Actuator speed.	Actuator speed (Feedback)
Scenario-34	UCA-3-1	The reactor operations enter the low-power mode with Automatic transition, but the Master controller incorrectly believes that the operation mode is Normal. This could cause it to provide an inappropriate speed set point to the Pump controller [UCA-3-1], resulting the reactor water level to be either too high or too low [H-1,H-2]. This flawed process model will occur if the received measurement of Feedwater flow is incorrect or not received.	Feedwater flow (Feedback)

Scenario-35	UCA-3-1	The reactor operations enter the low-power mode with Automatic transition, but the Master controller incorrectly believes that the operation mode is Normal. This could cause it to provide an inappropriate speed set point to the Pump controller [UCA-3-1], resulting the reactor water level to be either too high or too low [H-1,H-2]. This flawed process model will occur if an incorrect measurement of steam flow is received or if not received at all.	Steam flow (External)
Scenario-36	UCA-3-2, UCA-3-3	The Master controller calculates the speed set point with incorrect information about the reactor water level, causing the Pump controller to receive an incorrect speed set point during normal operations or a Scram [UCA-3-2, UCA-3-3], resulting the reactor water level to be either too high or too low [H-1,H-2]. This flawed process model will occur if the received measurement of reactor water level is incorrect or not received.	Reactor water level (Feedback)
Scenario-37	UCA-3-2, UCA-3-3	The Master controller calculates the speed set point with incorrect information about feedwater flow, causing the Pump controller to receive an incorrect speed set point during normal operations or a Scram [UCA-3-2, UCA-3-3], resulting the reactor water level to be either too high or too low [H-1,H-2]. This flawed process model will occur if the received measurement of Feedwater flow is incorrect or not received.	Feedwater flow (Feedback)
Scenario-38	UCA-3-2, UCA-3-3	The Master controller calculates the speed set point with incorrect information about steam flow, causing the Pump controller to receive an incorrect speed set point during normal operations or a Scram [UCA-3-2, UCA-3-3], resulting the reactor water level to be either too high or too low [H-1,H-2]. This flawed model could be due to receiving incorrect information about the steam flow from the Steam lines (external to this system).	Steam flow (External)
Scenario-39	UCA-3-2, UCA-3-3	The Master controller calculates the speed set point based on an incorrect Water level set point, causing the Pump controller to receive an incorrect speed set point during normal operations or a Scram [UCA-3-2, UCA-3-3], resulting the reactor water level to be either too high or too low [H-1,H-2]. This flawed process model will occur if the received water level set point is incorrect.	Water level set point (Control Input)
Scenario-40	UCA-3-2	The Scram component in the Master controller malfunctions causing the Master controller recognize a false Scram event, causing the Master controller to provide an incorrect speed set point to the Pump controller during normal operations [UCA-3-2], resulting in too little water in the reactor during a Scram [H-1].	
Scenario-41	UCA-3-3	The Scram component in the Master controller fails causing the Master controller to not recognize a Scram event, causing the Master controller to provide an incorrect speed set point to the Pump controller [UCA-3-3], resulting in too high water level in the reactor during a Scram [H-2].	
Scenario-42	UCA-3-4, UCA-3-5	One or more hardware components fail in the Master controller when the reactor is operational, causing it to not provide the pump speed set point to the Pump controller [UCA-3-4,UCA-3-5]. As a result, the reactor water level could be either too high or too low [H-1,H-2]	
Scenario-43	UCA-3-4	The reactor operations enter the normal mode with Automatic transition, but the Master controller incorrectly believes that the operation mode is still Low-power. This could cause it to not provide a speed set point to the Pump controller during normal operation [UCA-3-4], resulting the reactor water level to be either too high or too low [H-1,H-2]. This flawed process model will occur if the received measurement of Feedwater flow is incorrect or not received.	
Scenario-44	UCA-3-6	The Master controller recognizes the Scram in the system but the Pump speed set point is provided too late [UCA-3-6] to the Pump controller due to processing delays in the Master controller. As a result, the reactor water level could be too high [H-2].	
Scenario-45	UCA-4-1	The reactor operations enter the normal mode with Automatic transition, but the Low-power controller incorrectly believes that the operation mode is Low-power. This could cause it to control the pumps during Normal operation and not transfer over to the Master controller [UCA-4-1], resulting the reactor water level to be either too high or too low [H-1,H-2]. This flawed process model will occur if the received measurement of Feedwater flow is incorrect or not received.	Feedwater flow (Feedback)
Scenario-46	UCA-4-1	The reactor operations enter the normal mode with Automatic transition, but the Low-power controller incorrectly believes that the operation mode is Low-power. This could cause it to control the pumps during Normal operation and not transfer over to the Master controller [UCA-4-1], resulting the reactor water level to be either too high or too low [H-1,H-2]. This flawed process model will occur if the received measurement of Steam flow is incorrect or not received.	Steam flow (External)
Scenario-47	UCA-4-1	The reactor operations enter the normal mode with Automatic transition, but the Low-power controller does not transfer the pump controlling to the Master controller, incorrectly believing that the Manual transition selected [UCA-4-1], resulting the reactor water level to be either too high or too low [H-1,H-2]. This flawed process model will occur if the received feedback Control mode of the pumps is incorrect or not received.	
Scenario-48	UCA-4-3	The Low-power controller calculates the speed set point with an incorrect reactor water level measurement received from the Master controller, causing the Pump controller to receive an incorrect speed set point during low-power operation [UCA-4-3], resulting the reactor water level to be either too high or too low [H-1,H-2]. This flawed process model can occur due to: - incorrect information being sent by the Master controller - the interference on connection between the Master controller and the Low-power controller	
Scenario-49	UCA-4-3	The Low-power controller calculates the speed set point with incorrect information about feedwater flow, causing the Pump controller to receive an incorrect speed set point during low-power operations [UCA-4-3], resulting the reactor water level to be either too high or too low [H-1,H-2]. This flawed process model will occur if the received measurement of Feedwater flow is incorrect or not received.	Feedwater flow (Feedback)
Scenario-50	UCA-4-3	The Low-power controller calculates the speed set point with incorrect information about steam flow, causing the Pump controller to receive an incorrect speed set point during low-power operations [UCA-4-3], resulting the reactor water level to be either too high or too low [H-1,H-2]. This flawed model could be due to receiving incorrect information about the steam flow from the Steam lines (external to this system).	Steam flow (External)
Scenario-51	UCA-4-4	One or more hardware components fail in the Low-power controller when the reactor is operational, causing it to not provide the pump speed set point to the Pump controller [UCA-4-4]. As a result, the reactor water level could be either too high or too low [H-1,H-2].	
Scenario-52	UCA-4-4	The reactor operations enter the Low-power mode but the Low-power controller incorrectly believes that the operation mode is still the Normal mode. This could cause it to not provide a speed set point to the Pump controller during Low-power operation [UCA-4-4], resulting the reactor water level to be either too high or too low [H-1,H-2]. This flawed process model will occur if the received measurement of Feedwater flow is incorrect or not received.	Feedwater flow (Feedback)

Scenario-53	UCA-4-4	The reactor operations enter the Low-power mode but the Low-power controller incorrectly believes that the operation mode is still the Normal mode. This could cause it to not provide a speed set point to the Pump controller during Low-power operation [UCA-4-4], resulting the reactor water level to be either too high or too low [H-1,H-2]. This flawed process model will occur if the received measurement of Steam flow is incorrect or not received.	Steam flow (External)
Scenario-54	UCA-4-5	The Low-power controller starts the low-power operation but the Pump speed set point is provided too late [UCA-4-5] to the Pump controller due to processing delays in the Low-power controller. As a result, the reactor water level could be too high[H-2].	
Scenario-55	UCA-5-1	The pumps are being operated manually and the operator accidentally increases the pump speed, when the speed needs to be decreased [UCA-5-1]. As a result the reactor water level could become too high [H-2].	
Scenario-56	UCA-5-2	The pumps are being operated manually and the operator accidentally increases the pump speed, when changing the speed is not required [UCA-5-2]. As a result the reactor water level could become too high [H-2].	
Scenario-57	UCA-5-3	The pumps are being operated manually and the operator accidentally decreases the pump speed, when the speed needs to be increased [UCA-5-3]. As a result the reactor water level could become too low [H-1].	
Scenario-58	UCA-5-4	The pumps are being operated manually and the operator accidentally decreases the pump speed, when changing the speed is not required [UCA-5-4]. As a result the reactor water level could become too low [H-1].	
Scenario-59	UCA-5-1, UCA-5-2	The pumps are being controlled manually and the operator increases the pump speed when not desired [UCA-5-1,UCA-5-2], based on an incorrect information on actual pump speed. As a result the reactor water level could be too high [H-2]. This flawed process model can occur due to the errors in the Actual pump speed feedback.	Actual pump speed (Feedback)
Scenario-60	UCA-5-1, UCA-5-2	The pumps are being controlled manually and the operator increases the pump speed when not desired [UCA-5-1,UCA-5-2], based on an incorrect information on actuator position. As a result the reactor water level could be too high [H-2]. This flawed process model can occur due to the errors in the Actuator position feedback.	Actuator position (Feedback)
Scenario-61	UCA-5-1, UCA-5-2	The pumps are being controlled manually and the operator increases the pump speed when not desired [UCA-5-1,UCA-5-2], based on an incorrect information on actuator speed. As a result the reactor water level could be too high [H-2]. This flawed process model can occur due to the errors in the Actuator speed feedback.	Actuator speed (Feedback)
Scenario-62	UCA-5-1, UCA-5-2	The pumps are being controlled manually and the operator increases the pump speed when not desired [UCA-5-1,UCA-5-2], following an incorrect procedure. As a result the reactor water level could be too high [H-2]. This flawed process model can occur due: - Operator following an inappropriate procedure mistakenly - the process not being updated accordingly - procedure being updated and not being communicated properly	
Scenario-63	UCA-5-1, UCA-5-2	The pumps are being controlled manually and due to a failure in the physical control panel, the control panel indicates the received feedback/information incorrectly. This causes the operator to increase the pump speed when not required [UCA-5-1,UCA-5-2] resulting the reactor water level to be too high [H-2].	
Scenario-64	UCA-5-3, UCA-5-4	The pumps are being controlled manually and the operator decreases the pump speed when not desired [UCA-5-3,UCA-5-4], based on an incorrect information on actual pump speed. As a result the reactor water level could be too low [H-1]. This flawed process model can occur due to the errors in the Actual pump speed feedback.	Actual pump speed (Feedback)
Scenario-65	UCA-5-3, UCA-5-4	The pumps are being controlled manually and the operator decreases the pump speed when not desired [UCA-5-3,UCA-5-4], based on an incorrect information on the actuator position. As a result the reactor water level could be too low [H-1]. This flawed process model can occur due to the errors in the Actuator position feedback.	Actuator position (Feedback)
Scenario-66	UCA-5-3, UCA-5-4	The pumps are being controlled manually and the operator decreases the pump speed when not desired [UCA-5-3,UCA-5-4], based on an incorrect information on the actuator speed. As a result the reactor water level could be too low [H-1]. This flawed process model can occur due to the errors in the Actuator speed feedback.	Actuator speed (Feedback)
Scenario-67	UCA-5-3, UCA-5-4	The pumps are being controlled manually and the operator decreases the pump speed when not desired [UCA-5-3,UCA-5-4], following an incorrect procedure. As a result the reactor water level could be too low [H-1]. This flawed process model can occur due: - Operator following an inappropriate procedure mistakenly - the process not being updated accordingly - procedure being updated and not being communicated properly	
Scenario-68	UCA-5-3, UCA-5-4	The pumps are being controlled manually and due to a failure in the physical control panel, the control panel indicates the received feedback/information incorrectly. This causes the operator to decrease the pump speed when not required [UCA-5-3,UCA-5-4] resulting the reactor water level to be too low [H-1].	
Scenario-69	UCA-5-5, UCA-5-6	The pumps are being operated manually and the operator accidentally stops responding to the pump speed controlling [UCA-5-5,UCA-5-6]. As a result the reactor water level could become either too high or too low [H-1,H-2].	
Scenario-70	UCA-5-5, UCA-5-6	The pumps are being controlled manually and the operator does not change the pump speed as expected [UCA-5-3], based on an incorrect information on actual pump speed. As a result the reactor water level could be either too high or too low [H-1,H-2]. This flawed process model can occur due to the errors in the Actual pump speed feedback.	Actual pump speed (Feedback)
Scenario-71	UCA-5-5, UCA-5-6	The pumps are being controlled manually and the operator does not change the pump speed as expected [UCA-5-3], based on an incorrect information on actuator position. As a result the reactor water level could be either too high or too low [H-1,H-2]. This flawed process model can occur due to the errors in the Actuator position feedback.	Actuator position (Feedback)

Scenario-72	UCA-5-5, UCA-5-6	The pumps are being controlled manually and the operator does not change the pump speed as expected [UCA-5-3], based on an incorrect information on actuator speed. As a result the reactor water level could be either too high or too low [H-1,H-2]. This flawed process model can occur due to the errors in the Actuator speed feedback.	Actuator speed (feedback)
Scenario-73	UCA-5-5, UCA-5-6	The pumps are being controlled manually and the operator does not change the pump speed as expected [UCA-5-3], following an incorrect procedure. As a result the reactor water level could be either too high or too low [H-1,H-2]. This flawed process model can occur due: - Operator following an inappropriate procedure mistakenly - the process not being updated accordingly - procedure being updated and not being communicated properly	
Scenario-74	UCA-5-5, UCA-5-6	The pumps are being controlled manually and due to a failure in the physical control panel, the control panel indicates the received feedback/information incorrectly. This causes the operator to not control the pump speed appropriately [UCA-5-5,UCA-5-6] resulting the reactor water level to be either too low or too high [H-1,H-2].	
Scenario-75	UCA-5-5, UCA-5-6	The pumps are being controlled manually but the operator incorrectly believes that the pumps are set to automatic control. This causes the operator to not control the pump speed appropriately [UCA-5-5,UCA-5-6] resulting the reactor water level to be either too low or too high [H-1,H-2].	
Scenario-76	UCA-5-7	The pumps are being controlled manually and the operator increases the pump speed too late [UCA-5-7], due to delays of the operators actions. As a result the reactor water level could be too low [H-1].	
Scenario-77	UCA-5-7	The pumps are being controlled manually and the operator increases the pump speed too late [UCA-5-7], due to delay of receiving feedback/information. As a result the reactor water level could be too low [H-1]. This flawed process model can occur due to the delays in the Actual pump speed feedback.	
Scenario-78	UCA-5-7	The pumps are being controlled manually and the operator increases the pump speed too late [UCA-5-7], due to delay of receiving feedback/information. As a result the reactor water level could be too low [H-1]. This flawed process model can occur due to the delays in the Actuator position feedback.	
Scenario-79	UCA-5-7	The pumps are being controlled manually and the operator increases the pump speed too late [UCA-5-7], due to delay of receiving feedback/information. As a result the reactor water level could be too low [H-1]. This flawed process model can occur due to the delays in the Actuator speed feedback.	
Scenario-80	UCA-5-7	The pumps are being controlled manually and the operator increases the pump speed too late [UCA-5-7], due to delay of receiving feedback/information. As a result the reactor water level could be too low [H-1]. This flawed process model can occur due to the delays in the Control panel indicators.	
Scenario-81	UCA-5-8	The pumps are being controlled manually and the operator decreases the pump speed too late [UCA-5-8], due to delays of the operators actions. As a result the reactor water level could be too high [H-2].	
Scenario-82	UCA-5-8	The pumps are being controlled manually and the operator decreased the pump speed too late [UCA-5-8], due to delay of receiving feedback/information. As a result the reactor water level could be too high [H-2]. This flawed process model can occur due to the delays in the Actual pump speed feedback.	
Scenario-83	UCA-5-8	The pumps are being controlled manually and the operator decreased the pump speed too late [UCA-5-8], due to delay of receiving feedback/information. As a result the reactor water level could be too high [H-2]. This flawed process model can occur due to the delays in the Actuator position feedback.	
Scenario-84	UCA-5-8	The pumps are being controlled manually and the operator decreased the pump speed too late [UCA-5-8], due to delay of receiving feedback/information. As a result the reactor water level could be too high [H-2]. This flawed process model can occur due to the delays in the Actuator speed feedback.	
Scenario-85	UCA-5-8	The pumps are being controlled manually and the operator decreased the pump speed too late [UCA-5-8], due to delay of receiving feedback/information. As a result the reactor water level could be too high [H-2]. This flawed process model can occur due to the delays in the Control panel indicators.	
Scenario-86	UCA-5-9	The pumps are being controlled manually and the operator accidentally applies the signal to increase the pump speed for too long [UCA-5-9], causing the pumps to go beyond the desired speed level. As a result the reactor water level could be too high [H-2].	
Scenario-87	UCA-5-10	The pumps are being controlled manually and the operator accidentally applies the signal to decrease the pump speed for too long [UCA-5-10], causing the pumps to fall below the desired speed level. As a result the reactor water level could be too low [H-1].	
Scenario-88	UCA-5-11	The pumps are being controlled manually and the operator accidentally stops the signal to increase the pump speed for too soon [UCA-5-11], causing the pumps to not reach the desired speed level. As a result the reactor water level could be too low [H-1].	
Scenario-89	UCA-5-12	The pumps are being controlled manually and the operator accidentally stops the signal to decrease the pump speed for too soon [UCA-5-12], causing the pumps to not reach the desired speed level. As a result the reactor water level could be too high [H-2].	
Scenario-90	UCA-5-9, UCA-510, UCA-5-11, UCA-5-12	The pumps are being controlled manually and the operator applies the signal to increase/decrease the pump speed for an incorrect duration based on insufficient feedback/information [UCA-5-9,UCA-5-10,UCA-5-11,UCA-5-12], causing the pump speed to be different from the desired speed. As a result the reactor water level could be either too low or too high [H-1,H-2]. This flawed process model can occur due to insufficient Actual pump speed feedback.	Actual pump speed (Feedback)
Scenario-91	UCA-5-9, UCA-510, UCA-5-11, UCA-5-12	The pumps are being controlled manually and the operator applies the signal to increase/decrease the pump speed for an incorrect duration based on insufficient feedback/information [UCA-5-9,UCA-5-10,UCA-5-11,UCA-5-12], causing the pump speed to be different from the desired speed. As a result the reactor water level could be either too low or too high [H-1,H-2]. This flawed process model can occur due to insufficient Actuator position feedback.	Actuator position (Feedback)
Scenario-92	UCA-5-9, UCA-510, UCA-5-11, UCA-5-12	The pumps are being controlled manually and the operator applies the signal to increase/decrease the pump speed for an incorrect duration based on insufficient feedback/information [UCA-5-9,UCA-5-10,UCA-5-11,UCA-5-12], causing the pump speed to be different from the desired speed. As a result the reactor water level could be either too low or too high [H-1,H-2]. This flawed process model can occur due to insufficient Actuator speed feedback.	Actuator speed (Feedback)
Scenario-93	UCA-5-9, UCA-510, UCA-5-11, UCA-5-12	The pumps are being controlled manually and the operator applies the signal to increase/decrease the pump speed for an incorrect duration based on insufficient feedback/information due to a failure in the control panel [UCA-5-9,UCA-5-10,UCA-5-11,UCA-5-12], causing the pump speed to be different from the desired speed. As a result the reactor water level could be either too low or too high [H-1,H-2].	

Scenario-94	UCA-6-1, UCA-6-3, UCA-6-9	The physical pump controller malfunctions and provides the signal to Increase the speed continuously [UCA-6-1, UCA-6-3, UCA-6-9], causing the pumps to go over the speed set point. As a result the water level in the reactor may be too high [H-2].	
Scenario-95	UCA-6-2, UCA-6-4, UCA-6-10	The physical pump controller malfunctions and provides the signal to decrease the speed continuously [UCA-6-2, UCA-6-4, UCA-6-10], causing the pumps to go below the speed set point. As a result the water level in the reactor may be too low [H-1].	
Scenario-96	UCA-6-1, UCA-6-3, UCA-6-9	The pump controller incorrectly believes that the Actual pump speed is lower than the speed set point and increases the speed further [UCA-6-1,UCA-6-3,UCA-6-9]. As a result the pump speed could go over the set point and the water level in the reactor may be too high [H-2]. This flawed process model can be caused due to the pump controller receiving incorrect feedback/information regarding the Actual pump speed.	Actual pump speed (Feedback)
Scenario-97	UCA-6-1, UCA-6-3, UCA-6-9	The pump controller increases the pump speed incorrectly past the set point due to incorrect feedback received on Actuator speed [UCA-6-1,UCA-6-3,UCA-6-9]. As a result the pump speed could go over the set point and the water level in the reactor may be too high [H-2]. This flawed process model can be caused due to the pump controller receiving incorrect feedback/information regarding the Actuator speed.	Actuator speed (Feedback)
Scenario-98	UCA-6-1, UCA-6-3, UCA-6-9	The pump controller increases the pump speed incorrectly past the set point due to incorrect feedback received on Actuator position [UCA-6-1,UCA-6-3,UCA-6-9]. As a result the pump speed could go over the set point and the water level in the reactor may be too high [H-2]. This flawed process model can be caused due to the pump controller receiving incorrect feedback/information regarding the Actuator position.	Actuator position (Feedback)
Scenario-99	UCA-6-2, UCA-6-4, UCA-6-10	The pump controller incorrectly believes that the Actual pump speed is higher than the speed set point and decreases the speed further [UCA-6-2,UCA-6-4,UCA-6-10]. As a result the pump speed could go below the set point and the water level in the reactor may be too low [H-1]. This flawed process model can be caused due to the pump controller receiving incorrect feedback/information regarding the Actual pump speed.	Actual pump speed (Feedback)
Scenario-100	UCA-6-2, UCA-6-4, UCA-6-10	The pump controller decreases the pump speed incorrectly past the set point due to incorrect feedback received on Actuator speed [UCA-6-2,UCA-6-4,UCA-6-10]. As a result the pump speed could go below the set point and the water level in the reactor may be too low [H-1]. This flawed process model can be caused due to the pump controller receiving incorrect feedback/information regarding the Actuator speed.	Actuator speed (Feedback)
Scenario-101	UCA-6-2, UCA-6-4, UCA-6-10	The pump controller decreases the pump speed incorrectly past the set point due to incorrect feedback received on Actuator position [UCA-6-2,UCA-6-4,UCA-6-10]. As a result the pump speed could go below the set point and the water level in the reactor may be too low [H-1]. This flawed process model can be caused due to the pump controller receiving incorrect feedback/information regarding the Actuator position.	Actuator position (Feedback)
Scenario-102	UCA-6-5	The physical pump controller fails during the operations and does not provide the increase signal to the feedwater pumps when the actual pump speed falls below the set point [UCA-6-5]. As a result the reactor water level may be too low [H-1].	
Scenario-103	UCA-6-6	The physical pump controller fails during the operations and does not provide the decrease signal to the feedwater pumps when the actual pump speed goes above the set point [UCA-6-6]. As a result the reactor water level may be too high [H-2].	
Scenario-104	UCA-6-5	The pump controller incorrectly believes that the actual pump speed is at the set point and does not provide the speed increase signal to the pumps when the pumps speed falls below the set point (speed needs to be increased). As a result the reactor water level may become too low [H-1]. This flawed process model can be caused due to the pump controller receiving incorrect feedback/information regarding the Actual pump speed.	Actual pump speed (Feedback)
Scenario-105	UCA-6-6	The pump controller incorrectly believes that the actual pump speed is at the set point and does not provide the speed decrease signal to the pumps when the pumps speed goes above the set point (speed needs to be decreased). As a result the reactor water level may become too high [H-2]. This flawed process model can be caused due to the pump controller receiving incorrect feedback/information regarding the Actual pump speed.	Actual pump speed (Feedback)
Scenario-106	UCA-6-7	The feedwater pump speed falls below the set point, but the processing delays of the pump controller delays the signal to increase the speed [UCA-6-7]. As a result the reactor water level could become too low [H-1].	
Scenario-107	UCA-6-7	The feedwater pump speed falls below the set point, but the delay of the actual pump speed signal delays the signal to increase the speed [UCA-6-7]. As a result the reactor water level could become too low [H-1].	
Scenario-108	UCA-6-7	The pump controller follows an incorrect Actual pump speed and applies the signal to increase the pump speed too late after the pump speed falls below the set point [UCA-6-7]. As a result the water level in the reactor may be too low [H-1]. This flawed process model can be caused due to the pump controller receiving incorrect feedback/information regarding the Actual pump speed.	Actual pump speed (Feedback)
Scenario-109	UCA-6-8	The feedwater pump speed goes above the set point, but the processing delays of the pump controller delays the signal to decrease the speed [UCA-6-8]. As a result the reactor water level could become too high [H-2].	
Scenario-110	UCA-6-8	The feedwater pump speed goes above the set point, but the delay of the actual pump speed signal delays the signal to decrease the speed [UCA-6-8]. As a result the reactor water level could become too high [H-2].	
Scenario-111	UCA-6-8	The pump controller follows an incorrect Actual pump speed and applies the signal to decrease the pump speed too late after the pump speed goes above the set point [UCA-6-8]. As a result the water level in the reactor may be too high [H-2]. This flawed process model can be caused due to the pump controller receiving incorrect feedback/information regarding the Actual pump speed.	Actual pump speed (Feedback)
Scenario-112	UCA-6-9	The feedwater pump speed is below the set point and the pump controller is applying the Increase signal to the feedwater pumps. Due to a malfunction in the physical pump controller the Increase signal applies continuously even after the pump speed reaches the set point [UCA-6-9] and fails to stop in-time. As a result the water level inside the reactor can become too high [H-2].	

Scenario-113	UCA-6-9	The pump controller follows an incorrect Actual pump speed and applies the signal to increase the pump speed too long after the pump speed reaches the set point [UCA-6-9]. As a result the water level in the reactor may be too high [H-2]. This flawed process model can be caused due to the pump controller receiving incorrect feedback/information regarding the Actual pump speed.	Actual pump speed (Feedback)
Scenario-114	UCA-6-10	The feedwater pump speed is above the set point and the pump controller is applying the decrease signal to the feedwater pumps. Due to a malfunction in the physical pump controller the decrease signal applies continuously even after the pump speed reaches the set point [UCA-6-10] and fails to stop in-time. As a result the water level inside the reactor can become too low [H-1].	
Scenario-115	UCA-6-10	The pump controller follows an incorrect Actual pump speed and applies the signal to decrease the pump speed too long after the pump speed reaches above the set point [UCA-6-9]. As a result the water level in the reactor may be too high [H-2]. This flawed process model can be caused due to the pump controller receiving incorrect feedback/information regarding the Actual pump speed.	Actual pump speed (Feedback)
Scenario-116	UCA-6-11, UCA-6-12	The pump controller is increasing/decreasing the pump speed and stops the signal before the speed reached the set point [UCA-6-11, UCA-6-12], incorrectly believing the speed is at the set point. This causes the feedwater pumps to have too high or too low speed, resulting the reactor water level to be either too high or too low [H-1,H-2]. This incorrect process model can be due to incorrect information about the actual pump speed.	Actual pump speed (Feedback)
Scenario-117	UCA-6-11, UCA-6-12	The pump controller is increasing/decreasing the pump speed and a pump controller hardware malfunction stops the signal before the speed reached the set point [UCA-6-11, UCA-6-12]. This causes the feedwater pumps to have too high or too low speed, resulting the reactor water level to be either too high or too low [H-1,H-2].	
Scenario-118	UCA-7-1	The reactor operations are in Low-power mode and the Low-power controller is providing the set point to the Feedwater valve controller. However, a malfunction in the Low-power controller causes the provided valve position set point to be fixed at 0% [UCA-7-1], closing the valves fully, interrupting the feedwater flow into the reactor. As a result the reactor water level can be too low [H-1].	
Scenario-119	UCA-7-1	The reactor operations are in Low-power mode and the Low-power controller is providing the set point to the Feedwater valve controller. However, a malfunction in the Low-power controller causes the provided valve position set point to be fixed at 100% [UCA-7-1], opening the valves fully and providing too much feedwater into the reactor. As a result the reactor water level can be too high [H-2].	
Scenario-120	UCA-7-1	The reactor operations are in Low-power mode, but the Low-power controller incorrectly believes that the operation mode is Normal. This could cause it to keep the feedwater control valves 100% open instead of providing an appropriate valve position set point to the feedwater control valve controller [UCA-7-1], resulting the reactor water level to too high [H-2]. This flawed process model will occur if the received measurement of Feedwater flow is incorrect or not received.	Feedwater flow (Feedback)
Scenario-121	UCA-7-1	The reactor operations are in Low-power mode, but the Low-power controller incorrectly believes that the operation mode is Normal. This could cause it to keep the feedwater control valves 100% open instead of providing an appropriate valve position set point to the feedwater control valve controller [UCA-7-1], resulting the reactor water level to too high [H-2]. This flawed process model will occur if the received measurement of Steam flow is incorrect or not received.	Steam flow (External)
Scenario-122	UCA-7-1	The reactor operations are in Low-power mode, but the Low-power controller incorrectly calculates the valve position set point based on incorrect information received, providing an incorrect valve position set point to the feedwater control valve controller [UCA-7-1], resulting the reactor water level to be either too high or too low [H-1,H-2]. This flawed process model will occur if the received measurement of Feedwater flow is incorrect or not received.	Feedwater flow (Feedback)
Scenario-123	UCA-7-1	The reactor operations are in Low-power mode, but the Low-power controller incorrectly calculates the valve position set point based on incorrect information received, providing an incorrect valve position set point to the feedwater control valve controller [UCA-7-1], resulting the reactor water level to be either too high or too low [H-1,H-2]. This flawed process model will occur if the received measurement of Steam flow is incorrect or not received.	Steam flow (External)
Scenario-124	UCA-7-2	The reactor operations are in Normal mode and the Low-power controller is keeping the set point for the Feedwater valve controller at 100%. However, a malfunction in the Low-power controller causes the provided valve position set point to differ from 100% [UCA-7-2], causing the valves to not open fully and interrupting the feedwater flow into the reactor. As a result the reactor water level can be too low [H-1].	
Scenario-125	UCA-7-2	The reactor operations are in Normal mode, but the Low-power controller incorrectly believes that the operation mode is Low-power. This could cause it to not keep the feedwater control valves 100% open and instead provide an inappropriate valve position set point to the feedwater control valve controller [UCA-7-2], resulting the reactor water level to too low [H-1]. This flawed process model will occur if the received measurement of Feedwater flow is incorrect or not received.	Feedwater flow (Feedback)
Scenario-126	UCA-7-2, UCA-7-3	The reactor operations are in Normal mode, but the Low-power controller incorrectly believes that the operation mode is Low-power. This could cause it to not keep the feedwater control valves 100% open and instead provide an inappropriate valve position set point to the feedwater control valve controller [UCA-7-2], resulting the reactor water level to too low [H-1]. This flawed process model will occur if the received measurement of Steam flow is incorrect or not received.	Steam flow (External)
Scenario-127	UCA-7-3, UCA-7-4	One or more hardware components fail in the Low-power controller when the reactor is operational, causing it to not provide the valve position set point to the feedwater control valve controller [UCA-7-3,UCA-7-4]. As a result, the reactor water level could be either too high or too low [H-1,H-2].	
Scenario-128	UCA-7-5	The operations enter the low-power mode, however the low-power controller provides an appropriate valve position set point to the feedwater control valve controller too late [UCA-7-5] due to processing delays in the Low-power controller. As a result the reactor water level could be too high [H-2].	
Scenario-129	UCA-7-5	The operations enter the low-power mode, however due to the processing delays in the low-power controller, the low-power mode is recognized too late, causing delays in providing an appropriate valve position set point to the feedwater control valve controller [UCA-7-5]. As a result the reactor water level could be too high [H-2].	
Scenario-130	UCA-7-5	The operations enter the low-power mode, however the low-power controller recognizes the low-power mode too late, causing delays in providing an appropriate valve position set point to the feedwater control valve controller [UCA-7-5]. As a result the reactor water level could be too high [H-2]. This flawed process model could be due to delays in the external information received regarding Steam flow.	Steam flow (External)

Scenario-131	UCA-7-5	The operations enter the low-power mode, however the low-power controller recognizes the low-power mode too late, causing delays in providing an appropriate valve position set point to the feedwater control valve controller [UCA-7-5]. As a result the reactor water level could be too high [H-2]. This flawed process model could be due to delays in the information received regarding feedwater flow.	Feedwater flow (Feedback)
Scenario-132	UCA-7-6	The operations enter the normal mode, however the low-power controller sets the valve position set point to 100% for the feedwater control valve controller too late [UCA-7-6] due to processing delays in the Low-power controller. As a result the reactor water level could be too low [H-1].	
Scenario-133	UCA-7-6	The operations enter the normal mode, however due to the processing delays in the low-power controller, the normal mode is recognized too late, causing delays in setting the valve position set point to 100% for the feedwater control valve controller [UCA-7-6]. As a result the reactor water level could be too low [H-1].	
Scenario-134	UCA-7-6	The operations enter the normal mode, however the low-power controller recognizes the low-power mode too late, causing delays in setting the valve position set point to 100% for the feedwater control valve controller [UCA-7-6]. As a result the reactor water level could be too low [H-1]. This flawed process model could be due to delays in the external information received regarding Steam flow.	
Scenario-135	UCA-7-6	The operations enter the low-power mode, however the low-power controller recognizes the low-power mode too late, causing delays in setting the valve position set point to 100% for the feedwater control valve controller [UCA-7-6]. As a result the reactor water level could be too low [H-1]. This flawed process model could be due to delays in the information received regarding feedwater flow.	
Scenario-136	UCA-8-1	The reactor operations are in Low-power mode and the Low-power controller is providing the set point to the Recirculation valve controller. However, a malfunction in the Low-power controller causes the provided valve position set point to be fixed at 0% [UCA-7-1], closing the valves fully, interrupting the recirculation flow. As a result the reactor water level can be too high [H-2].	
Scenario-137	UCA-8-1	The reactor operations are in Low-power mode and the Low-power controller is providing the set point to the Recirculation valve controller. However, a malfunction in the Low-power controller causes the provided valve position set point to be fixed at 100% [UCA-7-1], opening the valves fully and causing too much recirculation flow. As a result the reactor water level can be too low [H-1].	
Scenario-138	UCA-8-1, UCA-8-4	The reactor operations are in Low-power mode, but the Low-power controller incorrectly believes that the operation mode is Normal. This could cause it to keep the recirculation control valves 0% open instead of providing an appropriate valve position set point to the recirculation control valve controller [UCA-8-1,UCA-8-4], resulting the reactor water level to be too high [H-2]. This flawed process model will occur if the received measurement of Feedwater flow is incorrect or not received.	Feedwater flow (Feedback)
Scenario-139	UCA-8-1, UCA-8-4	The reactor operations are in Low-power mode, but the Low-power controller incorrectly believes that the operation mode is Normal. This could cause it to keep the recirculation control valves 0% open instead of providing an appropriate valve position set point to the recirculation control valve controller [UCA-8-1,UCA-8-4], resulting the reactor water level to be too high [H-2]. This flawed process model will occur if the received measurement of Steam flow is incorrect or not received.	Steam flow (External)
Scenario-140	UCA-8-1	The reactor operations are in Low-power mode, but the Low-power controller incorrectly calculates the valve position set point based on incorrect information received, providing an incorrect valve position set point to the recirculation control valve controller [UCA-8-1], resulting the reactor water level to be either too high or too low [H-1,H-2]. This flawed process model will occur if the received measurement of Feedwater flow is incorrect or not received.	Feedwater flow (Feedback)
Scenario-141	UCA-8-1	The reactor operations are in Low-power mode, but the Low-power controller incorrectly calculates the valve position set point based on incorrect information received, providing an incorrect valve position set point to the recirculation control valve controller [UCA-8-1], resulting the reactor water level to be either too high or too low [H-1,H-2]. This flawed process model will occur if the received measurement of Steam flow is incorrect or not received.	Steam flow (External)
Scenario-142	UCA-8-2, UCA-8-3	The reactor operations are in Normal mode and the Low-power controller is keeping the set point for the Recirculation valve controller at 0%. However, a malfunction in the Low-power controller causes the provided valve position set point to differ from 0% [UCA-8-2], causing the valves to not close fully. As a result the reactor water level can be too low [H-1].	
Scenario-143	UCA-8-2, UCA-8-3	The reactor operations are in Normal mode, but the Low-power controller incorrectly believes that the operation mode is Low-power. This could cause it to not keep the recirculation control valves 0% open and instead provide an inappropriate valve position set point to the recirculation control valve controller [UCA-8-2], resulting the reactor water level to too low [H-1]. This flawed process model will occur if the received measurement of Feedwater flow is incorrect or not received.	Feedwater flow (Feedback)
Scenario-144	UCA-8-2, UCA-8-3	The reactor operations are in Normal mode, but the Low-power controller incorrectly believes that the operation mode is Low-power. This could cause it to not keep the recirculation control valves 0% open and instead provide an inappropriate valve position set point to the recirculation control valve controller [UCA-8-2], resulting the reactor water level to too low [H-1]. This flawed process model will occur if the received measurement of Steam flow is incorrect or not received.	Steam flow (External)
Scenario-145	UCA-8-3, UCA-8-4	One or more hardware components fail in the Low-power controller when the reactor is operational, causing it to not provide the valve position set point to the recirculation control valve controller [UCA-8-3,UCA-8-4]. As a result, the reactor water level could be either too high or too low [H-1,H-2]	
Scenario-146	UCA-8-5	The operations enter the low-power mode, however the low-power controller provides an appropriate valve position set point to the recirculation control valve controller too late [UCA-8-5] due to processing delays in the Low-power controller. As a result the reactor water level could be too high [H-2].	
Scenario-147	UCA-8-5	The operations enter the low-power mode, however due to the processing delays in the low-power controller, the low-power mode is recognized too late, causing delays in providing an appropriate valve position set point to the recirculation control valve controller [UCA-8-5]. As a result the reactor water level could be too high [H-2].	
Scenario-148	UCA-8-5	The operations enter the low-power mode, however the low-power controller recognizes the low-power mode too late, causing delays in providing an appropriate valve position set point to the recirculation control valve controller [UCA-8-5]. As a result the reactor water level could be too high [H-2]. This flawed process model could be due to delays in the external information received regarding Steam flow.	Steam flow (External)

Scenario-149	UCA-8-5	The operations enter the low-power mode, however the low-power controller recognizes the low-power mode too late, causing delays in providing an appropriate valve position set point to the recirculation control valve controller [UCA-8-5]. As a result the reactor water level could be too high [H-2]. This flawed process model could be due to delays in the information received regarding feedwater flow.	Feedwater flow (Feedback)
Scenario-150	UCA-8-6	The operations enter the normal mode, however the low-power controller sets the valve position set point to 0% for the recirculation control valve controller too late [UCA-8-6] due to processing delays in the Low-power controller. As a result the reactor water level could be too low [H-1].	
Scenario-151	UCA-8-6	The operations enter the normal mode, however due to the processing delays in the low-power controller, the normal mode is recognized too late, causing delays in setting the valve position set point to 0% for the recirculation control valve controller [UCA-8-6]. As a result the reactor water level could be too low [H-1].	
Scenario-152	UCA-8-6	The operations enter the normal mode, however the low-power controller recognizes the low-power mode too late, causing delays in setting the valve position set point to 0% for the recirculation control valve controller [UCA-8-6]. As a result the reactor water level could be too low [H-1]. This flawed process model could be due to delays in the external information received regarding Steam flow.	Steam flow (External)
Scenario-153	UCA-8-6	The operations enter the normal mode, however the low-power controller recognizes the low-power mode too late, causing delays in setting the valve position set point to 0% for the recirculation control valve controller [UCA-8-6]. As a result the reactor water level could be too low [H-1]. This flawed process model could be due to delays in the information received regarding Feedwater flow.	Feedwater flow (Feedback)
Scenario-154	UCA-9-1	The Low-power controller malfunctions during the low-power operations and sends the open signal to the feedwater shutoff valve controller [UCA-9-1], causing the feedwater flow into the reactor to increase. As a result, the reactor water level can become too high [H-2].	
Scenario-155	UCA-9-1	The Low-power controller incorrectly identified the operations to be in the Normal mode, when actually in Low-power mode and sends the Open signal to feedwater shutoff valve controller [UCA-9-1], causing the feedwater flow into the reactor to increase. As a result, the reactor water level can become too high [H-2]. This flawed process model can be due to information received regarding feedwater flow being incorrect or not receiving.	Feedwater flow (Feedback)
Scenario-156	UCA-9-1	The Low-power controller incorrectly identified the operations to be in the Normal mode, when actually in Low-power mode and sends the Open signal to feedwater shutoff valve controller [UCA-9-1], causing the feedwater flow into the reactor to increase. As a result, the reactor water level can become too high [H-2]. This flawed process model can be due to information received regarding Steam flow being incorrect or not receiving.	Steam flow (External)
Scenario-157	UCA-9-2	The Low-power controller malfunctions during a Scram and sends the open signal to the feedwater shutoff valve controller [UCA-9-2], causing the feedwater flow into the reactor to increase. As a result, the reactor water level can become too high [H-2].	
Scenario-158	UCA-9-3	The Low-power controller malfunctions during the normal operation and sends the Close signal to the feedwater shutoff valve controller [UCA-9-3], causing the feedwater flow into the reactor to increase. As a result, the reactor water level can become too low [H-1].	
Scenario-159	UCA-9-3	The Low-power controller incorrectly identified the operations to be in the Low-power mode, when actually in Normal mode and sends the Close signal to feedwater shutoff valve controller [UCA-9-3], causing the feedwater flow into the reactor to decrease. As a result, the reactor water level can become too low [H-1]. This flawed process model can be due to information received regarding feedwater flow being incorrect or not receiving.	Feedwater flow (Feedback)
Scenario-160	UCA-9-3	The Low-power controller incorrectly identified the operations to be in the Low-power mode, when actually in Normal mode and sends the Close signal to feedwater shutoff valve controller [UCA-9-3], causing the feedwater flow into the reactor to decrease. As a result, the reactor water level can become too low [H-1]. This flawed process model can be due to information received regarding Steam flow being incorrect or not receiving.	Steam flow (External)
Scenario-161	UCA-9-4, UCA-9-5	The Low-power controller cannot send Open/Close signals to the feedwater shutoff valve controller [UCA-9-4,UCA-9-5] due to a failure in the physical Low-power controller. As a result the water level inside the reactor can be either too high or too low [H-1,H-2].	
Scenario-162	UCA-9-4	The reactor operations enters into Normal operation from Low-power operation but the Low-power controller fails to recognize the change. This causes the Open signal not to be sent to the feedwater shutoff valve controller [UCA-9-4], resulting too low reactor water level in the reactor [H-1]. This flawed process could be due to the information regarding feedwater flow being incorrect or not receiving.	Feedwater flow (Feedback)
Scenario-163	UCA-9-4	The reactor operations enters into Normal operation from Low-power operation but the Low-power controller fails to recognize the change. This causes the Open signal not to be sent to the feedwater shutoff valve controller [UCA-9-4], resulting too low reactor water level in the reactor [H-1]. This flawed process could be due to the information regarding Steam flow being incorrect or not receiving.	Steam flow (External)
Scenario-164	UCA-9-5	The reactor operations enters into Low-power operation from Normal operation but the Low-power controller fails to recognize the change. This causes the Close signal not to be sent to the feedwater shutoff valve controller [UCA-9-5], resulting too high reactor water level in the reactor [H-2]. This flawed process could be due to the information regarding feedwater flow being incorrect or not receiving.	Feedwater flow (Feedback)
Scenario-165	UCA-9-5	The reactor operations enters into Low-power operation from Normal operation but the Low-power controller fails to recognize the change. This causes the Close signal not to be sent to the feedwater shutoff valve controller [UCA-9-5], resulting too high reactor water level in the reactor [H-2]. This flawed process could be due to the information regarding Steam flow being incorrect or not receiving.	Steam flow (External)
Scenario-166	UCA-9-6	The operations enter the low-power mode, however the low-power controller provides the Close signal to the feedwater shutoff valve controller too late [UCA-9-6] due to processing delays in the Low-power controller. As a result the reactor water level could be too high [H-2].	
Scenario-167	UCA-9-6	The operations enter the low-power mode, however due to the processing delays in the low-power controller, the low-power mode is recognized too late, causing delays in providing the Close signal to the feedwater shutoff valve controller [UCA-9-6]. As a result the reactor water level could be too high [H-2].	

Scenario-168	UCA-9-6	The operations enter the low-power mode, however the low-power controller recognizes the low-power mode too late, causing delays in providing the Close signal to the feedwater shutoff valve controller [UCA-9-6]. As a result the reactor water level could be too high [H-2]. This flawed process model could be due to delays in the external information received regarding Steam flow.	Steam flow (External)
Scenario-169	UCA-9-6	The operations enter the low-power mode, however the low-power controller recognizes the low-power mode too late, causing delays in providing the Close signal to the feedwater shutoff valve controller [UCA-9-6]. As a result the reactor water level could be too high [H-2]. This flawed process model could be due to delays in the external information received regarding Feedwater flow.	Feedwater flow (Feedback)
Scenario-170	UCA-9-7	The operations enter the normal mode, however the low-power controller provides the Open signal to the feedwater shutoff valve controller too late [UCA-9-7] due to processing delays in the Low-power controller. As a result the reactor water level could be too low [H-1].	
Scenario-171	UCA-9-7	The operations enter the normal mode, however due to the processing delays in the low-power controller, the normal mode is recognized too late, causing delays in providing the Open signal to the feedwater shutoff valve controller [UCA-9-7]. As a result the reactor water level could be too low [H-1].	
Scenario-172	UCA-9-7	The operations enter the normal mode, however the low-power controller recognizes the low-power mode too late, causing delays in providing the Open signal to the feedwater shutoff valve controller [UCA-9-7]. As a result the reactor water level could be too low [H-1]. This flawed process model could be due to delays in the external information received regarding Steam flow.	Steam flow (External)
Scenario-173	UCA-9-7	The operations enter the normal mode, however the low-power controller recognizes the low-power mode too late, causing delays in providing the Open signal to the feedwater shutoff valve controller [UCA-9-7]. As a result the reactor water level could be too low [H-1]. This flawed process model could be due to delays in the external information received regarding Feedwater flow.	Feedwater flow (Feedback)
Scenario-174	UCA-10-1	The Low-power controller malfunctions during the normal operations and sends the open signal to the recirculation shutoff valve controller [UCA-10-1], starting the recirculation flow. As a result, the reactor water level can become too low [H-1].	
Scenario-175	UCA-10-1	The Low-power controller incorrectly identified the operations to be in the Low-power mode, when actually in Normal mode and sends the Open signal to recirculation shutoff valve controller [UCA-10-1], causing the feedwater flow into the reactor to decrease. As a result, the reactor water level can become too low [H-1]. This flawed process model can be due to information received regarding feedwater flow being incorrect or not receiving.	Feedwater flow (Feedback)
Scenario-176	UCA-10-1	The Low-power controller incorrectly identified the operations to be in the Low-power mode, when actually in Normal mode and sends the Open signal to recirculation shutoff valve controller [UCA-10-1], causing the feedwater flow into the reactor to decrease. As a result, the reactor water level can become too low [H-1]. This flawed process model can be due to information received regarding Steam flow being incorrect or not receiving.	Steam flow (External)
Scenario-177	UCA-10-2	The Low-power controller malfunctions during the Low-power operation and sends the Close signal to the recirculation shutoff valve controller [UCA-10-2], causing the feedwater flow into the reactor to increase. As a result, the reactor water level can become too high [H-2].	
Scenario-178	UCA-10-2	The Low-power controller incorrectly identified the operations to be in the Normal mode, when actually in Low-power mode and sends the Close signal to feedwater shutoff valve controller [UCA-10-2], causing the feedwater flow into the reactor to increase. As a result, the reactor water level can become too high [H-2]. This flawed process model can be due to information received regarding feedwater flow being incorrect or not receiving.	Feedwater flow (Feedback)
Scenario-179	UCA-10-2	The Low-power controller incorrectly identified the operations to be in the Normal mode, when actually in Low-power mode and sends the Close signal to feedwater shutoff valve controller [UCA-10-2], causing the feedwater flow into the reactor to increase. As a result, the reactor water level can become too high [H-2]. This flawed process model can be due to information received regarding Steam flow being incorrect or not receiving.	Steam flow (External)
Scenario-180	UCA-10-3, UCA-10-4	The Low-power controller cannot send Open/Close signals to the recirculation shutoff valve controller [UCA-9-4,UCA-9-5] due to a failure in the physical Low-power controller. As a result the water level inside the reactor can be either too high or too low [H-1,H-2].	
Scenario-181	UCA-10-3	The reactor operations enters into Low-power operation from Normal operation but the Low-power controller fails to recognize the change. This causes the Open signal not to be sent to the recirculation shutoff valve controller [UCA-10-3], resulting too high reactor water level in the reactor [H-2]. This flawed process could be due to the information regarding feedwater flow being incorrect or not receiving.	Feedwater flow (Feedback)
Scenario-182	UCA-10-3	The reactor operations enters into Low-power operation from Normal operation but the Low-power controller fails to recognize the change. This causes the Open signal not to be sent to the recirculation shutoff valve controller [UCA-10-3], resulting too high reactor water level in the reactor [H-2]. This flawed process could be due to the information regarding Steam flow being incorrect or not receiving.	Steam flow (External)
Scenario-183	UCA-10-4	The reactor operations enters into Normal operation from Low-power operation but the Low-power controller fails to recognize the change. This causes the Close signal not to be sent to the recirculation shutoff valve controller [UCA-10-4], resulting too low reactor water level in the reactor [H-1]. This flawed process could be due to the information regarding feedwater flow being incorrect or not receiving.	Feedwater flow (Feedback)
Scenario-184	UCA-10-4	The reactor operations enters into Normal operation from Low-power operation but the Low-power controller fails to recognize the change. This causes the Close signal not to be sent to the recirculation shutoff valve controller [UCA-10-4], resulting too low reactor water level in the reactor [H-1]. This flawed process could be due to the information regarding Steam flow being incorrect or not receiving.	Steam flow (External)
Scenario-185	UCA-10-5	The operations enter the normal mode, however the low-power controller provides the Close signal to the feedwater shutoff valve controller too late [UCA-10-5] due to processing delays in the Low-power controller. As a result the reactor water level could be too low [H-1].	
Scenario-186	UCA-10-5	The operations enter the normal mode, however due to the processing delays in the low-power controller, the normal mode is recognized too late, causing delays in providing the Close signal to the recirculation shutoff valve controller [UCA-10-5]. As a result the reactor water level could be too low [H-1].	

Scenario-187	UCA-10-5	The operations enter the normal mode, however the low-power controller recognizes the low-power mode too late, causing delays in providing the Close signal to the recirculation shutoff valve controller [UCA-10-5]. As a result the reactor water level could be too low [H-1]. This flawed process model could be due to delays in the external information received regarding Steam flow.	Steam flow (External)
Scenario-188	UCA-10-5	The operations enter the normal mode, however the low-power controller recognizes the low-power mode too late, causing delays in providing the Close signal to the recirculation shutoff valve controller [UCA-10-5]. As a result the reactor water level could be too low [H-1]. This flawed process model could be due to delays in the external information received regarding Feedwater flow.	Feedwater flow (Feedback)
Scenario-189	UCA-10-6	The operations enter the low-power mode, however the low-power controller provides the Open signal to the recirculation shutoff valve controller too late [UCA-10-6] due to processing delays in the Low-power controller. As a result the reactor water level could be too high [H-2].	
Scenario-190	UCA-10-6	The operations enter the low-power mode, however due to the processing delays in the low-power controller, the low-power mode is recognized too late, causing delays in providing the Open signal to the recirculation shutoff valve controller [UCA-10-6]. As a result the reactor water level could be too high [H-2].	
Scenario-191	UCA-10-6	The operations enter the low-power mode, however the low-power controller recognizes the low-power mode too late, causing delays in providing the Open signal to the recirculation shutoff valve controller [UCA-10-6]. As a result the reactor water level could be too high [H-2]. This flawed process model could be due to delays in the external information received regarding Steam flow.	Steam flow (External)
Scenario-192	UCA-10-6	The operations enter the low-power mode, however the low-power controller recognizes the low-power mode too late, causing delays in providing the Open signal to the recirculation shutoff valve controller [UCA-10-6]. As a result the reactor water level could be too high [H-2]. This flawed process model could be due to delays in the external information received regarding Feedwater flow.	Feedwater flow (Feedback)
Scenario-193	UCA-11-1	The feedwater control valves are being operated manually and the operator accidentally increases the feedwater control valve opening, when it needs to be decreased [UCA-11-1]. As a result the reactor water level could become too high [H-2].	
Scenario-194	UCA-11-2	The feedwater control valves are being operated manually and the operator accidentally increases the feedwater control valve opening, when changing the opening is not required [UCA-11-2]. As a result the reactor water level could become too high [H-2].	
Scenario-195	UCA-11-3	The feedwater control valves are being operated manually and the operator accidentally decreases the feedwater control valve opening, when it needs to be increased [UCA-11-3]. As a result the reactor water level could become too low [H-1].	
Scenario-196	UCA-11-4	The feedwater control valves are being operated manually and the operator accidentally decreases the feedwater control valve opening, when changing the opening is not required [UCA-11-4]. As a result the reactor water level could become too low [H-1].	
Scenario-197	UCA-11-1, UCA-11-2	The feedwater control valves are being controlled manually and the operator increases the feedwater control valve opening when not desired [UCA-11-1,UCA-11-2], based on an incorrect information on actual valve position. As a result the reactor water level could be too high [H-2]. This flawed process model can occur due to the errors in the Actual valve position feedback.	Actual valve position (Feedback)
Scenario-198	UCA-11-1, UCA-11-2	The feedwater control valves are being controlled manually and the operator increases the feedwater control valve opening when not desired [UCA-11-1,UCA-11-2], following an incorrect procedure. As a result the reactor water level could be too high [H-2]. This flawed process model can occur due: - Operator following an inappropriate procedure mistakenly - the process not being updated accordingly - procedure being updated and not being communicated properly	
Scenario-199	UCA-11-1, UCA-11-2	The feedwater control valve opening are being controlled manually and due to a failure in the physical control panel, the control panel indicates the received feedback/information incorrectly. This causes the operator to increase the pump speed when not required [UCA-11-1,UCA-11-2] resulting the reactor water level to be too high [H-2].	
Scenario-200	UCA-11-3, UCA-11-4	The feedwater control valves are being controlled manually and the operator decreases the feedwater control valves when not desired [UCA-11-3,UCA-11-4], based on an incorrect information on actual valve position. As a result the reactor water level could be too low [H-1]. This flawed process model can occur due to the errors in the Actual valve position feedback.	Actual valve position (Feedback)
Scenario-201	UCA-11-3, UCA-11-4	The feedwater control valves are being controlled manually and the operator decreases the feedwater control valves when not desired [UCA-11-3,UCA-11-4], following an incorrect procedure. As a result the reactor water level could be too low [H-1]. This flawed process model can occur due: - Operator following an inappropriate procedure mistakenly - the process not being updated accordingly - procedure being updated and not being communicated properly	
Scenario-202	UCA-11-3, UCA-11-4	The feedwater control valves are being controlled manually and due to a failure in the physical control panel, the control panel indicates the received feedback/information incorrectly. This causes the operator to decrease the feedwater control valves when not required [UCA-11-3,UCA-11-4] resulting the reactor water level to be too low [H-1].	
Scenario-203	UCA-11-5, UCA-11-6	The feedwater control valves are being operated manually and the operator accidentally stops controlling the feedwater control valve opening [UCA-11-5,UCA-11-6]. As a result the reactor water level could become either too high or too low [H-1,H-2].	
Scenario-204	UCA-11-5, UCA-11-6	The feedwater control valves are being controlled manually and the operator does not change the feedwater control valve opening as expected [UCA-11-3], based on an incorrect information on actual valve position. As a result the reactor water level could be either too high or too low [H-1,H-2]. This flawed process model can occur due to the errors in the Actual valve position feedback.	Actual valve position (Feedback)

Scenario-205	UCA-11-5, UCA-11-6	The feedwater control valves are being controlled manually and the operator does not change the feedwater control valve opening as expected [UCA-11-3], following an incorrect procedure. As a result the reactor water level could be either too high or too low [H-1,H-2]. This flawed process model can occur due: - Operator following an inappropriate procedure mistakenly - the process not being updated accordingly - procedure being updated and not being communicated properly	
Scenario-206	UCA-11-5, UCA-11-6	The feedwater control valves are being controlled manually and due to a failure in the physical control panel, the control panel indicates the received feedback/information incorrectly. This causes the operator to not control the feedwater control valve opening appropriately [UCA-11-5,UCA-11-6] resulting the reactor water level to be either too low or too high [H-1,H-2].	
Scenario-207	UCA-11-5, UCA-11-6	The feedwater control valves are being controlled manually but the operator incorrectly believes that the feedwater control valves are set to automatic control. This causes the operator to not control the feedwater control valve opening appropriately [UCA-11-5,UCA-11-6] resulting the reactor water level to be either too low or too high [H-1,H-2].	
Scenario-208	UCA-11-7	The feedwater control valves are being controlled manually and the operator increases the feedwater control valve opening too late [UCA-11-7], due to delays of the operators actions. As a result the reactor water level could be too low [H-1].	
Scenario-209	UCA-11-7	The feedwater control valves are being controlled manually and the operator increases the feedwater control valve opening too late [UCA-11-7], due to delay of receiving feedback/information. As a result the reactor water level could be too low [H-1]. This flawed process model can occur due to the delays in the Actual valve position feedback.	
Scenario-210	UCA-11-7	The feedwater control valves are being controlled manually and the operator increases the feedwater control valve opening too late [UCA-11-7], due to delay of receiving feedback/information. As a result the reactor water level could be too low [H-1]. This flawed process model can occur due to the delays in the Control panel indicators.	
Scenario-211	UCA-11-8	The feedwater control valves are being controlled manually and the operator decreases the feedwater control valve opening too late [UCA-11-8], due to delays of the operators actions. As a result the reactor water level could be too high [H-2].	
Scenario-212	UCA-11-8	The feedwater control valves are being controlled manually and the operator decreased the feedwater control valve opening too late [UCA-11-8], due to delay of receiving feedback/information. As a result the reactor water level could be too high [H-2]. This flawed process model can occur due to the delays in the Actual valve position feedback.	
Scenario-213	UCA-11-8	The feedwater control valves are being controlled manually and the operator decreased the feedwater control valve opening too late [UCA-11-8], due to delay of receiving feedback/information. As a result the reactor water level could be too high [H-2]. This flawed process model can occur due to the delays in the Control panel indicators.	
Scenario-214	UCA-11-9	The feedwater control valves are being controlled manually and the operator accidentally applies the signal to increase the feedwater control valve opening for too long [UCA-11-9], causing the valve position to go beyond the desired level. As a result the reactor water level could be too high [H-2].	
Scenario-215	UCA-11-10	The feedwater control valves are being controlled manually and the operator accidentally applies the signal to decrease the feedwater control valve opening for too long [UCA-11-10], causing the valve position to fall below the desired level. As a result the reactor water level could be too low [H-1].	
Scenario-216	UCA-11-11	The feedwater control valves are being controlled manually and the operator accidentally stops the signal to increase the feedwater control valve opening for too soon [UCA-11-11], causing the valve opening to not reach the desired level. As a result the reactor water level could be too low [H-1].	
Scenario-217	UCA-11-12	The feedwater control valves are being controlled manually and the operator accidentally stops the signal to decrease the feedwater control valve opening for too soon [UCA-11-12], causing the valve opening to not reach the desired level. As a result the reactor water level could be too high [H-2].	
Scenario-218	UCA-11-9, UCA-11-10, UCA-11-11, UCA-11-12	The feedwater control valves are being controlled manually and the operator applies the signal to increase/decrease the feedwater control valve opening for an incorrect duration based on insufficient feedback/information [UCA-11-9,UCA-11-10,UCA-11-11,UCA-11-12], causing the valve opening to be different from the desired position. As a result the reactor water level could be either too low or too high [H-1,H-2]. This flawed process model can occur due to insufficient Actual valve position feedback.	Actual valve position (Feedback)
Scenario-219	UCA-11-9, UCA-11-10, UCA-11-11, UCA-11-12	The feedwater control valves are being controlled manually and the operator applies the signal to increase/decrease the feedwater control valve opening for an incorrect duration based on insufficient feedback/information due to a failure in the control panel [UCA-11-9,UCA-11-10,UCA-11-11,UCA-11-12], causing the feedwater control valve opening to be different from the desired speed. As a result the reactor water level could be either too low or too high [H-1,H-2].	
Scenario-220	UCA-12-1	The recirculation control valves are being operated manually and the operator accidentally increases the recirculation control valve opening, when it needs to be decreased [UCA-12-1]. As a result the reactor water level could become too low [H-1].	
Scenario-221	UCA-12-2	The recirculation control valves are being operated manually and the operator accidentally increases the recirculation control valve opening, when changing the opening is not required [UCA-12-2]. As a result the reactor water level could become too low [H-1].	
Scenario-222	UCA-12-3	The recirculation control valves are being operated manually and the operator accidentally decreases the recirculation control valve opening, when it needs to be increased [UCA-12-3]. As a result the reactor water level could become too high [H-1].	
Scenario-223	UCA-12-4	The recirculation control valves are being operated manually and the operator accidentally decreases the recirculation control valve opening, when changing the opening is not required [UCA-12-4]. As a result the reactor water level could become too high [H-1].	
Scenario-224	UCA-12-1, UCA-12-2	The recirculation control valves are being controlled manually and the operator increases the recirculation control valve opening when not desired [UCA-12-1,UCA-12-2], based on an incorrect information on actual valve position. As a result the reactor water level could be too low [H-1]. This flawed process model can occur due to the errors in the Actual valve position feedback.	Actual valve position (Feedback)

Scenario-225	UCA-12-1, UCA-12-2	The recirculation control valves are being controlled manually and the operator increases the recirculation control valve opening when not desired [UCA-12-1,UCA-12-2], following an incorrect procedure. As a result the reactor water level could be too low [H-1]. This flawed process model can occur due: - Operator following an inappropriate procedure mistakenly - the process not being updated accordingly - procedure being updated and not being communicated properly	
Scenario-226	UCA-12-1, UCA-12-2	The recirculation control valve opening are being controlled manually and due to a failure in the physical control panel, the control panel indicates the received feedback/information incorrectly. This causes the operator to increase the pump speed when not required [UCA-12-1,UCA-12-2] resulting the reactor water level to be too low [H-1].	
Scenario-227	UCA-12-3, UCA-12-4	The recirculation control valves are being controlled manually and the operator decreases the recirculation control valves when not desired [UCA-12-3,UCA-12-4], based on an incorrect information on actual valve position. As a result the reactor water level could be too high [H-1]. This flawed process model can occur due to the errors in the Actual valve position feedback.	Actual valve position (Feedback)
Scenario-228	UCA-12-3, UCA-12-4	The recirculation control valves are being controlled manually and the operator decreases the recirculation control valves when not desired [UCA-12-3,UCA-12-4], following an incorrect procedure. As a result the reactor water level could be too high [H-1]. This flawed process model can occur due: - Operator following an inappropriate procedure mistakenly - the process not being updated accordingly - procedure being updated and not being communicated properly	
Scenario-229	UCA-12-3, UCA-12-4	The recirculation control valves are being controlled manually and due to a failure in the physical control panel, the control panel indicates the received feedback/information incorrectly. This causes the operator to decrease the recirculation control valves when not required [UCA-12-3,UCA-12-4] resulting the reactor water level to be too high [H-1].	
Scenario-230	UCA-12-5, UCA-12-6	The recirculation control valves are being operated manually and the operator accidentally stops controlling the recirculation control valve opening [UCA-12-5,UCA-12-6]. As a result the reactor water level could become either too high or too low [H-1,H-2].	
Scenario-231	UCA-12-5, UCA-12-6	The recirculation control valves are being controlled manually and the operator does not change the recirculation control valve opening as expected [UCA-12-3], based on an incorrect information on actual valve position. As a result the reactor water level could be either too high or too low [H-1,H-2]. This flawed process model can occur due to the errors in the Actual valve position feedback.	Actual valve position (Feedback)
Scenario-232	UCA-12-5, UCA-12-6	The recirculation control valves are being controlled manually and the operator does not change the recirculation control valve opening as expected [UCA-12-3], following an incorrect procedure. As a result the reactor water level could be either too high or too low [H-1,H-2]. This flawed process model can occur due: - Operator following an inappropriate procedure mistakenly - the process not being updated accordingly - procedure being updated and not being communicated properly	
Scenario-233	UCA-12-5, UCA-12-6	The recirculation control valves are being controlled manually and due to a failure in the physical control panel, the control panel indicates the received feedback/information incorrectly. This causes the operator to not control the recirculation control valve opening appropriately [UCA-12-5,UCA-12-6] resulting the reactor water level to be either too low or too high [H-1,H-2].	
Scenario-234	UCA-12-5, UCA-12-6	The recirculation control valves are being controlled manually but the operator incorrectly believes that the recirculation control valves are set to automatic control. This causes the operator to not control the recirculation control valve opening appropriately [UCA-12-5,UCA-12-6] resulting the reactor water level to be either too low or too high [H-1,H-2].	
Scenario-235	UCA-12-7	The recirculation control valves are being controlled manually and the operator increases the recirculation control valve opening too late [UCA-12-7], due to delays of the operators actions. As a result the reactor water level could be too high [H-1].	
Scenario-236	UCA-12-7	The recirculation control valves are being controlled manually and the operator increases the recirculation control valve opening too late [UCA-12-7], due to delay of receiving feedback/information. As a result the reactor water level could be too high [H-1]. This flawed process model can occur due to the delays in the Actual valve position feedback.	
Scenario-237	UCA-12-7	The recirculation control valves are being controlled manually and the operator increases the recirculation control valve opening too late [UCA-12-7], due to delay of receiving feedback/information. As a result the reactor water level could be too high [H-1]. This flawed process model can occur due to the delays in the Control panel indicators.	
Scenario-238	UCA-12-8	The recirculation control valves are being controlled manually and the operator decreases the recirculation control valve opening too late [UCA-12-8], due to delays of the operators actions. As a result the reactor water level could be too low [H-1].	
Scenario-239	UCA-12-8	The recirculation control valves are being controlled manually and the operator decreased the recirculation control valve opening too late [UCA-12-8], due to delay of receiving feedback/information. As a result the reactor water level could be too low [H-1]. This flawed process model can occur due to the delays in the Actual valve position feedback.	
Scenario-240	UCA-12-8	The recirculation control valves are being controlled manually and the operator decreased the recirculation control valve opening too late [UCA-12-8], due to delay of receiving feedback/information. As a result the reactor water level could be too low [H-1]. This flawed process model can occur due to the delays in the Control panel indicators.	
Scenario-241	UCA-12-9	The recirculation control valves are being controlled manually and the operator accidentally applies the signal to increase the recirculation control valve opening for too long [UCA-12-9], causing the valve position to go beyond the desired level. As a result the reactor water level could be too low [H-1].	

Scenario-242	UCA-12-10	The recirculation control valves are being controlled manually and the operator accidentally applies the signal to decrease the recirculation control valve opening for too long [UCA-12-10], causing the valve position to fall below the desired level. As a result the reactor water level could be too high [H-1].	
Scenario-243	UCA-12-11	The recirculation control valves are being controlled manually and the operator accidentally stops the signal to increase the recirculation control valve opening for too soon [UCA-12-11], causing the valve opening to not reach the desired level. As a result the reactor water level could be too high [H-1].	
Scenario-244	UCA-12-12	The recirculation control valves are being controlled manually and the operator accidentally stops the signal to decrease the recirculation control valve opening for too soon [UCA-12-12], causing the valve opening to not reach the desired level. As a result the reactor water level could be too low [H-1].	
Scenario-245	UCA-12-9, UCA-12-10, UCA-12-11, UCA-12-12	The recirculation control valves are being controlled manually and the operator applies the signal to increase/decrease the recirculation control valve opening for an incorrect duration based on insufficient feedback/information [UCA-12-9,UCA-12-10,UCA-12-11,UCA-12-12], causing the valve opening to be different from the desired position. As a result the reactor water level could be either too low or too high [H-1,H-2]. This flawed process model can occur due to insufficient Actual valve position feedback.	Actual valve position (Feedback)
Scenario-246	UCA-12-9, UCA-12-10, UCA-12-11, UCA-12-12	The recirculation control valves are being controlled manually and the operator applies the signal to increase/decrease the recirculation control valve opening for an incorrect duration based on insufficient feedback/information due to a failure in the control panel [UCA-12-9,UCA-12-10,UCA-12-11,UCA-12-12], causing the recirculation control valve opening to be different from the desired speed. As a result the reactor water level could be either too low or too high [H-1,H-2].	
Scenario-247	UCA-13-1	The feedwater shutoff valve is being operated manually and the operator accidentally Open the feedwater shutoff valve, when it needs to be Closed [UCA-13-1]. As a result the reactor water level could become too high [H-2].	
Scenario-248	UCA-13-2	The feedwater shutoff valve is being operated manually and the operator accidentally Close the feedwater shutoff valve, when it needs to be Opened [UCA-13-2]. As a result the reactor water level could become too low [H-1].	
Scenario-249	UCA-13-3	The feedwater shutoff valve is being operated manually and the operator accidentally Stops the feedwater shutoff valve, when it does not need to be stopped (e.g. during emergencies) [UCA-13-3]. As a result the reactor water level could become either too low or too high [H-1,H-2].	
Scenario-250	UCA-13-1	The feedwater shutoff valves are being controlled manually and the operator Opens the feedwater shutoff valve when it needs to be closed [UCA-13-1], following an incorrect procedure. As a result the reactor water level could be too high [H-2]. This flawed process model can occur due: - Operator following an inappropriate procedure mistakenly - the process not being updated accordingly - procedure being updated and not being communicated properly	
Scenario-251	UCA-13-2	The feedwater shutoff valves are being controlled manually and the operator Closes the feedwater shutoff valve when it needs to be opened [UCA-13-2], following an incorrect procedure. As a result the reactor water level could be too high [H-2]. This flawed process model can occur due: - Operator following an inappropriate procedure mistakenly - the process not being updated accordingly - procedure being updated and not being communicated properly	
Scenario-252	UCA-13-3	The feedwater shutoff valves are being controlled manually and the operator Stops the feedwater shutoff valve when it does not need to be stopped (e.g. during emergencies) [UCA-13-3], following an incorrect procedure. As a result the reactor water level could be either too low or too high [H-1,H-2]. This flawed process model can occur due: - Operator following an inappropriate procedure mistakenly - the process not being updated accordingly - procedure being updated and not being communicated properly	
Scenario-253	UCA-13-4, UCA-13-5, UCA-13-6	The feedwater shutoff valves are being operated manually and the operator accidentally stops controlling the feedwater shutoff valve [UCA-13-3,UCA-13-4,UCA-13-5]. As a result the reactor water level could become either too high or too low [H-1,H-2].	
Scenario-254	UCA-13-4, UCA-13-5, UCA-13-6	The feedwater shutoff valves are being controlled manually and the operator does not control the feedwater shutoff valve as expected [UCA-13-3,UCA-13-4,UCA-13-5], following an incorrect procedure. As a result the reactor water level could be either too high or too low [H-1,H-2]. This flawed process model can occur due: - Operator following an inappropriate procedure mistakenly - the process not being updated accordingly - procedure being updated and not being communicated properly	
Scenario-255	UCA-13-4, UCA-13-5, UCA-13-6	The feedwater shutoff valves are being controlled manually but the operator incorrectly believes that the feedwater shutoff valves are set to automatic control. This causes the operator to not control the feedwater shutoff valve appropriately [UCA-13-3,UCA-13-4,UCA-13-5] resulting the reactor water level to be either too low or too high [H-1,H-2].	
Scenario-256	UCA-13-6	The feedwater shutoff valves are being operated manually and the operator does not Stop the feedwater shutoff valve in an emergency [UCA-13-6] due to not being aware of the situation. As a result the reactor water level could become either too high or too low [H-1,H-2].	
Scenario-257	UCA-13-7	The feedwater shutoff valves are being controlled manually and the operator opens the feedwater shutoff valve too late [UCA-13-7], due to delays of the operators actions. As a result the reactor water level could be too low [H-1].	
Scenario-258	UCA-13-8	The feedwater shutoff valves are being controlled manually and the operator closes the feedwater shutoff valve too late [UCA-13-8], due to delays of the operators actions. As a result the reactor water level could be either too low or too high [H-1,H-2].	

Scenario-259	UCA-13-9	The feedwater shutoff valves are being controlled manually and the operator Stops the feedwater shutoff valve too late [UCA-13-9] during an emergency, due to delays of the operators actions. As a result the reactor water level could be either too low or too high [H-1,H-2].
Scenario-260	UCA-14-1	The recirculation shutoff valve is being operated manually and the operator accidentally Open the recirculation shutoff valve, when it needs to be Closed [UCA-14-1]. As a result the reactor water level could become too low [H-1].
Scenario-261	UCA-14-2	The recirculation shutoff valve is being operated manually and the operator accidentally Close the recirculation shutoff valve, when it needs to be Opened [UCA-14-2]. As a result the reactor water level could become too high [H-2].
Scenario-262	UCA-14-3	The recirculation shutoff valve is being operated manually and the operator accidentally Stops the recirculation shutoff valve, when it does not need to be stopped (e.g. during emergencies) [UCA-14-3]. As a result the reactor water level could become either too low or too high [H-1,H-2].
Scenario-263	UCA-14-1	The recirculation shutoff valves are being controlled manually and the operator Opens the recirculation shutoff valve when it needs to be closed [UCA-14-1], following an incorrect procedure. As a result the reactor water level could be too low [H-1]. This flawed process model can occur due: - Operator following an inappropriate procedure mistakenly - the process not being updated accordingly
Scenario-264	UCA-14-2	The recirculation shutoff valves are being controlled manually and the operator Closes the recirculation shutoff valve when it needs to be opened [UCA-14-2], following an incorrect procedure. As a result the reactor water level could be too high [H-2]. This flawed process model can occur due: - Operator following an inappropriate procedure mistakenly - the process not being updated accordingly - procedure being updated and not being communicated properly
Scenario-265	UCA-14-3	The recirculation shutoff valves are being controlled manually and the operator Stops the recirculation shutoff valve when it does not need to be stopped (e.g. during emergencies) [UCA-14-3], following an incorrect procedure. As a result the reactor water level could be either too high or too low [H-1,H-2]. This flawed process model can occur due: - Operator following an inappropriate procedure mistakenly - the process not being updated accordingly - procedure being updated and not being communicated properly
Scenario-266	UCA-14-4, UCA-14-5, UCA-14-6	The recirculation shutoff valves are being operated manually and the operator accidentally stops controlling the recirculation shutoff valve [UCA-14-3,UCA-14-4,UCA-14-5]. As a result the reactor water level could become either too high or too low [H-1,H-2].
Scenario-267	UCA-14-4, UCA-14-5, UCA-14-6	The recirculation shutoff valves are being controlled manually and the operator does not control the recirculation shutoff valve as expected [UCA-14-3,UCA-14-4,UCA-14-5], following an incorrect procedure. As a result the reactor water level could be either too high or too low [H-1,H-2]. This flawed process model can occur due: - Operator following an inappropriate procedure mistakenly - the process not being updated accordingly - procedure being updated and not being communicated properly
Scenario-268	UCA-14-4, UCA-14-5, UCA-14-6	The recirculation shutoff valves are being controlled manually but the operator incorrectly believes that the recirculation shutoff valves are set to automatic control. This causes the operator to not control the recirculation shutoff valve appropriately [UCA-14-3,UCA-14-4,UCA-14-5] resulting the reactor water level to be either too low or too high [H-1,H-2].
Scenario-269	UCA-14-6	The recirculation shutoff valves are being operated manually and the operator does not Stop the recirculation shutoff valve in an emergency [UCA-14-6] due to not being aware of the situation. As a result the reactor water level could become either too high or too low [H-1,H-2].
Scenario-270	UCA-14-7	The recirculation shutoff valves are being controlled manually and the operator opens the recirculation shutoff valve too late [UCA-14-7], due to delays of the operators actions. As a result the reactor water level could be too high [H-2].
Scenario-271	UCA-14-8	The recirculation shutoff valves are being controlled manually and the operator closes the recirculation shutoff valve too late [UCA-14-8], due to delays of the operators actions. As a result the reactor water level could be too low [H-1].
Scenario-272	UCA-14-9	The recirculation shutoff valves are being controlled manually and the operator Stops the recirculation shutoff valve too late [UCA-14-9] during an emergency, due to delays of the operators actions. As a result the reactor water level could be either too low or too high [H-1,H-2].
Scenario-273	UCA-15-1, UCA-15-3, UCA-15-9	The physical feedwater control valve controller malfunctions and provides the signal to Increase the valve opening continuously [UCA-15-1, UCA-15-3, UCA-15-9], causing the valves to go over the valve opening set point. As a result the water level in the reactor may be too high [H-2].
Scenario-274	UCA-15-2, UCA-15-4, UCA-15-10	The physical feedwater control valve controller malfunctions and provides the signal to Decrease the valve opening continuously [UCA-15-2, UCA-15-4, UCA-15-10], causing the valves to go below the valve opening set point. As a result the water level in the reactor may be too low [H-1].
Scenario-275	UCA-15-1, UCA-15-3, UCA-15-9	The feedwater control valve controller incorrectly believes that the Actual valve position is lower than the valve opening set point and increases the opening further [UCA-15-1,UCA-15-3,UCA-15-9]. As a result the valve opening could go over the set point and the water level in the reactor may be too high [H-2]. This flawed process model can be caused due to the feedwater control valve controller receiving incorrect feedback/information regarding the Actual valve position.

[Actual valve position \(Feedback\)](#)

Scenario-276	UCA-15-2, UCA-15-4, UCA-15-10	The feedwater control valve controller incorrectly believes that the Actual valve position is higher than the valve opening set point and decreases the opening further [UCA-15-2, UCA-15-4, UCA-15-10]. As a result the valve opening could go below the set point and the water level in the reactor may be too low [H-1]. This flawed process model can be caused due to the feedwater control valve controller receiving incorrect feedback/information regarding the Actual valve position.	Actual valve position (Feedback)
Scenario-277	UCA-15-5	The physical feedwater control valve controller fails during the operations and does not provide the Increase signal to increase the feedwater control valve opening when the actual valve position falls below the set point [UCA-15-5]. As a result the reactor water level may be too low [H-1].	
Scenario-278	UCA-15-6	The physical feedwater control valve controller fails during the operations and does not provide the Decrease signal to decrease the feedwater control valve opening when the actual valve position goes past the set point [UCA-15-6]. As a result the reactor water level may be too high [H-2].	
Scenario-279	UCA-15-5	The feedwater control valve controller incorrectly believes that the actual valve position is at the set point and does not provide the signal to increase the valve opening to the feedwater control valve when the actual valve position falls below the set point (valve opening needs to be increased) [UCA-15-5]. As a result the reactor water level may become too low [H-1]. This flawed process model can be caused due to the feedwater control valve controller receiving incorrect feedback/information regarding the Actual valve position.	Actual valve position (Feedback)
Scenario-280	UCA-15-6	The feedwater control valve controller incorrectly believes that the actual valve position is at the set point and does not provide the signal to decrease the valve opening to the feedwater control valve when the actual valve position goes above the set point (valve opening needs to be decreased) [UCA-15-6]. As a result the reactor water level may become too high [H-2]. This flawed process model can be caused due to the feedwater control valve controller receiving incorrect feedback/information regarding the Actual valve position.	Actual valve position (Feedback)
Scenario-281	UCA-15-7	The feedwater control valve opening speed falls below the set point, but the processing delays of the feedwater control valve controller delays the signal to increase the valve opening [UCA-15-7]. As a result the reactor water level could become too low [H-1].	
Scenario-282	UCA-15-7	The feedwater control valve opening falls below the set point, but the delay of the actual valve position signal delays the signal to increase the valve opening [UCA-15-7]. As a result the reactor water level could become too low [H-1].	
Scenario-283	UCA-15-7	The feedwater control valve controller follows an incorrect Actual valve position and applies the signal to increase the valve opening too late after the actual valve opening falls below the set point [UCA-15-7]. As a result the water level in the reactor may be too low [H-1]. This flawed process model can be caused due to the feedwater control valve controller receiving incorrect feedback/information regarding the Actual valve position.	Actual valve position (Feedback)
Scenario-284	UCA-15-8	The feedwater control valve opening speed goes above the set point, but the processing delays of the feedwater control valve controller delays the signal to decrease the valve opening [UCA-15-8]. As a result the reactor water level could become too high [H-2].	
Scenario-285	UCA-15-8	The feedwater control valve opening goes above the set point, but the delay of the actual valve position signal delays the signal to decrease the valve opening [UCA-15-8]. As a result the reactor water level could become too high [H-2].	
Scenario-286	UCA-15-8	The feedwater control valve controller follows an incorrect Actual valve position and applies the signal to decrease the valve opening too late after the actual valve opening goes above the set point [UCA-15-8]. As a result the water level in the reactor may be too high [H-2]. This flawed process model can be caused due to the feedwater control valve controller receiving incorrect feedback/information regarding the Actual valve position.	Actual valve position (Feedback)
Scenario-287	UCA-15-9	The feedwater control valve opening is below the set point and the feedwater control valve controller is applying the Increase signal to the feedwater control valve. Due to a malfunction in the physical feedwater control valve controller, the Increase signal applies continuously even after the valve position reaches the set point [UCA-15-9] and fails to stop in-time. As a result the water level inside the reactor can become too high [H-2].	
Scenario-288	UCA-15-9	The feedwater control valve controller follows an incorrect Actual valve position and applies the signal to increase the valve opening too long after the pump speed reaches the set point [UCA-15-9]. As a result the water level in the reactor may be too high [H-2]. This flawed process model can be caused due to the feedwater control valve controller receiving incorrect feedback/information regarding the Actual valve position.	Actual valve position (Feedback)
Scenario-289	UCA-15-10	The feedwater control valve opening is above the set point and the feedwater control valve controller is applying the Decrease signal to the feedwater control valve. Due to a malfunction in the physical feedwater control valve controller, the Decrease signal applies continuously even after the valve position reaches the set point [UCA-15-10] and fails to stop in-time. As a result the water level inside the reactor can become too low [H-1].	
Scenario-290	UCA-15-10	The feedwater control valve controller follows an incorrect Actual valve position and applies the signal to decrease the valve opening too long after the pump speed reaches the set point [UCA-15-10]. As a result the water level in the reactor may be too low [H-1]. This flawed process model can be caused due to the feedwater control valve controller receiving incorrect feedback/information regarding the Actual valve position.	Actual valve position (Feedback)
Scenario-291	UCA-15-11, UCA-15-12	The feedwater control valve controller is increasing/decreasing the valve opening and stops the signal before the valve position reaches the set point [UCA-15-11, UCA-15-12], incorrectly believing the valve position is at the set point. This causes the feedwater control valves to have too high or too low openings, resulting the reactor water level to be either too high or too low [H-1,H-2]. This incorrect process model can be due to incorrect information about the actual valve position.	Actual valve position (Feedback)
Scenario-292	UCA-15-11, UCA-15-12	The feedwater control valve controller is increasing/decreasing the valve opening and a feedwater control valve controller hardware malfunction stops the signal before the valve opening reached the set point [UCA-15-11, UCA-15-12]. This causes the feedwater control valves to have too high or too low valve opening, resulting the reactor water level to be either too high or too low [H-1,H-2].	
Scenario-293	UCA-16-1, UCA-16-3, UCA-16-9	The physical recirculation control valve controller malfunctions and provides the signal to Increase the valve opening continuously [UCA-16-1, UCA-16-3, UCA-16-9], causing the valves to go over the valve opening set point. As a result the water level in the reactor may be too low [H-1].	
Scenario-294	UCA-16-2, UCA-16-4, UCA-16-10	The physical recirculation control valve controller malfunctions and provides the signal to Decrease the valve opening continuously [UCA-16-2, UCA-16-4, UCA-16-10], causing the valves to go below the valve opening set point. As a result the water level in the reactor may be too high [H-2].	

Scenario-295	UCA-16-1, UCA-16-3, UCA-16-9	The recirculation control valve controller incorrectly believes that the Actual valve position is lower than the valve opening set point and increases the opening further [UCA-16-1,UCA-16-3,UCA-16-9]. As a result the valve opening could go over the set point and the water level in the reactor may be too low [H-1]. This flawed process model can be caused due to the recirculation control valve controller receiving incorrect feedback/information regarding the Actual valve position.	Actual valve position (Feedback)
Scenario-296	UCA-16-2, UCA-16-4, UCA-16-10	The recirculation control valve controller incorrectly believes that the Actual valve position is higher than the valve opening set point and decreases the opening further [UCA-16-2, UCA-16-4, UCA-16-10]. As a result the valve opening could go below the set point and the water level in the reactor may be too high [H-2]. This flawed process model can be caused due to the recirculation control valve controller receiving incorrect feedback/information regarding the Actual valve position.	Actual valve position (Feedback)
Scenario-297	UCA-16-5	The physical recirculation control valve controller fails during the operations and does not provide the Increase signal to increase the recirculation control valve opening when the actual valve position falls below the set point [UCA-16-5]. As a result the reactor water level may be too high [H-2].	
Scenario-298	UCA-16-6	The physical recirculation control valve controller fails during the operations and does not provide the Decrease signal to decrease the recirculation control valve opening when the actual valve position goes past the set point [UCA-16-6]. As a result the reactor water level may be too low [H-1].	
Scenario-299	UCA-16-5	The recirculation control valve controller incorrectly believes that the actual valve position is at the set point and does not provide the signal to increase the valve opening to the recirculation control valve when the actual valve position falls below the set point (valve opening needs to be increased) [UCA-16-5]. As a result the reactor water level may become too high [H-2]. This flawed process model can be caused due to the recirculation control valve controller receiving incorrect feedback/information regarding the Actual valve position.	Actual valve position (Feedback)
Scenario-300	UCA-16-6	The recirculation control valve controller incorrectly believes that the actual valve position is at the set point and does not provide the signal to decrease the valve opening to the recirculation control valve when the actual valve position goes above the set point (valve opening needs to be decreased) [UCA-16-6]. As a result the reactor water level may become too low [H-1]. This flawed process model can be caused due to the recirculation control valve controller receiving incorrect feedback/information regarding the Actual valve position.	Actual valve position (Feedback)
Scenario-301	UCA-16-7	The recirculation control valve opening speed falls below the set point, but the processing delays of the recirculation control valve controller delays the signal to increase the valve opening [UCA-16-7]. As a result the reactor water level could become too high [H-2].	
Scenario-302	UCA-16-7	The recirculation control valve opening falls below the set point, but the delay of the actual valve position signal delays the signal to increase the valve opening [UCA-16-7]. As a result the reactor water level could become too high [H-2].	
Scenario-303	UCA-16-7	The recirculation control valve controller follows an incorrect Actual valve position and applies the signal to increase the valve opening too late after the actual valve opening falls below the set point [UCA-16-7]. As a result the water level in the reactor may be too high [H-2]. This flawed process model can be caused due to the recirculation control valve controller receiving incorrect feedback/information regarding the Actual valve position.	Actual valve position (Feedback)
Scenario-304	UCA-16-8	The recirculation control valve opening speed goes above the set point, but the processing delays of the recirculation control valve controller delays the signal to decrease the valve opening [UCA-16-8]. As a result the reactor water level could become too low [H-1].	
Scenario-305	UCA-16-8	The recirculation control valve opening goes above the set point, but the delay of the actual valve position signal delays the signal to decrease the valve opening [UCA-16-8]. As a result the reactor water level could become too low [H-1].	
Scenario-306	UCA-16-8	The recirculation control valve controller follows an incorrect Actual valve position and applies the signal to decrease the valve opening too late after the actual valve opening goes above the set point [UCA-16-8]. As a result the water level in the reactor may be too low [H-1]. This flawed process model can be caused due to the recirculation control valve controller receiving incorrect feedback/information regarding the Actual valve position.	Actual valve position (Feedback)
Scenario-307	UCA-16-9	The recirculation control valve opening is below the set point and the recirculation control valve controller is applying the Increase signal to the recirculation control valve. Due to a malfunction in the physical recirculation control valve controller, the Increase signal applies continuously even after the valve position reaches the set point [UCA-16-9] and fails to stop in-time. As a result the water level inside the reactor can become too low [H-1].	
Scenario-308	UCA-16-9	The recirculation control valve controller follows an incorrect Actual valve position and applies the signal to increase the valve opening too long after the pump speed reaches the set point [UCA-16-9]. As a result the water level in the reactor may be too low [H-1]. This flawed process model can be caused due to the recirculation control valve controller receiving incorrect feedback/information regarding the Actual valve position.	Actual valve position (Feedback)
Scenario-309	UCA-16-10	The recirculation control valve opening is above the set point and the recirculation control valve controller is applying the Decrease signal to the recirculation control valve. Due to a malfunction in the physical recirculation control valve controller, the Decrease signal applies continuously even after the valve position reaches the set point [UCA-16-10] and fails to stop in-time. As a result the water level inside the reactor can become too high [H-2].	
Scenario-310	UCA-16-10	The recirculation control valve controller follows an incorrect Actual valve position and applies the signal to decrease the valve opening too long after the pump speed reaches the set point [UCA-16-10]. As a result the water level in the reactor may be too high [H-2]. This flawed process model can be caused due to the recirculation control valve controller receiving incorrect feedback/information regarding the Actual valve position.	Actual valve position (Feedback)
Scenario-311	UCA-16-11, UCA-16-12	The recirculation control valve controller is increasing/decreasing the valve opening and stops the signal before the valve position reaches the set point [UCA-16-11, UCA-16-12], incorrectly believing the valve position is at the set point. This causes the recirculation control valves to have too high or too low openings, resulting the reactor water level to be either too high or too low [H-1,H-2]. This incorrect process model can be due to incorrect information about the actual valve position.	Actual valve position (Feedback)
Scenario-312	UCA-16-11, UCA-16-12	The recirculation control valve controller is increasing/decreasing the valve opening and a recirculation control valve controller hardware malfunction stops the signal before the valve opening reached the set point [UCA-16-11, UCA-16-12]. This causes the recirculation control valves to have too high or too low valve opening, resulting the reactor water level to be either too high or too low [H-1,H-2].	

Scenario-313	UCA-17-1	The physical feedwater shutoff valve controller malfunctions and sends the Open signal to the feedwater shutoff valve continuously without providing the Close signal [UCA-17-1], causing the valve to remain open. As a result the reactor water level can be too high [H-2].
Scenario-314	UCA-17-2	The physical feedwater shutoff valve controller malfunctions and sends the Close signal to the feedwater shutoff valve continuously without providing the Open signal [UCA-17-2], causing the valve to remain close. As a result the reactor water level can be too low [H-1].
Scenario-315	UCA-17-3	The physical feedwater shutoff valve controller malfunctions and fails to Open the feedwater shutoff valve when required [UCA-17-3]. As a result the reactor water level may be too low [H-1].
Scenario-316	UCA-17-4	The physical feedwater shutoff valve controller malfunctions and fails to Close the feedwater shutoff valve when required [UCA-17-4]. As a result the reactor water level may be too high [H-2].
Scenario-317	UCA-17-5	The feedwater shutoff valve controller is requested to close the feedwater shutoff valve but the Close signal is delayed due to processing delays of the feedwater shutoff valve controller [UCA-17-5]. As a result the water level in the reactor may be too high [H-2].
Scenario-318	UCA-17-6	The feedwater shutoff valve controller is requested to open the feedwater shutoff valve but the Open signal is delayed due to processing delays of the feedwater shutoff valve controller [UCA-17-6]. As a result the water level in the reactor may be too low [H-1].
Scenario-319	UCA-18-1	The physical recirculation shutoff valve controller malfunctions and sends the Open signal to the recirculation shutoff valve continuously without providing the Close signal [UCA-18-1], causing the valve to remain open. As a result the reactor water level can be too low [H-1].
Scenario-320	UCA-18-2	The physical recirculation shutoff valve controller malfunctions and sends the Close signal to the recirculation shutoff valve continuously without providing the Open signal [UCA-18-2], causing the valve to remain close. As a result the reactor water level can be too high [H-2].
Scenario-321	UCA-18-3	The physical recirculation shutoff valve controller malfunctions and fails to Open the recirculation shutoff valve when required [UCA-18-3]. As a result the reactor water level may be too high [H-2].
Scenario-322	UCA-18-4	The physical recirculation shutoff valve controller malfunctions and fails to Close the recirculation shutoff valve when required [UCA-18-4]. As a result the reactor water level may be too low [H-1].
Scenario-323	UCA-18-5	The recirculation shutoff valve controller is requested to close the recirculation shutoff valve but the Close signal is delayed due to processing delays of the recirculation shutoff valve controller [UCA-18-5]. As a result the water level in the reactor may be too low [H-1].
Scenario-324	UCA-18-6	The recirculation shutoff valve controller is requested to open the recirculation shutoff valve but the Open signal is delayed due to processing delays of the recirculation shutoff valve controller [UCA-17-6]. As a result the water level in the reactor may be too high [H-2].
Scenario-325	CA-1	Control mode for the pumps are correctly provided by the operator but is not received correctly by the Low-power controller due a failure in the physical control panel. As a result the water level in the reactor may be too low or too high [H-1,H-2].
Scenario-326	CA-1	Control mode for the pumps are correctly provided by the operator but is not received correctly by the Low-power controller due a failure in the connection between the control panel and the Low-power controller. As a result the water level in the reactor may be too low or too high [H-1,H-2].
Scenario-327	CA-1	Control mode for the pumps are correctly provided by the operator and sent properly by the control panel. However, the Low-power controller does not recognize the signal due to a malfunction in the Low-power controller. As a result the water level in the reactor may be too low or too high [H-1,H-2].
Scenario-328	CA-2	Operator provides the signal to transfer the pumps control over to the Master controller but is not received by the Low-power controller due to a failure in the physical control panel. As a result the water level in the reactor may be too low or too high [H-1,H-2].
Scenario-329	CA-2	The signal to transfer the pumps control over to the Master controller is correctly provided by the operator but is not received correctly by the Low-power controller due a failure in the connection between the control panel and the Low-power controller. As a result the water level in the reactor may be too low or too high [H-1,H-2].
Scenario-330	CA-2	The signal to transfer the pumps control over to the Master controller is correctly provided by the operator and sent properly by the control panel. However, the Low-power controller does not recognize the signal due to a malfunction in the Low-power controller. As a result the water level in the reactor may be too low or too high [H-1,H-2].
Scenario-331	CA-3	The pump speed set point is correctly calculated and provided by the Master controller. However, it is not received by the Pump controller due to a failure in the connection between the Master controller and the Pump controller. As a result the water level in the reactor may be too low or too high [H-1,H-2].
Scenario-332	CA-3	The pump speed set point is correctly calculated and provided by the Master controller. However, it is misinterpreted by the Pump controller due to a malfunction in the Pump controller. As a result the water level in the reactor may be too low or too high [H-1,H-2].
Scenario-333	CA-3	The pump speed set point is correctly calculated and provided by the Master controller. However, it is misinterpreted by the Pump controller due to a software error in the Pump controller. As a result the water level in the reactor may be too low or too high [H-1,H-2].
Scenario-334	CA-4	The pump speed set point is correctly calculated and provided by the Low-power controller. However, it is not received by the Pump controller due to a failure in the connection between the Low-power controller and the Pump controller. As a result the water level in the reactor may be too low or too high [H-1,H-2].
Scenario-335	CA-4	The pump speed set point is correctly calculated and provided by the Low-power controller. However, it is misinterpreted by the Pump controller due to a malfunction in the Pump controller. As a result the water level in the reactor may be too low or too high [H-1,H-2].
Scenario-336	CA-4	The pump speed set point is correctly calculated and provided by the Low-power controller. However, it is misinterpreted by the Pump controller due to a software error in the Pump controller. As a result the water level in the reactor may be too low or too high [H-1,H-2].
Scenario-337	CA-5	The pump speed is controlled manually by the operator. However, it is not received by the Pump controller due to a failure in the connection between the operator and the Pump controller. As a result the water level in the reactor may be too low or too high [H-1,H-2].

Scenario-338	CA-5	The pump speed is controlled manually by the operator. However, it is not sent correctly to the Pump controller due to a failure in the physical control panel. As a result the water level in the reactor may be too low or too high [H-1,H-2].	
Scenario-339	CA-5	The pump speed is controlled manually by the operator. However, it is misinterpreted by the Pump controller due to a malfunction in the Pump controller. As a result the water level in the reactor may be too low or too high [H-1,H-2].	
Scenario-340	CA-5	The pump speed is controlled manually by the operator. However, it is misinterpreted by the Pump controller due to a software error in the Pump controller. As a result the water level in the reactor may be too low or too high [H-1,H-2].	
Scenario-341	CA-6	Pump controller provides the appropriate speed increase/decrease signal to the Feedwater pumps. However, failures in the physical pump actuators cause the pumps to not have the desired speed. As a result the water level in the reactor may be too low or too high [H-1,H-2].	Pump actuators
Scenario-342	CA-6	Pump controller provides the appropriate speed increase/decrease signal to the Feedwater pumps. However, failures in the connection between the Pump controller and the Pump actuators cause the Pump actuators to receive an incorrect signal or not receive the signal at all. As a result the water level in the reactor may be too low or too high [H-1,H-2].	
Scenario-343	CA-6	Pump controller provides the appropriate speed increase/decrease signal to the Feedwater pumps. However, failures in the mechanical coupling between the Pump actuators and the pumps can cause the pumps to not have the desired speed. As a result the water level in the reactor may be too low or too high [H-1,H-2].	
Scenario-344	CA-6	Pump controller provides the appropriate speed increase/decrease signal to the Feedwater pumps. However, one or more feedwater pumps fails. As a result the water level in the reactor may be too low [H-1].	Feedwater pump
Scenario-345	CA-7	The feedwater control valve set point is correctly calculated and provided by the Low-power controller. However, it is not received by the Feedwater control valve controller due to a failure in the connection between the Low-power controller and the Feedwater control valve controller. As a result the water level in the reactor may be too low or too high [H-1,H-2].	
Scenario-346	CA-7	The feedwater control valve set point is correctly calculated and provided by the Low-power controller. However, it is misinterpreted by the Feedwater control valve controller due to a malfunction in the Feedwater control valve controller. As a result the water level in the reactor may be too low or too high [H-1,H-2].	
Scenario-347	CA-7	The feedwater control valve set point is correctly calculated and provided by the Low-power controller. However, it is misinterpreted by the feedwater control valve controller due to a software error in the Feedwater control valve controller. As a result the water level in the reactor may be too low or too high [H-1,H-2].	
Scenario-348	CA-8	The open/close to the feedwater shutoff valve signal is correctly provided by the Low-power controller. However, it is not received by the Feedwater shutoff valve controller due to a failure in the connection between the Low-power controller and the Feedwater shutoff valve controller. As a result the water level in the reactor may be too low or too high [H-1,H-2].	
Scenario-349	CA-8	The open/close to the feedwater shutoff valve signal is correctly provided by the Low-power controller. However, it is misinterpreted by the Feedwater shutoff valve controller due to a malfunction in the Feedwater shutoff valve controller. As a result the water level in the reactor may be too low or too high [H-1,H-2].	
Scenario-350	CA-8	The open/close to the feedwater shutoff valve signal is correctly provided by the Low-power controller. However, it is misinterpreted by the Feedwater shutoff valve controller due to a software error in the Feedwater shutoff valve controller. As a result the water level in the reactor may be too low or too high [H-1,H-2].	
Scenario-351	CA-9	The recirculation control valve set point is correctly calculated and provided by the Low-power controller. However, it is not received by the Recirculation control valve controller due to a failure in the connection between the Low-power controller and the Recirculation control valve controller. As a result the water level in the reactor may be too low or too high [H-1,H-2].	
Scenario-352	CA-9	The recirculation control valve set point is correctly calculated and provided by the Low-power controller. However, it is misinterpreted by the Recirculation control valve controller due to a malfunction in the Recirculation control valve controller. As a result the water level in the reactor may be too low or too high [H-1,H-2].	
Scenario-353	CA-9	The recirculation control valve set point is correctly calculated and provided by the Low-power controller. However, it is misinterpreted by the recirculation control valve controller due to a software error in the Recirculation control valve controller. As a result the water level in the reactor may be too low or too high [H-1,H-2].	
Scenario-354	CA-10	The open/close to the recirculation shutoff valve signal is correctly provided by the Low-power controller. However, it is not received by the Recirculation shutoff valve controller due to a failure in the connection between the Low-power controller and the Recirculation shutoff valve controller. As a result the water level in the reactor may be too low or too high [H-1,H-2].	
Scenario-355	CA-10	The open/close to the recirculation shutoff valve signal is correctly provided by the Low-power controller. However, it is misinterpreted by the Recirculation shutoff valve controller due to a malfunction in the Recirculation shutoff valve controller. As a result the water level in the reactor may be too low or too high [H-1,H-2].	
Scenario-356	CA-10	The open/close to the recirculation shutoff valve signal is correctly provided by the Low-power controller. However, it is misinterpreted by the Recirculation shutoff valve controller due to a software error in the Recirculation shutoff valve controller. As a result the water level in the reactor may be too low or too high [H-1,H-2].	
Scenario-357	CA-11	The valve opening is controlled manually by the operator. However, it is not received by the Feedwater control valve controller due to a failure in the connection between the operator and the Feedwater control valve controller. As a result the water level in the reactor may be too low or too high [H-1,H-2].	
Scenario-358	CA-11	The valve opening is controlled manually by the operator. However, it is not sent correctly to the Feedwater control valve controller due to a failure in the physical control panel. As a result the water level in the reactor may be too low or too high [H-1,H-2].	
Scenario-359	CA-11	The valve opening is controlled manually by the operator. However, it is misinterpreted by the Feedwater control valve controller due to a malfunction in the Feedwater control valve controller. As a result the water level in the reactor may be too low or too high [H-1,H-2].	
Scenario-360	CA-11	The valve opening is controlled manually by the operator. However, it is misinterpreted by the Feedwater control valve controller due to a software error in the Feedwater control valve controller. As a result the water level in the reactor may be too low or too high [H-1,H-2].	

Scenario-361	CA-12	The valve opening is controlled manually by the operator. However, it is not received by the Recirculation control valve controller due to a failure in the connection between the operator and the Recirculation control valve controller. As a result the water level in the reactor may be too low or too high [H-1,H-2].	
Scenario-362	CA-12	The valve opening is controlled manually by the operator. However, it is not sent correctly to the Recirculation control valve controller due to a failure in the physical control panel. As a result the water level in the reactor may be too low or too high [H-1,H-2].	
Scenario-363	CA-12	The valve opening is controlled manually by the operator. However, it is misinterpreted by the Recirculation control valve controller due to a malfunction in the Recirculation control valve controller. As a result the water level in the reactor may be too low or too high [H-1,H-2].	
Scenario-364	CA-12	The valve opening is controlled manually by the operator. However, it is misinterpreted by the Recirculation control valve controller due to a software error in the Recirculation control valve controller. As a result the water level in the reactor may be too low or too high [H-1,H-2].	
Scenario-365	CA-13	The valve opening is controlled manually by the operator. However, it is not received by the Feedwater shutoff valve controller due to a failure in the connection between the operator and the Feedwater shutoff valve controller. As a result the water level in the reactor may be too low or too high [H-1,H-2].	
Scenario-366	CA-13	The valve opening is controlled manually by the operator. However, it is not sent correctly to the Feedwater shutoff valve controller due to a failure in the physical control panel. As a result the water level in the reactor may be too low or too high [H-1,H-2].	
Scenario-367	CA-13	The valve opening is controlled manually by the operator. However, it is misinterpreted by the Feedwater shutoff valve controller due to a malfunction in the Feedwater shutoff valve controller. As a result the water level in the reactor may be too low or too high [H-1,H-2].	
Scenario-368	CA-13	The valve opening is controlled manually by the operator. However, it is misinterpreted by the Feedwater shutoff valve controller due to a software error in the Feedwater shutoff valve controller. As a result the water level in the reactor may be too low or too high [H-1,H-2].	
Scenario-369	CA-14	The valve opening is controlled manually by the operator. However, it is not received by the Recirculation shutoff valve controller due to a failure in the connection between the operator and the Recirculation shutoff valve controller. As a result the water level in the reactor may be too low or too high [H-1,H-2].	
Scenario-370	CA-14	The valve opening is controlled manually by the operator. However, it is not sent correctly to the Recirculation shutoff valve controller due to a failure in the physical control panel. As a result the water level in the reactor may be too low or too high [H-1,H-2].	
Scenario-371	CA-14	The valve opening is controlled manually by the operator. However, it is misinterpreted by the Recirculation shutoff valve controller due to a malfunction in the Recirculation shutoff valve controller. As a result the water level in the reactor may be too low or too high [H-1,H-2].	
Scenario-372	CA-14	The valve opening is controlled manually by the operator. However, it is misinterpreted by the Recirculation shutoff valve controller due to a software error in the Recirculation shutoff valve controller. As a result the water level in the reactor may be too low or too high [H-1,H-2].	
Scenario-373	CA-15	The correct Open/Close signal is applies to the Feedwater control valve actuator by the Feedwater control valve controller. But due a failure in the Control valve actuator, the signal does not transfer to the Feedwater control valve. As a result the water level in the reactor may be too low or too high [H-1,H-2].	Control valve actuator
Scenario-374	CA-15	The correct Open/Close signal is applies to the Feedwater control valve actuator by the Feedwater control valve controller. However, failures in the connection between the Feedwater control valve controller and the Control valve actuator cause the Control valve actuator to receive an incorrect signal or not receive the signal at all. As a result the water level in the reactor may be too low or too high [H-1,H-2].	
Scenario-375	CA-15	The correct Open/Close signal is applies to the Feedwater control valve actuator by the Feedwater control valve controller. However, failures in the mechanical coupling between the Control valve actuator and the Feedwater control valve cause the Feedwater control valve to not open as desired. As a result the water level in the reactor may be too low or too high [H-1,H-2].	
Scenario-376	CA-15	The correct Open/Close signal is applies to the Feedwater control valve actuator by the Feedwater control valve controller. However, a failure in the physical Feedwater control valve cause the valves to not respond to the provided signals. As a result the water level in the reactor may be too low or too high [H-1,H-2].	Control valve
Scenario-377	CA-16	The correct Open/Close signal is applies to the Recirculation control valve actuator by the Recirculation control valve controller. But due a failure in the Control valve actuator, the signal does not transfer to the Recirculation control valve. As a result the water level in the reactor may be too low or too high [H-1,H-2].	Control valve actuator
Scenario-378	CA-16	The correct Open/Close signal is applies to the Recirculation control valve actuator by the Recirculation control valve controller. However, failures in the connection between the Recirculation control valve controller and the Control valve actuator cause the Control valve actuator to receive an incorrect signal or not receive the signal at all. As a result the water level in the reactor may be too low or too high [H-1,H-2].	
Scenario-379	CA-16	The correct Open/Close signal is applies to the Recirculation control valve actuator by the Recirculation control valve controller. However, failures in the mechanical coupling between the Control valve actuator and the Recirculation control valve cause the Recirculation control valve to not open as desired. As a result the water level in the reactor may be too low or too high [H-1,H-2].	
Scenario-380	CA-16	The correct Open/Close signal is applies to the Recirculation control valve actuator by the Recirculation control valve controller. However, a failure in the physical Recirculation control valve cause the valves to not respond to the provided signals. As a result the water level in the reactor may be too low or too high [H-1,H-2].	Control valve
Scenario-381	CA-17	The correct Open/Close signal is applies to the Feedwater shutoff valve actuator by the Feedwater shutoff valve controller. But due a failure in the shutoff valve actuator, the signal does not transfer to the Feedwater shutoff valve. As a result the water level in the reactor may be too low or too high [H-1,H-2].	Shutoff valve actuator
Scenario-382	CA-17	The correct Open/Close signal is applies to the Feedwater shutoff valve actuator by the Feedwater shutoff valve controller. However, failures in the connection between the Feedwater shutoff valve controller and the shutoff valve actuator cause the shutoff valve actuator to receive an incorrect signal or not receive the signal at all. As a result the water level in the reactor may be too low or too high [H-1,H-2].	

Scenario-383	CA-17	The correct Open/Close signal is applies to the Feedwater shutoff valve actuator by the Feedwater shutoff valve controller. However, failures in the mechanical coupling between the shutoff valve actuator and the Feedwater shutoff valve cause the Feedwater shutoff valve to not open as desired. As a result the water level in the reactor may be too low or too high [H-1,H-2].	
Scenario-384	CA-17	The correct Open/Close signal is applies to the Feedwater shutoff valve actuator by the Feedwater shutoff valve controller. However, a failure in the physical Feedwater shutoff valve cause the valves to not respond to the provided signals. As a result the water level in the reactor may be too low or too high [H-1,H-2].	Shutoff valve
Scenario-385	CA-18	The correct Open/Close signal is applies to the Recirculation shutoff valve actuator by the Recirculation shutoff valve controller. But due a failure in the shutoff valve actuator, the signal does not transfer to the Recirculation shutoff valve. As a result the water level in the reactor may be too low or too high [H-1,H-2].	Shutoff valve actuator
Scenario-386	CA-18	The correct Open/Close signal is applies to the Recirculation shutoff valve actuator by the Recirculation shutoff valve controller. However, failures in the connection between the Recirculation shutoff valve controller and the shutoff valve actuator cause the shutoff valve actuator to receive an incorrect signal or not receive the signal at all. As a result the water level in the reactor may be too low or too high [H-1,H-2].	
Scenario-387	CA-18	The correct Open/Close signal is applies to the Recirculation shutoff valve actuator by the Recirculation shutoff valve controller. However, failures in the mechanical coupling between the shutoff valve actuator and the Recirculation shutoff valve cause the Recirculation shutoff valve to not open as desired. As a result the water level in the reactor may be too low or too high [H-1,H-2].	
Scenario-388	CA-18	The correct Open/Close signal is applies to the Recirculation shutoff valve actuator by the Recirculation shutoff valve controller. However, a failure in the physical Recirculation shutoff valve cause the valves to not respond to the provided signals. As a result the water level in the reactor may be too low or too high [H-1,H-2].	Shutoff valve
Scenario-389	Feedwater flow (Feedback)	Failure in the connection between the flow sensor and the controller. Invalid/Out of range inputs provided by the sensor being misinterpreted by the controller. Issues with the physical flow sensor.	Flow sensor
Scenario-390	Steam flow (Control input)	Failure in the steam line and the system it belongs to. Failure in the connection between the steam flow sensor and the master controller. Issues with the physical flow sensor.	Flow sensor
Scenario-391	Flow sensor (System element)	Failure in the physical flow sensor. Flow sensor is out of power. Flow sensor provides wrong signal due to calibration and tuning errors. Flow sensor is installed at inappropriate location. Flow sensor is tampered with during maintenance.	-
Scenario-392	Reactor water level measurement (Feedback)	Failure in the connection between the level sensor and the controller. Invalid/Out of range inputs provided by the sensor being misinterpreted by the controller. At least one of the sensors provides a wrong water level signal causing the average to be incorrect. Issues with the physical level sensor.	Water level sensor
Scenario-393	Water level sensor (System element)	Failure in the Physical water level sensor. Water level sensor is out of power. Water level sensor is installed at inappropriate position. Water level sensor is not calibrated or tuned properly. Water level sensor is tampered with during maintenance.	-
Scenario-394	Actuator position (Feedback)	Failure in the connection between the position sensor and the controller. Invalid/Out of range inputs provided by the sensor being misinterpreted by the controller. Issues with the physical position sensor.	Position sensor
Scenario-395	Actuator speed (Feedback)	Failure in the connection between the speed sensor (tachometer) and the controller. Invalid/Out of range inputs provided by the sensor being misinterpreted by the controller. Issues with the physical speed sensor (tachometer).	Tachometer
Scenario-396	Actual pump speed (Feedback)	Failure in the connection between the speed sensor (tachometer) and the controller. Invalid/Out of range inputs provided by the sensor being misinterpreted by the controller. Issues with the physical speed sensor (tachometer).	Tachometer
Scenario-397	Tachometer (System element)	Failure in the physical tachometer. Tachometer is out of power. Tachometer provides wrong signal due to calibration and tuning errors. Tachometer is installed at inappropriate location. Tachometer is tampered with during maintenance.	-

Scenario-398	Position Sensor (System elements)	<p>Failure in the Physical position sensor.</p> <p>Position sensor is out of power.</p> <p>Position sensor is installed at inappropriate position.</p> <p>Position sensor is not calibrated or tuned properly.</p> <p>Position sensor is tampered with during maintenance.</p>	-
Scenario-399	Actual valve position (Feedback)	<p>Failure in the connection between the position sensor and the controller.</p> <p>Invalid/Out of range inputs provided by the sensor being misinterpreted by the controller.</p> <p>Issues with the physical position sensor.</p>	Position sensor
Scenario-400	Pump Actuators (System elements)	<p>Mechanical Failures in the pump actuators.</p> <p>Errors made during maintenance and repair.</p> <p>Failure of power supply to the actuator.</p>	
Scenario-401	Feedwater pump (System element)	<p>Failure in the physical pump.</p> <p>Errors made during maintenance and repair.</p> <p>Failure of power supply to the actuator.</p>	
Scenario-402	Control valve actuator (System element)	<p>Mechanical Failures in the Control valve actuators.</p> <p>Errors made during maintenance and repair.</p> <p>Failure of power supply to the actuator.</p>	
Scenario-403	Shutoff valve actuator (System element)	<p>Mechanical Failures in the Shutoff valve actuators.</p> <p>Errors made during maintenance and repair.</p> <p>Failure of power supply to the actuator.</p>	
Scenario-404	Control valve (System element)	<p>Mechanical failures in the valves.</p> <p>Errors made during maintenance and repair.</p>	
Scenario-405	Shutoff valve (System element)	<p>Mechanical failures in the valves.</p> <p>Errors made during maintenance and repair.</p>	