Lappeenranta-Lahti University of Technology LUT
LUT School of Energy Systems
Degree Programme in Energy Technology
Master's thesis

Mikko Turunen

OVERALL SAFETY OF SMALL MODULAR REACTORS

Examiner: Professor, D.Sc. (Tech.) Juhani Hyvärinen
Supervisor: D.Sc. (Tech.) Juhani Vihavainen
Lappeenranta 2.12.2020

ABSTRACT

Lappeenranta-Lahti University of Technology LUT
LUT School of Energy Systems
Degree Programme in Energy Technology

Mikko Turunen

Overall safety of small modular reactors

Master's thesis
2020
87 pages, 17 figures and 16 tables

Examiner: Professor, D.Sc. (Tech.) Juhani Hyvärinen
Supervisors: Professor, D.Sc. (Tech.) Juhani Hyvärinen
D.Sc. (Tech.) Juhani Vihavainen

Keywords: overall safety, defence-in-depth, front-line safety systems, SMR, nuclear

Overall safety and Small Modular Reactors are currently topical subjects in the Finnish nuclear safety community as overall safety is still little researched and SMR designs are currently being developed. In this master's thesis, the safety systems of U.S. EPR and NuScale are studied and compared with each other by researching their Design Control Documents. The objective is to create a comprehensive framework for the overall safety of SMRs from a functional Defence-in-Depth point of view.

Instead of five diverse safety systems for each individual level of defence, the same safety systems often provide safety-related functions on multiple different levels either during Operational States or Accident Conditions. Some systems provide safety-related functions on multiple different levels regardless of plant state, and some systems have two different main safety functions.

In addition, SMRs require fewer components and they utilize more passive features in their design to protect the reactor core than traditional nuclear power plants. This leads to the safety systems in SMRs being functionally less dependent on other safety and support systems to achieve their safety functions than in Light Water Reactors.

TIIVISTELMÄ

Lappeenrannan-Lahden teknillinen yliopisto LUT
LUT School of Energy Systems
Energiatekniikan koulutusohjelma

Mikko Turunen

Pienten modulaaristen reaktorien kokonaisturvallisuus

Diplomityö
2020
87 sivua, 17 kuvaa ja 16 taulukkoa

Tarkastaja: Professori, TkT Juhani Hyvärinen
Ohjaajat: Professori, TkT Juhani Hyvärinen
TkT Juhani Vihavainen

Hakusanat: kokonaisturvallisuus, syvyyspuolustus, turvallisuusjärjestelmät, pienreaktori

Kokonaisturvallisuus ja pienreaktorit ovat ajankohtaisia aiheita suomalaisessa ydinturvallisuusyhteisössä, sillä kokonaisturvallisuus on vielä toistaiseksi vähän tutkittu aihealue ja pienreaktorien kehitys etenee kovaa vauhtia. Tässä diplomityössä U.S. EPR:n ja NuScalen turvallisuusjärjestelmiä tutkitaan ja vertaillaan keskenään niiden turvallisuusselosteista löytyvien tietojen perusteella. Tavoitteena on luoda kokonaisvaltainen kuva pienreaktorien kokonaisturvallisuudesta toiminnallisen syvyyspuolustuksen näkökulmasta.

Sen sijaan, että jokaisella viidellä puolustustasolla olisi erillinen turvallisuusjärjestelmä, samoja järjestelmiä hyödynnetään usein monella eri puolustustasolla joko laitoksen käyttötilojen tai onnettomuuksien aikana. Joitakin järjestelmiä hyödynnetään kuitenkin useammalla eri puolustustasolla riippumatta laitoksen tilasta, ja joitakin järjestelmiä useamman eri pääturvallisuustoiminnon toteuttamiseen.

Pienreaktorit tarvitsevat vähemmän turvallisuusjärjestelmiä ja ne hyödyntävät enemmän passiivisia toimintoja takaamaan reaktorisydämen turvallisuuden kuin perinteiset isot ydinvoimalaitokset. Tämä tekee niiden turvallisuusjärjestelmistä myös toiminnallisesti riippumattomampia muista turvallisuus- ja tukijärjestelmistä kuin kevytvesireaktoreissa.

ACKNOWLEDGEMENTS

This master's thesis was written as part of the Nuclear Engineering department at LUT University. I want to express my gratitude to my supervisors Juhani Hyvärinen and Juhani Vihavainen for offering me the possibility to work on this master's thesis subject during this challenging year of 2020. The expertise and guidance of Juhani Hyvärinen helped me get through all the troubles I faced in my master's thesis. I also want to thank everyone responsible for all the fascinating courses and lectures that have been invaluable to me throughout my Nuclear Engineering studies.

Finally, I want to thank the people with whom I have spent time, had memorable conversations and drank numerous cups of coffee at the guild room of our student organization Armatuuri ry during my university years. I am especially grateful to Annamaria Tielinen and Tiia Heino for their endless support, encouragement, and friendship through thick and thin. You have had quite an impact on me, and I hope it was for the better. And even though these years have so far been the best of my life and I will always look back at them fondly, I am also ready to close this chapter of my life and start a new one.

Mikko Turunen
2nd December 2020
Lappeenranta, Finland

TABLE OF CONTENTS

LIST OF SYMBOLS AND ABBREVIATIONS

Subscripts

e	Electrical
th	Thermal

Abbreviations

12UPS	Non-Class 1E 12-hour Uninterruptible Power Supply System
AAPS	Auxiliary AC Power Source
ADAMS	Agencywide Documents Access and Management System
AOO	Anticipated Operational Occurrences
ATWS	Anticipated Transients Without Scram
BDBE	Beyond Design Basis Event
BDG	Backup Diesel Generator
BOL	Beginning-Of-Life
BPSS	Backup Power Supply System
CBVS	Containment Building Ventilation System
CCWS	Component Cooling Water System
CDF	Core Damage Frequency
CFDS	Containment Flooding and Drain System
CGCS	Combustible Gas Control System
CHRS	Control Room Habitability System
CIS	Containment Isolation System
CIV	Containment Isolation Valves
CMSS	Core Melt Stabilization System
CNV	Containment Vessel
CRA	Control Rod Assembly
CRACS	Main Control Room Air Conditioning System
CRDS	Control Rod Drive System
CRE	Control Room Envelope
CRVS	Control Room Ventilation System
CVCS	Chemical and Volume Control System

CWS	Circulating Water System
DBA	Design Basis Accident
DBE	Design Basis Event
DCA	Design Certification Application
DCD	Design Control Document
DEC	Design Extension Condition
DHRS	Decay Heat Removal System
DiD	Defence-in-Depth
EBS	Extra Borating System
ECCS	Emergency Core Cooling System
EDG	Emergency Diesel Generator
EDSS	Highly Reliable Direct Current Power System
EDSS-C	EDSS-Common
EDSS-MS	EDSS-Module Specific
EFWS	Emergency Feedwater System
EPGBVS	Emergency Power Generating Building Ventilation System
EPR	Evolutionary Pressurized Reactor
EPSS	Class 1E Emergency Power Supply System
ESF	Engineered Safety Feature
ESWPBVS	Essential Service Water Pump Building Ventilation System
ESWS	Essential Service Water System
EUPS	Class 1E Uninterruptible Power Supply System
FSAR	Final Safety Analysis Report
FSER	Final Safety Evaluation Report
FWIV	Feedwater Isolation Valve
Gd_2O_3	Gadolinia
HMI	Human-Machine Interface
HPME	High Pressure Melt Ejection
I&C	Instrumentation and Control
IAEA	International Atomic Energy Agency
ICIS	In-Core Instrumentation System

IE	Infrequent Event
iPWR	Integral Pressurized Water Reactor
IRWST	In-containment Refueling Water Storage Tank
LHSI	Low Head Safety Injection
LOCA	Loss-Of-Coolant Accident
LOOP	Loss Of Offsite Power
LTC	Long-Term Cooling
LWR	Light Water Reactor
MCP	Main Coolant Pump
MCR	Main Control Room
MFWS	Main Feedwater System
MHSI	Medium Head Safety Injection
MM-CDF	Multi-Module Core Damage Frequency
MPS	Module Protection System
MSIV	Main Steam Isolation Valve
MSLB	Main Steam Line Break
MSRT	Main Steam Relief Train
MSSS	Main Steam Supply System
MSSV	Main Steam System Valve
MTC	Moderator Temperature Coefficient
“N/A”	Not Applicable
NO	Normal Operation
NPM	NuScale Power Module
NPSS	Normal Power Supply System
ORSAC	Overall safety conceptual framework
OSAFE	Development of Framework for justification of Overall Safety
PACS	Priority Actuation and Control System
PAS	Process Automation System
PDS	Primary Depressurization System
PDSV	Primary Depressurization System Valves
PPS	Preferred Power System

PRA	Probabilistic Risk Assessment
PRT	Pressurizer Relief Tank
PS	Protection System
PSCIV	Primary System Containment Isolation Valve
PSRV	Pressurizer Safety Relief Valves
PWR	Pressurized Water Reactor
RBVS	Reactor Building Ventilation System
RCB	Reactor Containment Building
RCCA	Rod Cluster Control Assembly
RCCWS	Reactor Component Cooling Water System
RCP	Reactor Coolant Pump
RCPB	Reactor Coolant Pressure Boundary
RCS	Reactor Coolant System
RCSL	Reactor Control, Surveillance and Limitation
RHRS	Residual Heat Removal System
RPV	Reactor Pressure Vessel
RRV	Reactor Recirculation Valve
RSB	Reactor Shield Building
RSV	Reactor Safety Valve
RVV	Reactor Vent Valve
SAFIR2022	Safety of Nuclear Power Plants – Finnish National Research Programme 2022
SAHRS	Severe Accident Heat Removal System
SA I&C	Severe Accident Instrumentation and Control
SAM	Severe Accident Management
SAS	Safety Automation System
SBO	Station Blackout
SBODG	Station Blackout Diesel Generator
SBORVS	Station Blackout Room Ventilation System
SBVS	Safeguard Building Controlled-Area Ventilation System
SBVSE	Electrical Division of Safeguard Building Ventilation System

SCWS	Site Cooling Water System
SFP	Spent Fuel Pool
SG	Steam Generator
SGTR	Steam Generator Tube Rupture
SICS	Safety Information and Control System
SIS	Safety Injection System
SIS/RHR	Safety Injection System/Residual Heat Removal
SMR	Small Modular Reactor
SRS	Safety Report Series
SSCIV	Secondary System Containment Isolation Valve
STUK	Radiation and Nuclear Safety Authority in Finland
TG	Turbine Generator
TG I&C	Turbine Generator Instrumentation and Control
UHS	Ultimate Heat Sink
UO_2	Uranium dioxide
U.S. EPR	United States Evolutionary Pressurized Reactor
U.S. NRC	United States Nuclear Regulatory Commission
YVL	Regulatory Guides on Nuclear Safety

1 INTRODUCTION

The concept of "overall safety" has been discussed in the nuclear safety community since around 2015. An early proposal for the framework of overall safety can be seen in Figure 1.1 below. The pivotal parts seen in Figure 1.1 are Security, Safety, and Safeguards, which are complemented by Society and Sustainability.

Nuclear "Safety" always boils down to means to limit dispersion of radioactive materials – therefore the overall safety shown in Figure 1.1 covers radioactive materials in the reactor core, in fresh fuel, in spent fuel, and associated waste management. "Security" covers all items associated with the prevention of unlawful activities and actions that could endanger the safety or integrity of a nuclear plant or nuclear materials. "Safeguards" refers to the various activities implemented to ensure nuclear materials and knowledge are only used for peaceful purposes. (Hyvärinen 2018, p. 6, 14, 17–19).

The threat behind "Safety" is seen as releases from within the plant as a result of internal initial events or hazards, while the threat for "Security" and "Safeguards" involves intrusion from outside of the plant. "Sustainability" is an issue of profitability and the impact on natural resources and the environment. And finally, there are diverse and often ill-defined expectations from "Society". It is the interaction, the synergies, and contradictions between different S's that motivate the development and study of the framework of overall safety. (Hyvärinen 2018, p. 6, 14, 17–19).

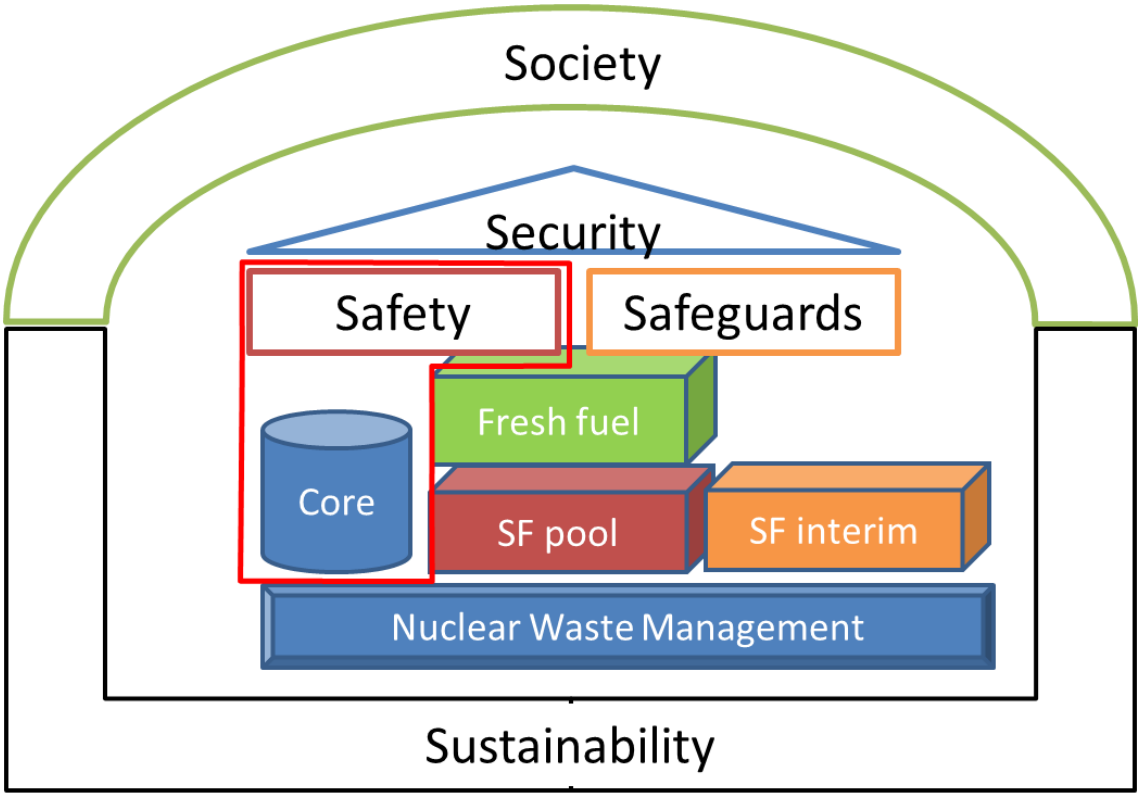

Figure 1.1. The scope of overall safety for this master's thesis (Edited from Hyvärinen 2018, p. 18). The focus of this thesis – the safety of materials in the reactor core – is indicated by the red outline.

Because overall safety is such a large entity, the scope of this master's thesis is defined to be about the technical side of the overall safety, composed of only the Safety and the Core as indicated by the red outline in Figure 1.1. Fuel management, Spent Fuel Pool (SFP), Spent Fuel interim and nuclear waste management are excluded from consideration. Only systems and components related to the operation of the plant safety are considered.

From the design point of view, overall safety is ultimately based on Defence-in-Depth (DiD) principle, which is applied as a functional concept and as a barrier concept. To achieve their safety objectives, functional DiD is implemented as successive, redundant safety functions and barrier DiD is implemented as successive, redundant safety barriers

(Hyvärinen 2018, p. 7). The concept of overall safety and DiD in the scope of this master's thesis are further discussed in Chapter 2.

The overall safety from the design point of view for Small Modular Reactors (SMRs) is studied by researching and comparing front-line safety systems of two different nuclear power plant designs. The first facility is a traditional, high power Light Water Reactor (LWR) called United States Evolutionary Pressurized Reactor (U.S. EPR). It operates with proven technology, which means that it serves as a useful reference for the overall safety of SMRs. The second facility is an integral Pressurized Water Reactor (iPWR) called NuScale. It is the first SMR design ever to have been issued a Final Safety Evaluation Report (FSER) by the United States Nuclear Regulatory Commission (U.S. NRC) to mark approval for its Design Certification Application (DCA) (U.S. NRC 2020b). These two facilities are further discussed in Chapter 3.

The front-line safety systems are researched from the Final Safety Analysis Report (FSAR) documents provided by Areva NP, Inc for U.S. EPR and from the DCA documents provided by NuScale Power, LLC. for NuScale. They are studied in Chapter 4. The comparison is greatly facilitated by the fact that both plants have been designed to the same set of regulatory requirements by U.S. NRC, and both documents have been structured according to Regulatory Guide 1.206 (Areva NP, Inc. 2013a, p. 1.1-2; NuScale Power, LLC. 2020a, p. 1.1-2).

NuScale implements new safety features, such as passive decay heat removal and containment heat removal systems to provide Long-Term Cooling (LTC) in its design. By implementing passive features, it requires less safety-related components and power systems as opposed to traditional power plants. As part of the overall safety research, the safety systems of both U.S. EPR and NuScale are studied from the functional DiD point of view in Chapter 5.

The safety systems between these two facilities are compared in Chapter 6 to find out what safety systems found in U.S. EPR design are not implemented in NuScale design. Chapter 7 focuses on observations of functionalities, where the similarities and

differences between safety systems implemented in both facilities are studied. Finally, the main findings are concluded in Chapter 8.

This master's thesis is a part of the Overall safety conceptual framework (ORSAC) project carried out by LUT Nuclear Engineering, which is funded by the Development of Framework for justification of Overall Safety (OSAFE) project. OSAFE is one of the research projects in a national Safety of Nuclear Power Plants – Finnish National Research Programme 2022 (SAFIR2022). The objective of SAFIR2022 is "to ensure that should new matters related to the safe use of nuclear power plants arise, the authorities possess sufficient technical expertise and other competence required for rapidly determining the significance of the matters." (Hämäläinen & Suolanen 2020, p. 4). This justifies researching the overall safety of SMRs in this master's thesis, as SMR designs are currently being developed and will be of interest for the Finnish nuclear safety community as well in the future.

2 CONCEPT OF OVERALL SAFETY

In their ORSAC report, Hyvärinen et al. (2016) proposed an overall safety concept based on the functional Defence-in-Depth principle developed by International Atomic Energy Agency (IAEA) presented in Figure 2.1 below.

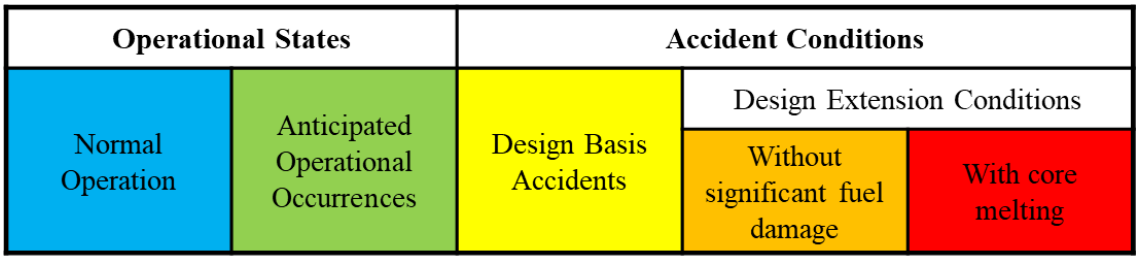

Figure 2.1. Functional Defence-in-Depth concept developed by IAEA (Edited from Hyvärinen et al. 2016, p. 32). Initial events, actual or hypothetical, are allocated into different "states" or "conditions" according to their estimated frequency of occurrence.

Normal Operation (NO) and Anticipated Operational Occurrences (AOOs) are defined as Operational States, while Design Basis Accidents (DBAs) and Design Extension Conditions (DECs) without significant fuel degradation and with core melting are defined as Accident Conditions. An AOO is expected to occur at least once during a plant lifetime and a limiting frequency of $< 10^{-2}$/a for AOOs seems to be universally accepted, so that frequency limit is used to separate Operational States and Accident Conditions. Core Damage Frequency (CDF) is another significant frequency limit separating accidents without or with core melt from each other, but there aren't any universally accepted criteria for it. U.S. NRC defines the limit for CDF to be $< 10^{-4}$/a (Nuclear Energy Agency 2007, p. 170). This master's thesis is focused on two reactor designs from the United States. and because U.S. NRC is the governing authority for reactors designed there, their criteria for CDF is applied.

In addition to the functional concept, DiD can be applied as a barrier concept, where consecutive barriers enclose radioactive materials and failure of any one barrier will not lead to release because other barriers will continue to retain the radioactivity.

Theoretically, the barriers should be mutually independent, but Hyvärinen et al. (2016) note that in practice, barrier independence is imperfect as shown in Figure 2.2 below (Hyvärinen et al. 2016, p. 31). Reactor systems are connected to the outside of the containment structure, which violates containment isolation.

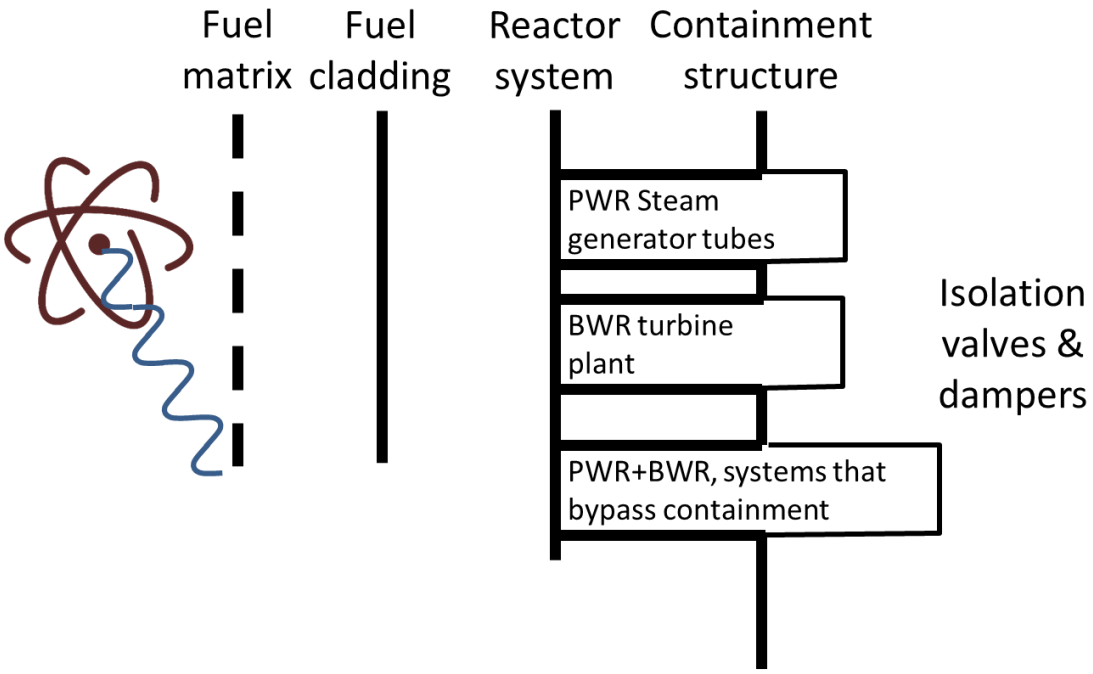

Figure 2.2. Structural barrier Defence-in-Depth concept (Hyvärinen et al. 2016, p. 31). Theoretical independence of the barriers is not feasible in practice.

The containment function depends on the capability of the safety valves of the Steam Generator (SGs) for staying closed and leak-tight when expected, as they must be connected outside of the Steam Generator for overpressure protection. When developing their overall safety concept, Hyvärinen et al. (2016) recognize that the performance of the safety barriers depends on the severity of the physical damage done to them. The barriers will be subjected to different amounts of physical load, and if the load exceeds the failure threshold, a failure occurs with some statistical uncertainty. However, the barrier can be damaged before that, without even experiencing a failure. Safety margins are put in place to account for statistical uncertainty and keep the load below the failure threshold.

(Hyvärinen et al. 2016, p. 51–53). In their Safety Report Series (SRS), IAEA has studied in detail what are the typical loads for different levels of defence for LWRs and how are they mitigated. Hyvärinen et al. (2016) composed the following Figure 2.3 from there.

<table>
<tr><td>Load</td><td>Equipment failure</td><td>Minor transients</td><td>Random failures, Hazards</td><td>Common Mode Failures</td><td>Fuel and reactor system failed</td></tr>
<tr><td rowspan="2">Level, Functional Barrier</td><td rowspan="2">1
Normal Operation, High quality & procedures</td><td rowspan="2">2
Anticipated Operational Occurrences, Surveillance & limitation</td><td rowspan="2">3
Design Basis Accidents, Engineered Safety Features</td><td colspan="2">4
Design Extension Conditions</td></tr>
<tr><td>Without significant fuel degradation</td><td>With core melting, SAM features</td></tr>
<tr><td>Mitigation</td><td>Proven technology</td><td>Safety margins</td><td>Redundancy, separation</td><td>Diversity</td><td>Independence of systems</td></tr>
</table>

Figure 2.3. Typical loads, barriers, and mitigation features combined with the functional Defence-in-Depth levels (Edited from Hyvärinen et al. 2016, p. 54).

For the first two levels of defence, organizational procedures are the safety barriers against single equipment failures and minor transients. The organization is responsible for implementing high standards and means to ensure high quality and procedures of work with proven technology. Process parameters are surveilled and if needed, limited to keep the parameters within acceptable safety margins.

For the third level of defence, the typical loads are random failures and hazards. Engineered Safety Feature (ESF) systems usually consist of containment systems, emergency core cooling systems, habitability systems, and fission product removal and control systems. Many of the front-line safety systems fall under these categories. Their safety-related functions are protected with redundancy, which is often managed with backup or fail-safe systems. Physical separation of components protects the system from hazards, such as fires, destroying more a single component.

Typical loads for the fourth level of defence are common cause failures, which can be mitigated with diverse components to prevent associated subsystems from failing for the same reasons. And when it comes to the fifth level of defence and core melt accidents, the typical load is fuel and reactor system failure. Severe Accident Management (SAM) features consist of independent safety systems designed to prevent and mitigate the radiological consequences. The independence of these safety systems in SAM cannot be neglected. As discussed earlier, safety systems from previous levels of defence can be used to prevent and mitigate the consequences of severe accidents, if it doesn't interfere with their primary functions.

To protect the confinement of radioactive materials and containment isolation, the functional DiD concept implements three main safety functions to minimize the damage to the structural barriers, presented in Table 2.1 below. (Hyvärinen et al. 2016, p. 31).

Table 2.1. The front-line safety systems must achieve three main safety functions for the safe operation of a nuclear power plant (Hyvärinen et al. 2016, p. 31). Accident Conditions are a result of failure to achieve one or more of these safety functions.

"1. control of reactor power; this often translates to capability to shut the reactor down and subsequently maintain subcriticality"
"2. (fuel) heat removal, or maintenance of cooling that is proportionate to the reactor power (the fuel may be capable of withstanding momentary overheating)"
"3. confinement of radioactive materials inside closed systems, or capability to isolate the containment, maintain it leak-tight, and also prevent leakages from process systems carrying radioactive materials. Severe Accident Management, measures aim ensure containment and confinement integrity in a core melt accident. Such measures include reactor coolant system depressurization, preventing high-pressure melt ejection and also protecting the steam generator tubes, hydrogen management, preventing detonation loads, and containment cooling, mitigating slow pressurization."

When these main safety functions are implemented as active systems, power supply and room cooling are required to keep them operating, which leads to main support functions presented in Table 2.2 below (Hyvärinen et al. 2016, p. 31–32). Some recent passive plant design, both large and SMR, implement safety systems designed to operate without external power supply, but in almost all cases, some form of (temporary) power supply will be needed to initiate the safety functions. For instance, Instrumentation & Control (I&C) powered by a battery-backed DC power supply to detect process conditions that require triggering a function; and often also small valve operations.

Table 2.2. Two main support functions must be achieved to support the operation of the front-line safety systems (Hyvärinen et al. 2016, p. 31–32).

"4. emergency power supply, to power safety features of the plant, including control room"
"5. heating, ventilation and cooling (HVAC), to maintain operating conditions in safety equipment rooms."

The overall safety concept proposed by Hyvärinen et al. (2016) is based on combining the main safety functions, the main support functions and the functional Defence-in-Depth concept developed by IAEA together to create Figure 2.4 below.

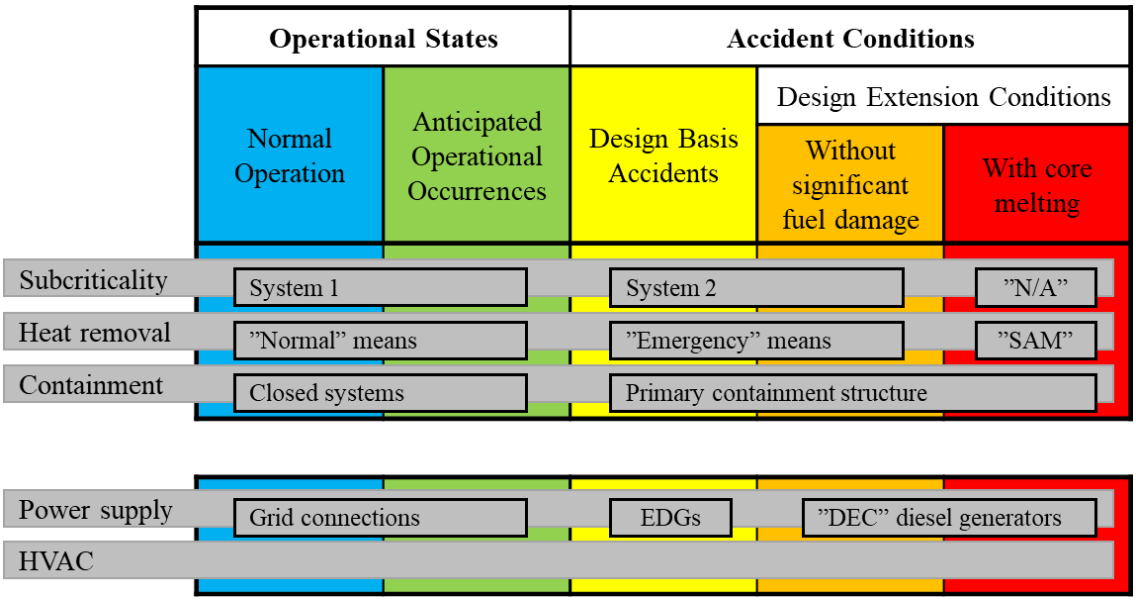

Figure 2.4. Main safety functions and main support functions combined with the functional Defence-in-Depth concept (Edited from Hyvärinen et al. 2016, p. 38). This creates a template on which different plant systems can be placed.

Figure 2.4 can be viewed as a 5x5 matrix, where three rows are dedicated to the front-line safety systems and two rows for their supporting systems. The levels of defence from the functional DiD concept are on their respective columns. Power plant systems and components designed to fulfil the main safety functions and main support functions for each level of defence can then be placed into the matrix. It is in the scope of this master's thesis to study the front-line safety systems and their supporting systems of U.S. EPR and Nuscale and then place them into the template presented in Figure 2.4. This is done in Chapters 4 and 5.

This template is not only limited to safety and support systems. For instance, plant control and protection systems can be placed on this template as well. To demonstrate, I&C systems for U.S. EPR design are placed on this template in Figure 2.5 below.

Operational States		Accident Conditions		
Normal Operation	Anticipated Operational Occurrences	Design Basis Accidents	Design Extension Conditions	
			Without significant fuel damage	With core melting
PAS		SAS		
TG I&C	RCSL	PS		SA I&C

Figure 2.5. The I&C systems of U.S. EPR. Interdependency between different I&C systems comes from Priority Actuation and Control System (PACS).

In U.S. EPR design, Instrumentation and Control architecture is divided into three levels. Level 0 is the process interface, which consists of actuators, sensors and signal processing equipment. They send out the signals to level 1, which is system-level automation. The safety-related functions are performed in level 1, and their interfaces are provided within level 2, the supervisory control. This means Human-Machine Interface (HMI). The level 1 systems are presented in Table 2.3 below.

Table 2.3. U.S. EPR Level 1 Instrumentation and Control systems.

Process Automation System (PAS)
Safety Automation System (SAS)
Turbine Generator Instrumentation and Control (TG I&C)
Reactor Control, Surveillance and Limitation (RCSL)
Protection System (PS)
Severe Accident Instrumentation and Control (SA I&C)
Priority Actuation and Control System (PACS)

Process Automation System (PAS) and Turbine Generator Instrumentation and Control (TG I&C) operate during NO, and Reactor Control, Surveillance and Limitation (RCSL)

system during AOOs. Protection System (PS) and Safety Automation System (SAS) operate during DBAs. Severe Accident Instrumentation and Control (SA I&C) is designed to function during worst-case scenarios. All of these automation systems want to control the plant safety systems during the different Operational States and Accident Conditions, which means that they send actuation commands to individual components through a Priority Actuation and Control System (PACS). The function of PACS is to prioritize these requests, and then drive the actuation of the safety system components. PACS receives signals from PS, SAS, Safety Information and Control System (SICS) and SA I&C. SICS is used as a backup HMI for the operators. (Areva NP, Inc. 2007, p. 2-2–2-6). Plant control and protection systems will not be discussed further as they are beyond the scope of this master's thesis, but it is evident that the functionalities of (main) automation systems can be allocated on the functional DiD levels of defence. Complexity becomes obvious only once when one follows how the process system implements the commands from the I&C.

In theory, there should be five different safety systems for each main safety function, one for each level of defence in the template as presented in Figure 2.4. In practice, this is often not the case; in contrast, the same equipment is credited on multiple levels of defence. In the Regulatory Guides on Nuclear Safety (YVL) Guide B.1 by the Radiation and Nuclear Safety Authority in Finland (STUK), independence of the Defence-in-Depth levels is recognized as imperfect as shown in Table 2.4 below.

Table 2.4. Independence of the Defence-in-Depth levels as defined in the YVL Guide B.1 (STUK 2019, p. 20).

"425. …the levels of defence required under the defence-in-depth principle shall be as independent of one another *as is reasonably achievable*."
"426. Independence between the levels of defence shall be based on the *adequate application* of functional isolation, the diversity principle and physical separation."
"428. The systems, structures and components required for each postulated initiating event shall be identified, and it shall be shown by means of deterministic analyses that the systems, structures and components required for implementing any one level of defence in depth are *sufficiently independent* from the other levels. The adequacy of the achieved independence shall also be judged by probabilistic analyses."
"429. The systems required for implementing different levels of defence according to the defence-in-depth principle shall be functionally isolated from one another, in such a way that a failure on one level shall not prevent the implementation of necessary functions at other levels of defence."
"431. The systems intended for reaching and maintaining a controlled state in severe reactor accidents (level 4 of the defence in depth concept) shall be functionally and physically separated from the systems intended for normal operation and anticipated operational occurrences and for controlling postulated accidents and design extension conditions (levels 1, 2, 3a and 3b). The defence-in-depth level 4 systems intended for controlling severe reactor accidents may, for sound reasons, also be used for preventing severe core damage in design extension conditions provided that this will not undermine the ability of the systems to perform their primary function in case the conditions evolve into a severe reactor accident."

As can be seen from Table 2.4, it is clearly stated that the levels of defence must be "as independent as is reasonably achieved", the safety systems for each level of defence must

be “sufficiently independent from other levels” and that a failure on one level of defence cannot prevent the other levels from implementing their safety functions in the Finnish regulations. This allows the same front-line safety system to be used on multiple levels of defence, given that a possible failure on a lower safety class cannot prevent the primary safety function from being achieved. The wording “as is reasonably achievable” and “sufficiently independent” allow for some acceptable margin of operation. This is often achieved with redundant trains or additional front-line safety systems for the levels that share safety systems between multiple levels of defence. U.S. NRC implements similar reasoning as STUK for safety system independency with acceptable margins of operation. Implementing same safety systems on multiple levels of defence are in the scope of this master’s thesis and they are studied for U.S. EPR and NuScale in Chapter 4.

Emergency power systems can be viewed as an example of this. As can be seen from Figure 2.4, the power to the safety systems is supplied through a transmission grid or from the generator house load during NO and AOOs. Emergency Diesel Generators (EDGs) are the primary source of electricity during DBAs when offsite power can’t be guaranteed. If the power supply from EDGs is lost during DECs, Station Blackout Diesel Generators (SBODGs) are the last line of defence during severe accidents. As Hyvärinen et al. (2016) point out, this is in clear violation of the independence principle. However, as shown in Table 2.4, item 431. from YVL Guide B.1 allows EDGs to supply power to the safety systems during severe accidents in case the power supply from SBODGs is lost if it doesn’t interfere with their primary function. (Hyvärinen et al. 2016, p. 44).

3 FACILITIES IN COMPARISON

In this master's thesis, front-line safety systems of two different nuclear power plants are studied and compared to get a better understanding of the overall safety for Small Modular Reactors. The first facility is an Evolutionary Pressurized Reactor (EPR) designed by Areva NP, Inc. It is a four-loop plant with a rated thermal output of 4590 MW_{th} and electric output of 1600 MW_e (Areva NP, Inc. 2013b, p. 1.1-1, 1.2-1). In 2020, two EPRs Taishan 1 and 2 in China are already in commercial operation and four more EPRs are under construction: Olkiluoto 3 in Finland, Flamanville 3 in France, and Hinkley Point C 1 and C 2 in the United Kingdom. However, the application status for the U.S. EPR plant is currently suspended (U.S. NRC 2020a).

The second facility studied in this master's thesis is NuScale, which is a Pressurized Water Reactor (PWR) with an integrated primary circuit designed by NuScale Power, LLC. Each NuScale Power Module (NPM) can produce a rated thermal output of 160 MW_{th} and electric output of 50 MW_e, and a NuScale power plant consists of from one to 12 NuScale SMRs (NuScale Power, LLC. 2020a, p. 1.1-2). During this master's thesis in August 2020, U.S. NRC issued an FSER for NuScale, meaning that their review of its DCA was completed (U.S. NRC 2020b). The first NuScale power plant is expected to begin construction in the mid-2020s.

Because U.S. NRC is the governing authority for both NuScale and U.S. EPR, they are designed through the same set of regulatory requirements. In addition, the majority of the technical details are public and available online from Agencywide Documents Access and Management System (ADAMS), which is the official recordkeeping system for U.S. NRC. For U.S. EPR, the technical details are obtained from the FSAR documents provided by Areva NP, Inc. and from the DCA documents for NuScale provided by NuScale Power, LLC.

3.1 U.S. EPR

Reactor Coolant System (RCS) in U.S. EPR design consists of a conventional four-loop design, each loop containing one Main Coolant Pump (MCP), one Steam Generator and their associated piping and control systems. In addition to the loops, the RCS consists of a Pressurizer connected to one hot leg pipe via a surge line, and a Reactor Pressure Vessel (RPV), which contains the fuel assemblies. (Areva NP, Inc. 2013a, p. 1.2-9). The general primary circuit arrangement for EPRs is shown in Figure 3.1.

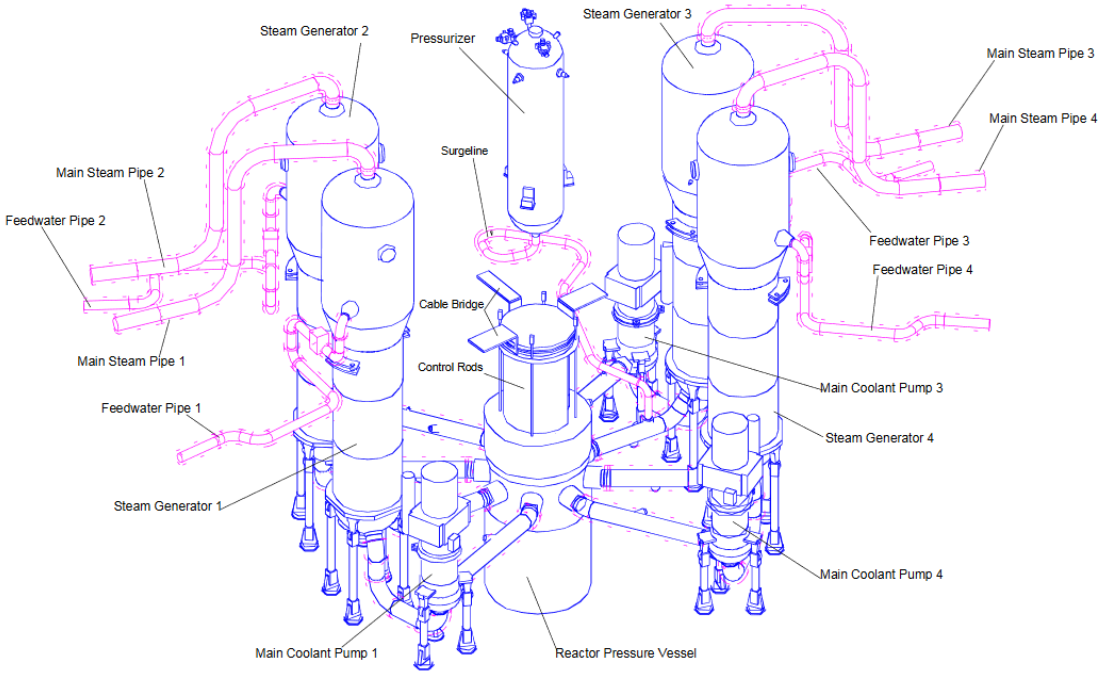

Figure 3.1. The arrangement of an EPR primary circuit (Mast & Carrer, p. 6). The primary circuit is drawn as blue and the secondary circuit as pink.

As can be seen from Figure 3.1, water coolant enters the RPV through cold leg pipes connected to the Main Coolant Pumps. The coolant is forced to flow down to the bottom of the vessel, where it gets deflected and goes through the reactor core and leaves through the hot leg pipes to the SGs. From there the coolant flows back to the cold leg pipes through the MCPs and the cycle repeats. The coolant flow is naturally circulated inside the SGs. (Areva NP, Inc. 2013a, p. 1.2-9, 1.2-11). On the secondary side, feedwater is

pumped to the SGs through the feedwater pipes. The feedwater is vaporized and leaves as steam through the main steam pipes to drive the Turbine Generator (TG).

The Defence-in-Depth categorization used by U.S. EPR has four different levels of defence as opposed to the five in the implementation used in this master's thesis. They are based on deterministic analyses complemented by probabilistic analyses and are presented in Table 3.1

Table 3.1. Defence-in-Depth concept used in U.S. EPR design (Areva NP, Inc. 2013a, p. 1.2-2).

"1. A combination of conservative design, quality assurance, and surveillance activities to prevent departures from normal operation."
"2. Detection of deviations from normal operation and protection devices and control systems to cope with them. This level of protection supports the integrity of the fuel cladding and the reactor coolant pressure boundary (RCPB) to prevent accidents."
"3. ESFs and protective systems that are provided to mitigate accidents and consequently to prevent their evolution into severe accidents."
"4. Measures to preserve the integrity of the containment and enable control of severe accidents."

Judging from Table 3.1, the first three levels are basically identical to the implementation of DiD used in this master's thesis shown in Figure 2.1 and can be directly transposed. The difference comes on the fourth level because severe accidents without significant core degradation and with core melt are not separated from each other. The safety systems used during this fourth level of defence on U.S. EPR design must be further divided into two categories to fit into the DiD scope implemented in this master's thesis.

The CDF due to internal events at full power is calculated to be $2{,}4 \cdot 10^{-7}$/a for U.S. EPR, which is well below the U.S. NRC criteria of $< 10^{-4}$/a mentioned earlier. Internal events

contribute half of the total CDF at full power. The CDF due to internal events at full power is dominated by a Loss Of Offsite Power (LOOP) initiating event, which contributes over 40 % of the CDF alone. This is logical because U.S. EPR design implements active safety systems requiring electrical power to work and achieve their safety-related functions. (Areva NP, Inc. 2013i, p. 19.1-53–19.1-54, 19.1-887).

3.2 NuScale

Each NPM is a modularized and movable object, which consists of an RPV with an integrated primary circuit. The RPV is concealed inside a Containment Vessel (CNV) made from steel. The primary circuit includes the reactor core, a Pressurizer, two SGs and their associated piping. (NuScale Power, LLC. 2020a, p. 1.2-1). A cutaway view of a single NPM is shown in Figure 3.2 below.

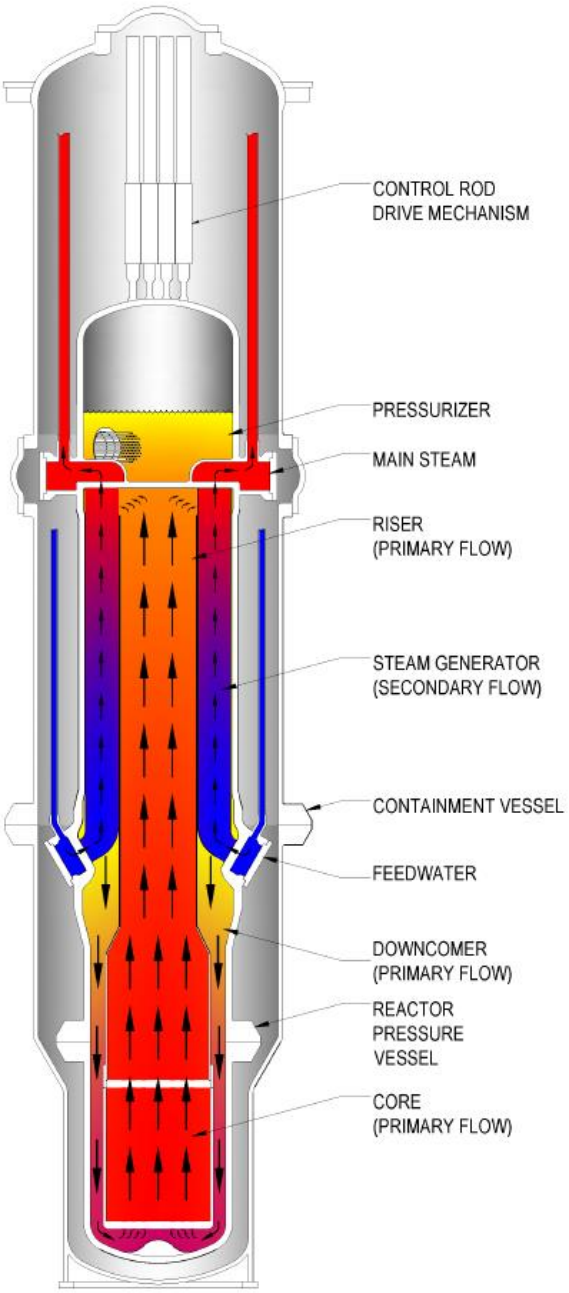

Figure 3.2. The arrangement of a single NuScale Power Module (NuScale Power, LLC. 2020a, p. 1.2-26). The arrows indicate the natural circulation paths for primary and secondary circuit.

As can be seen from Figure 3.2, the primary circuit flow is completely naturally circulated as it does not need to utilize any Reactor Coolant Pumps (RCPs). From the bottom of the core, the water coolant flows upwards in the central hot leg riser through the reactor core as it heats up, causing its density to decrease. At the top of the reactor core, the coolant starts to flow downwards through the helical coil SGs and transfers the heat to the secondary side as it cools down, causing its density to increase. This drives the coolant to flow downwards in the downcomer back to the bottom of the core for the cycle to repeat itself. On the secondary side, feedwater is pumped to the helical coil SGs through the feedwater line. The feedwater is vaporized and leaves as superheated steam through the main steam line to drive the TG. (NuScale Power, LLC. 2020a, p. 1.2-3).

NuScale classifies its Design Basis Events (DBEs) into three different categories based on their event frequency and radiological consequences: AOOs, Infrequent Events (IEs) and DBAs. NuScale classifies IEs as events that are not expected to occur during the plant lifetime but have more restrictive acceptance criteria for radiological consequences compared to DBAs. For them, the worst-case single-failure or single-operator error is assumed to occur. (NuScale Power, LLC. 2020h, p. 15.0-2–15.0-3). To fit them into this master's thesis Defence-in-Depth scope, they are conservatively classified as AOOs. As stated in Chapter 2, the event frequency limit for AOOs is 10^{-2}/a. In addition to DBEs, NuScale considers Beyond Design Basis Events (BDBEs), which can be translated as Design Extension Conditions and are further divided to accidents that lead and do not lead to core damage in this master's thesis, just like with U.S. EPR. Multi-failure accidents are classified as BDBEs (NuScale Power, LLC. 2020h, p. 15.0-2).

The mean value of the CDF due to internal events at full power is calculated to be $3{,}0 \cdot 10^{-10}$/a for a single NPM, which is significantly below the U.S. NRC criteria. It is dominated by a Loss-Of-Coolant-Accident (LOCA) inside containment and LOOP initiating event sequences, which both contribute 22 % of the CDF. In addition to the single module CDF, a Multi-Module Core Damage Frequency (MM-CDF) is calculated. It conservatively assumes that a failure in two or more NPMs affects all NPMs. The mean value of the MM-CDF due to internal events at full power is calculated to be $4{,}1 \cdot 10^{-11}$/a. It is

dominated by a LOOP initiating event sequences contributing 54 % of the MM-CDF, followed by LOCA inside containment initiating event contributing 31 % of the MM-CDF. The reason behind the low CDF is the integral primary circuit with natural circulation. By utilizing fewer components and simple design, many of the plant challenges associated with external piping contributing to the CDF are eliminated. (NuScale Power LLC. 2020i, p. 19.1-5, 19.1-39, 19.1-111).

3.3 Comparison of operating parameters between U.S. EPR and NuScale

The reactor and main steam system operating parameters between U.S. EPR and a single NuScale Power Module are compared in Table 3.2 below.

Table 3.2. Comparison between the operating parameters for U.S. EPR and a single NPM (Edited from Areva NP, Inc. 2013a, p. 1.3-2–1.3.3; Areva NP, Inc. 2013b, p. 4.1-7–4.1-8; Areva NP, Inc. 2013g, p. 10.3-22; NuScale Power, LLC. 2020a, p. 1.3-2; NuScale Power, LLC. 2020b, p. 4.1-6; NuScale Power, LLC. 2020g, p. 10.3-14).

Operating parameters (per reactor)	**U.S. EPR**	**NuScale**
Nominal gross electrical output [MW_e]	1600	50
Core thermal output [MW_{th}]	4590	160
Core operating pressure [MPa]	15,5	12,8
Core inlet temperature [°C]	295	258
Core outlet temperature [°C]	330	310
Best estimate reactor flow rate [kg/h]	$83{,}5 \cdot 10^6$	$2{,}1 \cdot 10^6$
Steam operating pressure [MPa]	7,66	3,45
Steam operating temperature [°C]	292	302

Steam flow rate [kg/h]	$9{,}38 \cdot 10^6$	$0{,}241 \cdot 10^6$
Average linear power density [kW/m]	17,13	8,2
Number of fuel assemblies	241	37
Rod array	17x17	17x17
Fuel rods per assembly	265	264
Number of control rod assemblies	89	16
Control rods per assembly	24	24

NuScale operates at lower temperatures and pressures than U.S. EPR. In addition, steam gets superheated in NuScale helical coil Steam Generators (NuScale Power, LLC. 2020a, p. 1.2-3). As a result, a NuScale power plant with 12 reactor modules would have a nominal gross electrical output of 50 $MW_e \cdot 12 = 600$ MW_e and a core thermal output of 160 $MW_{th} \cdot 12 = 1920$ MW_{th}. Total efficiency for U.S. EPR can be calculated to be 1600 MW_e/4590 $MW_{th} = 0{,}35$ and for NuScale 50 MW_e/160 $MW_{th} = 0{,}31$.

From Table 3.2, the average linear power density for NuScale is considerably smaller as opposed to U.S. EPR. Furthermore, there are 37 fuel assemblies in a single NPM, which means that there would be 444 fuel assemblies in a 12-module NuScale power plant. Other than that, the nuclear fuel is similar for both facilities. They both utilize up to 4,95 % enriched uranium dioxide (UO_2) with Zirconium alloy-based, M5™ cladding as their nuclear fuel (Areva NP, Inc. 2013b, p. 4.2-19; NuScale Power, LLC. 2020b, p. 4.3-5). It is apparent that with a lower core power density NuScale design is safer, but it is achieved at the cost of energy efficiency.

4 FRONT-LINE SAFETY SYSTEMS

The major operating systems, as well as the front-line safety systems used in U.S. EPR and NuScale designs, are described shortly in this Chapter. Only systems and components related to the operation of the plant Safety and the Core as indicated in Figure 1.1 are considered. Fuel management, SFP, Spent Fuel interim and nuclear waste management are excluded from consideration. Some systems might not be credited or required to operate in the Design Control Documents (DCDs) but have an impact on plant safety during Accident Conditions. In U.S. NRC practice, during severe accidents with core melt all available plant systems, safety and non-safety, can be used to mitigate consequences of the accident.

4.1 Front-line safety systems of U.S. EPR

Systems used for subcriticality functions in U.S. EPR design are described shortly and presented in Table 4.1 below.

Table 4.1. Systems used for subcriticality functions in U.S. EPR.

Chemical and Volume Control System (CVCS)
Rod Cluster Control Assembly (RCCA)
Soluble boron
Gadolinia
Medium Head Safety Injection (MHSI)
Extra Borating System (EBS)

Chemical and Volume Control System (CVCS) is a typical system found in nuclear reactor designs. It is an operating system and as such, it has multiple operational functions, but only the safety-related functions used to control subcriticality are within the framework of this master's thesis. It maintains and adjusts boron concentration for the

RCS during expected reactivity changes and minor transients, maintains the integrity of Reactor Coolant Pressure Boundary (RCPB) and supplies reactor coolant makeup water as part of Emergency Core Cooling Systems. (Areva NP, Inc. 2013f, p. 9.3-55–9.3-57).

Rod Cluster Control Assembly (RCCA) and soluble neutron poison in the RCS are the two methods of controlling excess reactivity during operation. There are RCCAs contained within 89 of the 241 fuel assemblies and each of them contains 24 individual control rods. They are used for operational control, shutdown functions and controlling fast reactivity changes in the core. (Areva NP, Inc. 2013b, p. 4.2-58, 4.3-6–4.3-8, 4.3-26).

Soluble neutron poison is B-10 enriched soluble boron used to control slow reactivity changes in the reactor core. In addition, to prevent positive Moderator Temperature Coefficient (MTC) at Beginning-Of-Life (BOL) caused by using soluble neutron poison alone, integral burnable absorbers in the fuel are used. Selected fuel assemblies contain burnable absorber rods, containing gadolinia (Gd_2O_3) mixed in the enriched uranium dioxide pellets. (Areva NP, Inc. 2013b, p. 4.1-3, 4.2-1, 4.2-19, 4.3-9, 4.3-27).

Medium Head Safety Injection (MHSI) system has mainly heat removal functions, but it also has subcriticality functions by providing RCS boration and coolant inventory. And finally, Extra Borating System (EBS) injects high-pressure boric acid solution working as neutron poison into the RCS for reactivity control. (Areva NP, Inc. 2013b, p. 4.6-6; Areva NP, Inc. 2013d, p. 6.3-2–6.3-4).

Systems used for heat removal functions in U.S. EPR design are described shortly and presented in Table 4.2 below.

Table 4.2. Systems used for heat removal functions in U.S. EPR.

Steam generator (SG)
Main Feedwater System (MFWS)
Emergency Feedwater System (EFWS)
Main Steam Supply System (MSSS)
Condenser
Circulating Water System (CWS)
Atmosphere
Residual Heat Removal System (RHRS)
Low Head Safety Injection (LHSI)
Medium Head Safety Injection (MHSI)
Core Melt Stabilization System (CMSS)
Component Cooling Water System (CCWS)
Essential Service Water System (ESWS)
Ultimate Heat Sink (UHS)
In-Containment Refueling Water Storage Tank (IRWST)

Four Steam Generators in U.S. EPR design are primarily made from low alloy steel. They are vertical shell, U-tube heat exchangers, with an integral moisture separator included. Heat is removed from the primary circuit to the secondary circuit as coolant flows through the Steam Generator tubes. Feedwater to the SGs is supplied by Main Feedwater System

(MFWS) and Emergency Feedwater System (EFWS). Feedwater is generated into steam in the SGs. EFWS consists of four separate trains, each independent of MFWS. Overpressure protection in the secondary side is provided by Main Steam Supply System (MSSS) valves, consisting of four Main Steam Relief Trains (MSRTs) and eight Main Steam System Valves (MSSVs). They are part of the RCPB. (Areva NP, Inc. 2013c, p. 5.4-8, 5.4-13; Areva NP, Inc. 2013g, p. 10.3-1, 10.3-3, 10.3-11, 10.4-73–10.4-74).

In the secondary circuit, steam rejected from the Turbine goes to Main Condenser to be condensed. It receives cooling water from non-safety-related Circulating Water System (CWS), which is the normal heat sink for U.S. EPR power plant. Heat is rejected to the Atmosphere through Ultimate Heat Sink (UHS) cooling towers. UHS consists of five redundant divisions, four of which are safety-related. Areva NP, Inc. 2013f, p. 9.2-118; Areva NP, Inc. 2013g, p. 10.4-21).

U.S. EPR design implements a Residual Heat Removal System (RHRS) that provides cooldown of the reactor coolant by removing residual heat, and a Safety Injection System (SIS) that provides emergency core cooling functions with a safety injection. These two systems work in conjunction as a Safety Injection System/Residual Heat Removal (SIS/RHR) system that consists of supply and return trains, each containing a Low Head Safety Injection (LHSI) pump, Medium Head Safety Injection pump and an accumulator. There are four physically separated and independent SIS/RHR system trains divided into four functionally identical divisions in total, one for each RCS loop and according to Areva NP, Inc. and only one of them is needed to supply the required core cooling. MHSI pumps inject borated water directly into cold legs, and LHSI pumps inject water into cold legs through their associated LHSI heat exchangers as their emergency heat removal function. In addition, LHSI heat exchangers remove post-accident decay heat from the RCS and provide post-accident containment cooling. To maintain safe operation, individual trains can be subjected to maintenance. (Areva NP, Inc. 2013c, p. 5.4-26–5.4-27; Areva NP, Inc. 2013d, p. 6.3-1, 6.3-6).

During severe accidents with core melt, emergency core cooling is provided by Core Melt Stabilization System (CMSS) by cooling molten core debris with a cooling structure located in the spreading compartment. It also has containment functions that are discussed later. (Areva NP, Inc. 2013i, p. 19.2-11).

Component Cooling Water System (CCWS) and Essential Service Water System (ESWS) function as safety-related cooling mediums in U.S. EPR design. CCWS provides cooling to different safety-related systems and components by removing their generated heat loads. Cooling water to CCWS and different auxiliary systems is provided by ESWS, so CCWS functions as an intermediate system between radioactive systems and ESWS. It consists of five independent trains, four of which are safety-related. ESWS consists of five separate and redundant divisions, four of which are safety-related. Each division contains a single pump operating at 100 % capacity. (Areva NP, Inc. 2013f, p. 9.2-1–9.2-3, 9.2-25).

Functioning as a water inventory, heat sink, and return reservoir, In-containment Refueling Water Storage Tank (ITWST) is an open pool located at the bottom of the containment, surrounding core melt spreading compartment. It is connected to some safety systems and contains sufficient water volume to fill the reactor cavity, internal storage pool, Reactor Building transfer pool, and the RCS. It also provides a heat sink and water inventory to flood the containment spreading area in case a core melt accident occurs. (Areva NP, Inc. 2013d, p. 6.3-9).

Systems used for containment functions in U.S. EPR design are described shortly and presented in Table 4.3 below.

Table 4.3. Systems used for containment functions in U.S. EPR.

Reactor Coolant Pressure Boundary (RCBP)
Reactor Pressure Vessel (RPV)
Pressurizer Safety Relief Valves (PSRV)
Primary Depressurization System (PDS)
Pressurizer Relief Tank (PRT)
Containment Isolation System (CIS)
Reactor Containment Building (RCB)
Combustible Gas Control System (CGCS)
Core Melt Stabilization System (CMSS)
Severe Accident Heat Removal System (SAHRS)
Component Cooling Water System (CCWS)
Essential Service Water System (ESWS)
Ultimate Heat Sink (UHS)

Reactor Coolant Pressure Boundary must be maintained in a nuclear power plant to prevent radiological releases from occurring. Closed systems in the primary circuit and the secondary circuit are the first barriers maintaining the RCPB. If they fail, RPV is the final barrier in maintaining the RCPB. RPV is the main component of the RCS, contains fuel assemblies and directs the flow of reactor coolant through the reactor core. (Areva NP, Inc. 2013c, p. 5.1-3).

Overpressure protection for the RCS is provided by three Pressurizer Safety Relief Valves (PSRVs) and Primary Depressurization System (PDS) consisting of two trains of four Primary Depressurization System Valves (PDSVs). They are normally closed and function as a part of the RCPB. PSRVs are actuated passively by design, while PDSVs are active, consisting of a single DC powered depressurization valve and an isolation valve, operating at 2 x 100 % capacity. RCS pressure is relieved when a large differential pressure opens the main relief disk. A single inadvertent opening of a PSRV does not lead to an accident. For overpressure protection to condense and cool discharged steam, inside the Reactor Building is located a horizontal, cylindrical Pressurizer Relief Tank (PRT). (Areva NP, Inc. 2013c, p. 5.2-6, 5.2-30, 5.4-43–5.4-47; Areva NP, Inc. 2013i, p. 19.2-18–19.2-19).

Containment Isolation System (CIS) provides containment isolation functions by isolating fluid systems that penetrate the containment boundary to confine possible radioactive releases inside the containment. CIS is not a diverse system as itself but is comprised of isolation barriers, system piping and associated I&C circuits to generate actuation signals. (Areva NP, Inc. 2013d, p. 6.2-256).

Reactor Containment Building (RCB) is a cylindrical, post-tensioned concrete pressure vessel, completely enclosed by a Reactor Shield Building (RSB), protecting RCB from external hazards, such as aircraft collisions. Between the RCB and the RSB is an annulus space. The RCB functions as a barrier to retain the uncontrolled release of fission products to the environment. (Areva NP, Inc. 2013a, p. 1.2-6; Areva NP, Inc. 2013d, p. 6.2-242).

Hydrogen can be generated in the containment as a result of different Accident Conditions. To keep the hydrogen concentration below acceptable levels in the containment, Combustible Gas Control System (CGCS) limits the concentration of hydrogen by recombining it with oxygen to protect containment integrity from overpressure and hydrogen combustion. CGCS consists of hydrogen mixing dampers, rupture foils and convection foils. (Areva NP, Inc. 2013d, p. 6.2-291–6.2-292; Areva NP, Inc. 2013i, p. 19.2-31).

During severe accidents with core melt, CMSS and Severe Accident Heat Removal System (SAHRS) are the containment safety systems, which prevent core debris from breaching containment integrity. Melt retention within RPV is not feasible in a large reactor like U.S. EPR, which is why the function of CMSS is to passively transport molten core debris into a spreading compartment to prevent containment failure. In case the molten core melts through the reactor vessel, it reaches the reactor cavity, which is covered with sacrificial concrete and protective layers. The sacrificial concrete guides the core debris toward a melt plug, which provides a defined failure location. The core debris then enters a melt discharge channel leading to a spreading area (core catcher), where the debris spreads to a large area to be stabilized. (Areva NP, Inc. 2013i, p. 19.2-11–19.2-13). An overview of CMSS is presented in Figure 4.1 below.

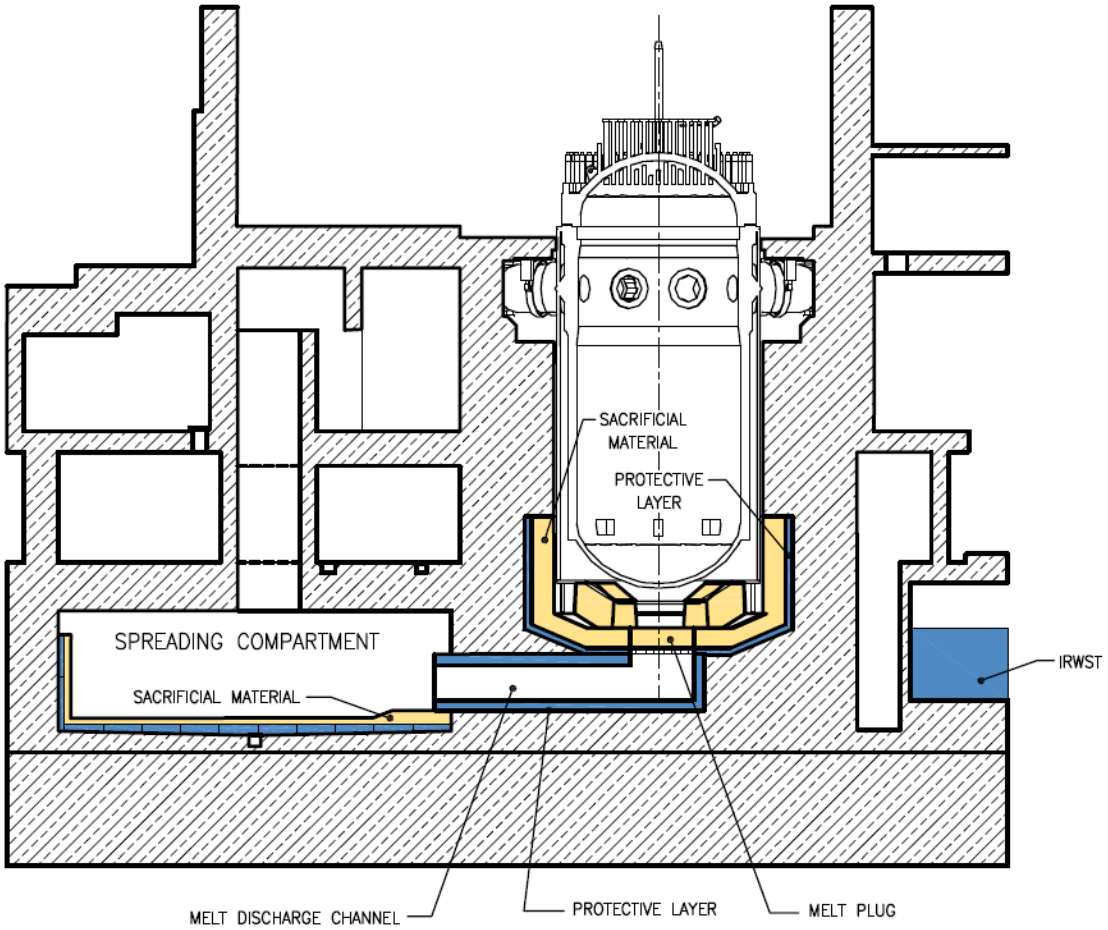

Figure 4.1. Overview of Core Melt Stabilization System (Areva NP, Inc. 2013i, p. 19.2-87). During severe accidents with core melt, the molten core is discharged to a spreading compartment to prevent it from breaching containment integrity.

SAHRS is used to control containment pressure, and to provide Long-Term Cooling of the molten corium and the containment during severe accidents with core melt. It employs both active and passive means during four different modes of operation as the melt retention progresses, each with different safety-related functions. There is only a single train working at 100 % capacity, which consists of a heat exchanger, a recirculation pump, a suction line and a discharge line, and three discharge pathways from the heat exchanger to containment spray, to the spreading compartment and sump screen flushing device.

(Areva NP, Inc. 2013i, p. 19.1-101, 19.3-14–19.2-15). An overview of SAHRS is presented in Figure 4.2 below.

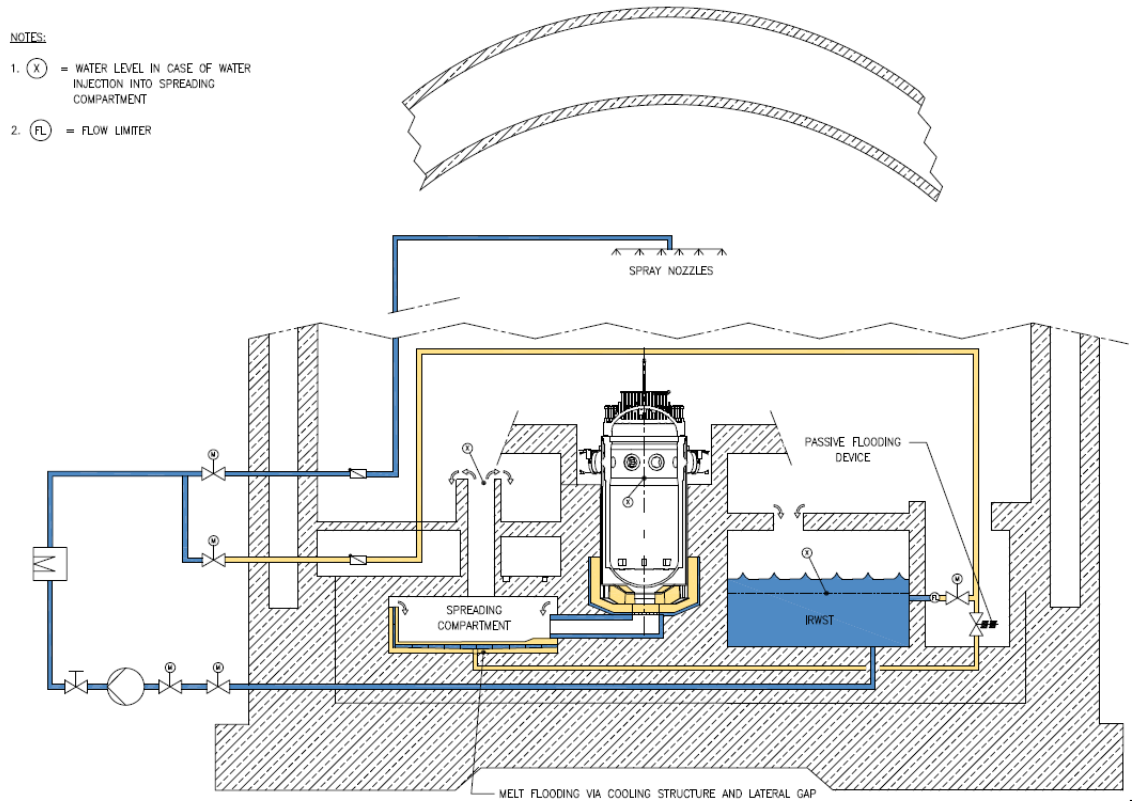

Figure 4.2. Overview of Severe Accident Heat Removal System (Areva NP, Inc. 2013i, p. 19.2-88). During severe accidents, SAHRS provides active and passive core melt cooling functions to prevent containment integrity from being breached.

Systems used for support functions in U.S. EPR design are described shortly and presented in Table 4.4 below.

Table 4.4. Systems used for support functions in U.S. EPR.

Non-Class 1E Normal Power Supply System (NPSS)
Class 1E Emergency Power Supply System (EPSS)
Station Blackout Diesel Generators (SBODG)
Class 1E Uninterruptible Power Supply (EUPS)
Non-class 1E 12-hour UPS (12UPS)
Main Control Room Air Conditioning System (CRACS)
Safeguard Building Controlled-Area Ventilation System (SBVS)
Electrical Division of Safeguard Building Ventilation System (SBVSE)
Essential Service Water Pump Building Ventilation System (ESWPBVS)
Containment Building Ventilation System (CBVS)
Emergency Power Generating Building Ventilation System (EPGBVS)
Station Blackout Room Ventilation System (SBORVS)

In U.S. EPR design, offsite power is provided by two utility transmission lines connected to a switchyard. Onsite power is received through the same station switchyard, which is interfaced at main generator output and four-station auxiliary transformers. There is not a traditional unit auxiliary transformer, which connects the plant electrical distributional system directly into the main generator as normal power. Two of the auxiliary transformers provide power through a Preferred Power Supply (PPS) system to a non-safety-related, Non-Class 1E Normal Power Supply System (NPSS) and the other two provide power supply to a safety-related, Class 1E Emergency Power Supply System (EPSS). (Areva NP, Inc. 2013e, p. 8.1-1).

Active safety systems are primarily provided power by offsite power supplied by NPSS and secondarily by offsite power supplied by EPSS. In addition, onsite power can be provided by four divisions of EPSS, each connected to a standby EDG. U.S. EPR design also implements two SBODGs that are completely independent of the other plant power sources. They have the capacity and capability to bring the plant to a hot standby and maintain it in that state following a Station Blackout (SBO). (Areva NP, Inc. 2013e, p. 8.1-1–8.1-2, 8.4-1–8.4-2).

Safety-related AC and DC loads are provided power supply by a Class 1E Uninterruptible Power Supply (EUPS) in each EPSS division during initial conditions of an SBO. EUPS batteries can provide power for 2 hours without battery chargers and can provide continuous power supply with the battery chargers. 12 Hour Uninterruptible Power Supply (12UPS) does not have any safety-related functions but it provides power during severe accidents and an SBO to selected components and systems. (Areva NP, Inc. 2013e, p. 8.1-5, 8.3-45–8.3-46, 8.4-7).

The main function of Main Control Room Air Conditioning System (CRACS) is to provide a safe environment in Control Room Envelope (CRE) area to allow operators to safely remain and to support operability of components inside the Main Control Room (MCR). (Areva NP, Inc. 2013d, p. 6.4-1; Areva NP, Inc. 2013f, p. 9.4-1).

Safeguard Building Controlled-Area Ventilation System (SBVS) and Electrical Division of Safeguard Building Ventilation System (SBVSE) each provide acceptable ambient conditions in their respective functional areas of Safeguard Building. They provide isolation and confinement of Safeguard Building. (Areva NP, Inc. 2013f, p. 9.4-47–9.4-49).

Essential Service Water Pump Building Ventilation System (ESWPBVS) provides acceptable ambient conditions in four Essential Service Water Pump Building. Four independent ventilation systems recirculate the air inside ESWS Pump Buildings. (Areva NP, Inc. 2013f, p. 9.4-132).

Containment Building Ventilation System (CBVS) is an ESF ventilation system that provides acceptable ambient conditions in the Containment Building. It removes radioactive materials from the air and exhausts air from the containment. (Areva NP, Inc. 2013f, p. 9.4-85).

Emergency Power Generating Building Ventilation System (EPGBVS) provides acceptable ambient conditions in four divisions of Emergency Power Generating Buildings. Four independent divisions of EPGBVS ventilate the air inside diesel hall, electric room and main tank room. (Areva NP, Inc. 2013f, p. 9.4-114).

Station Blackout Room Ventilation System (SBORVS) provides acceptable ambient conditions in two divisions of Station Blackout Rooms. Two independent divisions of SBORVS ventilate the air inside Switchgear Building, diesel hall, fuel tank room, and associated electrical rooms. (Areva NP, Inc. 2013f, p. 9.4-125).

4.2 Front-line safety systems of NuScale

Systems used for subcriticality functions in NuScale design are described shortly and presented in Table 4.5 below.

Table 4.5. Systems used subcriticality functions in NuScale.

Chemical and Volume Control System (CVCS)
Control Rod Assembly (CRA)
Soluble boron
Gadolinia

Chemical and Volume Control System is also found in NuScale design. It is classified as a non-safety-related system, but it is equipped with two safety-related, demineralized water isolation valves to ensure that its operation does not inadvertently dilute the boron concentration of the RCS. In addition to its operational functions, it maintains and adjusts

boron concentration for the RCS during expected reactivity changes and minor transients, and supplies reactor coolant makeup water for the RCS. It is not relied upon to add boron to the RCS during Accident Conditions. (NuScale Power, LLC. 2020f, p. 9.3-52–9.3-56).

Control Rod Assembly (CRA) and soluble neutron poison in the RCS are the two methods of controlling excess reactivity during operation. There are 16 CRAs contained within 37 of the fuel assemblies, each of them containing 24 individual control rods. They are used for rapid reactivity adjustments. The 16 CRAs are symmetrically divided into two different banks of 8 assemblies, both with different safety-related functions. The first bank is a regulating bank, and the second bank is a shutdown bank. Both banks are further organized into two groups of four CRAs. (NuScale Power, LLC. 2020b, p. 4.1-1–4.1-2). Configuration of the CRAs is presented in Figure 4.3 below.

In addition to CRAs, there are 12 In-Core Instruments as part of In-Core Instrumentation System (ICIS) that measures neutron flux within the core and temperatures at the respective fuel assembly's inlet and outlet. Three-dimensional power distribution can be formed from the neutron flux, and proper coolant flow rates can be determined in a post-accident monitoring system from the temperatures. (NuScale Power, LLC. 2020b, p. 4.1-2, 4.4-22). The ICIS configuration is presented in Figure 4.3 below.

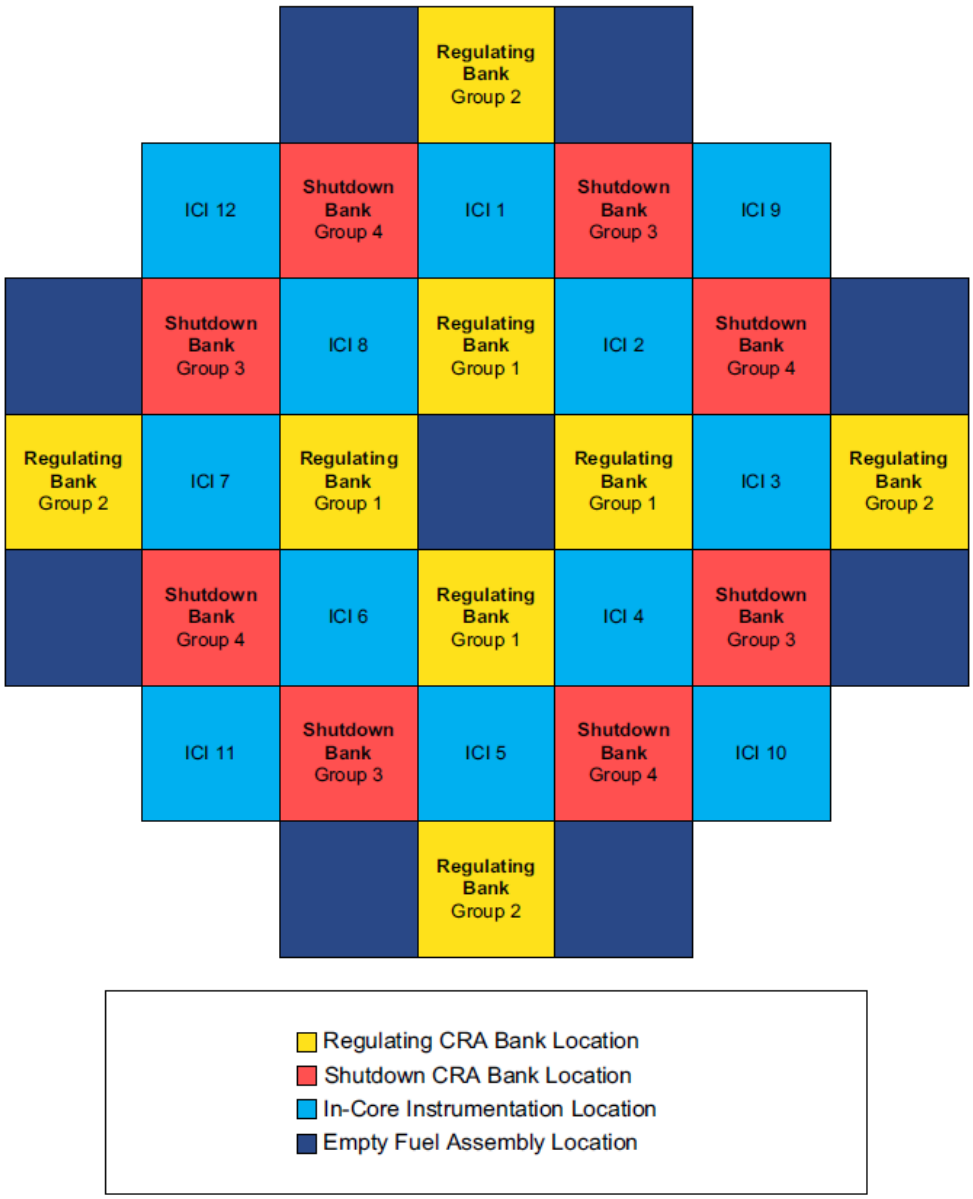

Figure 4.3. Locations of Control Rod Assemblies and In-Core Instruments in the NuScale reactor core (NuScale Power, LLC. 2020b, p. 4.3-56). Both CRA banks and In-Core Instruments are placed symmetrically around the core near fresh batches of fuel, where the burnup is highest.

Soluble neutron poison is soluble boron used to control slow reactivity changes in the reactor core. In addition, to prevent positive MTC at BOL caused by using soluble neutron

poison alone, integral burnable absorbers in the fuel are used. Selected fuel assemblies contain burnable absorber rods, containing gadolinia mixed in the enriched uranium dioxide pellets. (NuScale Power, LLC. 2020b, p. 4.1-2, 4.2-13, 4.3-19).

Systems used for heat removal functions in NuScale design are described shortly and presented in Table 4.6 below.

Table 4.6. Systems used for heat removal functions in NuScale.

Steam generator (SG)
Condenser
Circulating Water System (CWS)
Atmosphere
Reactor Component Cooling Water System (RCCWS)
Site Cooling Water System (SCWS)
Emergency Core Cooling System (ECCS)
Decay Heat Removal System (DHRS)
Ultimate Heat Sink (UHS)
Reactor Pressure Vessel (RPV)
Containment Vessel (CNV)
Containment Flooding and Drain System (CFDS)

There are two independent helical coil Steam Generators in a single NPM, which are a part of the RCPB. Heat is removed from the primary circuit to the secondary circuit as coolant flows through Steam Generator tubes. Feedwater to SGs is provided by a

Feedwater System, which does not perform any safety functions. Feedwater is generated into steam, which is superheated in the SGs. (NuScale Power LLC. 2020c, p. 5.4-1; NuScale Power, LLC. 2020g, p. 10.4-28).

In the secondary circuit, steam rejected from Turbine goes to Main Condenser to be condensed. It receives cooling water from non-safety-related Circulating Water System, which is the normal heat sink for NuScale power plant. And finally, the heat is rejected to the Atmosphere through a single cooling tower. (NuScale Power, LLC. 2020g, p. 10.4-1, 10.4-18–10.4-19).

Reactor Component Cooling Water System (RCCWS) and Site Cooling Water System (SCWS) function as non-safety-related cooling mediums in NuScale design. RCCWS provides cooling to different systems and components by removing their generated heat loads. Cooling water to RCCWS and different auxiliary systems is provided by SCWS, so it functions as an intermediate system between radioactive systems and nonradioactive SCWS. They are both classified as non-safety-related systems. (NuScale Power, LLC. 2020f, p. 9.2-2, 9.2-42).

Emergency Core Cooling System (ECCS) is a unique design in NuScale as compared to traditional Emergency Core Cooling Systems in LWRs. It provides passive core cooling with three Reactor Vent Valves (RVVs), two Reactor Recirculation Valves (RRVs), and their associated actuators. Each RVV and RRV is “a power-actuated relief valve that is hydraulically closed, spring-assist to open, normally closed, and fails open”. As they are normally closed in standby mode, they are part of the RCPB. The actuators consist of a trip valve, a reset valve and their solenoids. (NuScale Power, LLC. 2020d, p. 6.3-1, 6.3-5). Overview of ECCS is presented in Figure 4.4 below.

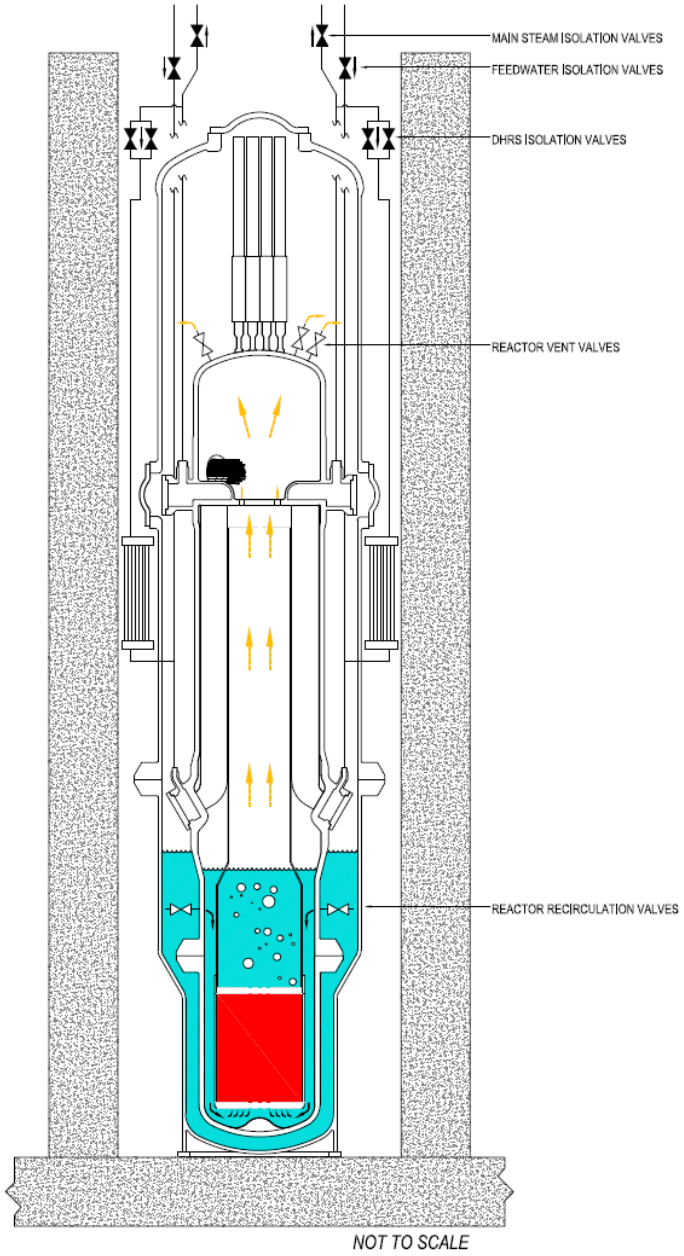

Figure 4.4. Schematic of Emergency Core Cooling System (NuScale Power, LLC. 2020a, p. 1.2-29).

Decay Heat Removal System (DHRS) is designed to remove decay and residual heat from the reactor core and to retain RCS inventory in the RPV. It consists of two separate DHRS trains, each connected to one SG and their associated main steam and feedwater lines. Four DHRS actuation valves, two for each train, prevent system flow within DHRS loop.

They are normally closed in standby mode. (NuScale Power, LLC. 2020c, p. 5.4-16–5.1-18; NuScale Power, LLC. 2020h, p. 15.0-33). Overview of DHRS is presented in Figure 4.5 below.

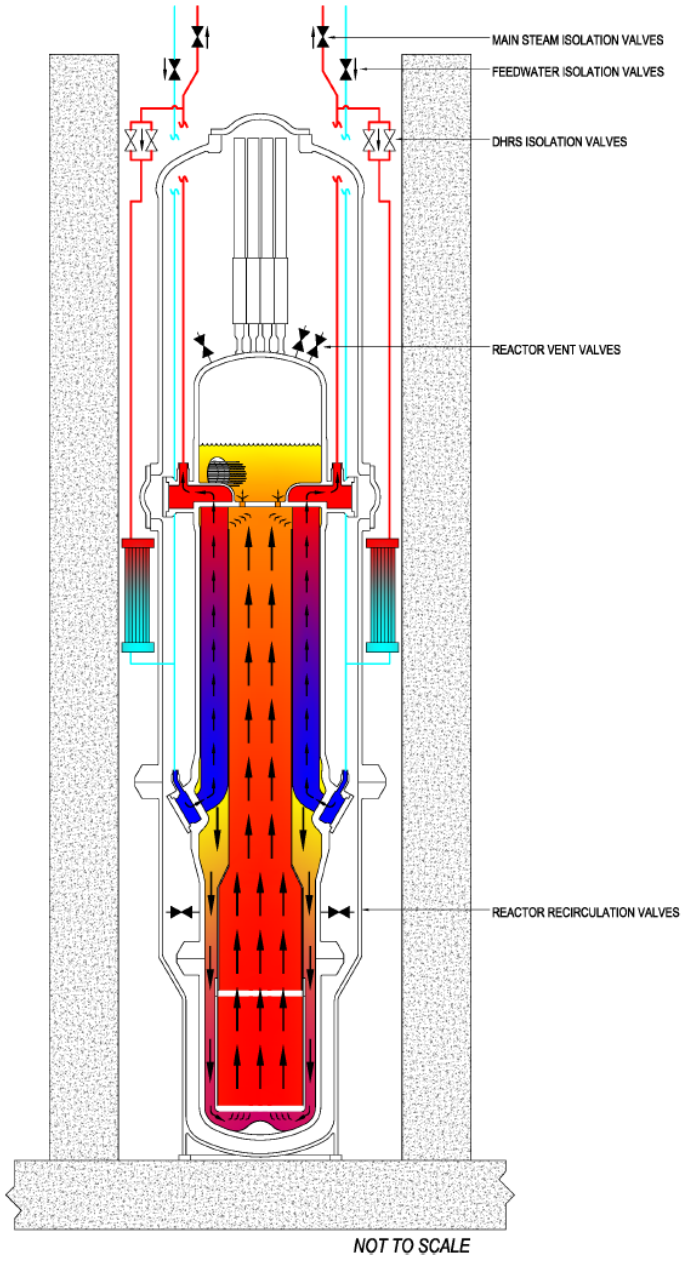

Figure 4.5. Schematic of Decay Heat Removal System (NuScale Power, LLC. 2020a, p. 1.2-28).

Ultimate Heat Sink consists of the reactor pool, refuelling pool, and Spent Fuel Pool. They are all open to each other, with only a weir wall separating the Spent Fuel Pool and the refuelling pool. The water volume inside the dry dock is not credited as part of the UHS. (NuScale Power, LLC. 2020f, p. 9.2-24–9.2-25; NuScale Power, LLC. 2020g, p. 10.4-1, 10.4-18). Configuration of the UHS is presented in Figure 4.6 below.

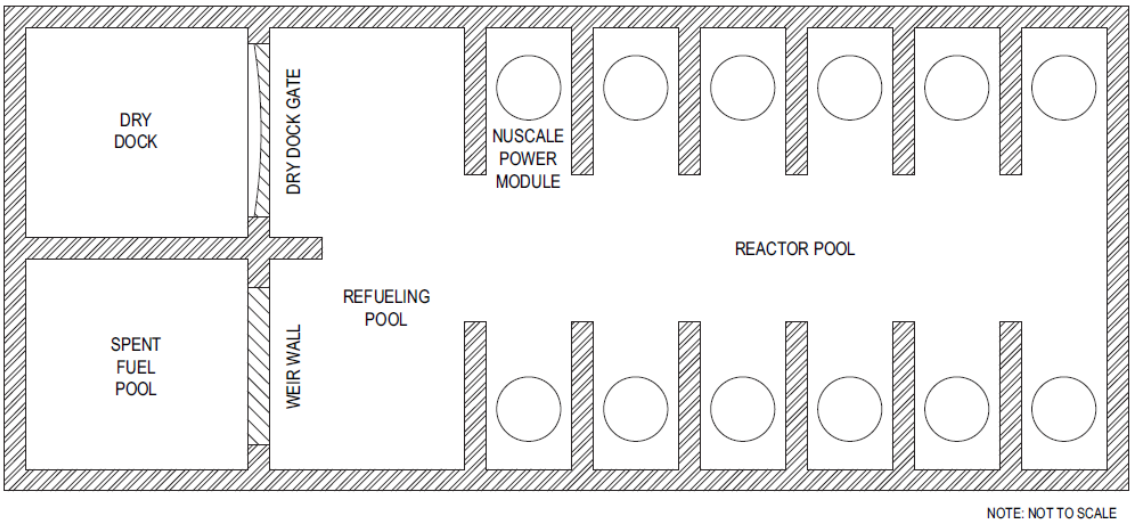

Figure 4.6. The layout of the Ultimate Heat Sink (NuScale Power, LLC 2020f p. 9.2-38). The reactor pool is shared between up to twelve NPMs.

A single NPM is comprised of Containment Vessel, Pressure Vessel and the components and associated piping inside. RPV is the main component of the RCS, which contains the fuel assemblies, two Steam Generators, Pressurizer and directs the flow of the reactor coolant through the reactor core. Inside the CNV are contained the RPV, Control Rod Drive Mechanisms and the associated piping and components between RPV and CNV. The CNV is designed to contain fission products and transfer heat generated inside the RPV to the reactor pool, and therefore to the UHS. Up to 12 NPMs are located in the reactor pool as can be seen from Figure 4.6. (NuScale Power, LLC. 2020a, p. 1.2-1; NuScale Power, LLC. 2020c, p. 5.3-1).

Containment Flooding and Drain System (CFDS) is used to inject borated water inventory from the reactor pool to the CNV. There are two independent subsystems, each consisting

of two parallel pumps, a drain separator tank and associated containment isolation valves. (NuScale Power, LLC. 2020f, p. 9.3-87, 9.3-91; NuScale Power, LLC. 2020i, p. 19.1-132).

Systems used for containment functions in NuScale design are described shortly and presented in Table 4.7 below.

Table 4.7. Systems used for containment functions in NuScale.

Reactor Coolant Pressure Boundary (RCBP)
Reactor Pressure Vessel (RPV)
Containment Vessel (CNV)
Reactor Safety Valves (RSV)
Containment Isolation Valves (CIVs)

Reactor Coolant Pressure Boundary must be maintained in a nuclear power plant to prevent radiological releases from occurring. Closed systems in the primary circuit and the secondary circuit are the first barriers maintaining the RCPB. If they fail, the RPV functions as a barrier to maintain RCPB. (NuScale Power, LLC. 2020c, p. 5.2-1; NuScale Power, LLC. 2020d, p. 6.2-27–6.2-28).

Overpressure protection for the RCS is provided by two redundant and safety-related Reactor Safety Valves (RSVs) installed above the Pressurizer on top of the RPV. They are spring operated pilot valves and are considered to be passive devices. RCS pressure is relieved upon large differential pressure across the main valve disk. They are also part of the RCPB. (NuScale Power, LLC. 2020c, p. 5.1-4, 5.2-4, 5.2-8, 5.2-10).

Containment Isolation Valves (CIVs) in NuScale design function similarly as a Containment Isolation System valves in a traditional nuclear power plant. Their function is to isolate fluid systems that penetrate the containment boundary to confine possible

radioactive releases inside the containment. The containment boundary is formed by CIVs, the CNV and passive containment isolation barriers. CIVs are grouped into Primary System Containment Isolation Valves (PSCIVs) and Secondary System Containment Isolation Valves (SSCIVs). SSCIV design is a single valve on each line and PSCIV design is two valves contained with a single valve body. They are both welded outside of the containment. (NuScale Power, LLC. 2020d, p. 6.2-26–6.2-28, 6.2-32–6.2-33).

Systems used for support functions in NuScale design are described shortly and presented in Table 4.8 below.

Table 4.8. Systems used for support functions in NuScale.

Turbine Generator (TG)
Highly Reliable Direct Current Power System (EDSS)
Backup Power Supply System (BPSS)
Reactor Building HVAC system (RBVS)
Control Room Area Ventilation System (CRVS)
Control Room Habitability System (CRHS)

NuScale power plant is designed to achieve and maintain safety functions without any reliance on electrical power. A safe state for the plant can be achieved and maintained entirely with passive safety systems. This is the reason why all electrical power systems can be classified as non-Class 1E systems in NuScale design. Even though electrical power systems are not required, onsite power sources are included in NuScale design. Offsite power source designs are site-specific. (NuScale Power, LLC. 2020e, p. 8.1-1, 8.2-1).

Normal power source for plant electrical loads of each NPM is their operating Turbine Generator connected to a station switchyard. NuScale design also includes a Highly

Reliable Direct Current Power System (EDSS) battery design, consisting of two subsystems: EDSS-Common (EDSS-C), which is shared between up to 12 NPMs, and EDSS-Module Specific (EDSS-MS), which is specific to all NPMs. It provides power for either 24- or 72-hour duty cycles, depending on the required load. In addition, Backup Power Supply System (BPSS) generates power to safety systems with two Backup Diesel Generators (BDGs) or an Auxiliary AC Power Source (AAPS). The design of the AAPS is site-specific. (NuScale Power, LLC. 2020e, p. 8.1-4–8.1-5, 8.3-1, 8.3-8, 8.3-21–8.3-22).

Control Room Area Ventilation System (CRVS) maintains ventilation and controls airborne radioactivity in the Control Building and in conjunction with Control Room Habitability System (CRHS), provides a safe environment in the CRE to allow operators to safely remain and to support operability of components inside the MCR. These include filtering of radioactive materials, toxic gases and smoke. (NuScale Power, LLC. 2020d, p. 6.4-1; NuScale Power, LLC. 2020f, p. 9.4-1).

Support functions of Reactor Building HVAC system (RBVS) are to maintain ventilation and to control airborne radioactivity in Reactor Building, which contains reactor pool, refuelling pool, Spent Fuel Pool, dry dock, new fuel storage, NPMs and their handling equipment. (NuScale Power, LLC. 2020f, p. 9.4-19–9.4-20).

5 SAFETY SYSTEM INTERDEPENDENCIES

As explained before, the major operating systems as well as the safety systems of both facilities are inserted in Figure 2.4. Different plant states divided as Operational States and Accident Conditions are placed vertically on the columns, three main safety functions and two main support functions are placed horizontally on the rows. This creates a 5x5 matrix, to which different front-line safety systems can be placed depending on their main safety or main support functions during different plant states.

It is important to remember that in theory, the safety systems should remain independent of each other during all plant states. Many safety systems appear on multiple plant states, some safety systems are functionally dependent on each other, and some safety systems contribute to multiple main safety functions. These factors directly compromise safety system independency. This Chapter is focused on analysing these compromises.

It should be noted that the Figures presented below are only simplifications. Just because a safety system is placed on some level of defence, it does not mean that it provides safety-related functions for all different conditions on that level of defence. Some safety systems are designed to provide safety-related functions only during certain Accident Conditions and do not provide safety-related functions during any other accident condition on that level of defence. For example, a Station Blackout is a Design Extension Condition and SBODGs are only used during an SBO. If the DECs do not lead to an SBO, the SBODGs do not have any safety-related functions, even though they are placed as a support system during the DEC level of defence.

5.1 Safety system interdependencies of U.S. EPR

The major operating systems as well as front-line safety systems implemented in U.S. EPR according to Figure 2.4 are presented in Figure 5.1 below. The safety systems are placed in their respective positions in the template based on their safety functions as discussed in U.S. EPR Final Safety Analysis Report documents.

	Operational States		Accident Conditions		
	Normal Operation	Anticipated Operational Occurrences	Design Basis Accidents	Design Extension Conditions	
				Without significant fuel damage	With core melting
Subcriticality	CVCS	CVCS			"N/A"
	RCCA	RCCA	RCCA		
	Soluble boron				
	Gadolinia				
			MHSI		
			EBS	EBS	
Heat removal	SG → Condenser → CWS → Atmosphere	SG → Condenser → CWS → Atmosphere			
	RHRS		LHSI →	MHSI →	CMSS
		SG → MSSS → Atmosphere	MSSS + MHSI →	MSSS + LHSI →	
	CCWS → ESWS → UHS	CCWS → ESWS → UHS	→ CCWS → ESWS → UHS	→ CCWS → ESWS → UHS	
	MFWS	EFWS	EFWS		
			IRWST	IRWST	IRWST
Containment	Closed piping (RCPB)	Closed piping (RCPB)	RPV	RPV	
	PSRVs → PRT	PSRVs → PRT	PDS → PRT	PDS → PRT	PDS → PRT
			CIS		
			RCB	RCB	RCB
			CGCS	CGCS	CGCS
					CMSS
					SAHRS → CCWS → ESWS → UHS
Power supply	NPSS	NPSS	EPSS (offsite/EDGs)	SBODG	SBODG
	EUPS	EUPS			
				12UPS	12UPS
HVAC	CRACS	CRACS	CRACS	CRACS	
	SBVS	SBVS	SBVS	SBVS	
	SBVSE	SBVSE	SBVSE	SBVSE	
	ESWPBVS	ESWPBVS	ESWPBVS		
	CBVS	CBVS	CBVS		
	EPGBWS	EPGBWS	EPGBWS		
	SBORVS	SBORVS	SBORVS	SBORVS	SBORVS

Figure 5.1. The major operating systems, as well as front-line safety systems implemented in U.S. EPR, placed on the functional Defence-in-Depth template.

In U.S. EPR design, some systems provide HVAC functions for components that are in standby mode and as such, are not generating internal heat loads. Due to this, supporting HVAC functions are not relevant until the components are in operation. These systems are indicated by a grey font in Figure 5.1 above.

As can be seen from Figure 5.1, CVCS provides safety-related functions only during Operational States and is not required to function during Accident Conditions. It maintains and adjusts the concentration of soluble boron during NO. In addition, gadolinia provides safety-related functions only during NO. RCCAs have safety-related functions during both Operational States and Accident Conditions by providing reactivity operational control during NO and AOOs, and reactor trip during DBAs. EBS is credited to provide high-pressure boric acid solution injection only during small break LOCAs and DECs. Subcriticality of the reactor core is not feasible during severe accidents with core melt, which is why they are indicated by Not Applicable ("N/A"). (Areva NP, Inc. 2013b, p. 4.3-6, 4.6-6; Areva NP, Inc. 2013f, p. 9.3-56–9.3-57).

Subcriticality functions of MHSI are limited to function only following a Main Steam Line Break (MSLB) and a Steam Generator Tube Rupture (SGTR). Heat removal functions of MHSI operate as a part of SIS/RHR system as explained below, but both subcriticality and heat removal functions are possible to accomplish simultaneously by drawing borated coolant water for the safety injection from IRWST. (Areva NP, Inc. 2013d, p. 6.3-2, 6.3-9; Areva NP, Inc. 2013i, p. 19.2-15–19.2-17). MHSI is one of the few safety systems in U.S. EPR design that has two different main safety functions.

The secondary circuit heat removal in U.S. EPR design is dependent on multiple different systems during Operational States. The heat removal chain starts from SGs to Main Condenser, and the heat continues to be transferred to the Atmosphere through CWS. Even though functional dependency occurs in this heat removal chain, it is not risk-significant as their safety-related functions are limited to the plant Operational States. Secondary circuit heat removal functions are not compromised during minor transients.

Additionally, the operation performance of the Main Condenser does not directly affect the operation of the primary circuit (Areva NP, Inc. 2013g, p. 10.4-3).

SIS/RHR system provides residual heat removal and emergency heat removal functions. It is a complex system that is dependent on other systems to achieve its safety-related functions. Firstly, the water for LHSI and MHSI safety injections is drawn from IRWST during DBAs and DECs. Secondly, LHSI heat exchangers remove residual heat to CCWS working as a cooling medium. CCWS rejects the heat to the final cooling medium ESWS, which in turn rejects it to the UHS during Operational States. And finally, the emergency heat removal functions of SIS/RHR system are dependent on the same CCWS and ESWS trains to transfer the heat to the UHS during DBAs and DECs. Each SIS train is powered by their separate electrical division, which is also backed by their assigned EDG following a LOOP. (Areva NP, Inc. 2013c, p. 5.4-26–5.4-27; Areva NP, Inc. 2013d, p. 6.3-1, 6.3-6–6.3-7; Areva NP, Inc. 2013f, p. 9.2-27).

To support LHSI and MHSI safety injections, MSSS also provides initial residual heat removal (Fast Cooldown) and secondary heat removal (Partial Cooldown) functions by discharging steam through MSRTs or MSSVs to Main Condenser or the Atmosphere during LOCAs and DECs (Areva NP, Inc. 2013i, p. 19.1-29, 19.1-41). This redundancy assists in achieving required heat removal and safe shutdown conditions for the complicated emergency heat removal chain that requires a lot of different components to achieve its safety-related functions. However, MSSS also provides safety-related functions during AOOs by depressurizing the steam circuit following a reactor trip through MSRTs (Areva NP, Inc. 2013g, p. 10.3-11). Even though secondary circuit overpressure protection is not dependent on SIS to function, it means that MSSS has safety-related functions during both Operational States and Accident Conditions.

ESWS also provides cooling water to CCWS heat exchangers, EDG heat exchangers, EPGBVS coolers, and ESWPBVS room coolers. Portions of CCWS and ESWS trains also support active heat removal from the containment to the UHS by SAHRS heat exchangers. This means that CCWS and ESWS are designed to be the cooling medium

during all phases of operation, as they already transfer heat from SIS/RHR system during Operational States and Accident Conditions. (Areva NP, Inc. 2013f, p. 9.2-1, 9.2-25). Additionally, it means that CCWS, ESWS and UHS heat removal chains occur in two different main safety functions, as SAHRS is a containment safety system.

Normal heat removal from the RCS is provided by MFWS by supplying feedwater to the SGs. EFWS provides the heat removal functions upon loss of normal feedwater. Its safety-related functions consist of maintaining SG water inventory, removing residual heat from the RCS, assisting in the depressurization of the RCS, isolating EFWS flow following an MSLB or an SGTR, and providing sufficient water inventory in storage pools. (Areva NP, Inc. 2013g, p. 10.4-73–10.4-74).

IRWST is relied upon to be the source of water for multiple plant safety systems. It contains sufficient borated water volume for CVCS operation and safety injections during DBAs. It provides gravity-driven coolant flow to CMSS cooling structure through SAHRS. And in addition, it provides water inventory for SAHRS active containment spray system and SAHRS active sump strainer backflush. (Areva NP, Inc. 2013d, p. 6.3-9; Areva NP, Inc. 2013i, p. 19.2-13–19.2-16).

The integrity of the RCPB in U.S. EPR is maintained by closed systems during Operational States and by RPV during Accident Conditions when closed piping is compromised, excluding core melt accidents because melt retention within the RPV is not feasible in a large reactor such as U.S. EPR. Overpressure protection is provided by PSRVs during Operational States and by PDSVs during Accident Conditions. In addition, PDSVs provide RCS heat removal during transients and LOCAs. During severe accidents, PDSV trains are manually actuated by an operator to prevent High Pressure Melt Ejection (HPME) and RCS failure at high pressure. They provide reliable depressurization of the RCS and as such, are required to survive from a severe accident with core melt. PSRVs and PDSVs are connected to the Pressurizer to ensure RCPB integrity and they are functionally independent of each other. Both discharge to the same

PRT for steam condensation and cooling. (Areva NP, Inc. 2013c, p. 5.4-47–5.4-48; Areva NP, Inc. 2013i, p. 19.2-11, 19.2-23, 19.1-100).

Containment isolation is required during DBAs to confine radioactive releases inside the containment. Protection System sends automatic actuation signals to containment isolation valves to isolate non-essential process lines during required plant conditions, if one initial condition regarding containment pressure, containment activity or safety injection is met during DBAs. As part of CIS design, non-essential containment penetrations are protected by double barriers in series, each actuated by a different PS division. These Containment Isolation Valves are supplied power by EUPS and backed up by EDGs and SBODGs. (Areva NP, Inc. 2013d, p. 6.2-245–6.2-257, 6.2-260–6.2-263).

The containment function of RCB is to work as a barrier to confine radioactive materials that are capable of withstanding the maximum pressure and temperature following the release of stored energy during LOCAs, MSLBs or severe accidents (p. 19.2-6).

CGCS has two containment safety-related functions. Its first safety-related function is to provide a mixed and homogenous gas atmosphere in the containment. Its second function is to control and maintain containment hydrogen concentration in the containment by volume during and following a severe accident leading to release of hydrogen in the containment atmosphere. It is required to mitigate the consequences of severe accidents with core melt. (Areva NP, Inc. 2013i, p. 19.2-23, 19.2-31).

SAHRS and CMSS both operate simultaneously to cool molten core debris. In addition to this heat removal function, CMSS also has a containment safety function as it catches the molten core in a spreading compartment during severe accidents with core melt. It is one of the few systems in U.S. EPR design that has two different main safety functions.

The debris is passively transported to and cooled in CMSS cooling structure, which is provided passive coolant flow from IRWST through SAHRS as its first mode of operation. The second mode of operation for SAHRS is to provide heat removal from the

containment with an active containment spray system suctioning water from IRWST. The spray system reduces containment pressure and temperature by condensing atmospheric steam into water that flows back to IRWST. In the third mode of operation, an active long-term recirculation is provided by pumping water from IRWST directly to the spreading compartment. The fourth mode provides backflushing for sump strainers to prevent a suction line to IRWST from being blocked by any debris. (Areva NP, Inc. 2013i, p. 19.2-14–19.2-17).

In addition, SAHRS has a cooling chain dedicated only to core melt accidents, where SAHRS heat exchangers transfer residual heat with portions of CCWS and ESWS trains to the UHS to support active heat removal from the containment. This cooling chain is not used to mitigate the consequences of DBAs. (Areva NP, Inc. 2013i, p. 19.2-17).

SAHRS is only used during core melt accidents in case SIS/RHR system fails to prevent Accident Conditions evolving into a severe accident with core melt. CMSS and SAHRS are both required to survive from a severe accident with core melt. Operator action is required to start the operation of SAHRS active containment spray. As a SAM -system, active components of SAHRS and the dedicated cooling chain can be powered by any available power sources. (Areva NP, Inc. 2013i, p. 19.2-14–19.2-17, 19.2-23). These features increase the reliability of the containment cooling during worst-case scenarios.

As explained in Chapter 4, the power supply to the active safety systems is provided by offsite power supplied by NPSS during Operational States. During DBAs and post-Accident Conditions, offsite power is supplied by EPSS through the same station switchyard. EPSS is also connected to four EDGs used during a LOOP accident, and it can be connected to non-safety-related SBODGs used during an SBO when both offsite and EDGs are unavailable to provide power. (Areva NP, Inc. 2013e, p. 8.1-1). Absent all other electrical power supply, SBODGs supply electricity to SAM -systems as well.

There are also two other power systems, EUPS and 12UPS, that provide power supply to some I&C and distribution systems. In addition, EUPS provides power to MSRT valves and CIVs in the event of an SBO, and 12UPS provides power to PDSVs and outer

containment isolation valves during severe accidents. EUPS and 12UPS are both battery-powered and their chargers are powered by SBODGs, creating functional dependency between EUPS and 12UPS to SBODGs. (Areva NP, Inc. 2013e, p. 8.1-3, 8.3-46, 8.3-51). Clearly, there is interdependency between safety-related power sources, but the backup power systems create a reliable power supply to U.S. EPR design. Critical depressurization valves and selected I&C systems are backed by passive battery systems, making them less dependent on active power systems.

CRACS provides a safe environment inside the MCR during Operational States and DBAs. In addition, it is a DEC system in the event of an SBO. The power supply is received from EDGs in the event of a LOOP and it is backed by two divisions of SBODGs to cope with an SBO event. (Areva NP, Inc. 2013f, p. 9.4-9–9.4-10). CRACS is an important habitability system to support other safety systems that require operator action. However, it is not credited during core melt accidents, which means that CRACS does not provide safety-related functions to support safety systems during core melt accidents. For example, operator action from the MCR is required to start SAHRS containment sprays (Areva NP, Inc. 2013i, p. 19.1-102). This is contradictory, as a safe environment for the operators in the MCR cannot be guaranteed by CRACS, even though it receives power supply from SBODGs that are credited to function during core melt accidents.

SBVS services HVAC functions in four divisions of hot mechanical areas of the Safeguard Building, and SBVSE services HVAC functions in four divisions of electrical, I&C and HVAC areas of Safeguard Building during Operational States, DBAs and DECs. ESF components, such as EFWS and CCWS components, are housed in the Safeguard Building controlled-area. As such, their internal heat loads are ventilated by SBVS and SBVSE. Power supply for both is received from EDGs in the event of a LOOP. They are both backed by SBODGs to cope with an SBO event. (Areva NP, Inc. 2013f, p. 9.4-49, 9.4-56–9.4-57, 9.4-67, 9.4-77).

ESWPBVS provides HVAC functions in ESWS pump areas and their associated electrical equipment areas during Operational States and DBAs. ESWS pumps are housed

in ESWS Pump Buildings. Power supply for ESWPBVS is provided by EPSS in the event of a LOOP and it is not backed by SBODGs, meaning that HVAC functions are not provided for ESWS pumps in the event of an SBO. This is contradictory, as ESWS itself is backed by SBODGs and continues to generate internal heat loads in the event of an SBO. CCWS is part of the same heat removal chain as ESWS, and CCWS components are ventilated by SBVS and SBVSE even in the event of an SBO. (Areva NP, Inc. 2013f, p. 9.2-12, 9.4-60, 9.4-67, 9.4-131, 9.4-135).

CBVS provides HVAC functions in the containment for operators and instruments operability during Operational States, and containment isolation by closing Containment Isolation Valves upon receiving a containment isolation signal. It is not explicitly stated in U.S. EPR FSAR, but CBVS operates as a part of CIS, as it provides closure of Containment Isolation Valves. The valves are provided power supply by alternate onsite power sources. (Areva NP, Inc. 2013f, p. 9.4-85–9.4-87, 9.4-91).

EPGBVS provides HVAC functions to support the operation of EDGs and their associated electrical control panels during Operational States and DBAs. However, as EDGs are in stand-by mode during Operational States, they are not generating internal heat loads during those plant states. EPGBVS does still provide HVAC functions but this is indicated with a grey font in Figure 5.1. EPGBVS is not affected by a LOOP event, as each division is provided power supply by their corresponding EDG. In addition, as EDGs are not operating in the event of an SBO, neither is EPGBVS required to operate. (Areva NP, Inc. 2013f, p. 9.4-114, 9.4-121).

SBORVS provides HVAC functions to support the operation of SBODGs and associated electrical equipment during DECs and severe accident with core melt. However, as SBODGs are in stand-by mode during Operational States and DBAs, they are not generating internal heat loads during those plant states. SBORVS does still provide HVAC functions but this is indicated with a grey font in Figure 5.1. SBORVS is not affected by an SBO event, as each division is provided power supply by their corresponding SBODG. (Areva NP, Inc. 2013f, p. 9.4-125, 9.4-128).

5.2 Safety system interdependencies of NuScale

The major operating systems, as well as front-line safety systems implemented in NuScale according to Figure 2.4, are presented in Figure 5.2 below. The safety systems are placed in their respective positions in the matrix based on their safety functions as discussed in NuScale Design Certification Application documents.

	Operational States		Accident Conditions		
	Normal Operation	Anticipated Operational Occurrences	Design Basis Accidents	Design Extension Conditions	
				Without significant fuel damage	With core melting
Subcriticality	CVCS	CVCS			"N/A"
	CRA	CRA	CRA		
	Soluble boron				
	Gadolinia				
Heat removal	SG → Condenser → CWS → Atmosphere	SG → Condenser → CWS → Atmosphere			
	RCCWS → SCWS → Atmosphere	RCCWS → SCWS → Atmosphere			
		ECCS → CNV → UHS	ECCS → CNV → UHS	ECCS → CNV → UHS	
		SG → DHRS → UHS	SG → DHRS → UHS	SG → DHRS → UHS	
			RPV → CNV → UHS	RPV → CNV → UHS → Atmosphere	RPV → CNV → UHS → Atmosphere
				CFDS	
Containment	Closed piping (RCPB)	Closed piping (RCPB)	RPV	RPV	
	RSVs → CNV	RSVs → CNV			
		CIVs	CIVs	CIVs	
Power supply	TG				
		EDSS	EDSS		
			BPSS	BPSS	
HVAC	CRVS	CRVS	CRHS	CRHS	
	RBVS	RBVS			

Figure 5.2. The major operating systems as well as front-line safety systems implemented in NuScale placed on the functional Defence-in-Depth template.

In NuScale design, some systems are shared between modules and these systems are indicated by a blue font in Figure 5.2 above. Shared systems have not been relevant with traditional single-unit nuclear power plants before multi-module SMRs started to implement them in their design. As there is little experience of sharing safety systems in nuclear power plants, they should be designed with great care.

As can be seen from Figure 5.2, CVCS provides safety-related functions only during Operational States and is not required to function during Accident Conditions. It maintains and adjusts the concentration of soluble boron during NO. In addition, gadolinia provides safety-related functions only during NO. The two banks of CRAs have safety-related functions during both Operational States and Accident Conditions. The regulating bank is used for operational reactivity control during Operational States. The shutdown bank is used for shutdown and reactor trip events during DBAs. The movement of CRAs is provided by Control Rod Drive System (CRDS), which releases CRAs and maintains the RCPB. (NuScale Power, LLC. 2020b, p. 4.1-1–4.1-2, 4.6-1).

NuScale does not implement an Anticipated Transients Without Scram (ATWS) system. In the event of an ATWS, the core is not required to remain subcritical, because heat removal from the core is modelled to be sufficient to prevent core damage. The reactor module remains at power low enough to be comparable with decay heat levels during DECs. (NuScale Power, LLC. 2020i, p. 19.1-70, 19.1-157, 19.2-2). And as usual, subcriticality of the reactor core is not feasible during severe accidents with core melt, which is why it is indicated by “N/A”.

The secondary circuit heat removal in NuScale design is dependent on multiple different systems during NO and AOOs and is quite similar to U.S. EPR design. The heat removal chain starts from SGs to Main Condenser, and the heat continues to be transferred to the Atmosphere through CWS. The only difference is that CWS consists of two subsystems each serving cooling water up to six Main Condensers at a time, as indicated by the blue font in Figure 5.2. It is stated that the loss of CWS functions would result in transients impacting multiple NPMs, but the safety-related functions would not be adversely

affected. (NuScale Power, LLC. 2020j, p. 21-12). This makes it less independent than in U.S. EPR, but it is still not very risk significant as their safety-related functions are limited to the plant Operational States. Secondary circuit heat removal functions are not compromised during minor transients.

RCCWS provides cooling to Control Rod Drive Mechanism electromagnetic coils housing, CVCS heat exchangers and other non-safety-related components. The heat load generated by these components are transferred by SCWS cooling towers to the Atmosphere. (NuScale Power, LLC. 2020f, p. 9.2-2). As was with the secondary circuit heat removal, this heat removal chain from RCCWS to SCWS, and from SCWS to the Atmosphere can also be compared to U.S. EPR heat removal chain of CCWS to ESWS and from ESWS to UHS. The differences are that both RCCWS and SCWS are shared systems and they have safety-related functions only during Operational States. RCCWS consists of two subsystems each serving up to six NPMs at a time, and SCWS is shared between up to 12 NPMs at a time, as indicated by the blue fonts in Figure 5.2 (NuScale Power, LLC. 2020j, p. 21-11–21-12).

It is stated that no single failure in RCCWS can cause loss of its heat removal functions for more than one NPM. In addition, a failure in SCWS could impact multiple NPMs, but the safety-related functions would not be adversely affected. A total loss of SCWS could result in reactor trips in multiple NPMs due to losing heat removal capabilities of RCCWS. (NuScale Power, LLC. 2020j, p. 21-11–21-12). This creates some interdependency between RCCWS and SCWS, but they are still not very risk significant as they do not have safety-related functions during Accident Conditions.

Emergency heat removal functions are provided by ECCS during AOOs, DBAs and DECs, and especially during LOCAs, so it has safety-related functions during both Operational States and Accident Conditions. The function of RVVs is to let steam discharge from the RPV to the CNV, where it condenses and fills the bottom of the CNV. The heat from the steam is transferred by passive convection to the CNV walls. The condensed water can then be recirculated back to the RPV through RRVs until the water

levels inside the RPV and the CNV are stabilized above the reactor core. The heat from the CNV walls is transferred by passive conduction to the reactor pool, which is a part of the UHS. Opening of RVVs reduces the reactor pressure and increases the containment pressure until they reach an equilibrium, after which both pressures decrease with time. (NuScale Power, LLC. 2020d, p. 6.3-1).

ECCS requires two RVVs and one RRV to open to sufficiently cool the reactor core. The valves are actuated either by a safety function signal sent by Module Protection System (MPS), loss of power from EDSS or by operator action that de-energizes the actuator trip valve solenoid. This means that ECCS valves are capable of actuation on stored energy. ECCS does not require any active AC or DC power current or additional makeup water to achieve its safety-related functions. (NuScale Power, LLC. 2020d, p. 6.3-2, 6.3-5).

DHRS provides residual heat removal and decay heat removal during AOOs, DBAs and DECs, and especially during non-LOCAs when the normal secondary side cooling is unavailable or otherwise not used. So, it has safety-related functions during both Operational States and Accident Conditions. When DHRS is actuated, Main Steam Isolation Valves (MSIVs) and Feedwater Isolation Valves (FWIVs) close, and DHRS actuation valves open. This allows steam from the SGs to flow into DHRS condensers to be condensed and heat to be transferred to the reactor pool and therefore to the UHS. The condensed water continues to flow back to the SGs with natural circulation to continue the loop. (NuScale Power, LLC. 2020c, p. 5.4-16; NuScale Power, LLC. 2020h, p. 15.0-34).

DHRS actuation valves are designed to open upon interruption of control system power or loss of power. They can also be opened manually from the MCR or a remote location outside the MCR. DHRS requires both MSIVs and FWIVs to close in order to function. If they do not, backup MSIVs and feedwater regulating valves are used to isolate DHRS. This creates some functional dependency between CIVs and DHRS. DHRS does not require any active AC or DC power current to achieve its safety-related functions. (NuScale Power, LLC. 2020c, p. 5.4-18–5.4-19).

The emergency heat removal chain by ECCS, and decay and residual heat removal chains by DHRS are straightforward and not dependent on other safety systems to achieve their safety-related functions. ECCS is only dependent on fail-safe valves to transfer heat passively from the core to the CNV and so on to the UHS. The DHRS only requires the Steam Generators to function to passively transfer heat from the core to the UHS through fail-safe valves. In addition, primary circuit functions with natural circulation during Operational States without reliance on power systems or Reactor Coolant Pumps. Utilizing natural phenomena such as gravity and passive heat transfer through conduction and convection in the operation and safety systems makes NuScale design less dependent on safety-related components and the intended safety-related functions reliable.

One unique feature of NuScale is that heat can passively transfer from the RPV to the CNV during Accident Conditions due to its modular design. Heat is transferred by conduction from the coolant to RPV walls and then by convection from the RPV walls to CNV walls. As the CNV is partially immersed in the reactor pool, the heat from the CNV walls is transferred by passive conduction to the UHS. The large water volume in the UHS provides Long-Term Cooling by removing the generated decay heat from all 12 NPMs without any active safety systems or additional makeup water and maintains the plant in a safe state for at least 72 hours. UHS is the only safety-related system that is shared between multiple NPMs. This is indicated by the blue font in Figure 5.2. (NuScale Power, LLC. 2020d, p. 6.2-22–6.2-23; NuScale Power, LLC. 2020f, p. 9.2-24–9.2-25, 9.2-32).

During Station Blackout, pool cooling systems shut down and water inside the UHS begins to boil, and heat is transferred to the Atmosphere through boiling and evaporation. The UHS is designed to contain water volume for greater than 30 days to cool the reactor core and to prevent fuel damage without operator action, makeup water or electric power before transitioning to Long-Term air Cooling. After 30 days, decay heat generated by a single NPM can be sufficiently cooled indefinitely by the containment air volume. (NuScale Power, LLC. 2020f, p. 9.2-28; Ingersoll et al. 2014, p. 87). Heat removal from the UHS is presented in Figure 5.3 below.

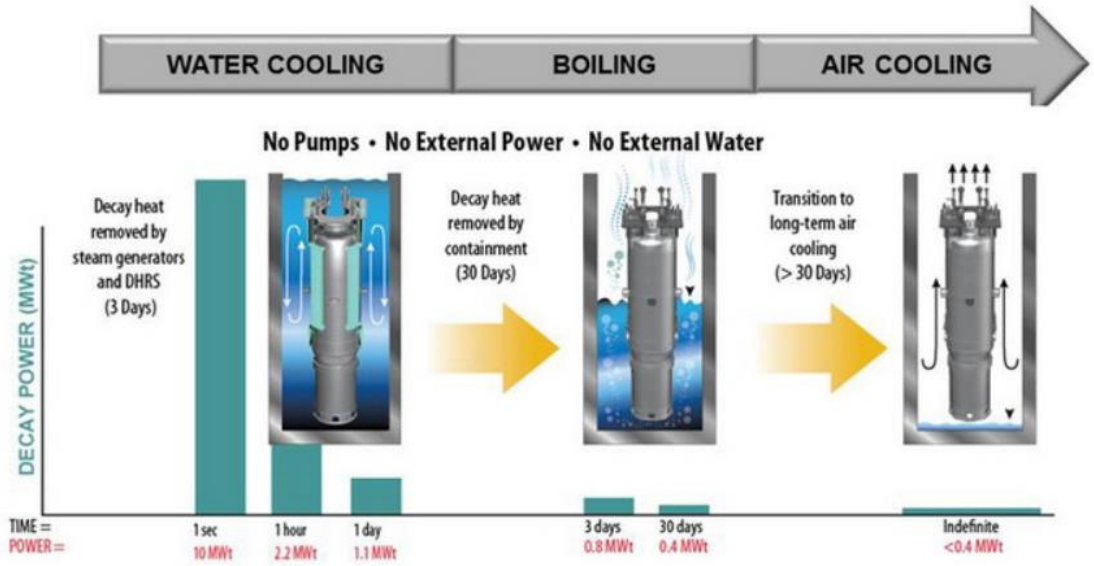

Figure 5.3. Long-Term Cooling during Station Blackout (Ingersoll et al. 2014, p. 88). Water volume in the UHS is sufficient to remove the combined heat load generated by all NPMs for at least 72 hours, and the decay heat generated by a single NPM for 30 days. After 30 days, the UHS transitions to Long-Term air Cooling.

Both CNV and UHS occur in multiple different heat removal chains. But heat removal chain from RPV walls to CNV walls, from the CNV walls to UHS and from the UHS to the Atmosphere is entirely passive, functionally independent of other safety systems and can occur simultaneously with them. Heat removal from the CNV walls to the UHS could also be classified as a containment cooling safety function, but it is kept as part of the same heat removal chain for simplicity. It occurs during all Accident Conditions because in-vessel retention of molten core debris in ensured in NuScale design. The RPV is unlikely to fail due to its large size as compared to core material inventory, low core power density and a large volume of water allowing passive heat transfer during core melt accidents. (NuScale Power, LLC. 2020i, p. 19.2-17).

CFDS is used for emergency flooding of the NPM to add decay heat removal capability during some DECs to prevent core damage. It does not have any safety-related functions, is not required to operate during or after any DBA and is not required to reach a safe

shutdown. It is an active system, but it functions as a Defence-in-Depth backup for passive DHRS and ECCS. Additionally, operator action from the MCR is required to actuate CFDS. It is a shared system between up to six NPMs as indicated by the blue font in Figure 5.2. As a result of the reliability of the passive heat removal systems, CFDS is found not to be risk significant. (NuScale Power, LLC. 2020f, p. 9.3-87, 9.3-91, 9.3-98; NuScale Power, LLC. 2020i, p. 19.1-138, 19.1-170).

The integrity of the RCPB in NuScale is maintained by closed systems during Operational States and by RPV during DBAs and DECs when closed piping is compromised. (NuScale Power, LLC. 2020c, p. 5.1-3). As this is a containment function, it means that RPV has two different main safety functions.

Overpressure protection by discharging steam directly to the CNV volume is provided by RSVs during Operational States. They are not used during Accident Conditions and NuScale design does not implement any diverse depressurization system, as pressure relief is accomplished by ECCS valves during Accident Conditions. (NuScale Power, LLC. 2020c, p. 5.2-4–5.2-6; NuScale Power, LLC. 2020h, p. 15.2-10–15.2-11). CNV is also a part of the ECCS heat removal chain, which means that it has two different main safety functions.

CIVs confine possible releases of radioactive material inside the containment during DBAs. In addition, CIVs provide safety-related functions during AOOs and DECs, because DHRS requires MSIVs and FWIVs to close to provide its safety-related functions. This means that CIVs have safety-related functions during both Operational States and Accident Conditions. They are hydraulically operated and designed to close upon loss of power, loss of hydraulic pressure or closure signal from MPS. Electrical power is not required for CIVs to close, as they close upon de-energization. (NuScale Power, LLC. 2020c, p. 5.4-19; NuScale Power, LLC. 2020d, p. 6.2-30).

As explained in Chapter 4, the safety systems for each NPM are powered by their corresponding Turbine Generator through the station switchyard during NO. During conditions when the TG is not operating and supplying power to its associated NPM, the

plant can be operated in an island mode where one or more Turbine Generators can supply power to other NPMs through the station switchyard. (NuScale Power, LLC. 2020e, p. 8.2-1). This design increases the interdependency between modules and the plant's self-sufficiency, as the plant safety systems can be operated without reliance on offsite power. However, the power to all NPMs is supplied through the same switchyard, making it more risk significant.

Even though there aren't safety-related loads and NuScale design doesn't rely on electrical power or operator action to achieve and maintain a safe shutdown, it includes a non-safety-related DC battery system and non-safety-related backup power supply system. EDSS provides a continuous DC power source to selected non-safety-related loads during AOOs and DBAs, and its battery system is charged by normal AC power sources. (NuScale Power, LLC. 2020e, p. 8.1-3–8.1-4, 8.3-22, 8.3-29). It is used during both Operational States and Accident Conditions.

BPSS provides an AC power source through two BDGs or AAPS during conditions when none of the 12 NPMs is operating to provide onsite power and offsite power sources are unavailable. It is not required to achieve a safe shutdown, even in the event of an SBO. (NuScale Power, LLC. 2020e, p. 8.1-2–8.1-4, 8.4-1). These power systems increase the safety of NuScale design even though they are not required to achieve a safe shutdown during Accident Conditions. NuScale design does not include any emergency power systems or SBODGs during core melt accidents, as the plant demonstrates "sufficient capacity and capability to ensure that the reactor core is cooled and appropriate containment integrity is maintained in the event of an SBO for the specified duration." (NuScale Power, LLC. 2020e, p. 8.4-1).

NuScale design does not include any safety-related HVAC systems, as operator action is not credited to achieve a safe shutdown during Accident Conditions. It does include non-safety-related HVAC systems that are designed to support personnel and equipment and to control radioactivity in the air.

Acceptable ambient conditions in the MCR are provided by CRVS during Operational States and by CRHS during DBAs and DECs. NuScale design does not include any HVAC systems during core melt accidents. If CRVS is unavailable to provide a safe environment for operators during certain accidents such as an SBO, CRHS isolates the CRE through CRVS dampers and provides clean breathing air to the MCR for 72 hours without reliance on electrical power. However, as operators are not credited and do not perform any safety-related functions either during or after 72 hours following a DBA, CRVS and CRHS are not classified as safety-related systems. Both systems are also shared between up to 12 NPMs, as indicated by the blue fonts in Figure 5.2. CRVS is powered by normal AC electrical distribution system and can be backed by BDGs through BPSS, in case normal AC power is lost. A loss of power from BDGs results in actuation of CRHS. As it does not rely on electrical power, it continues to operate in the event of an SBO. (NuScale Power, LLC. 2020d, p. 6.4-1-6.4-2, 6.4-5; NuScale Power, LLC. 2020e, p. 9.4-1–9.4-3, 9.4-9).

RBVS is a non-safety-related system that provides acceptable ambient conditions in the Reactor Building during NO and AOOs that have the potential for radioactive releases inside the Reactor Building, but not during DBAs. The Reactor Building is shared between up to 12 NPMs, meaning that RBVS is also shared between up to 12 NPMS, as indicated by the blue font in Figure 5.2. Its capability to operate is not significantly affected during an accident in one unit. (NuScale Power, LLC. 2020f, p. 9.4-19).

6 COMPARISON BETWEEN SAFETY SYSTEMS OF U.S. EPR AND NUSCALE

The safety systems between U.S. EPR and NuScale are compared in this Chapter. It is convenient to compile them together in Table 6.1 below to get a comprehensive overview of what traditional safety systems are not included in NuScale design.

Table 6.1. The safety systems and components required to protect the reactor core in U.S. EPR and NuScale.

Safety system or component	**U.S. EPR**	**NuScale**
Reactor Pressure Vessel	RPV	RPV
Containment Vessel	CNV	CNV
Reactor Coolant System	RCS	RCS
Decay Heat Removal System	LHSI	DHRS
Emergency Core Cooling System	SIS	ECCS
Control Rod Drive System	RCCA	CRA
Containment Isolation System	CIS	CIVs
Ultimate Heat Sink	UHS	UHS
Residual Heat Removal System	RHRS	DHRS/ECCS
Safety Injection System	SIS	ECCS
Refuelling Water Storage Tank	IRWST	-
Auxiliary Feedwater System	EFWS	-

Emergency Service Water System	ESWS	-
Hydrogen Recombiner or Ignition System	CGCS	-
Containment Spray System	SAHRS	-
Reactor Coolant Pumps	MCPs	-
Safety-Related Electrical Distribution System	EPSS	-
Alternative Offsite Power	PPS	-
Emergency Diesel Generators	EDGs	-
Safety-Related Class 1E Battery System	EUPS	-
Anticipated Transient Without Scram (ATWS) system	EBS	-

As can be seen from Table 6.1, traditional U.S. EPR implements more safety systems as compared to a simple and compact NuScale design. NuScale Power Module design implements an integrated primary circuit, which utilizes natural circulation to cool the reactor core. U.S. EPR design requires forced circulation with Main Coolant Pumps to create sufficient coolant flow to remove heat from the reactor core. Additionally, emergency heat removal systems are passive in NuScale design as opposed to more complex active heat removal systems in U.S. EPR design. These are the main reasons why NPM can be designed to be compact, as it does not require huge components, their associated piping or active safety systems to be built inside the NPM.

U.S. EPR design does not include a diverse Decay Heat Removal System or a diverse Emergency Core Cooling System. Two different systems function in conjunction as SIS/RHR system that provides residual heat removal via RHRS, decay heat removal via LHSI heat exchangers, emergency core cooling and safety injection via SIS. (Areva NP, Inc. 2013c, p. 5.4-26–5.4-27; Areva NP, Inc. 2013d, p 6.3-1). The same system

combination has multiple different safety-related functions, which is why diverse systems are not implemented.

NuScale design does not include a diverse Residual Heat Removal System. Decay heat and residual heat removal are provided by DHRS during non-LOCAs and by ECCS during LOCAs. Passive means of DHRS and ECCS residual heat removal are enough to ensure that specified acceptable fuel design limits are not exceeded, design conditions of the RCPB are not exceeded, and residual heat safety functions can be accomplished assuming a Loss Of Offsite Power or onsite power occurring simultaneously with a single failure. (NuScale Power, LLC. 2020e, p. 9.5-95; NuScale Power, LLC. 2020h, p. 15.0-33). For these reasons, a diverse Residual Heat Removal System is not needed.

NuScale design does not include a diverse Safety Injection System or a Containment Spray System. Sufficient heat removal and water inventory in the core is provided by ECCS through steam condensation and natural circulation (NuScale Power, LLC. 2020a, p. 1.9-15). A Refueling Water Storage Tank is not included in NuScale design either, because there isn't a system, such as a Safety Injection System or a Containment Spray System, that would draw water for their safety-related functions.

NuScale design does not include an Emergency Service Water System that has safety-related functions. SCWS provides Normal Service Water System functions as a cooling medium to transfer heat from RCCWS to the Atmosphere during Operational States, but it doesn't have safety-related functions during Accident Conditions. ESWS functions as a similar cooling medium to transfer heat from CCWS to the UHS in U.S. EPR, but it has safety-related functions during Accident Conditions as well. This is because U.S. EPR design implements safety-related systems that require heat removal functions from ESWS during Accident Conditions, while NuScale does not implement safety-related systems that require heat removal functions from SCWS during Accident Conditions.

NuScale design does not include a diverse Hydrogen Recombiner or Ignition System. The CNV is capable of withstanding the conditions created due to hydrogen combustion during the first 72 hours of Accident Conditions while the containment integrity and safe

shutdown capability are maintained, and radiological releases are prevented. (NuScale Power, LLC. 2020d, p. 6.2-45).

NuScale design does not include safety-related electrical power systems. Alternative Offsite Power systems are site-specific, and BDGs and Battery Systems are classified as non-safety-related because NuScale is designed to achieve and maintain a safe shutdown without any reliance on electrical power. (NuScale Power LLC. 2020e, p. 8.1-1, 8.1-4).

NuScale design does not include a diverse ATWS system. Traditionally the risk associated with ATWS events is reduced by implementing a diverse scram system that initiates an auxiliary feedwater or an emergency feedwater system, and a turbine trip under conditions indicative of an ATWS. NuScale design does not include an auxiliary feedwater or an emergency feedwater system, because DHRS performs some functions similar to an auxiliary feedwater system. In addition, NuScale does not include a diverse turbine trip system either, based on the diversity of Module Protection System design. ATWS contribution to CDF per reactor is $2{,}2 \cdot 10^{-11}$/a as a result of the reliability of the reactor trip function of MPS. It is well below the U.S. NRC requirement of $1{,}0 \cdot 10^{-5}$/a. (NuScale Power, LLC. 2020g, p. 10.4-40; NuScale Power, LLC. 2020h, p. 15.8-1; NuScale Power, LLC. 2020i, p. 19.1-120, 19.3-2).

In the event of an ATWS at full power, fuel heats up and moderator density decreases as a result of a large positive moderator density coefficient (negative MTC), leading to a decrease of core power. Sufficient heat removal from the core is maintained to avoid core damage and a subcritical state is achieved even without scram. However, NuScale Probabilistic Risk Assessment (PRA) analyses suggest that the core is not required to remain in a subcritical state to achieve successful end states. In the event of an ATWS, the core is left at a power level that is comparable to decay heat levels. This is feasible, because of the excess heat transfer capacity of passive cooling systems. It is a direct result of the relatively small core size, large coolant-to-power ratio and the passive heat transfer features in NuScale design. (NuScale Power, LLC. 2020i, p. 19.1-12, 19.1-41, 19.1-157, 19.1-170).

7 OBSERVATIONS OF FUNCTIONALITIES

The similarities and differences between the safety systems of U.S. EPR and NuScale are studied in this Chapter. As stated previously, some safety systems can provide safety-related functions on multiple levels of defence. And judging from Figures 5.1 and 5.2, instead of five individual levels of defence, a clear distinction between Operational States and Accident Conditions can be seen. In U.S. EPR design, there are some cases where the same safety systems have safety-related functions during both Operational States and Accident Conditions, but those safety-related functions are different. Contradictory to the independence of Defence-in-Depth levels, sharing the same safety systems between different levels of defence can improve the plant safety, as long the primary safety-related function is not compromised.

In U.S. EPR, control rods provide operational reactivity control during Operational States and reactor trip during DBAs. SIS/RHR system provides normal residual heat removal to assist reactor shutdown during NO and emergency core cooling during Accident Conditions. MSSS provides depressurization of steam circuit during AOOs and initial residual heat removal and secondary heat removal during Accident Conditions. CCWS and ESWS function as a cooling medium for different safety systems, depending on the plant state. EFWS provides RCS cooldown during AOOs and maintains water inventory during DBAs. PRT condenses and cools steam that is discharged to it from two different systems during Operational Sates and Accident Conditions. (Areva NP, Inc. 2013c, p. 5.4-26; Areva NP, Inc. 2013f, p. 9.2-1, 9.2-25; Areva NP, Inc. 2013g, p. 10.3-1, 10.4-74).

As a traditional LWR, operator action is required to mitigate the consequences during some Accident Conditions in U.S. EPR design. Because of this, HVAC systems are required to provide acceptable ambient conditions in their respective buildings regardless of the plant state. There aren’t any diverse HVAC systems, which means that the same systems provide acceptable ambient conditions during both Operational States and Accident Conditions. Only their supply of electrical power is diverse, depending on the plant state.

NuScale design implements safety systems that have safety-related functions during both Operational States and Accident Conditions too, but those functions are the same, apart from control rods. The safety-related functions of ECCS, DHRS, CIVs and their associated heat removal chains are the same regardless of plant conditions. The difference to U.S. EPR is that these systems function passively and are actuated upon loss of electrical power. Highly Reliable Direct Current Power System EDSS has safety-related functions during AOOs and DBAs too, but it is classified as a non-Class 1E system (NuScale Power LLC. 2020e, p. 8.3-23).

Judging from Figures 5.1 and 5.2, different safety systems provide the same safety function on different levels of defence in both facilities. This increases diversity and independency of plant safety. In U.S. EPR, heat removal from the reactor core is provided by SIS/RHR system during conditions when the core is intact, but heat removal from the molten core (debris) is provided by CMSS during core melt accidents. Upon loss of normal feedwater, the feedwater heat removal functions provided by MFWS are replaced by EFWS. Reactor Coolant Pressure Boundary functions are provided by the RPV during Accidents Conditions when the integrity of the RCPB cannot be maintained by closed piping. Overpressure protection of the RCS is provided by PSRVs during Operational States, but they are not credited during Accident Conditions. Instead, PDS provides overpressure protection with active PDSVs during Accident Conditions. Power to active safety systems is provided by NPSS, EPSS and SBODGs during different plant states. (Areva NP, Inc. 2013c, p. 5.4-26, 5.4-47; Areva NP, Inc. 2013e, p. 8.1-1; Areva NP, Inc. 2013g, p. 10.4-73, 10.4-78–10.4-79, 10.4-87; Areva NP, Inc. 2013i, p. 19.2-11).

In NuScale, RCPB functions are also provided by RPV during Accidents Conditions when the integrity of the RCPB cannot be maintained by closed piping. And as operator action is not required to mitigate the consequences during Accident Conditions, it implements fewer HVAC systems, none of which are classified as safety-related systems. Only in the MCR are acceptable ambient conditions provided for the operators during both Operational States and Accident Conditions, with two diverse systems. They are

normally provided by CRVS, and during conditions when it is unavailable, they are provided by CRHS. (NuScale Power, LLC. 2020d, p. 6.4-1).

As mentioned in Chapter 5, both facilities implement systems that have two different main safety functions. In U.S. EPR design, MHSI and CMSS genuinely provide two different main safety functions, while CCWS, ESWS and UHS heat removal chains just occur in two different main safety functions. They provide the function of being a cooling medium, but the systems they provide that same function to have two different main safety functions. In NuScale, RPV and CNV are just passive components without active systems that provide two different main safety functions due to their design. In none of these systems are their safety functions compromised for having two different main safety functions, as they can provide them simultaneously. This increases plant safety.

As discussed in Chapter 6, NuScale design implements fewer safety and support systems than U.S. EPR. Table 7.1 below illustrates how many safety systems combinations and support systems have safety-related functions between different levels of defence in both facilities.

Table 7.1. The number of safety system combinations and support systems that have safety-related functions between different levels of defence as shown in Figures 5.1 and 5.2.

Number of safety system combinations and support systems	**AOOs**	**DBAs**	**DECs**
U.S. EPR	17	21	15
NuScale	12	9	8

Because many of the safety system combinations and support systems have safety-related functions on multiple levels of defence, there are only 30 different safety system combinations and support systems used in U.S. EPR that are responsible for all of those numbers during those levels of defence in Table 7.1. In NuScale, there are only 15. In its

design, systems that occur in the most levels of defence in Table 7.1 are UHS and CNV. The UHS is a part of three different system combinations, which occur during eight of the levels. Similarly, the CNV is a part of three different combinations, which occur during six of the levels.

In addition, when comparing Figures 5.1 and 5.2, functional dependencies are less complicated and heat removal chains are more straightforward in NuScale than in U.S. EPR. Its safety systems do not have any complex dependencies to support systems required to achieve a safe shutdown, even though they are provided. During Accident Conditions, safety-related functions are achieved passively without any reliance on active systems or electrical power. They are only dependent on fail-safe valves to actuate and DHRS heat exchangers to function.

Judging from Figure 5.2, NuScale does not include any diverse safety systems during severe accidents with core melt. Only a single passive heat removal chain is explicitly stated to occur in the NuScale DCA because results of the in-vessel retention-RPV analysis indicate that "failure to retain core debris in the RPV after a core damage accident involving an intact containment does not occur". (NuScale Power, LLC. 2020i, p. 19.1-181, 19.2-17).

Unique to SMR designs, multi-module designs are considered in NuScale. Excluding the UHS, only some non-safety-related systems are shared between multiple modules and as such, their impact on the safety of other modules is limited. All modules are functionally independent of other modules. Initiating events that have the ability to affect multiple modules are mitigated by passive, module-specific safety-related systems and non-safety-related shared systems provide Defence-in-Depth backup to them. During any Accident Condition, CFDS is the only non-safety-related shared system used as a Defence-in-Depth measure, as it functions as a backup system to the passive heat removal systems. Due to these reasons, multi-module accident sequence contributions to the plant risk are insignificant. (NuScale Power LLC. 2020i, p. 19.1-114, 19.1-267). From the low MM-CDF, it can be concluded that core damage to multiple modules is unlikely to occur.

8 CONCLUSIONS

Instead of five diverse safety systems for each individual level of defence, the same safety systems often provide safety-related functions on multiple levels either during plant Operational States or Accident Conditions. Even though a clear distinction between plant Operational States and Accident Conditions can be seen, there are some exceptions where same safety systems have safety-related functions regardless of the plant state. These exceptions to safety system independency are justified differently in both facilities. In U.S. EPR, the safety-related functions of the same safety systems are different between plant Operational States and Accident Conditions. In NuScale, the safety-related functions of the same safety systems between plant Operational States and Accident Conditions are reliable, as they function passively and are actuated upon loss of electrical power.

Both facilities also implement safety systems that have two different main safety functions, but in none of these systems are their safety functions compromised for having two different main safety functions, as they can provide them simultaneously. As theoretically intended, there are also diverse systems that provide the same safety-related function on different levels of defence. This increases diversity and independency of plant safety.

Functional dependency occurs in both facilities, but when comparing the safety systems and heat removal chains, they are more complex and more dependent on other safety and support systems to achieve their safety-related functions in U.S. EPR than in NuScale. Heat removal to the UHS is provided by the same heat removal chain, servicing multiple front-line safety systems in U.S. EPR during Accident Conditions. In NuScale, safety-related functions are achieved passively without any reliance on active systems or electrical power during Accident Conditions. Utilizing natural phenomena such as gravity and passive heat transfer through conduction and convection in the operation and safety systems makes its design less dependent on safety-related components and the intended

safety-related functions reliable. It also leads to heat removal chains being more straightforward in NuScale.

NuScale design implements fewer safety systems than U.S. EPR, as it does not implement diverse Residual Heat Removal System, diverse scram system, diverse Safety Injection System, or Containment Spray system. It does not implement any diverse safety systems during severe accidents with core melt either, apart from a single passive heat removal chain occurring. Additionally, NuScale implements fewer support systems. As operator action, electrical power and additional makeup water are not required to achieve and maintain safe shutdown conditions in NuScale, it minimizes the need for safety-related power supply and HVAC systems.

NuScale shares some non-safety-related systems between modules, but their impact on plant safety are not risk-significant as all modules are functionally independent of each other. Some significant safety features of NuScale power plant are the large size of the RPV compared to the core material inventory, low core power density and a large volume of water in the UHS allowing passive heat transfer during core melt accidents.

REFERENCES

Areva NP, Inc. 2007. U.S. EPR Instrumentation and Control Diversity and Defense-in-Depth Methodology Topical Report. Available: https://www.nrc.gov/docs/ML0717/ML071760188.pdf

Areva NP, Inc. 2013a. U.S. EPR Final Safety Analysis Report. AREVA Design Control Document Rev. 5 - Tier 2 Chapter 01 - Introduction and General Description of the Plant. Available: https://www.nrc.gov/docs/ML1326/ML13261A475.html

Areva NP, Inc. 2013b. U.S. EPR Final Safety Analysis Report. AREVA Design Control Document Rev. 5 - Tier 2 Chapter 04 – Reactor. Available: https://www.nrc.gov/docs/ML1326/ML13261A526.html

Areva NP, Inc. 2013c. U.S. EPR Final Safety Analysis Report. AREVA Design Control Document Rev. 5 - Tier 2 Chapter 05 - Reactor Coolant System and Connected Systems. Available: https://www.nrc.gov/docs/ML1326/ML13261A529.html

Areva NP, Inc. 2013d. U.S. EPR Final Safety Analysis Report. AREVA Design Control Document Rev. 5 - Tier 2 Chapter 06 - Engineered Safety Features. Available: https://www.nrc.gov/docs/ML1326/ML13261A532.html

Areva NP, Inc. 2013e. U.S. EPR Final Safety Analysis Report. AREVA Design Control Document Rev. 5 - Tier 2 Chapter 08 - Electric Power. Available: https://www.nrc.gov/docs/ML1326/ML13261A548.html

Areva NP, Inc. 2013f. U.S. EPR Final Safety Analysis Report. AREVA Design Control Document Rev. 5 - Tier 2 Chapter 09 - Auxiliary Systems. Available: https://www.nrc.gov/docs/ML1326/ML13261A550.html

Areva NP, Inc. 2013g. U.S. EPR Final Safety Analysis Report. AREVA Design Control Document Rev. 5 - Tier 2 Chapter 10 - Steam and Power Conversion System. Available: https://www.nrc.gov/docs/ML1326/ML13261A551.html

Areva NP, Inc. 2013h. U.S. EPR Final Safety Analysis Report. AREVA Design Control Document Rev. 5 - Tier 2 Chapter 15 - Transient and Accident Analyses. Available: https://www.nrc.gov/docs/ML1326/ML13262A248.html

Areva NP, Inc. 2013i. U.S. EPR Final Safety Analysis Report. AREVA Design Control Document Rev. 5 - Tier 2 Chapter 19 - Probabilistic Risk Assessment and Severe Accident Evaluation. Available: https://www.nrc.gov/docs/ML1326/ML13262A290.html

Hyvärinen Juhani. 2018. SAFIR2018. Kokonaisturvallisuusseminaari. LUT University.

Hyvärinen Juhani, Kauppinen Otso-Pekka, Vihavainen Juhani. 2016. Overall Safety Conceptual Framework – ORSAC. Final Report Revision 1, December 20, 2016. Lappeenranta University of Technology.

Hämäläinen Jari, Suolanen Vesa. 2020. SAFIR2022 Annual Plan 2020. Available: http://safir2022.vtt.fi/pdf/SAFIR2022_Annual_Plan_2020_signed.pdf

Ingersoll Daniel, Houghton Z.J., Bromm Robert, Desportes C. 2014. NuScale small modular reactor for Co-generation of electricity and water. Available: https://www.sciencedirect.com/science/article/pii/S0011916414000885/pdfft?md5=0c4db15f379808426fdac5c94f52ac15&pid=1-s2.0-S0011916414000885-main.pdf

Mast Uwe, Carrer P.Y. Le. The EPR layout design. Available: https://inis.iaea.org/collection/NCLCollectionStore/_Public/33/011/33011210.pdf?r=1&r=1

Nuclear Energy Agency. 2009. Committee on the safety of nuclear installations. Probabilistic Risk Criteria and Safety Goals. Available: http://www.oecd-nea.org/jcms/pl_18870

NuScale Power, LLC. 2020a. NuScale Standard Plant Design Certification Application. Chapter One Introduction and General Description of the Plant Revision 4. Available: https://www.nrc.gov/docs/ML2003/ML20036D417.pdf

NuScale Power, LLC. 2020b. NuScale Standard Plant Design Certification Application. Chapter Four Reactor. Part 2 – Tier 2. Revision 4. Available: https://www.nrc.gov/docs/ML2003/ML20036D438.pdf

NuScale Power, LLC. 2020c. NuScale Standard Plant Design Certification Application. Chapter Five Reactor Coolant System and Connecting Systems. Part 2 – Tier 2. Revision 4. Available: https://www.nrc.gov/docs/ML2003/ML20036D439.pdf

NuScale Power, LLC. 2020d. NuScale Standard Plant Design Certification Application. Chapter Six Engineered Safety Features. Part 2 – Tier 2. Revision 4. Available: https://www.nrc.gov/docs/ML2003/ML20036D440.pdf

NuScale Power, LLC. 2020e. NuScale Standard Plant Design Certification Application. Chapter Eight Electric Power. Part 2 – Tier 2. Revision 4. Available: https://www.nrc.gov/docs/ML2003/ML20036D444.pdf

NuScale Power, LLC. 2020f. NuScale Standard Plant Design Certification Application. Chapter Nine Auxiliary Systems. Part 2 – Tier 2. Revision 4. Available: https://www.nrc.gov/docs/ML2003/ML20036D448.pdf

NuScale Power, LLC. 2020g. NuScale Standard Plant Design Certification Application. Chapter Ten Steam and Power Conversion System. Part 2 – Tier 2. Revision 4. Available: https://www.nrc.gov/docs/ML2003/ML20036D450.pdf

NuScale Power, LLC. 2020h. NuScale Standard Plant Design Certification Application. Chapter Fifteen Transient and Accident Analyses. Part 2 – Tier 2. Revision 4. Available: https://www.nrc.gov/docs/ML2003/ML20036D460.pdf

NuScale Power, LLC. 2020i. NuScale Standard Plant Design Certification Application. Chapter Nineteen Probabilistic Risk Assessment and Severe Accident Evaluation. Part 2 – Tier 2. Revision 4. Available: https://www.nrc.gov/docs/ML2003/ML20036D466.pdf

NuScale Power, LLC. 2020j. NuScale Standard Plant Design Certification Application. Chapter Twenty-One Multi-Module Design Considerations. Part 2 – Tier 2. Revision 4. Available: https://www.nrc.gov/docs/ML2003/ML20036D468.pdf

STUK. 2019. Guide YVL B.1. Safety design of a nuclear power plant. Regulatory Guides on Nuclear Safety (YVL). Available: http://www.finlex.fi/data/normit/41774-YVL_B.1e.pdf

U.S. NRC. 2020a. Design Certification Applications for New Reactors. Available: https://www.nrc.gov/reactors/new-reactors/design-cert.html [viewed 8.9.2020]

U.S. NRC. 2020b. Final Safety Evaluation Report for the NuScale standard plant design. Available: https://www.nrc.gov/docs/ML2023/ML20231A804.pdf