



OVERALL SAFETY AND THE '3S' OF SMALL MODULAR REACTORS

Master's thesis

Lappeenranta–Lahti University of Technology LUT

Degree Programme in Energy Technology

Master's thesis

2021

Aleksi Valkeapää

Examiners: Professor, D.Sc. (Tech.), Juhani Hyvärinen

D.Sc. (Tech.), Juhani Vihavainen

ABSTRACT

Lappeenranta–Lahti University of Technology LUT

LUT School of Energy Systems

Energy Technology

Aleksi Valkeapää

Overall Safety and the ‘3S’ of Small Modular Reactors

Master’s thesis

2021

143 pages, 48 figures, 23 tables and 15 appendices

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

Keywords: overall safety, small modular reactors, 3S, ORSAC, safety, security, safeguards, NuScale, BWRX-300, RUTA-70, KLT-40S, case study

The topic of this master’s thesis is the Overall Safety of nuclear power. Safety, Security and Safeguards are part of Overall Safety. These three form three safety entities ('the 3S') at the nuclear power plant.

The thesis contributes to research on Overall Safety in two different ways. The already existing tool (ORSAC) is developed further. Such development is done in the theory part by looking for similarities between ‘the 3S’. In addition, Safety, Security and Safeguards (‘3S’) are being surveyed in the context of small modular reactors. The work has been done as a case study for four different SMR designs (NuScale, BWRX-300, RUTA-70, and KLT-40S). The main emphasis has been on assessing the implementation of current technical requirements and safeguardability of the designs.

The development of the Overall safety conceptual framework resulted in an integrated tool for all three ‘S’. The integration of Safety, Security, and Safeguards was identified as possible using the Defence-in-Depth concept and the acceptance criteria of their levels. The safety design of small modular reactors was found to be systematically based on Defence-in-Depth principle and to include both passive safety systems and inherent safety features. The safety design was found to fulfil current requirements well. Regarding Security, the SMR designs under review were found to be following current requirements. With respect to Safeguards, conventional nuclear material accountancy and verification practices were largely identified as applicable. The simultaneous presence of several modules (NuScale), the design capability for misuse (RUTA-70), and the mobility of the floating power unit (KLT-40S) were identified as major challenges for Safeguards. Organizational requirements and design considerations were identified as important for Security and Safeguards.

TIIVISTELMÄ

Lappeenrannan–Lahden teknillinen yliopisto LUT

LUT Energiajärjestelmät

Energiatekniikka

Aleksi Valkeapää

Kokonaisturvallisuus ja pienten modulaaristen reaktoreiden '3S'

Energiatekniikan diplomityö

143 sivua, 48 kuvaa, 23 taulukkoa ja 15 liitettä

Tarkastajat: Professori, TkT, Juhani Hyvärinen, TkT, Juhani Vihavainen

Avainsanat: kokonaisturvallisuus, pienreaktorit, 3S, ORSAC, turvallisuus, turvajärjestelyt, ydinmateriaalivalvonta NuScale, BWRX-300, RUTA-70, KLT-40S, tapaustutkimus

Tämän diplomityön aiheena on ydinvoiman kokonaisturvallisuus (overall safety). Turvallisuus (safety), turvajärjestelyt (security) ja ydinmateriaalivalvonta (safeguards) ovat osa kokonaisturvallisuutta. Nämä kolme yhdessä muodostavat kolmen turvallisuuden kokonaisuuden ('the 3S') ydinvoimalaitoksella.

Diplomityössä edistetään kokonaisturvallisuutta koskevaa tutkimusta kahdella eri menetelmällä. Jo laadittua työkalua (kokonaisturvallisuuden viitekehystä) pyritään kehittämään eteenpäin. Tämä tehdään teoriaosuuden yhteydessä etsimällä samankaltaisuuksia kolmen turvallisuuden välillä. Lisäksi turvallisuutta, turvajärjestelyitä ja ydinmateriaalivalvontaa ('3S') tarkastellaan pienten modulaaristen reaktoreiden kontekstissa. Työ on tehty tapaustutkimuksena neljälle eri SMR-laitokselle (NuScale, BWRX-300, RUTA-70 ja KLT-40S). Pääpaino on ollut nykyisten teknisten vaatimusten ja laitosten ydinmateriaalivalvontakelpoisuuden arvioinnissa.

Kokonaisviitekehysten kehittämisen tuloksena saavutettiin integroitu työkalu kolmelle turvallisuudelle. Turvallisuuden, turvajärjestelyiden ja ydinmateriaalivalvonnan yhdistäminen todettiin mahdolliseksi syvyyspuolustuskonseptin ja siihen liittyvien tasojen hyväksymiskriteerien avulla. Pienten modulaaristen reaktoreiden turvallisuussuunnittelun havaittiin järjestelmällisesti noudattavan syvyyspuolustuksen periaatetta sekä käsittävän passiivisia turvajärjestelmiä ja luontaisia turvallisuusominaisuuksia. Laitosten turvallisuussuunnittelun arvioitiin täyttävän nykyisiä vaatimuksia hyvin. Turvallisuusjärjestelyjen suunnittelun osalta tarkastelun kohteena olleiden laitosten todettiin noudattavan nykyisiä teknisiä vaatimuksia. Ydinmateriaalivalvonnan osalta havaittiin laitosten seuraavan pitkälti perinteisiä ydinmateriaalikirjanpidon ja varmentamisen käytäntöjä. Useiden moduulien samanaikainen läsnäolo (NuScale), laitoksen väärinkäyttömahdollisuudet (RUTA-70) ja lauttalaitoksen liikutettavuus (KLT-40S) todettiin suurimmiksi ydinmateriaalivalvonnan haasteiksi. Organisatoriset vaatimus- ja suunnittelunäkökohdat todettiin tärkeiksi turvajärjestelyille ja ydinmateriaalivalvonnalle.

ACKNOWLEDGEMENTS

The opportunity to write this master's thesis was offered by the Department of Nuclear Engineering at LUT. I want to express my gratitude to professor Juhani Hyvärinen and Juhani Vihavainen for both providing me with such an interesting subject and supervising my work. I will also want to thank the whole Department of Nuclear Engineering for excellent lecturing and teaching in master's courses. I have learned a lot during my five-year studies and it is much to your credit. Has been a wonderful time and I'm glad to have my academic background built with your help.

I would like to thank my parents, who have been encouraging me to study all the way from elementary school. Furthermore, big thanks belong to my friends and siblings, I will appreciate your support and it has been important for me. Especially, I want to thank Henri Rapeli and Eero Salonen for the good times we had on working with group assignments and for many other moments during our studies. You both are real team players and friends. The road has been long, however learning and self-development have not yet come to an end. I am now eager to face new challenges, it is great to continue forward from such a milestone.

Aleksi Valkeapää

8th December 2021

Lappeenranta

ABBREVIATIONS

1-2 HX	Primary-Secondary Heat Exchanger
2-3 HX	Secondary-Tertiary Heat Exchanger
AC	Accident Condition
ACR	Automatic Control Rod
AIWAS	AC Independent Water Addition System
AOO	Anticipated Operational Occurrence
AP	Additional Protocol
ARI	Alternate Rod Insertion
ASEC	Passively Actuated Air Emergency Cooling System
ATWS	Anticipated Transient Without Scram
BOL	Beginning-Of-Life
BWR	Boiling Water Reactor
CA	Complementary Access
CAS	Central Alarm Station
CCF	Common Cause Failure
CCTV	Closed-circuit television system
CCWS	Component Cooling Water System
CDF	Core Damage Frequency
CFC	Containment Fan Cooler
CFV	Containment Filtered Vent
CGDM	Compensating Group Drive Mechanisms
CINS	Containment Inerting Nitrogen System

CIV	Containment Isolation Valve
CNV	Containment Vessel
CoT	Cut-off-Time
CoK	Continuity of Knowledge
CRA	Control Rod Assembly
CRDS	Control Rod Drive System
CRDSP	Control Rod Drive Supply Pump
C/S	Containment/Surveillance
CSA	Comprehensive Safeguards Agreement
CVCS	Chemical and Volume Control System
CWFS	Containment Water Filling System
CWS	Circulating Water System
DBA	Design Basis Accident
DBT	Design Basis Threat
DEC	Design Extension Condition
DHN	District Heating Network
DHRS	Decay Heat Removal System
DiD	Defence-in-Depth
DIQ	Design Information Questionnaire
DIV	Design Information Verification
ECCS	Emergency Core Cooling System
ECPRS	Emergency Containment Pressure Reduction System
EMWS	Emergency Make-up Water System
EPR	European Pressurized Water Reactor

ERVCS	External Reactor Vessel Cooling System
ESBWR	Economic Simplified Boiling Water Reactor
ESCS	Emergency Shutdown Cooling System
FA	Fuel Assembly
FKMP	Flow Key Measurement Point
FLCS	Feedwater Level Control System
FMCRD	Fine Motion Control Rod Drive
FNPP	Floating Nuclear Power Plant
FSA	Facility Safeguardability Analysis
FVS	Filtered Ventilation System
FWLB	Feed Water Line Break
FWS	Feed Water System
Gd ₂ O ₃	Gadolinium Oxide
GE-Hitachi	General Electric-Hitachi
GIF	Generation IV International Forum
HCU	Hydraulic Control Unit
HPSI	High-Pressure Safety Injection
HVAC	Heating, Ventilation, and Air Conditioning
HX	Heat Exchanger
IAEA	International Atomic Energy Agency
I&C	Instrumentation & Control systems
IC	Isolation Condenser
ICC	Intermediate Cooling Circuit
ICR	Inventory Change Report

ICS	Isolation Condenser System
IIT	Interim Inventory Taking
IIV	Interim Inventory Verification
IKMP	Inventory Key Measurement Point
INPRO	International Project on Innovative Nuclear Reactors and Fuel
INSAG	International Nuclear Safety Advisory Group
JSC OKBM	Joint-Stock Company OKB Mechanical Engineering
KMP	Key Measurement Point
LAIS	Liquid Absorber Injection System
LBLOCA	Large Break Loss-Of-Coolant Accident
LOCA	Loss-Of-Coolant Accident
LOF	Location Outside Facilities
LPSI	Low-Pressure Safety Injection
LRF	Large Release Frequency
LWR	Light Water Reactor
MBA	Material Balance Area
MBLOCA	Medium Break Loss-Of-Coolant Accident
MBP	Material Balance Period
MBR	Material Balance Report
MC	Main Condenser
MCP	Main Coolant Pump
MCR	Main Control Room, Manual Control Rod
MSSD	Minimum Safe Standoff Distance
MSLB	Main Steam Line Break

MSL	Main Steam Line
MTC	Moderator Temperature Coefficient
MUF	Material Unaccounted For
NDA	Non-Destructive Assay
NF	Nuclear Facility
NFCF	Nuclear Fuel Cycle Facility
NIKIET	N.A. Dollezhai Research and Development Institute of Power Engineering
NMA	Nuclear Material Accountancy
NM	Nuclear Material
NO	Normal Operation
NPM	NuScale Power Module
NPP	Nuclear Power Plant
NSSS	Nuclear Steam Supply System
NTA	National Threat Assessment
ORSAC	Overall safety conceptual framework
OSP	Other Strategic Point
PCCS	Passive Containment Cooling System
PCS	Purification and Cooldown System
PCV	Primary Containment Vessel
PIE	Postulated Initiating Event
PIL	Physical Inventory Listing
PIT	Physical Inventory Taking
PNNL	Pacific Northwest National Laboratory
PP	Physical Protection

PPS	Physical Protection System
PRA	Probabilistic Risk Assessment
PR	Proliferation Resistance
PSA	Probabilistic Safety Assessment
PSWS	Plant Service Water System
PWR	Pressurized Water Reactor
RCCWS	Reactor Component Cooling Water System
RCPB	Reactor Coolant Pressure Boundary
RCS	Reactor Coolant System
RMS	Remote Monitoring System
RP	Reactor Plant
RPAOPS	Reactor Pool Airspace Overpressure Protection System
RPIV	Reactor Pressure Vessel Isolation Valve
RPS	Reactor Protection System
RPV	Reactor Pressure Vessel
RSV	Reactor Safety Valve
RTS	Reactor Trip System
RV	Reactor Vessel
RVV	Reactor Vent Valve
SA	Safeguards Approach
SAS	Secondary Alarm Station
SBD	Safeguards by Design
SCS	Seawater Cooling System
SCWS	Site Cooling Water System

SDC	Shutdown Cooling System
SF	Safety Function
SG	Steam Generator
SLC	Standby Liquid Control System
SMR	Small Modular Reactor
SQ	Significant Quantity
SRA	State or Regional Authority responsible for safeguards implementation
SRDM	Safety Rod Drive Mechanisms
SR	Scram Rod
SSR	Specific Safety Requirements (IAEA)
SSAC	State System of Accounting for and Control of nuclear material
SSC	System, Structure, Component
STUK	Finnish Radiation and Nuclear Safety Authority
SWSS	Service Water Supply System
TG	Turbine-Generator
UHS	Ultimate Heat Sink
UMS	Unattended Monitoring System
UO ₂	Uranium Dioxide
UR	User Requirement
U.S NRC	United States Nuclear Regulatory Commission
WENRA	Western European Nuclear Regulators' Association
YVL	Regulatory guide for nuclear power plants, issued by the STUK

Table of contents

Abstract

Acknowledgements

Abbreviations

1. Introduction.....	13
2. Safety	14
2.1 Defence-in-Depth.....	17
2.2 Fundamental safety functions	21
2.3 Design for safety	23
2.4 Hazard evaluation.....	27
2.5 Acceptance criteria.....	28
3. Security	30
3.1 Threats.....	31
3.2 Risk-based physical protection system	32
3.3 Design Basis Threat	36
3.4 Security zones	38
3.4 Physical protection measures	41
3.4 Cyber security	45
4. Safeguards.....	48
4.1 Nuclear material accountancy and material balance areas.....	49
4.2 IAEA verification activities	53
4.3 IAEA safeguards measures	54
4.4 INPRO proliferation resistance assessment methodology	58
4.5 GIF PR/PP methodology.....	61
4.6 Safeguards and safety.....	62
4.7 Safeguards and security.....	64
4.8 Safeguards by design.....	66
5. Overall safety framework development.....	68
6. Case study SMRs in concern	70
6.1 NuScale	70

6.2	RUTA-70.....	72
6.3	BWRX-300	73
6.4	KLT-40S (Akademik Lomonosov)	74
7.	Safety results.....	76
7.1	NuScale	76
7.2	RUTA-70.....	80
7.3	BWRX-300	84
7.4	KLT-40S (Akademik Lomonosov)	89
8.	Security results.....	95
8.1	NuScale	95
8.1.1	Security descriptions.....	95
8.1.2	Observations	100
8.2	BWRX-300	102
8.2.1	Security descriptions.....	102
8.2.2	Observations	106
8.3	KLT-40S (Akademik Lomonosov)	107
9.	Safeguards results	111
9.1	NuScale	111
9.2.1	Challenges and similarities	113
9.1.2	Safeguards approach	114
9.2	RUTA-70.....	115
9.2.1	Challenges and similarities	117
9.3.1	Safeguards approach	119
9.3	KLT-40S (Akademik Lomonosov)	121
9.3.1	Challenges and similarities	123
9.3.2	Safeguards approach	126
10.	Discussion.....	127
11.	Summary.....	133
	References.....	134

Appendices

Appendix 1. The Fundamental Safety Principles

Appendix 2. INPRO PR evaluation table for material barriers

Appendix 3. System descriptions for NuScale

Appendix 4. System descriptions for RUTA-70

Appendix 5. System descriptions for BWRX-300

Appendix 6. System descriptions for KLT-40S

Appendix 7. YVL.B.1 requirement evaluation for NuScale

Appendix 8. YVL.B.1 requirement evaluation for RUTA-70

Appendix 9. YVL.B.1 requirement evaluation for BWRX-300

Appendix 10. YVL.B.1 requirement evaluation for KLT-40S

Appendix 11. YVL.A.11 requirement evaluation for NuScale

Appendix 12. YVL.A.11 requirement evaluation for BWRX-300

Appendix 13. Facility Safeguardability Analysis Tool for NuScale

Appendix 14. Facility Safeguardability Analysis Tool for RUTA-70

Appendix 15. Facility Safeguardability Analysis Tool for KLT-40S

1. Introduction

Climate change is a global problem, that proposes challenges to our energy systems. There is an endeavour to carbon-neutrality in every State, and the ongoing debate on solutions to decrease CO₂ emissions in the energy sector. Nuclear power has a major role as it enables carbon-free energy production in both electricity and heat markets. The reliable baseload, load follow potential and heat applications of nuclear provide the necessary support for renewables. Small Modular Reactors (SMRs) have been developed to answer such problems of conventional nuclear power plants (NPPs) as high costs due to delayed construction times. These are categorized as reactors with a maximum output of 300 MWe. SMRs often have a modular design, that allows serial fabrication and delivery of the ready-made reactors to the site. SMRs could be utilized for decentralized energy production for electricity, district heating, and industrial process heat applications. Safety has been the cornerstone of nuclear engineering and is the major requirement for the operation. Lately, the perspective has been broadened to incorporate both Security and Safeguards, and the term '3S' was born. This has led to the establishment of the concept of Overall Safety. However, it was quickly realized that such concept is not limited to NPP instead it is also dependent on the public and environment, thus Society and Sustainability were added to '3S' to have '5S' to complete Overall Safety (figure 1). Overall safety framework (ORSAC) was proposed to integrate the '3S' (Hyvärinen et al. 2016). Later a comparison study of EPR and NuScale designs was realized on Safety using ORSAC (Turunen 2020). Still, Security and Safeguards considerations have not yet been studied in-depth. This Master's thesis aims to contribute to Overall Safety in two ways. Firstly, the ORSAC is developed further with respect to Security and Safeguards. Secondly, insights on the implementation of Safety, Security, and Safeguards are surveyed in the context of SMRs. The thesis was written as part of the OSAFE project of the SAFIR2022.

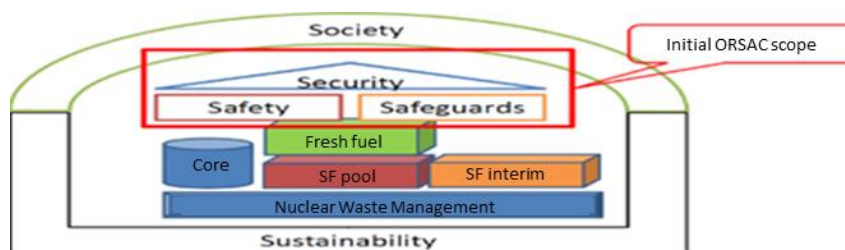


Figure 1. The scope of this masters's thesis within the concept of Overall Safety (modified from Hyvärinen 2021).

2. Safety

Safety is a major entity in the field of nuclear engineering as it constitutes the basis for the design and all the activities during the lifetime of an NPP or any other nuclear facility (NF). When it comes to the safety of a nuclear installation, many safety-related issues are covered by nuclear safety and radiation safety. Nuclear safety comprises the hazards concerning the use of a NF (e.g., nuclear reactor) and operational activities. The hazards for nuclear installations arise out from the fissile material and the inventory of radionuclides. It is the aim of nuclear safety to ensure that hazardous releases of radioactive material are prevented, and unintended or uncontrolled criticality of fissile material is ruled out. Radiation safety contributes to nuclear safety to ensure that harmful radiological consequences of radioactive material to the public, environment and personnel are controlled in both operation and possible accident conditions (AC). It is worth mentioning that conventional industrial hazards (e.g., chemical hazards) and the safety associated with these are also important and can influence nuclear and radiation safety.

IAEA has established Safety Standards Series to fulfil the requirement by its Statute to promote international cooperation. Regulating safety is a national responsibility and IAEA Safety Standards provide States and national authorities the basis for legislation and regulation. Operators and other nuclear-related organizations benefit from Safety Standards in their actions as they establish a consistent and comprehensive basis for the protection of people and the environment against radiation hazards. Usage of standards is highly recommended by IAEA as it supports States in meeting their obligations under general principles of international law, promotes confidence in safety, and enhances safety globally by increased cooperation. (IAEA 2006a, 1-2).

The IAEA Safety Standards Series consists of Safety Fundamentals, Safety Requirements, and Safety Guides (figure 2).

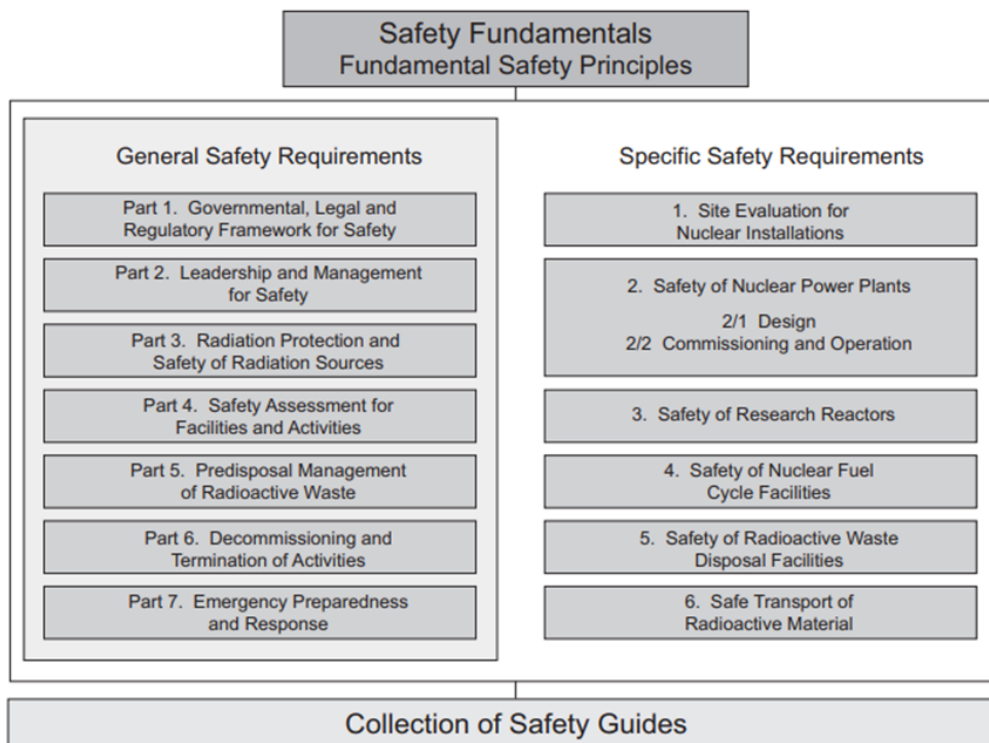


Figure 2. The structure of IAEA Safety Standard Series (IAEA 2016a).

IAEA Safety Fundamentals publication constitute the basis for safety requirements established in Safety Requirements Series (General Safety and Specific Safety). Safety Guides provide guidance in accomplishing the requirements for different issues in a proper manner.

Safety must be the cornerstone for any nuclear installation during its lifetime including planning, design, siting, manufacturing, construction, commissioning, operation, decommissioning, and closure. Radioactive waste management and transports are also considered since these are essential activities at nuclear facilities. The beneficial usage of nuclear facilities for power and heat production or other peaceful purpose need to prioritize safety in all activities. Radiation risks to people - individually and collectively – and the to the environment is considered a high priority in the design and all processes during the lifetime of a nuclear installation to fulfil the fundamental safety objective. (IAEA 2006a, 4-5).

The fundamental safety objective states:

“The fundamental safety objective is to protect people and the environment from harmful effects of ionizing radiation” (IAEA 2006a, 4).

It is mentioned in Fundamental Safety Principles paragraph 2.1 that protection must be achieved without unduly limiting the operation of facilities and conduct of activities, which give rise to the radiation risks. Three measures must be taken to ensure the highest standards of safety as reasonably achievable (IAEA 2006a, 4):

- a) To control the radiation exposure of people and the release of radioactive material to the environment.
- b) To restrict the likelihood of events that might lead to a loss of control over a nuclear reactor core, nuclear chain reaction, radioactive source, or any other source of radiation.
- c) To mitigate the consequences of such events if they were to occur.

The aim of nuclear and radiation safety is introduced here. It is essential to protect people and the environment from the release of radioactive material and associated radiation exposure. In addition, it is necessary to restrict the likelihood of any event which would initiate from uncontrolled criticality and affect safety. Measures must be provided to mitigate the consequences in case of an event leading to uncontrolled criticality or radiation release or exposure.

The Safety Fundamentals publication introduces ten fundamental safety principles (appendix 1), which have provided the basis for safety requirements to pursue the fundamental safety objective. The principles represent a set of entitlements that must be appropriately applied to constitute a comprehensive basis for safety requirements and measures. (IAEA 2006a, 5).

Although fundamental safety principles constitute the basis for all safety requirements, in the following the perspective is in the design of a NF, especially of an NPP, and the certain important aspects of safety in design are introduced.

2.1 Defence-in-Depth

The defence in depth (DiD) is the main concept that provides an overall strategy for safety measures and features for nuclear installations. The safe design and operation of an NF lies in this concept as Safety Fundamentals paragraph 3.31 states:

“The primary means of preventing and mitigating the consequences of accidents is ‘defence in depth’ ... it is implemented primarily through the combination of a number of consecutive and independent levels of protection that would have to fail before harmful effects could be caused to people or to the environment.” (IAEA 2006a, 13)

“If one level of protection or barrier were to fail, the subsequent level or barrier would be available ... when properly implemented no single technical, human, or organizational failure could lead to harmful effects, and that the combinations of failures that could give rise to significant harmful effects are of very low probability.” (IAEA 2006a, 13)

“The independent effectiveness of the different levels of defence is a necessary element of defence in depth.” (IAEA 2006a, 13)

IAEA SSR-2/1 (Safety of Nuclear Power Plant: Design) and SSR-4 (Safety of Nuclear Fuel Cycle Facilities) both state the same requirements (no. 7 and 10) for the application of DiD concept in design:

“The design of a nuclear power plant/nuclear fuel cycle facility shall incorporate defence in depth. The levels of defence in depth shall be independent as far as is practicable.” (IAEA 2016a, 14; IAEA 2017, 36)

The essential feature of the DiD concept is to isolate radioactive materials from the environment and confine them by using multiple physical barriers. This structural DiD is achieved, in the case of a light water reactor (LWR), by four physical barriers: the fuel matrix, the fuel rod cladding, the reactor coolant pressure boundary (RCPB), and the containment system. The aim of the DiD is to provide for multiple functional defence levels to protect the integrity of structural barriers and mitigate the radioactive releases in case of a failure (the first 4 levels) and to implement successful off-site emergency response in the event of a significant radioactive release (the 5th level). The main priority is to prevent accidents and, if prevention fails, to mitigate and limit potential consequences to prevent possible evolution to more severe conditions. An updated version of traditional INSAG DiD levels proposed by WENRA is shown in figure 3. (INSAG 1996, 4, 8).

	DiD level	Objective of the level	Essential means	Associated plant condition categories	Radiological consequences
Original design of the plant	Level 1	Prevention of abnormal operation and failure	Control, limiting and protection systems and other surveillance features	Normal operation	Regulatory operating limits and conditions
	Level 2	Control of abnormal operation and failure	Conservative design and high quality in construction and operation	Anticipated operational occurrences	Regulatory operating limits and conditions
	Level 3	Control of accident to limit radiological consequences and prevent escalation to core damage conditions	Safety systems Accident procedures	DiD level 3a Postulated single initiating events	No of site radiological impact
		Control of accident to limit radiological consequences and prevent escalation to core melt conditions	Engineered safety features Accident procedures	DiD level 3b Selected multiple failure events including possible failure or inefficiency of safety systems involved in DiD level 3a	or only minor radiological impact
	Level 4	Practical elimination of situation that could lead to early or large releases of radioactive material Control of accidents with core melt to limit off-site releases	Management of accidents with core melt (severe accidents) Engineered safety features to mitigate core melt	Postulated core melt accidents (short and long term)	Limited protective measures in area and time
Emergency planning	Level 5	Mitigation of radiological consequences of significant releases of radioactive material	Off-site emergency response Intervention levels	—	Off-site radiological impact necessitating protective measures

Figure 3. DiD levels proposed by WENRA (modified from WENRA 2009, 23).

The objective of the first level of defence is to prevent deviations from Normal Operation (NO) and the failures of items important to safety. This leads to a broad range of requirements that the NPP or any NF be rigorously and conservatively sited, designed, constructed, maintained, and operated. Importance must be given to quality in any activity or process during the lifecycle of the plant (e.g., manufacturing, analyses, design codes and engineering practices, construction, maintenance). Provisions to prevent deviations from the NO state can be seen as more effective and predictable than measures aimed at mitigation of such a departure, thus every aspect having importance to safety in any phase of the lifecycle must be considered. (IAEA 2016a, 7; IAEA 2017, 11; INSAG 1996, 4).

The second level of defence is intended to ensure that abnormal operation states, in case of anticipated operational occurrences (AOOs) or equipment failures, are controlled and the NO state is restored. The objective is to prevent plant deviations from escalating to ACs by detection and control. Provisions of control, limiting and protection systems, and other surveillance features are implemented in design with confirmed effectiveness and rigorously established operational procedures. Inherent plant features, such as thermal inertia and core stability, are credited as regarding the design. (IAEA 2016a, 7; IAEA 2017, 11; INSAG 1996, 9).

The third level is responsible for the defence if the AOOs or certain postulated initiating events (PIEs) propagate into accidents. The design of an NPP or other NF has taken into consideration such Design Basis Accidents (DBAs). The requirement for this level of defence is to provide for inherent and/or engineered safety features, Safety Systems, fail-safe design, and procedures to prevent core damage or release of radioactive material requiring off-site protection. The objective is to control the consequences of such an accident, to prevent extensive damage to the facility, to prevent significant off-site radioactive releases, and return the NPP/NF to a safe state. (IAEA 2016a, 8; IAEA 2017, 12).

The fourth level provides measures for Design Extension Conditions (DECs) in case of multiple failures or if an accident event propagates towards severe conditions, namely, core melt. The purpose is to prevent the progression of events to severe accidents and to mitigate consequences arising from a severe accident. The objective in case of a severe accident is that only protective actions that are limited in lengths of time and areas of application would be considered necessary. The protection of the containment system is important since it would be necessary to avoid or at least minimize off-site consequences. It is required that event sequences leading to a large radioactive release, or an early radioactive release would be ‘practically eliminated’. (IAEA 2016a, 8; IAEA 2017, 12; INSAG 1996, 11).

The fifth level takes into consideration the off-site response in case of potential radioactive release that could result from failure to mitigate severe ACs. The objective is to mitigate off-site radiological consequences to the public in cooperation with the regulator and off-site organizations involved. The emergency plans and adequately equipped emergency response facilities must be provided. Emergency procedures for off-site and on-site emergency response must be developed and exercised periodically. (IAEA 2016a, 8; IAEA 2017, 12, INSAG 1996, 12).

The DiD levels must remain available when in operation. When any relaxation is considered for a specific operational state, it must be justified as it is stated in SSR-1/2:

“All levels of defence in depth shall be kept available at all times and any relaxations shall be justified for specific modes of operation.” (IAEA 2016a, 14)

The DiD must be implemented in design so that challenges to barriers and their failures are taken into consideration as IAEA SSR-2/1 paragraph 4.12 and SSR-4 paragraph 6.22 both state for NPP and any Nuclear Fuel Cycle Facility (NFCF) (e.g., spent fuel storage facility):

“To ensure that the concept of defence in depth is maintained, the design shall prevent, as far as is practicable:” (IAEA 2016a, 15; IAEA 2017, 37)

- a) *Challenges to the integrity of physical barriers.*
- b) *Failure of one or more barriers.*
- c) *Failure of a barrier as a consequence of the failure of another barrier.*
- d) *The possibility of harmful consequences of errors in operation and maintenance.*

‘Challenges’ are defined as general mechanisms, processes, or conditions that may affect the performance of Safety Functions (SFs). ‘Mechanisms’ can be understood as more specific processes or situations consequences of which might evolve to challenges. By using ‘provisions’ such as system design features, inherent safety characteristics, operational procedures, safety margins, the performance of SFs can be enhanced so that mechanisms would be prevented. The interrelation between these for a defence level can be presented by an objective tree (figure 4). (IAEA 2005a, 9).

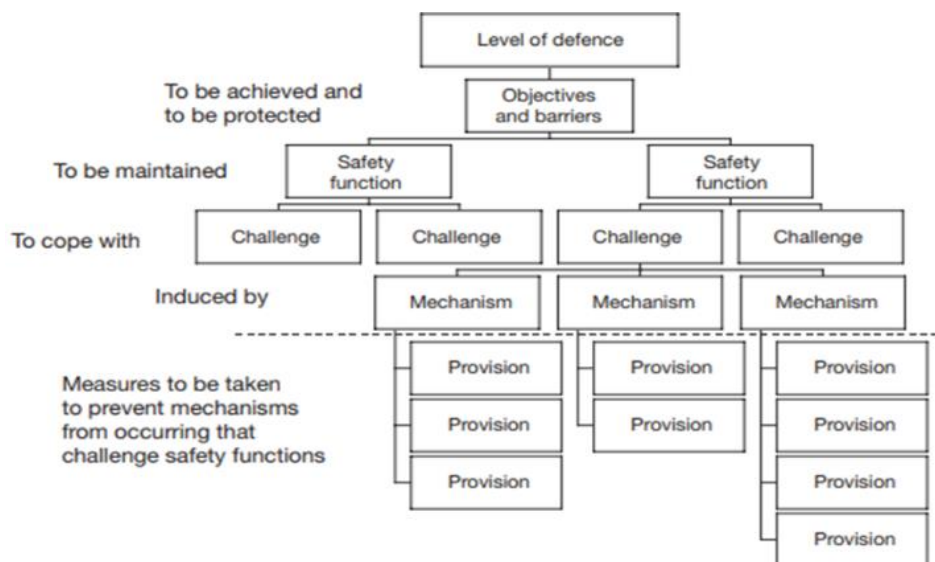


Figure 4. The interrelation between SFs, challenges, and provisions for a level of defence (IAEA 2005a, 9).

2.2 Fundamental safety functions

Although DiD concept aims to prevent abnormal conditions (Level 1) and restore the NPP/NF to the NO during AOOs with a help of engineered features and systems (Level 2), provisions must be made to response to possible ACs. The DiD strategy is aimed to preserve the three basic SFs, which eventually, in the case of AC, ensure that radioactive materials do not release into the environment. (INSAG 1999, 17).

The integrity of structural barriers in a nuclear reactor is ensured by three Fundamental SFs (IAEA 2016a, 12):

- 1) Control of reactivity
- 2) Control of heat removal
- 3) Confinement of radioactive material

According to IAEA SSR-1/2 in NPP design, it is stated for Fundamental SFs in requirement 4:

“Fulfilment of fundamental safety functions for a nuclear power plant shall be ensured for all plant states...” (IAEA 2016a, 12)

It is worth noting that in SSR-1/2 shielding against radiation, control of planned radioactive releases and limitation of accidental ones are included as part of the third Fundamental SF. It is also essential to note that, when NPP is in concern, the Fundamental SF ‘control of heat removal’ does not limit to the reactor since the cooling of irradiated fuel handling and storage systems must also be provided to prevent accidental melting of fuel and subsequent radioactive releases. As it is stated in SSR-1/2 requirement 80, paragraph 6.67 for the design of irradiated fuel handling and storage systems:

“The fuel handling and storage systems ... shall be designed: a) To permit adequate removal of heat from the fuel in operational states and in accident conditions.” (IAEA 2016a, 57)

Especially SSR-1/2 states for ‘practical elimination’ of early and large radioactive releases regarding the water pool type storages of irradiated fuel in paragraph 6.68:

“For reactors using a water pool system for fuel storage, the design shall be such as to prevent the uncovering of fuel assemblies in all plant states that are of relevance for the spent fuel pool so that the possibility of conditions arising that could lead to an early radioactive release, or a large radioactive release is ‘practically eliminated.’” (IAEA 2016a, 58)

“The design shall provide.” (IAEA 2016a, 58)

- a) the necessary fuel cooling capabilities.*
- b) features to prevent the uncovering of fuel assemblies in the event of a leak or a pipe break.*
- c) a capability to restore the water inventory.*

Also, regarding criticality safety it is stated for the non-irradiated and irradiated handling and storage systems in SSR-1/2 paragraph 6.67:

“Handling and storage systems shall be designed... a) to prevent criticality by a specified margin, by physical means or by means of physical processes, and preferably by use of geometrically safe configurations, even under conditions of optimum moderation.” (IAEA 2016a, 57)

Practically the Fundamental SFs seem to be a specific term reserved for NPPs, but the IAEA requirements provide similar SFs for NFCFs as it is shown in SSR-4 requirement 7 (Main safety functions):

“The design shall be such that the following main safety functions are met for all facility states of the nuclear fuel cycle facility.” (IAEA 2017, 32)

- a) Confinement and cooling of radioactive material and associated harmful materials.*
- b) Protection against radiation exposure.*
- c) Maintaining subcriticality of fissile material*

Furthermore, for transport of radioactive material, the IAEA SSR-6 section 104 states:

“The objective of these Regulations is to establish requirements that must be satisfied to ensure safety and to protect people, property, and the environment from harmful effects of ionizing radiation during the transport of radioactive material. This protection is achieved by requiring:” (IAEA 2018a, 2)

- a) *Containment of the radioactive contents*
- b) *Control of external dose rate.*
- c) *Prevention of criticality*
- d) *Prevention of damage caused by heat*

Thus, the three SFs provide the basis of safety for all NFs and associated operational activities.

2.3 Design for safety

According to IAEA SSR-1/2 requirement 13, all NPP's states shall be identified and shall be grouped into categories primarily based on their frequency of occurrence (IAEA 2016a, 18). The boundaries between different plant states corresponding to a frequency have not been explicitly stated. Though indicative frequency values for limits between different plant states have been provided by IAEA Guide SSG-2 (table 1). The frequency values can be seen consistent with a Core Damage Frequency (CDF) value of $10^{-5}/a$ proposed for new NPPs. (IAEA 2016b, 4; INSAG 1999, 11).

Table 1. Plant states with indicative limits for frequency of occurrence (modified from IAEA 2009a, 6).

Frequency [1/a]	Nature	Plant state (event category)	Terminology	Acceptance criterion
$10^{-2} - 1$	Expected	AOOs	Anticipated transients, frequent faults, incidents of moderate frequency, upset conditions, abnormal conditions	No (additional) fuel damage
$10^{-4} - 10^{-2}$	Possible	DBAs	Infrequent incidents, infrequent faults, limiting faults, emergency conditions	No radiological impact at all, or outside the exclusion area
$10^{-6} - 10^{-4}$	Unlikely	Beyond DBAs	Faulted conditions	Radiological consequences outside exclusion area but within limits
$< 10^{-6}$	Remote	Severe accidents	Faulted conditions	Emergency response needed

The approach for safe design is to evaluate all possible initiating events, which would challenge and possibly lead to failures of its systems, structures, and components. IAEA SSR-1/2 states requirement 16 regarding the identification of these PIEs:

“The design for the nuclear power plant shall apply a systematic approach to identifying a comprehensive set of PIEs such that all foreseeable events with the potential for serious consequences and all foreseeable events with a significant frequency of occurrence are anticipated and are considered in the design.” (IAEA 2016a, 19).

The PIEs shall include all foreseeable failures of SSCs, operating errors, and failures arising from internal and external hazards in all plant conditions. The expected behaviour of the plant in PIEs is to render the plant to a safe state by inherent characteristic, passive features or continuously active control systems, actuation of Safety Systems, or by following specified procedures. These are related to defence levels of DiD. The PIEs used for developing the performance requirements for items important to safety shall be grouped into a specified number of event sequences that identify bounding cases and provide a basis for the design and the operational limits. The capability of operators to act during PIEs shall be considered in the design by providing sufficient time between detection and required action, automatic actuation of systems when prompt response is necessary, adequate instrumentation, and control systems to restore the plant to a safe state. (IAEA 2016a, 19-20).

In NPP design certain postulated accidents are derived from PIEs providing the extreme design parameters for the Safety Systems (INSAG 1999, 10). Regarding these DBAs SSR-1/2 states in requirement 19:

“A set of accidents that are to be considered in the design shall be derived from postulated initiating events for the purpose of establishing the boundary conditions for the nuclear power plant to withstand, without acceptable limits for radiation protection being exceeded.” (IAEA 2016a, 23)

As the requirement states, the major objective is that no, or only minor, radiological consequences both on-site and off-site would result from DBAs. These should be used to define the design basis for Safety Systems and items important to safety with the aim that these accidents would be controlled, any consequences would be mitigated, and the plant would be returned to a safe state if, DBAs occur during the lifetime of an NPP. Some examples of DBAs include loss of coolant accidents (LOCAs), control rod ejection, MSLB,

FWLB, Main Coolant Pump (MCP) seizure or shaft break. In the design of items important to safety, such as Safety Systems, reliability is achieved by using diversity, redundancy, physical separation, and functional independence. The conservative approach is used to ensure that objective of the Safety Systems is met despite the uncertainties in analyses used in modeling plant response and performance of the equipment. (IAEA 2016a, 23,27; IAEA 2016b, 6, 39).

For new NPP designs, it is required to extend the accident analysis to more complex event sequences with multiple failures of systems and severe accidents, which would lead, if not prevented and mitigated, to more significant radiological consequences than DBAs. The purpose is to improve safety further in design by providing the enhanced capability of the plant to withstand such DECs. SSR-1/2 requirement 20 states for DECs:

“A set of design extension conditions shall be derived based on engineering judgement, deterministic assessments and probabilistic assessments for the purpose of further improving the safety of the nuclear power plant by enhancing the plant’s capabilities to withstand, without unacceptable radiological consequences, accidents that are either more severe than design basis accidents or that involve additional failures. These design extension conditions shall be used to identify the additional accident scenarios to be addressed in the design and to plan practicable provisions for the prevention of such accidents or mitigation of their consequences.” (IAEA 2016a, 24)

It is stated in associated paragraphs that the main technical objective is to assure that the design is such as to prevent accidents beyond DBAs or to mitigate their consequences, as far as reasonably practicable. Additional DEC Safety Features might be required in the design, or the capability of the Safety Systems to prevent severe accidents or mitigate their consequences to be provided. The possibility of an early or large radioactive release shall be ‘practically eliminated’ by maintaining the integrity of the containment and ensuring that the design can return the plant in a controlled state. As it was already mentioned with DiD level 4, the design shall be such that only protective actions that are limited in lengths of time and areas of application would be considered necessary for the protection of the public. It is worth noting that the single failure criterion is a requirement for the Safety Systems for DBAs, but it is not required for Safety Features for DECs. Also, less conservative assumptions might be used for the equipment. The best estimate approach is used for determining the accident scenario and environmental conditions for equipment dedicated to DECs. (IAEA 2016a, 24-25, 27; IAEA 2016b, 20, 40).

Practically, DECs are categorized into two groups, DECs without significant core degradation and DECs with core melt. Two different approaches exist to include DECs in DiD levels. The first is to divide the DiD level 3 into subsections 3a and 3b, the former deals with DBAs and the latter with DECs without core melt, thus the DiD level 4 deals with the control of severe accidents. In the second approach, the DiD level 4 deals with both, the control of postulated failures without core melt and postulated severe accidents, and the level is further divided into subsections 4a and 4b, former aims to prevent core melt conditions whereas the latter aims to mitigate the consequences of DECs with core melt. As previously introduced in figure 3 WENRA applies the first approach regarding DECs. (IAEA 2016b, 18-20).

2.4 Hazard evaluation

In NPP design internal hazards and external hazards are considered such as to ensure that SSC important to safety are capable to withstand loads due to their occurrence, to determine resulting PIEs, and essentially to provide a safe plant layout. As IAEA SSR-1/2 requirement 17 states for hazard evaluation:

“All foreseeable internal hazards and external hazards, including the potential for human induced events directly or indirectly to affect the safety of the nuclear power plant, shall be identified and their effects shall be evaluated. Hazards shall be considered in designing the layout of the plant and in determining the PIEs and generated loadings for use in the design of relevant items important to safety for the plant.” (IAEA 2016a, 21)

Internal hazards to be considered in design constitute for example following phenomena: fires, the spread of smoke and hazardous gases, flooding, missile generation, explosions, the collapse of structures, falling objects, jet forces, pipe whip, and falling of heavy loads. (IAEA 2016a, 22; STUK 2019a, 11).

External hazards are required to be identified and evaluated as a part of the site evaluation and this process shall be continuous over the lifetime of the plant. Both natural and human-induced external hazards and their impact are considered. Natural hazards to be considered can for example constitute the following extreme meteorological hazards (e.g., precipitation, wind, snow, storm surges), rare meteorological hazards (e.g., lightning, tornados, and cyclones), flooding hazards (e.g., tsunamis, seiches, river flooding), seismic hazards (e.g.,

earthquakes), volcanic hazards, geotechnical hazards (e.g., soil liquefaction, slope instability, subsidence or uplift of the site surface). Human-induced external hazards to be addressed shall include for example hazards arising from industrial facilities near the site (fire, explosions, releases of hazardous gases, missile generation), events associated with nearby land, sea, river, or air transport (e.g., aircraft crash, explosions) and electromagnetic interference. (IAEA 2019a, 11-12, 17-25).

The frequency of occurrence and severity of external events shall be considered. The possibility that combinations of different external events may occur simultaneously or within a short time frame shall be addressed. Causality between external events and interrelationships shall also be considered. Adequate margin to protect items important to safety against external hazards derived from site evaluation shall be provided. In addition, the design shall provide adequate margin to protect items ultimately necessary to prevent an early radioactive release or a large radioactive release (e.g., containment) in the event of natural hazards exceeding those considered in the design. (IAEA 2016a, 21-23).

Plant layout design provides essential means to protect NPP from hazards. For example, Safety Divisions holding redundant trains for each Safety System are placed in physically separated compartments to ensure that no external hazard or internal hazard would affect several items important to safety at the same time (e.g., airplane crash) or that their impacts would propagate to other SSCs important to safety (e.g., fires and floods). If multiple units are in operation at the site, the plant layout must ensure that impacts of hazards to several units or all units simultaneously are considered in the design. Regarding the traffic and access arrangements at the site area, the impact of external hazards must be considered to provide accessibility of buildings and structures so that preventive measures can be taken, or potential ACs mitigated. (IAEA 2016a, 21; STUK 2019a, 10-12).

2.5 Acceptance criteria

Equivalent radiation dose limits for an individual of the population are used as acceptance criteria for different event categories. Figure 6 presents dose constraints from the Finnish Government Decree (733/2008) on the Safety of Nuclear Power Plants, and the DiD concept of the Finnish Nuclear and Radiation Safety Authority (STUK). STUK divides the Level 3

(DBAs) into two event categories. Class I postulated accidents are assumed to occur less frequently than once during any period of a hundred years of operation, but at least once during thousand operating years. Class II postulated accidents can be assumed to occur less frequently than once in thousand years of operation. STUK perceives three classes of DECAs as ACs without core melt. DEC A is an accident where common cause failure (CCF) for Safety System is involved in association with AOO or Class I accident. DEC B refers to an accident caused by multiple failures which is identified as significant based on Probabilistic Safety Assessment (PSA). DEC C is an accident caused by a rare external event that NPP must withstand without severe fuel failure. (Finnish Government 2008, 1,3; STUK 2019b, 12).

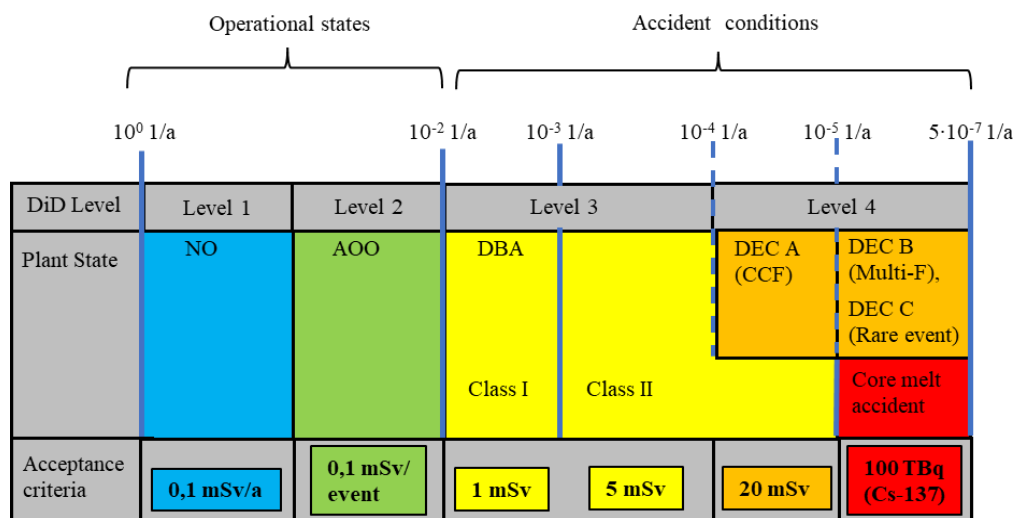


Figure 6. STUK's implementation of DiD concept with acceptance criteria and frequency limits for event categories. Dashed lines are indicative limits. There is an overlap between Class II postulated accidents and DEC A ($10^{-4} - 10^{-5}$). Similarly, DEC B and C overlap with Core melt accidents ($> 10^{-5}$) (Modified from Hyvärinen et al. 2016, 32).

It is worth noting that the acceptance criteria for core melt accidents is an atmospheric release of 100 TBq cesium-137, which is set to avoid long-term limitations of land use. However, this requirement is translated to 20 mSv dose limit during the first week after the severe accident within the emergency planning zone (radius of 20 km from the plant) according to STUK. In figure 6 frequencies from 10^0 to 10^{-4} are related to individual events and PSA acceptance criteria (10^{-5} for CDF and $5 \cdot 10^{-7}$ for large release frequency, LRF) are compound probabilities. These can be justified to be drawn on the same scale for two reasons: 1) from consequences point of view, a core melt or release is an individual event independent of what caused it in the first place 2) Generally, a handful of initiating events contribute to CDF and LRF, thus the frequencies of the most likely individual initiating events are close to the same order of magnitude as the sum. (Hyvärinen et al. 2016, 32-33).

3. Security

Nuclear security comprises all the aspects relevant to ensure that the NPP is protected from malicious acts of humans. The fundamental objective is to protect persons, property, society, and the environment from the harmful consequences of a threat event. The threats arising from harmful and criminal acts may aim to sabotage (facility, material, and activities) or to gain access to the nuclear and/or radioactive material. Nuclear security is not limited to physical protection system (PPS) and security measures of security organization. Instead, it comprises information security as well. The computer systems relevant for industrial process equipment (e.g., I&C), security-related systems, and information systems can be potential targets for a cyberattack. Therefore, cyber security has become important. Such attacks may directly target important systems or could be used as indirect means to facilitate adversaries' objectives to commit malicious acts. (IAEA 2011a, 4-5, 13-14; IAEA 2011b, 5, 10-11; IAEA 2013a, 3-4, 8; IAEA 2018b, 23-37, 43-44, 87-90).

Amendment to the Convention on the Physical Protection of Nuclear Material states following four objectives considering the State's physical protection (PP) regime (IAEA 2006b, 33):

- 1) To protect against unauthorized removal (theft or unauthorized taking of nuclear and/or radioactive material)
- 2) To locate and recover nuclear material if the material is missing (stolen or missing)
- 3) To protect against sabotage (nuclear and/or radioactive material, associated facilities, and activities)
- 4) To mitigate and minimize effects of sabotage (measures regarding potential radiological consequences)

The responsibility for taking the necessary measures and implementing an effective PPS to ensure the above-mentioned objectives lies primarily on the operator of the NF. As it is stated in fundamental principle E in the Convention on the Physical Protection of Nuclear Material:

“The prime responsibility for the implementation of physical protection of nuclear material or of facilities rests with the holders of the licenses.” (IAEA 2006b, 34)

The State has the responsibility to provide for continuous evaluation of the threat environment as it is stated in the fundamental principle G:

“State’s physical protection should be based on the State’s current evaluation of the threat.”
(IAEA 2006b, 34)

The consequences of sabotage and unauthorized access to nuclear or radioactive can vary within a wide spectrum regarding the target. The security requirements are implemented by using a graded approach (fundamental principle H) considering, the evaluation of the current threat environment, the attractiveness, and vulnerability of targets (e.g. properties and nature of the material), and possible consequences (radiological consequences and usage of theft material for harmful purposes). These require the operator to provide a higher level of protection for targets where higher risks are involved. (IAEA 2011a, 14; IAEA 2018b, 26-36).

The DiD is also applied in the design of nuclear security (fundamental principle I). In practice, the PPS must provide consecutive layers of protection which adversaries must break through or circumvent before they can reach their targets. (IAEA 2011a, 15; IAEA 2018b, 38-40).

In the following the PPS of an NPP is discussed further from a perspective of design aspects of such system and in relation to above mentioned important elements. The aim has been to find connections between safety and security.

3.1 Threats

Threats arising from humans can be categorized by several different means. The adversary type is one way, it can be an external individual/group, insider/group of insiders, or constitute collusion between both types of adversaries (e.g., insider facilitates to external adversaries to commit the malicious act). Also, threats can be categorized for the intention as the objective may be to sabotage (the facility, activities, and nuclear or radioactive material) or to steal hazardous material (nuclear or radioactive). Nuclear material (NM) may be targeted for building a nuclear explosive device or to gain economic benefits. Radioactive material may

be pursued to cause harmful consequences in public. The attack type is also a way to categorize. The adversaries may commit an overt attack with force, use deceive or stealth tactics, stand-off attacks, implement cyberattack or commit an attack by a combination of both cyber and physical elements, just to mention a few. Practically, the adversary attributes and characteristics identified by National Threat Assessment (NTA) permit the derivation of several categorizations. (IAEA 2021a, 7-8, 18-19, 29; IAEA 2019b, 24-26, 39).

3.2 Risk-based physical protection system

The requirements of PPS are derived by State and regulatory authority using a risk-based approach with an aim to ensure that operators' design measures can keep the threat risks below the acceptable levels. The risk can be quantitatively defined as a product of frequency of event and consequence of a malicious act (equation 1). (IAEA 2018b, 25).

$$Risk = Frequency \cdot Consequences \quad (1)$$

The quantitative risk assessment considers the probability of the event of occurring and the quantitatively expressed consequences of malicious act in concern. There are challenges associated with the quantitative method since the probabilities may be difficult to determine. Furthermore, the consequences may be challenging to quantify for successful malicious act if there is no appropriate way to express them. Furthermore, the consequences may be challenging to quantify for successful malicious act if there is no appropriate way to express them. At least radiological consequences can be defined quantitatively and used for several malicious acts, including sabotage and unauthorized removal of radioactive material (if the aim is to cause harm using material). (IAEA 2018b, 25).

The qualitative method can also be used in risk assessments (figure 7). In such case the likelihood of a malicious act and the associated risk are not quantified. The approach is to consider different factors (e.g., consequences, threat likelihood, adversary capabilities) indicating a risk and use them to form combinations of features, which can be used to represent low-, medium- and high levels of risks. (IAEA 2018b, 25).

Potential Consequences	Tolerable			Significant			Intolerable		
Adversary Capability	Inadequate	Adequate	Robust	Inadequate	Adequate	Robust	Inadequate	Adequate	Robust
	Event Frequency								
Expected	Low	Low	Medium	Medium	High	High	High	High	High
Possible	Drop	Drop	Low	Low	Medium	High	Medium	Medium	High
Unlikely	Drop	Drop	Drop	Drop	Low	Low	Low	Low	Medium
Remote	Drop	Drop	Drop	Drop	Drop	Drop	Drop	Low	Low

* Risk classes are 'drop' = negligible risk, 'low' risk, 'medium' risk and 'high' risk

Figure 7. Risk assessment matrix as an example of qualitative method (modified from IAEA 2019b, 123).

Concerning theft of NM, the graded approach can be implemented by categorizing the material considering the properties relevant to its potential to be used in a nuclear explosive device (element, isotopic composition, quantity). In addition, other characteristics of NM such as irradiation level, chemical and physical form and degree of dilution can be used as these may affect the attractiveness of material (radiation health effects and difficulties). The NM is categorized to classes I-III, of which the class I NM has the most stringent protective requirements. The fourth class 'below the class III' may not need excessive means of protection, but still should be secured by at least with access control. Similarly, radioactive material is categorized to classes requiring certain levels of protection in respect to relevant factors (physical and chemical properties, quantity, mobility, availability, and accessibility). Figure 8 shows the categorization scheme for NM. (IAEA 2018b, 28-33; IAEA 2011b, 14-15).

Material	Form	Category I	Category II	Category III
1. Plutonium ^A	Unirradiated ^B	2 kg or more	Less than 2 kg but more than 500 g	500 g or less but more than 15 g
2. Uranium-235 (²³⁵ U)	Unirradiated ^B			
	– Uranium enriched to 20% ²³⁵ U or more	5 kg or more	Less than 2 kg but more than 500 g	1 kg or less but more than 15 g
	– Uranium enriched to 10% ²³⁵ U but less than 20% ²³⁵ U		10 kg or more	Less than 10 kg but more than 1 kg
	– Uranium enriched above natural but less than 10% ²³⁵ U			10 kg or more
3. Uranium-233 (²³³ U)	Unirradiated ^B	2 kg or more	Less than 2 kg but more than 500 g	500 g or less but more than 15 g
4. Irradiated fuel (The categorization of irradiated fuel in the table is based on international transport considerations. The State may assign a different category for domestic use, storage, and transport, taking all relevant factors into account)			Depleted or natural uranium, thorium or low enriched fuel (less than 10% fissile content) ^{D,E}	

^A All plutonium except that with isotopic concentration exceeding 80% in ²³⁸Pu.

^B Material not irradiated in a reactor or material irradiated in a reactor but with a radiation level equal to or less than 1 Gy/h at 1 m unshielded.

^C Quantities not falling in Category III and natural uranium, depleted uranium and thorium should be protected at least accordance with prudent management practice.

^D Although this level of protection is recommended, it would be open to States, upon evaluation of the specific circumstances, to assign a different category of physical protection.

^E Other fuel which by virtue of its original fissile material content is classified as Category I or II before irradiation may be reduced one category level while the radiation level from the fuel exceeds 1 Gy/h at 1 m unshielded.

Figure 8. The categorization of nuclear material to classes with different levels of protection required (IAEA 2018b, 27).

The graded approach for determining the required levels of protection for sabotage targets such as SSCs is based on two threshold values, unacceptable and high radiological consequences (URC and HRC) defined by the State. The targets of sabotage, which may lead to radiological consequences exceeding the HRC should be provided the highest means of protection to prevent any severe conditions (significant radioactive release affecting the population and environment). URC defines a level above which protection measures should be implemented. URC permits to identify all targets which should need an appropriate level of protection. The potential radiological consequences arising from sabotage may be graded to reflect several ranges of severity and required level of protection can be defined to be corresponding to these. HRC and URC may include criteria for the release of the radionuclides (e.g., total activity or release of specific radionuclides) and dose criteria (equivalent dose of an individual). Figure 9 presents, how a graded approach is implemented to derive PPS requirements within these two thresholds. (IAEA 2018b, 34-36).



Figure 9. The relationship between the protection requirements and threshold values for HRC and URC (IAEA 2018b, 36).

The risk-based approach for PPS indicates connections between safety and security. As it already can be clear from the above discussion three coupling points between security and safety can be introduced: 1) damage done to SSCs, 2) radiological consequences (equivalent dose for an individual) and 3) the event frequency of occurrence (Hyvärinen et al 2016, 70).

The damage done to plant SSCs is mainly associated with sabotage, whether it is aimed to cause high radiological consequences (e.g., terrorism) or to disrupt the operator activities (e.g., extreme activists). The malicious acts involving sabotage and plant events are interrelated because sabotage of SSCs could lead to PIEs like any internal hazard, such as fire or flood. The adversaries' sabotage acts are precursors of PIEs, thus providing a link between safety and security. Thus, it is possible to connect DiD levels with the sabotage act in concern by considering the plant event category resulting from such threat. (IAEA 2014a, 105-112).

For example, the terroristic attack (e.g., large airplane crash) may represent sabotage which could be related to DiD level 4 (DEC) and an event regarding the extreme activists provoking the operator to shut down the reactor could fit in DiD level 2 (AOO), based on damage done to NPP.

The risk-based approach used both in safety (Deterministic Analysis and PSA) and security makes it possible to have a common ground for the design of SSCs and PPS by using integrated analyses, at least when sabotage is in concern (IAEA 2014a, 105-112). Theft of nuclear and/or radioactive material may need a different approach.

Similar probabilistic calculation methods (e.g. fault trees and event trees) are used for security event sequences (attack scenarios) as are for accident sequences (accident scenarios) when PSA is done in safety analyses (IAEA 2019b, 38, 57-58; IAEA 2010, 24, 34, 37-39).

Although event frequency of occurrence for malicious acts can be difficult to determine, the analogy between probabilistic methods in security and safety analyses indicates that it might be possible to determine security event frequencies or at least define indicative values. The frequency of occurrence for initiation of the malicious act may not be quantified, but the approach could be to evaluate the frequency of events leading to successful penetration through PPS to different security zones, for which data may be derived from practical exercises. Thus, the event frequency could be a valid coupling point between safety (DiD levels) and security (threat events).

The radiological consequences (equivalent dose for an individual) provide an evident coupling point between safety and security events involving sabotage. The above-mentioned categorization for nuclear and radioactive material may provide means to connect security events involving theft of material to DiD levels.

3.3 Design Basis Threat

DBT is a threat statement developed by the regulatory authority. It is used in providing information on the threats against which the operator should design security arrangements. (PPS and organizational security). DBT is derived from NTA done in cooperation between several competent authorities and State agencies (e.g., military services, law enforcement agencies, ministries, and the regulator body for nuclear safety). NTA includes characterization of all credible nuclear security threats, which may challenge the State. The output of NTA is an overall description of threats, including the capabilities, motives, and intentions of potential adversaries. The State has primary responsibility for threats beyond DBT, such as adversaries with high capabilities. Still, cooperation between the operator and the State is essential to protect from nuclear security threats of any kind. DBT is a tool for the operator to derive attack scenarios for designing PPS evaluating its performance requirements. (IAEA 2021a, 12-19, 26; IAEA 2009b, 3-7).

STUK has developed a DBT using a risk-based graded approach, resulting in a scheme with progressive levels of threat (figure 10). Potential radiological consequences are used as criteria for threat events. The threat levels represent the relative severity of the threat, whether the attempted malicious act is theft, sabotage, or other harmful act endangering the safety of the NPP. The highest threat level corresponds to threats with the most severe consequences, namely extreme sabotage, and theft of class I NM. The protection objectives for each level have been derived from dose limits set for different plant states in the Nuclear Energy Decree 161/1988. It is worth noting that information security, cyber security, and transports have been considered. (STUK 2020a, 2-4).

Threat levels and dose constraints (mSv)		Threats beyond the design basis threat		Obtaining of nuclear material	
		Level	mSv		
Threat types	Extreme sabotage, theft	5	X	Proliferation of sensitive information	Illegal trade in other nuclear commodities and dual-use items
	Airplane crash	4	20		
	Sabotage, theft	3	5 0.1	Proliferation	
	Widescale vandalism, information system disruption, theft	2	0.1		
	Vandalism, influencing through information networks, random theft	1	0.1		
	Vandalism, sabotage, theft	Level	mSv		

mSv: Annual dose constraint for an individual of the population (not specified for a theft or proliferation threat)
Level 3: Nuclear facility 5 mSv, transport 0.1 mSv
Level 5-X: Over 20 mSv during the first week to an unprotected person – a need for evacuation outside the precautionary action zone must not be created at the nuclear facility, safety distance for an individual of the population must be ensured during transport
Levels 1–5 apply to Class 1 nuclear facilities
Levels 1–3 and 5 apply to transport of spent nuclear fuel
Levels 1–3 apply to Class 2 nuclear facilities
Levels 1–2 apply to Class 3 nuclear facilities and transport of fresh nuclear fuel

Figure 10. The structure of the DBT developed by STUK (STUK 2020a, 4).

Such DBT provides an analogy between safety and security since the threat levels represent similar functional levels as DiD levels for safety (Hyvärinen et al. 2016, 56). For both, the severity of the potential consequences increases with the level, and the likelihood of an event of a level decreases. STUK utilizes radiological doses harmonized with limits set for nuclear facilities as introduced in chapter 2.5. The harmonization of acceptance criteria between safety and security is a desirable option as it provides a coupling between DiD levels of safety and threat levels of DBT.

3.4 Security zones

According to IAEA NSS-27G, the PP of NPP should be based on an approach involving structurally separated areas, which provide a graded level of protection for potential targets. The protection areas (as IAEA tends to call these zones) follow the concept of DiD, as these are nested and separated by physical structures between them. Similarly, STUK has established a concept of security zones in its guide YVL.A.11 as it is stated in Regulation STUK Y.3 section 4 (2):

“Security shall be based on the utilization of security zones placed within each other so that SSCs important to safety, and nuclear material and nuclear waste, are protected based on their safety significance and access control and the control of goods traffic can be arranged appropriately.” (STUK 2020b, 3)

The outermost security zone is the restricted area (site area), which constitutes a large area surrounding the NPP where movement and stay are limited (usually fenced-off). The plant area is inside the restricted area, and it constitutes all the buildings associated with the plant’s operation surrounded by double-fence. The protected areas are those bounded by the outer walls of the buildings within the plant area. Such buildings should have heavily protective structures against unlawful actions. The innermost security zones are the vital areas limited inside the protected areas. These contain the targets with the highest potential consequences (e.g., class I NM and physically separated Safety Divisions). (STUK 2021, 10-11; Hyvärinen et al. 2016, 57-58).

IAEA NSS-27G presents three protection areas, limited access area, protected area, and vital/inner areas. Inner areas contain class I NM (in hardened rooms or enclosures). Vital areas have the equipment and/or radioactive material, sabotage of which could result in HRC. Protected areas contain class II NM, and limited access areas may contain class III NM. The sabotage targets with consequences between URC and HRC are within protected areas. Figure 11 visualizes the concept of security zones. (IAEA 2018b, 73-75).

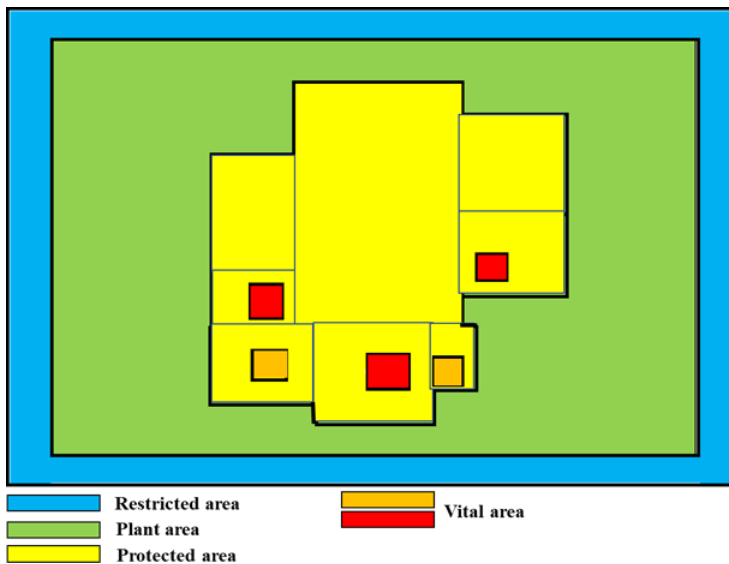


Figure 11. Representative security zones of NPP. Note that only buildings, which constitute protected area are shown (both restricted, and plant area contain several other buildings also).

The concept of security zones points out an analogy between security and safety as it resembles a similar structural DiD aspect as the consecutive confinement barriers are for DiD concept (Hyvärinen et al. 2016, 56-57). The boundaries between security zones constitute consecutive physical barriers (site fence, plant double-fence, the outer surfaces of buildings, the robust structures protecting the vital areas), which the adversaries must be able to defeat without getting interrupted to reach the potential target. The threat could be thought to proceed progressively with respect to passing security zones. As closer to HRC targets adversary gets, the more severe consequences could occur if the attempt succeeds.

In this sense threat levels introduced in chapter 3.3 could be linked to the security zones (figure 12) by allocating the levels to different security zones and considering the potential consequences of threats of certain threat levels. The functional DiD concept for security could be then thought quite similarly as in the case of safety using functional levels for security (threat levels) each aiming to keep the threat from progressing towards potential HRC targets. For each threat level, functional protection measures are provided to prevent the threat from progressing through the associated physical barrier to the next security zone and to mitigate the consequences, if the barrier is reached or defeated.

Threat increases
→

Zone	Restricted area	Plant area	Protected area	Vital area	
Threat level	Level 1	Level 2	Level 3	Level 4	Level 5
Possible threats	Vandalism Intrusion attempt Random theft	Wide-scale vandalism Disruption of plant activities Theft of plant property	Theft of class II or III nuclear material Theft of radioactive material Sabotage of targets between URC and HRC	Airplane crash Sabotage of HRC targets Theft of class I nuclear material	Extreme sabotage of HRC targets Extreme theft of class I nuclear material
	Site fence	Plant double-fence	Outer surfaces of protected buildings	Robust structures	

Figure 12. The possible interrelation between security zones and threat levels. As the adversary proceeds within security zones, more severe malicious acts become possible, and the threat of intrusion increases.

The structural aspect of DiD clarifies the objectives for both security and safety, although they are somewhat different. The ultimate objective for safety is to confine the radioactive material using consecutive physical layers of protection and to prevent/mitigate the threat of radiological release by functional measures (defined in DiD levels) whereas for security it is to block adversaries’ access to their targets (safety-significant equipment/material or other valuable goods) by PP barriers between security zones and functional protective measures implemented within consecutive security zones. Figure 13 demonstrates a similar structural DiD basis for both security and safety.

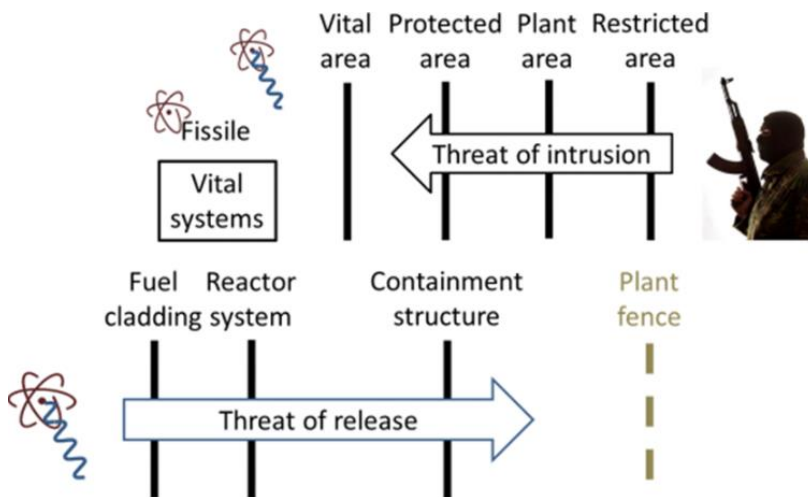


Figure 13. The structural DiD is the basis for both security and safety. Protective barriers are used for two primary purposes to confine the release of radioactive material and to block the path from intruders (Hyvärinen et al. 2016, 57).

3.4 Physical protection measures

DiD concept applied as a basic principle for PP design should provide several layers of protection (security zones and structural barriers between them) and protection methods to prevent threats and mitigate potential consequences of intrusion. To achieve this protection measures of detection, delay, and response are used in a complementary manner. Also, preventive measures such as deterrence and access control are used against threats. Both technical organizational aspects are important when these are implemented. (IAEA 2018b, 38,40, 66-68, 76-82).

Detection is accomplished by using hardware (sensors, monitoring, and communication systems) and human surveillance (guard patrols). Detection is not instantaneous since an alarm triggered by a sensor (or human observation) must be transmitted, reported, and eventually assessed by security personnel before the process is complete. The time needed for detection is defined as detection time. The shorter the detection time, the more likely the response is to be executed in time. Diversity is achieved by using different sensors, which do not respond to the same nuisance alarms. Redundancy is provided using multiple complementary sensors and human surveillance. The central alarm station (CAS) is established to enable monitoring, assessment of alarms, and communication between both guards and response forces. The reliability of communication and alarm transmission is ensured by using redundancy (multiple communication systems and secondary alarm station SAS), diversity (different physical paths), and separation. (IAEA 2018b, 60, 66, 76-78).

The purpose of the delay is to slow an adversary's progress towards a target, thereby providing time for a response to be initiated. Delay is accomplished by distances and areas that must be crossed without getting detected and by using barriers that need to be bypassed or defeated (e.g., fences, gates, doors, locks). The use of multiple layers of diverse physical barriers complicates the attempted intrusion and increases delay time. Detection systems and barriers should be used in a complementary manner to enable immediate detection of intruders before the barrier is reached to provide time to respond after detection is completed. (IAEA 2021b, 97-98; IAEA 2018b, 67-68,78-79).

The response aims to interrupt and neutralize an adversary and mitigate the potential consequences of an act. The response forces consist of persons on-site (nuclear security officers) and off-site (law enforcement agencies) who are properly trained, appropriately

equipped, and armed to manage the threats. The guards, in turn, are responsible for monitoring and assessing alarms, patrolling the area, controlling access, and providing detection of intrusion. However, guards may also provide an initial response depending on national legal practices. A command center is established for communication between on-site response forces and CAS, plant operations, and off-site response forces. (IAEA 2018b, 68, 80-82; STUK 2021, 11,13-14, 19). Figure 14 demonstrates the relation between functions of detection, delay, and response.

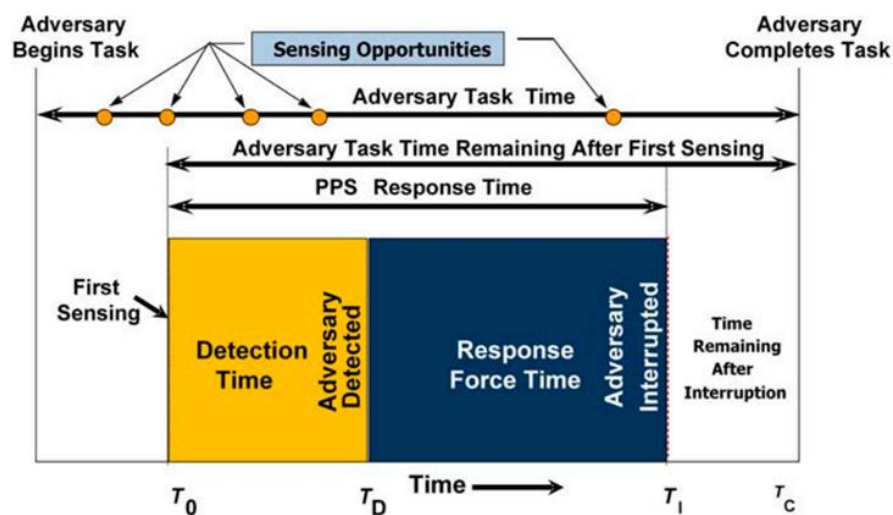


Figure 14. The relation between detection, delay, and response. The adversary task time is the time adversary needs to complete the act. The PPS response time is the time needed from the first successful sensing until the adversary can be interrupted. In this figure, first sensing occurs early enough to allow the interruption. (IAEA 2018b, 59).

Deterrence can be used as a preventive protection measure by promoting the effectiveness of PPS. This may lead the NPP to be an unattractive target as the low probability of success and possible negative consequences may override benefits. The drawback is that some security-related information may require to be made public to communicate adversaries about the effectiveness of PPS. Concerning insider threats, deterrence can be a way to protect against malicious acts (e.g., promoting continuous monitoring and surveillance of activities, and using the two-person rule for entry into a vital area). (IAEA 2021b, 4-5; IAEA 2018b, 66; IAEA 2019b, 125-126).

The access control of people, material, and vehicles can be seen as a preventive measure since its main objective is to allow only authorized persons and vehicles to enter certain areas and to ensure that access rights are granted only for those whose trustworthiness and actual

need are confirmed by following appropriate procedures (e.g., trustworthiness check, identification measures, surveillance, and records). However, access control also provides detection for unauthorized access and prohibited or stolen material/equipment (e.g., alarm and identity verification systems, search systems for explosives, NM and metal detection, guard surveillance) and delay by use of barriers such as portals, turnstiles, and vehicle gates. (IAEA 2021b, 73-97; IAEA 2018b, 79-80; IAEA 2013b, 32-33; IAEA 2011a, 23,25,55).

The PP measures indicate an analogy between security and safety in respect to the functional DiD concept, which for safety aims to maintain the integrity of structural barriers using functional measures aiming for prevention and mitigation. The delay (area and structural barriers) and detection (hardware and human observation) could be thought of as similar ‘barrier’ which ‘integrity’ (to keep adversaries from progressing towards HRC targets) is aimed to be maintained by functional measures such as prevention (e.g., deterrence and access control) and mitigation (response). Deterrence, delay, detection, and response could also be thought of as fundamental security functions.

In respect to nuclear security, adversaries can be seen as challenges for which PP measures are implemented to cope with and to ensure the integrity of the barrier (security zone and its surrounding physical barriers) used to keep threat from progressing towards higher level (targets with HRC). Adversaries as challenges to the PPS are induced by their capabilities and preventive measures are established as provisions to prepare for these. Similar objective tree could be drawn for security as it was previously presented for safety (figure 15).

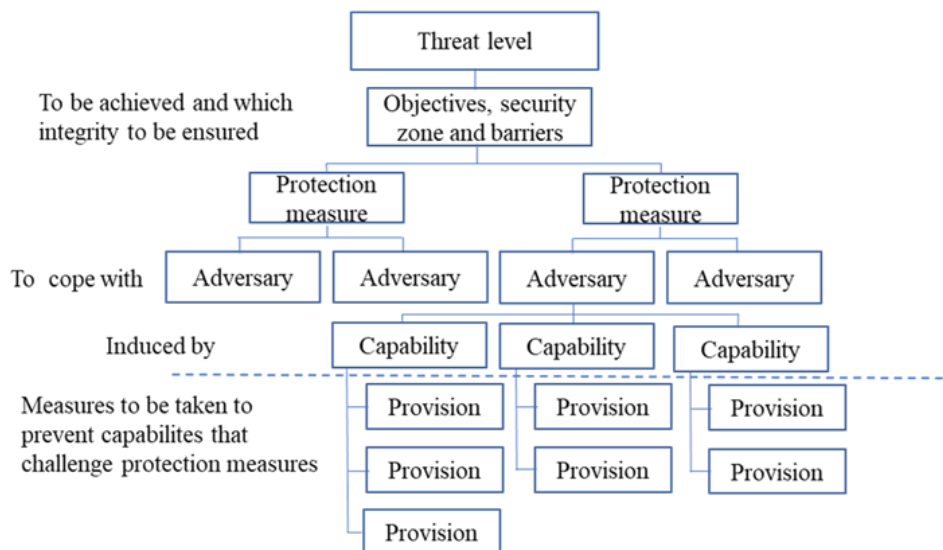



Figure 15. The interrelation between protection measures, challenges (adversaries), and provisions for a threat level or a security zone.

Figure 16 demonstrates such DiD concept and provides some examples for each protection measure.

Defence in depth: multiple protection layers (security zones with barriers) and physical protection measures to ensure their integrity



Prevention		Barrier		Mitigation
Access control	Deterrence	Detection	Delay	Response
Trustworthiness check	Promoting the PPS by appropriate information made public	Sensors	Large areas and distances	On-site response forces (nuclear security officers)
Access rights		Video cameras	Low security barriers (wooden, fabric and wire fences at the outermost boundary)	Off-site response forces (local and national police, special operations unit, military)
Identification measures	Maintaining the confidentiality of sensitive information related to the PPS	Human observation	Security fences (with e.g. barbed tape coil)	Command center
Escorting visits	Crime prevention through environmental design (lightning, visible protection structures, vehicle barriers, guard towers, armoured response vehicles)	Seals or tamper indicating devices	Structural barriers (e.g. concrete walls, floors, ceilings and roofs)	
	Random patrols (guards and response forces)	Central alarm station	Strengthened doors and associated frames, hinges, bolts and locks	
	Random searches		Boundary penetration barriers (e.g. for windows)	
	Two-person rule		Dispensable and specified barriers (for targets)	
			Vehicle barriers	
			Airborne barriers (e.g. pools)	
			Marine barriers (fixed and floating)	
		Access control		
		Credentials check	Locks and keys	
		Search systems (e.g. metal and x-ray detectors)	Personnel portals	
		Identity verification systems	Metal and hardened turnstiles	
		Personnel tracking	Hardened steel grated doors	
			Barrier doors	
			Vehicle gates	

Figure 16. The PPS design in respect to DiD concept with example protection measures.

3.4 Cyber security

Attention to security issues with computer systems, networks, and data management has increased as vulnerabilities of systems have come to light. Vulnerabilities may be exploited to carry out malicious acts to information and systems relevant to security (e.g., access control systems, alarm, and tracking systems), safety (I&C and safety-related systems) and operations (e.g., process control systems). Cyber-attacks provide new capabilities for adversaries such as gathering information, executing direct attacks to relevant systems (security or safety), and combined attacks involving both physical intrusion and cyberattack elements. Cyber security is a cross-cutting discipline that has interactions with all other security areas (PP, information security, and personnel security) and safety. It is important for both safety and security design. (IAEA 2011c, 2, 11-13, 27-29).

Similar DiD concept as for PPS is used as a basis for cyber security design. It is implemented through the combination of several consecutive and independent levels of protection that would have to fail before a compromise in the computer system could occur. No single failure (whether technical, human, or organizational) in one level or barrier would lead to computer system compromise since the subsequent defence levels or barriers provide prevention and mitigation against the consequences of security breaches. When properly implemented the probability for a combination of computer system failures is ensured to be low. The risk informed approach is used, and graded levels of protection are provided for computer assets while considering the potential consequences resulting from the security breaches. (IAEA 2011c, 13, 29).

Computer systems with the same or similar importance concerning security and safety should be grouped into a zone (barrier) that is administrated and which builds a trusted area for internal communication between computer systems within the zone. For each zone, a security level (prevention and mitigation) should be assigned to indicate those protective measures to be applied for all computer systems in that zone. A security level may have multiple zones assigned to it. The zones are a logical and physical groupings of computer systems. (IAEA 2011c, 30).

The security levels define the degrees of security protection required by computer systems. Each graded level constitutes a set of protective measures to satisfy the security requirements of that level. Some protective measures are applied for all computer systems defined at the

general security level. The possible choice of specific security levels could vary and should be tailored according to the facility specificities, the considered environment, and the insights derived from security risk analysis. (IAEA 2011c, 29, 31-35).

DiD concept with zones and security levels is quite similar to security zones and threat levels of PPS design. The plant PPS design envelope can be proposed by combining all the relevant concepts introduced so far (figure 17).

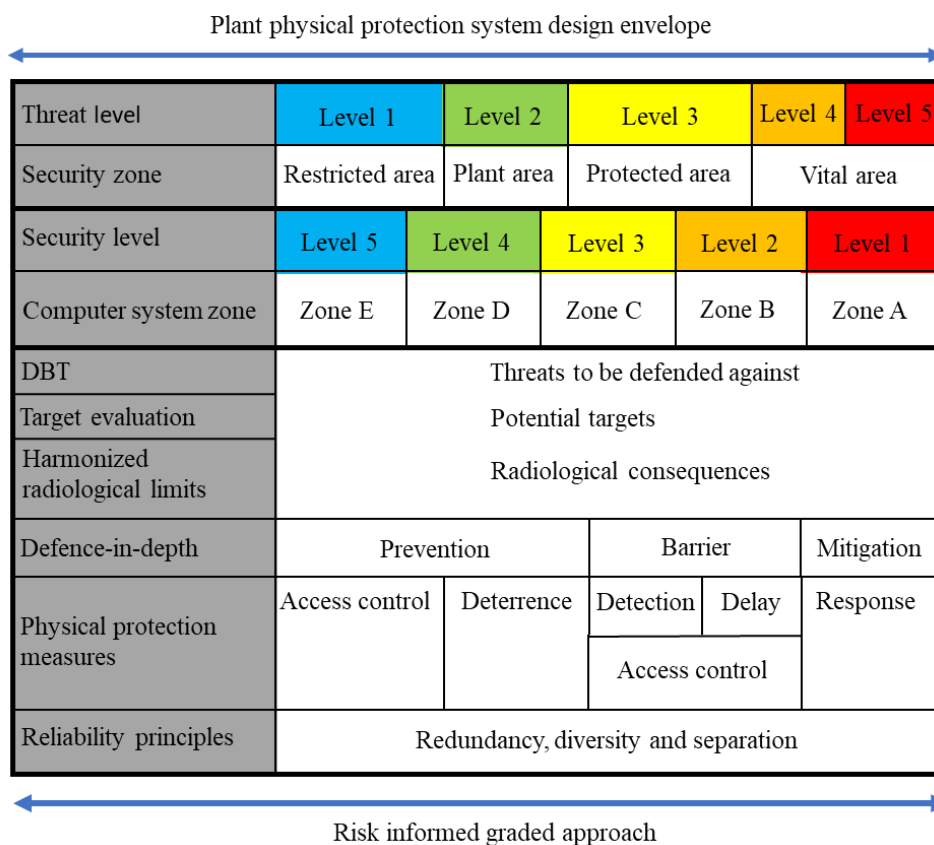


Figure 17. The plant PPS design envelope.

The risk-informed graded approach constitutes the frame for all essential security design aspects. An example implementation of computer security levels from 1 (most protection needed) to 5 (least protection needed) based on IAEA Computer Security Guidance is shown in figure 18.

Zone	Zone E	Zone D	Zone C	Zone B	Zone A
Security level	Level 5	Level 4	Level 3	Level 2	Level 1
Example system	Systems not directly important to technical control or operational purposes ^E	Technical data management systems ^D	Real time systems not required for operations ^C	Systems with high security requirements ^B	Systems vital to the facility ^A
Protective measures	<p>Only approved and qualified users are allowed to make modifications</p> <p>Access to the Internet from systems is allowed provided adequate protective measures are applied.</p> <p>Remote external access is allowed for authorized users provided that appropriate controls are in place</p>	<p>Access to the Internet from systems may be given provided adequate protective measures are applied</p> <p>Security gateways to protect from uncontrolled traffic from external company or site networks, and to allow specific and controlled activities</p> <p>Only approved and qualified users are allowed to make modifications</p> <p>Physical connections to the systems should be controlled</p> <p>Remote maintenance access is allowed and controlled</p> <p>System functions available to users are controlled by access control</p>	<p>Access to the Internet from systems is not allowed</p> <p>Security gateways to protect from uncontrolled traffic from level 4 systems, and to allow only specific and limited activity</p> <p>Remote maintenance access is allowed on a case by case basis and is robustly controlled</p> <p>Physical connections to the systems should be controlled</p> <p>Access rights to the systems is kept minimum</p> <p>System functions available to users are controlled by access control</p>	<p>Only an outward, oneway networked flow of data is allowed from level 2 to level 3 systems</p> <p>Only necessary messages can be accepted in inward direction</p> <p>Remote maintenance access may be allowed for a defined working period and with use of strong protective measures</p> <p>Physical connections to the systems should be strictly controlled</p>	<p>No data flow from systems in weaker security levels</p> <p>No remote maintenance access is allowed</p> <p>Physical access to systems is strictly controlled</p> <p>Access rights to the systems is limited to an absolute minimum</p> <p>Two-person rule is applied when modifications are made</p>
Generic level requirements					

A: E.g protection systems – I&C systems that are used for automatically initiated reactor and plant protection actions

B: E.g operational control systems

C: E.g process real time supervision systems in a control room

D: E.g work permit, work order, documentation management systems

E: E.g office automation systems

Figure 18. Zones and security levels with example systems and possible protective measures for each level.

4. Safeguards

Safeguards are activities and technical measures through which the IAEA aims to ensure that the party States of the Non-Proliferation Treaty fulfil their obligations regarding the prevention of the spread of nuclear weapons. The objective of safeguards is the timely detection of a significant diversion of NM from declared activities and provision of deterrence by early detection of diversion and facility misuse. Thus, safeguards verify that material and technology are being used only for peaceful purposes.

Each Non-Nuclear Weapon State under the NPT is required to conclude a Safeguards Agreement with the IAEA to apply safeguards. Generally, three kinds of agreements are used, comprehensive safeguards agreements (CSA), voluntary offer agreements, and item-specific safeguards agreements. The State may also have an additional protocol (AP) to any of these agreements to strengthen the safeguards measures. Most safeguards agreements in force are CSAs. Under CSA safeguards are applied to all NM in facilities and locations outside facilities (LOFs). Objectives of CSA are to detect undeclared NM, to detect undeclared production or processing of NM in declared facilities or LOFs, and to detect diversion of declared NM from declared activities both in facilities and LOFs. (IAEA 2014b, 4-5; IAEA 2016d 3-5, 7).

Safeguard measures are applied to ensure the correctness and completeness of the State's declared NM and its associated activities. For CSAs, these measures can be divided into three basic activities, nuclear material accountancy (NMA), off-site verification, and on-site verification. NMA means continuous bookkeeping of NM within the facilities (or LOFs). A variety of information is required to be provided to IAEA under CSA including NMA reports, facility (or LOF) related information and advanced notifications of imports and exports of NM, just to mention a few. IAEA assesses the information by comparing different records and previously submitted reports. In addition, IAEA uses operational and State reports and open sources for information assessment purposes. (IAEA 2021c; IAEA 2016c, 4-7, 10-13).

IAEA on-site verification activities include inspections, which may include measures such as auditing facility's NMA and operational records, comparing records to reports, verifying NM inventory and its changes (measurements and item counting), taking environmental samples, and IAEA equipment checks. On-site visits are done for Design Information Verification (DIV) during the lifecycle of a facility. Technical safeguards measures are applied to maintain Continuity of Knowledge (CoK) on previously verified NMs and operations (e.g., storage, transfers, and handling of nuclear items). (IAEA 2021c; IAEA 2016d, 43-48; IAEA 2014b, 5-9; IAEA 2014c, 17-21, 24).

AP provides IAEA complementary inspection authority (complementary access, CA) by granting expanded access rights to both sites and information. Under AP the State is required to provide more information on its nuclear program by declarations. These include information about nuclear fuel cycle-related research and development activities not involving NM, sites and its buildings, State's nuclear fuel cycle plans for the 10 years, imports and exports of certain equipment and material, locations, and processing of intermediate and high-level waste, just to mention a few. (IAEA 2021c; IAEA 2014c, 3-4; IAEA 2016c, 77).

Although safeguards are a state-level activity the scope of this thesis is to focus on facility-level implementation. Efficient and effective safeguards for an NPP requires 'safeguardability' which means that the design should facilitate the implementation of verification such as inspections and installation of IAEA safeguards (IAEA 2014d, 1). The following sections introduce plant safeguards issues to be considered. The aim is to discover connections with both safety and security while reflecting DiD as the basis.

4.1 Nuclear material accountancy and material balance areas

Operators are required to maintain facility records and report NMA entries to the State system of accounting for and control of nuclear material (SSAC) for NMA and control purposes. State or Regional Authority responsible for safeguards implementation (SRA) reviews and approves the reports before their submission to the IAEA. IAEA delivers verification results to the SRA after necessary activities have been conducted (evaluation of submitted information, comparison to other sources, and verification activities on-site).

Provision of information is an essential activity for IAEA safeguards, thus a variety of other information along with NMA reports are delivered to the IAEA (nuclear plant documents, information about imports and exports of NM, AP declarations etc.). Figure 19 demonstrates the information flow from the operator to the IAEA. (IAEA 2016c 5-7, 10-11; IAEA 2016d, 51-52).

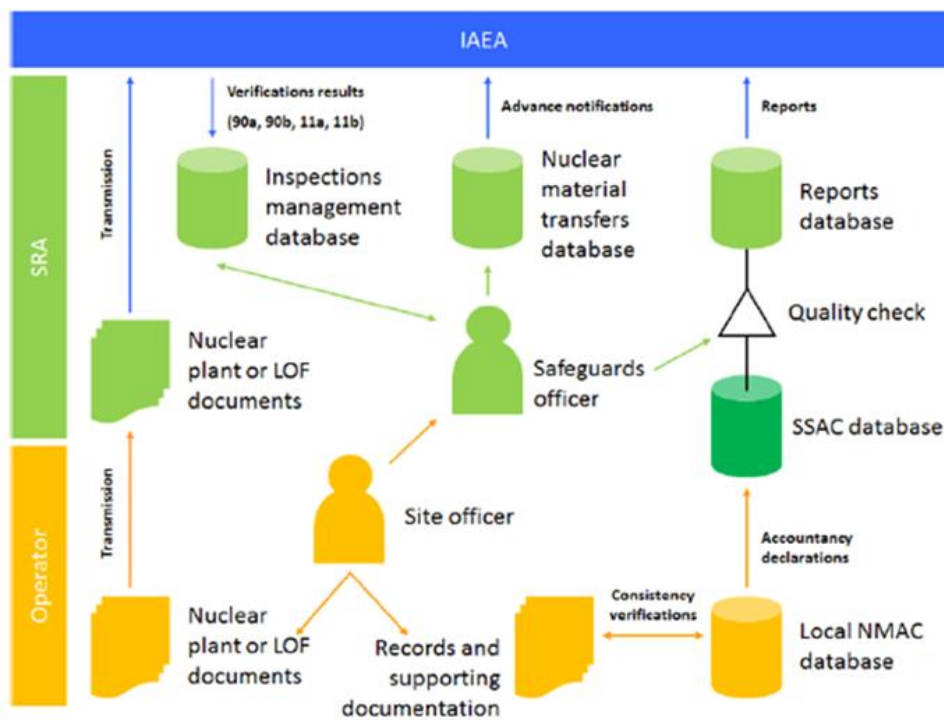


Figure 19. Example of information flows between operator, SRA, and IAEA. (IAEA 2016c, 10).

The NMA and reporting system at a facility should provide an ability to relate an accounting entry with corresponding facility record and enable tracking of accounting records to initial information regarding nuclear items and batches. Facility records can be divided to three categories, source data, supporting documents and accounting records. The source data refers to initial data (e.g., quantity and quality measurement data) and information (e.g., transaction documents) based on which nuclear items or batches can be identified. The supporting documents include reports which are not required to be delivered to IAEA but assist the operator in accounting and reporting (e.g., tracking movements of NM within material balance area (MBA) and maintaining lists of physical items). Accounting records are maintained for whole MBA (general ledger) and for specific key measurement points (KMPs) within this area (subsidiary ledger). (IAEA 2016c, 12-13; STUK 2019c, 26-28).

NMA reports include inventory change reports (ICRs), material balance reports (MBRs), and physical inventory listing (PIL). Briefly, ICR provides information about changes in the inventory of NM, MBR is a summary of the material balance in MBA reflecting all inventory changes for a material balance period (MBP) and PIL provides separate material identification and batch data for all NM batches at KMPs. (IAEA 2016c, 6; STUK 2019c, 32-34). Figure 20 demonstrates the relation between accounting reports and facility records.

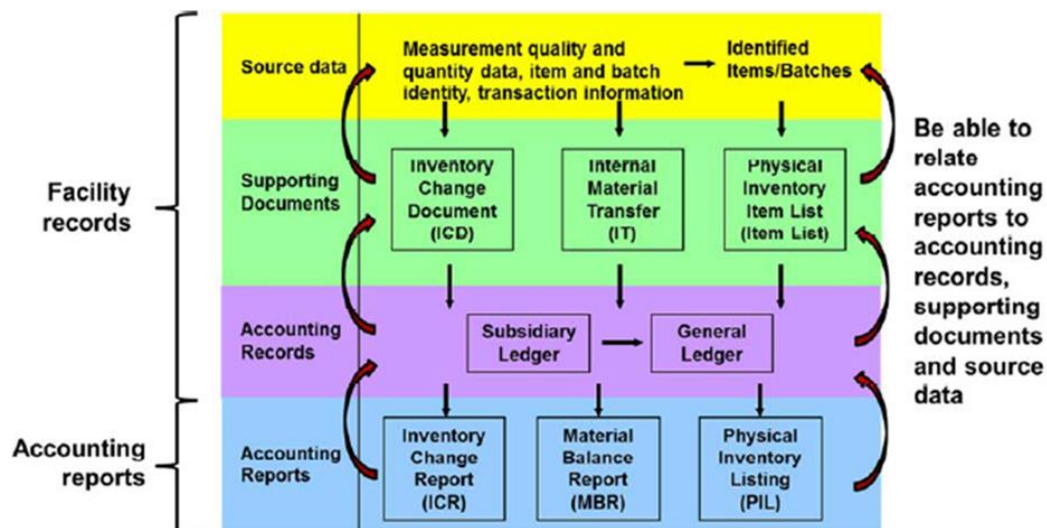


Figure 20. Relation between accounting reports and facility records (IAEA 2016c, 13).

NMA and control are implemented within an area defined as an MBA. It is an area for which NM balance for IAEA safeguards purposes can be established and maintained. For the NPP, one MBA is used which covers the whole facility site. Any material crossing the boundary of an MBA should be reported as inventory change (ICR) and NM within the area as physical inventory (PIL). The end book value of material and associated changes (material transactions, movements within MBA, nuclear loss and production) for a given period are reported in MBR. Typically, this period is between two physical inventory takings (PITs). (IAEA 2016c, 28-29, 33).

During PIT IAEA verifies the physical inventory of NM (item counting and measurements). The book value of MBR is compared to physically verified material inventory and the resulting difference (material unaccounted for, MUF) is included in MBR. Statistically significant MUF may indicate that NM is diverted from declared use, thus it is an important

value for NMA, though many other reasons may exist for small deviations (e.g., measurement uncertainties). (IAEA 2016c, 37; STUK 2019c, 44).

KMPs are locations within MBA where the material is in a form that can be measured or counted for determining inventory or flow (figure 21). Flow key measurement points (FKMPs) are locations associated with fuel transfers (used for ICRs). Inventory key measurement points (IKMPs) are locations that contain nuclear inventory such as storages and reactor core (used for PILs). Opportunities to use Containment/Surveillance (C/S) at KMPs should be utilized to maintain the CoK of NM inventories and flows. (IAEA 2016c, 29, 32; IAEA 2016d, 51-52).

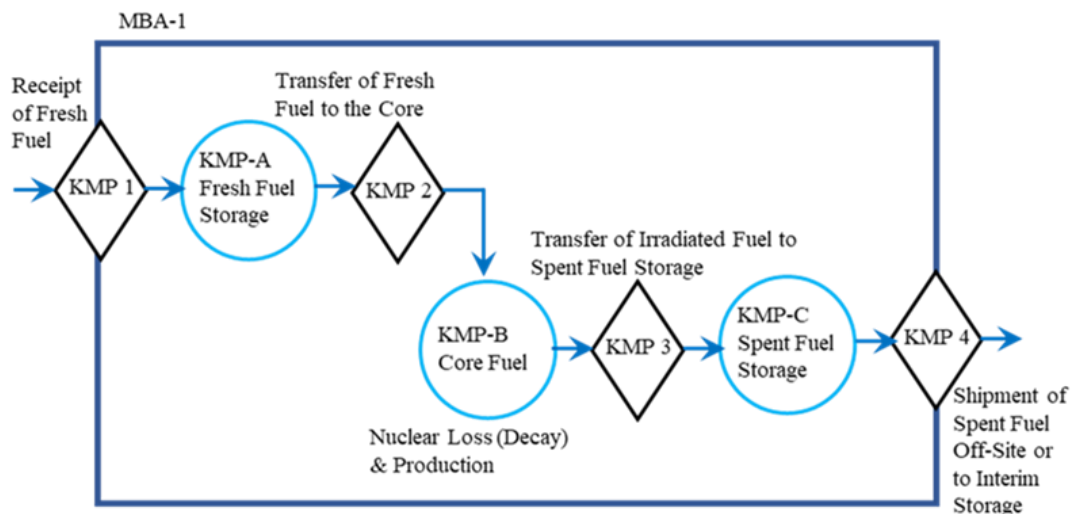


Figure 21. Typical MBA for LWR with four flow KMPs (1, 2, 3 and 4) and three inventory KMPs (A, B and C) (IAEA 2014b, 15).

Typically, four FKMPs and three IKMPs are applied for LWRs. However, plant designs may differ such as whether the spent fuel storage facility resides within the plant site or in a different site. It is not required to maintain material balances on a KMP basis; however, operators typically track balances for sub-areas within MBA (e.g., reactor core and spent fuel storage pool) to effectively localize and investigate possible losses. Such sub-areas for NMA may also enhance IAEA verification. (IAEA 2014b, 15; IAEA 2016c, 32).

4.2 IAEA verification activities

On-site verification activities can be sorted into three categories (figure 22), DIV, inspections, and CA (if AP is in force). To facilitate these activities, the IAEA inspectors must be provided with access to locations and information necessary for objectives to be fulfilled. If inspections are not appropriately considered, operations, safety, and security may contradict. C/S methods and monitoring systems support verification and decrease the number of on-site visits. (IAEA 2016d, 8-10; IAEA 2014b, 2, 9-10).

IAEA Verification Activities		
Design Information Verification	Inspections	Complementary Access
Examination of facility documentation	Checking consistency between facility records and IAEA reports	Visual observation (photographing)
Facility walkthrough (comparison of DIQ drawings with plant layout)	Verification of nuclear material:	Collection of samples (environmental and other)
Collection of environmental samples	<ul style="list-style-type: none"> • Identifying items and their locations • NDA measurements • Collecting samples for DA analysis 	Radiation and NDA measurements
Physical dimension measurements		Other measurements (for non-nuclear material)
Assesment of nuclear material accountancy and measurement system	Confirming the calibration of operator measurement systems	Use of seals and tamper indicating devices
Assesment of declared capacity and throughput of the facility (volume of vessel, containers, piping connections)	Servicing C/S and monitoring systems	Operator interviews
Assesment of access routes and nuclear material flows (ducts, large ventilation sytems, maintenance hatchways)	Verification of the sealing systems	Examination of records (quantities, origin or description of nuclear material)
	Collection of environmental samples	
	Checking the operational status of the plant	

Figure 22. IAEA on-site verification activities with examples.

DIV refers to activities aiming to verify the safeguards-relevant information on facility characteristics and processes which are submitted to IAEA using a Design Information Questionnaire (DIQ) and used in developing safeguards approach (SA) (MBAs, strategic points, C/S measures, safeguards equipment, etc.). It is conducted periodically during all stages of the facility life cycle. DIV aims to ensure continued accuracy and completeness of safeguards-relevant design information, to assure that no undeclared modifications have occurred, and to evaluate for possible improvements. Activities involve examination of facility documentation (design documents, records, and accountancy/operation procedures), comparing DIQ drawings with the actual layout, physical measurements, assessing access

routes, flows of NM, and inventory capacity of the facility. DIV requires that IAEA inspectors have broader access to locations than typically visited during routine inspections (strategic points). (IAEA 2014c, 7-11; IAEA 2016d, 44).

Three kinds of inspections are conducted, ad-hoc, routine, and special. Ad-hoc inspections are done to verify information in the initial report on NM and to identify any changes to it before the SA has been concluded. Access is provided to any location relevant to verify the NM before strategic points have been specified. In addition, ad-hoc inspections refer to NM verification in locations where NM transfers are intended to occur during import (receipt) and export (shipment). Routine inspections can be announced or unannounced and are restricted to locations that are defined as strategic points. The main objectives of routine inspections are to verify the location, identity, quantity, and composition of all NM, consistency between NMA reports and records, and information on possible deviations in the book inventory. Special inspections are conducted if deemed necessary and include supplementary efforts to the routine inspections and access to additional information or locations. CA refers to IAEA's authority under AP to request access to a variety of other locations in a site such as buildings to verify the absence of undeclared material and activities or other information relevant to AP declarations. (IAEA 2016d, 44-48).

4.3 IAEA safeguards measures

IAEA applies three kinds of technical safeguards measures (figure 23) to maintain CoK of NM and associated operational activities. The safeguards measures assist IAEA to achieve its verification objectives. These are based on technical systems, seals, and physical structures.

C/S methods are used as complementary measures to ease verification activities material as access to material can be controlled and undeclared transfers of material detected, thus maintaining CoK. In addition, detection of facility misuse can be established by surveillance of operations. C/S is based on optical surveillance systems (video cameras) and sealing systems. These are applied or installed in strategic points that IAEA has determined in its SA for certain facility design. The strategic points include all diversion paths considered credible in the facility that are KMPs (such as fresh fuel receipt and spent fuel storage pool)

and associated fuel transfer pathways and handling areas. The use of such methods decreases on-site verification activities and thus provides cost savings and less interference for operations. In addition, C/S is applied to detect unauthorized access to IAEA safeguards equipment. (IAEA 2014b, 8; IAEA 2014c, 24; IAEA 2011d, 55).

Technical Safeguards Measures		
Containment	Surveillance	Monitoring Systems (UMS/RMS)
Containers and structures Tampering indicating enclosures Seals: • Metal seals • Optic-fibre seals • Electronic seals	Single camera systems Multiple camera systems Underwater cameras	Radiation detectors (gamma and neutron) NDA instruments Other sensors (pressure, temperature, flow)

Figure 23. Technical safeguards measures with examples.

In NPP surveillance cameras are mounted on locations in the reactor hall that provide an effective field of view and cover all activities and areas of safeguards interest. Along with the continuous monitoring of reactor core and storage pools, the surveillance of fuel handling equipment such as lifting and transfer machines for fuel assemblies (FAs), caskets, and storage racks (polar crane, refueling bridge, and other machines used for transfers) is relevant. Underwater cameras are used to observe fuel handling activities that occur in fuel storage ponds or reactor pools (e.g. verification of spent fuel identifiers). The provision of appropriate illumination is essential for optical surveillance systems. Optical surveillance is intrinsically an unattended safeguards method. Both single and multiple camera systems are applied depending on the complexity of activities. Early considerations regarding facility design (e.g., containment layout) and operations (e.g., maintenance activities) should be taken to avoid any interferences between safeguards implementation and facility operations (e.g., obstruct of camera view due to use of equipment). (IAEA 2014b, 16-17, 22-23; IAEA 2014c; 51-52; IAEA 2011d, 55-56, 61-64).

Containment refers to applying containers for NM (e.g., fresh fuel containers, spent fuel caskets) and tamper-indicating enclosures for safeguards equipment (e.g., for video cameras, sensors, IAEA equipment cabinets, and associated cables) with different sealing systems. In addition, the physical structures such as walls of containment, spent fuel pool, and fuel transfer canal provide containment of NM. The purpose is to maintain the integrity of

knowledge of verified NM between inspections and to indicate any attempt to access the NM or safeguards equipment. Seals are applied to certain fuel transfer paths (e.g., canal gate between the reactor core and spent fuel pond) and containment penetrations to assure that no misuse or diversion has occurred. Each seal has a unique identity and is used to identify containers having NM. Most IAEA seals are passive metal seals, but active fibre-optic seals and electronic seals are also used. The integrity of seals and enclosures is verified by the IAEA during on-site inspections. Sealing requires certain procedures whenever nuclear fuel is unpacked (seal detached) or packed (seal attached) during receipt, transfers within facility, and shipment as IAEA inspectors are those only authorized to handle the seals. During refueling, the sealing of the reactor vessel (RV) is verified, and a new seal is attached. The containment and sealing can be supported by the early provision of design and operational program information. (IAEA 2014b, 19-23; IAEA 2014c, 52-54; IAEA 2011d, 55, 69).

Figures 24 and 25 demonstrate the implementation of C/S in two different containment layout configurations.

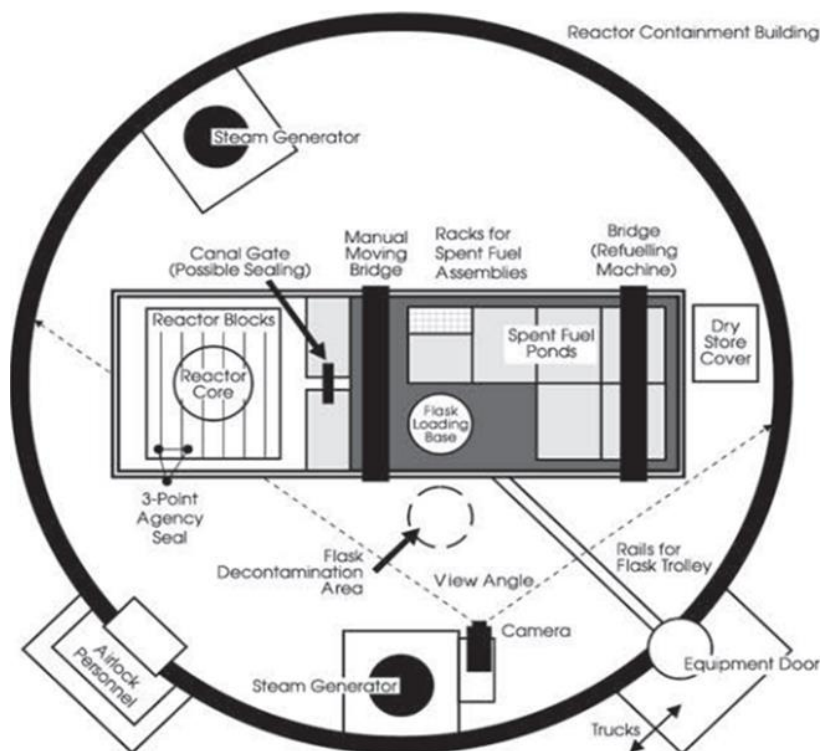


Figure 24. Typical C/S measures for a reactor with spent fuel storage located inside containment (IAEA 2014b, 16).

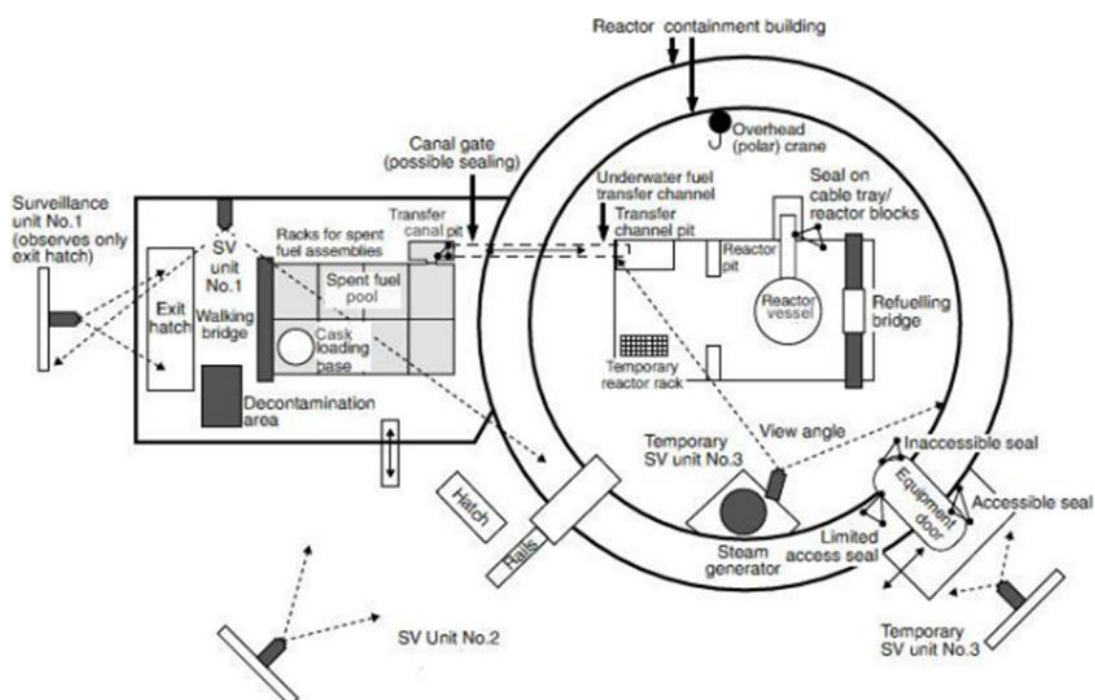


Figure 25. Typical C/S measures for a reactor with spent fuel storage located outside containment (Coles et al. 2013, 59).

IAEA takes much advantage of unattended monitoring systems (UMS). UMS is a system comprised of sensors such as radiation sensors (gamma or neutron) and optical sensors (video cameras) that continuously monitor NM inventories, flows and related operational activities at strategic points without the need for inspector presence. UMSs may include instruments for non-destructive assay (NDA) measurements (e.g., determination of isotopic composition). UMSs can be utilized for multiple purposes such as to detect and track NM movements (sensors), to provide verification data on NM (NDA), and to survey NM and operations (video cameras). (IAEA 2014c, 49-50; IAEA 2011d, 42-43, 78).

The data collected by sensors and instrumentation is transmitted and stored in data collection units that are contained in IAEA secure cabinets. The data may be directly delivered to the IAEA if agreed between the State and IAEA, that is when UMS is implemented as a remote monitoring system (RMS). Two kinds of data are transmitted to the IAEA, equipment state of health data used for determining the operational status of the systems and facility data used for safeguards verification purposes. If RMS is not used the data is reviewed by IAEA inspectors on-site and a hard copy may be delivered to IAEA headquarters. As to ensure IAEA's capability to draw independent safeguards conclusions, the data is not usually shared with the operator. (IAEA 2014c, 54-59; IAEA 2011d, 42-43, 78, 80-81, 123,132-133).

4.4 INPRO proliferation resistance assessment methodology

The International Project on Innovative Nuclear Reactors and Fuel Cycles (INPRO) has developed a proliferation resistance (PR) evaluation methodology that provides both a framework for assessing PR and guidance to improve it for a nuclear energy system. The INPRO PR methodology is based on basic principle, five user requirement (UR) and their indicators, evaluation parameters, and acceptance limits. The evaluation and its components reflect on the basic principle that a nuclear system should have intrinsic features and extrinsic measures to ensure that it continues to be an unattractive target through its full life cycle. (IAEA 2012, 1, 25-31).

The methodology is used on three levels of evaluation, State, nuclear system, and facility level. URs 1-3 represent proliferation barriers that can be categorized as 1. State barriers for technical difficulty in making weapons (State level), 2. barriers for difficulty in handling and processing material (all levels), and 3. safeguards barriers for difficulty in diversion and misuse (facility level). The fourth UR is about multiplicity and robustness of barriers, thus introducing yet another DiD concept. The URs form a layered hierarchy (figure 26). Now the focus is on safeguards at the facility level, thus URs 2-4 are discussed further. (IAEA 2012, 39).

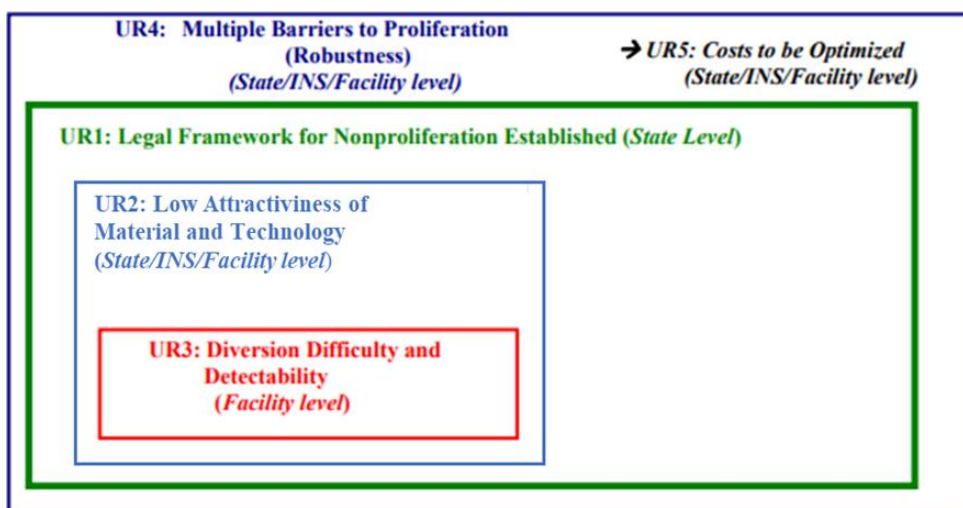


Figure 26. The hierarchy of user requirements (IAEA 2012, 39).

UR 2 is that nuclear systems should have low attractiveness of NM and technology for use in weapons. The attractiveness of NM depends on two intrinsic features, the conversion time and amount needed for one significant quantity (SQ, figure 27) of material that is directly usable in a nuclear explosive. At the facility level, this UR refers to proliferation barriers concerning the characteristic of material and technology that make it difficult to handle and process NM. Generally, there are three kinds of material barriers, quality, quantity, and classification barriers. (IAEA 2012, 25-28).

Material	SQ
<i>Direct use nuclear material</i>	
Pu ^a	8 kg Pu
²³³ U	8 kg ²³³ U
HEU (²³⁵ U > 20 %)	25 kg ²³⁵ U
<i>Indirect use nuclear material</i>	
U (²³⁵ U < 20%) ^b	75 kg ²³⁵ U (or 10 t natural U or 20 depleted U)
Th	20 t Th

a For Pu containing less than 80% ²³⁸Pu.

b Including low enriched, natural and depleted uranium.

Figure 27. SQs of NM according to IAEA. Note that these are different from those used for security (material classification) (IAEA 2002, 23).

Quality barriers can be features such as NM category, isotopic composition, radiation field, heat generation, and spontaneous neutron emission, which make the material not suitable for weapon purposes and difficult to handle (appendix 2). Quantity barriers are those related to mass and quantity of items such as mass of an item, mass of bulk material, and the number of items required for one SQ. These may hinder material diversion and/or acquisition if the use of special equipment is needed. Classification barrier refers to physical and/or chemical characteristics of certain material class that makes it difficult to process NM to separate weapon usable material and convert it to metallic form. (IAEA 2012, 25-28).

UR 3 is essentially related to the design of the facility. This UR states that reasonable difficulty and detectability of diversion and facility misuse should be fulfilled by the designer. UR 3 introduces extrinsic safeguards barriers that can be divided into four main categories, C/S, monitoring, NMA, and detectability barriers. C/S and monitoring barriers

are those sealing, surveillance, and monitoring systems that support IAEA verification activities and make diversion or facility misuse difficult. NMA barrier refers to inspectors' capability to verify NMA records and to successfully identify suspicious MUF for specific material. Furthermore, detectability barrier can be defined as the capability of the system (UMS/RMS) to be able to detect NM. It depends on both technical and material characteristics, thus UR2 and UR3 are interrelated. UR 1 is essential for UR 3 barriers as it provides the legal framework for SA implementation. (IAEA 2012, 29-31).

UR 4 states that the nuclear system should incorporate multiple PR features (intrinsic) and measures (extrinsic) which should overlap in a layered fashion to provide multiple barriers to each possible acquisition/diversion path. Two criteria have been defined, the multiplicity of barriers and their robustness. The multiplicity of barriers is evaluated by identifying all plausible diversion/acquisition paths and assessing the contribution of different proliferation barriers (intrinsic features and extrinsic measures) to efficiently cover all these paths. The robustness of barriers describes the effectiveness of barriers (difficulty of defeating barriers in time and effort) and is measured by determining if the safeguards goals can be met. It is defined as the integrated value of all barriers described in URs 1,2 and 3. (IAEA 2012, 1, 30, 32-33, 35). Figure 28 summarizes the PR DiD concept discussed so far.

User Requirement 4: Defence-in-depth		
Criteria 4.1: Multiplicity of barriers	Criteria 4.2: Robustness of barriers	
User Requirement 2: Low attractiveness of nuclear material and technology	User Requirement 3: Difficulty and detectability for diversion and misuse	
Proliferation barriers		
Intrinsic	Extrinsic	
Material barriers	Safeguards barriers	
Quality barriers	Accountancy barrier	
Quantity barriers	C/S barriers	
Form (Classification) barriers	Monitoring barriers	
	Detectability barriers	

Figure 28. The PR DiD concept based on INPRO PR methodology.

4.5 GIF PR/PP methodology

The Generation IV International Forum (GIF) has developed another PR evaluation methodology. However, the GIF PR/PP methodology has a bit different viewpoint as it focuses to be a tool for designers to consider both PR and PP issues. The methodology is based on challenges, system response, and outcomes with an evaluation done using measures (e.g., detection probability) that characterize the attractiveness of pathways for proliferation attempts or security attacks. PR or PP challenges are identified by threat definition that identifies possible actors, their objectives, capabilities, and strategies. The system response is evaluated by using the pathway analysis method for which nuclear system or facility is divided into elements, targets are identified/categorized, plausible pathways defined and subdivided into segments, and representative measures are estimated for the pathways. The outcomes of the system response to threat are concluded by comparing different pathways in respect to measures to identify the most vulnerable ones. (GIF 2011, 9-15).

What is worth noticing is that GIF PR/PP methodology is structured based on a common method, which forms an appropriate way to integrate both safeguards (PR at facility level) and security-related challenges to be dealt with within one single methodology. As already mentioned, accident scenario analysis and attack scenario analysis are somewhat similar approaches and for sabotage threats, these provide synergies between safety and security. While PR/PP methodology considers only safeguards and security it is also recognized that safety could also be integrated into the methodology as accident scenario analysis has a similar methodological approach (figure 29). (GIF 2011, 20-21).

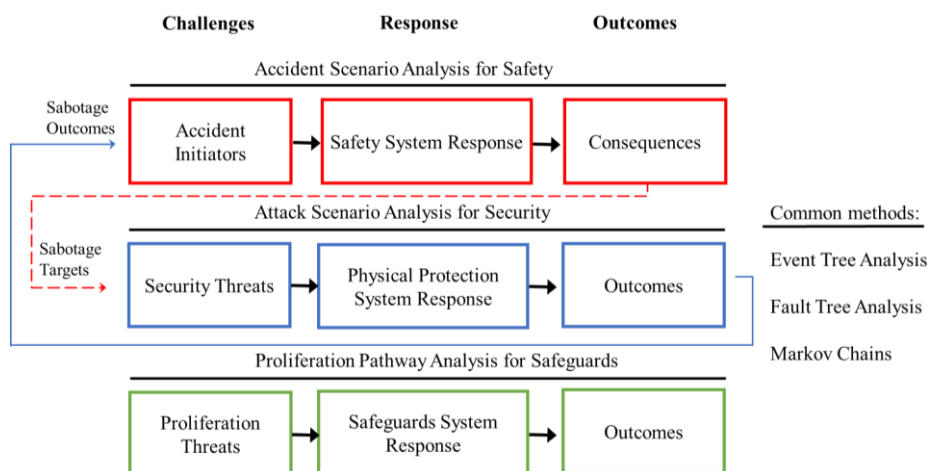


Figure 29. The commonalities and relations between methods of the '3S'. Attack scenario provides information for accident analysis, whereas accident scenario analysis for security analysis.

The GIF methodology provides the designer essential input considering safeguards and PP challenges and should be applied starting from the initial conceptual design phase to establish the necessary dialogue between ‘the 3S’. The method elucidates the interactions between intrinsic features and extrinsic measures and provides guidance on optimal design. Concerning safeguards design, GIF methodology is a useful tool for considering relevant design issues of safeguardability of the facility. The INPRO PR evaluation uses the proliferation path analysis scheme defined in GIF PR/PP methodology, thus they are interrelated. (GIF 2011, 37, 49, 52, 55, 58; IAEA 2012, 38).

4.6 Safeguards and safety

It is noticeable that safeguards and safety have commonalities. Safety aims to confine NM inside structural barriers to prevent the release of radioactive and nuclear material. Similarly, safeguards aim to hold NM inside containment structures and keep them in specific locations to preserve continuous knowledge of NM and facilitate IAEA verification activities. The implementation of safeguards at the NPP relies on three ‘fundamental safeguards functions’ that are NMA, C/S, and monitoring (UMS/RMS). These are used for maintaining the ‘integrity’ of knowledge of NM and safeguards-relevant operations within the MBA. The objective is to detect diversion and facility misuse for weapon production purposes. An analogy can be seen with safety, as these three ‘fundamental safeguards functions’ resemble fundamental SFs that are applied for maintaining the integrity of confinement barriers.

It seems that DiD concept is also applicable for safeguards although the progressive levels may not be evident. INPRO PR methodology provides insights on the structural DiD aspect by considering intrinsic material barriers and extrinsic safeguards barriers which as an integral whole establishes multiple defence layers against proliferation. The material barriers could be thought of as the first ‘structural’ barrier. The NM is to be/flow in specified locations and KMPs within MBA, which could be the second ‘structural’ barrier and should be ensured by the operator (records and reports) and verified by the IAEA. The safeguards barriers are essentially applied within MBA at KMPs and locations that comprise those strategic points at which NM inventories, flows, and facility operations should be monitored and controlled. Safeguards equipment provide detection and the proliferator must be able to defeat such a third ‘structural’ barrier to conceal diversion or misuse attempts. The physical

structures such as locked rooms, buildings, and delay barriers can be seen as final barriers against proliferation, which points out a connection between safeguards and security.

Prevention and mitigation can be also considered relevant for safeguards DiD implementation. It could be suggested that IAEA verification activities form the functional DiD aspect of safeguards as these aim to prevent deviations and when necessary, mitigate the failure of the SA in maintaining the safeguards knowledge of the facility. Verification activities are used to maintain the integrity of 'structural' barriers as completeness and correctness of the information, operability of systems, and feasibility of the SA (DIV) are verified. The 'structural' barriers and functional verification activities can be related, for example, CA is done for site buildings and locations (physical structures). In addition, such relations could be thought of as 'progressive levels' to some extent, for example, CA and PP as the most 'severe' level. The proposed safeguards DiD concept is shown in figure 30.

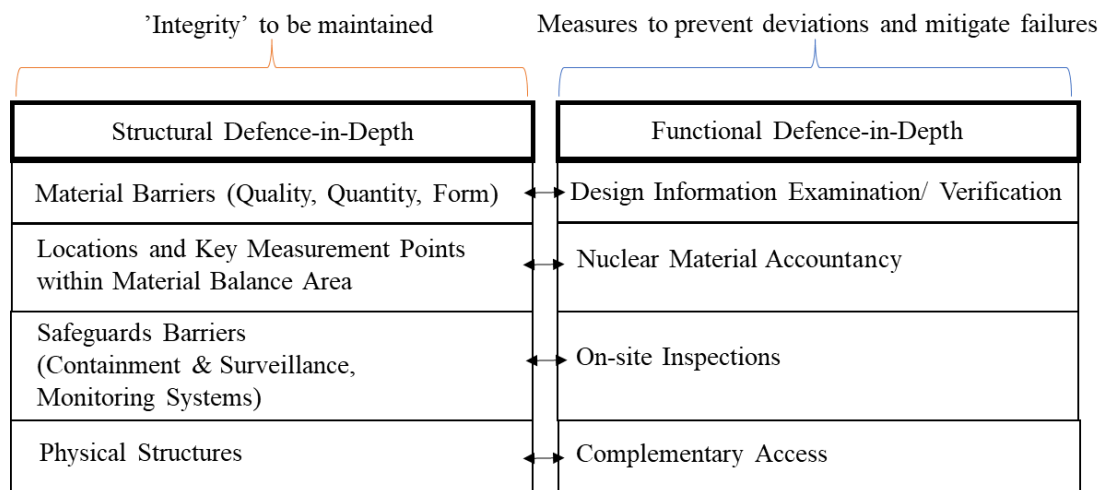


Figure 30. Structural and functional aspects of the proposed DiD concept for safeguards. 'Structural' barriers can be considered to have corresponding functional verification activities. Such correspondence could be thought as 'progressive levels' of safeguards to some extent.

An objective tree similar to safety/security can be drawn for safeguards based on the above discussion on maintaining the 'integrity' of knowledge on NM and related operational activities (SA) (figure 31).

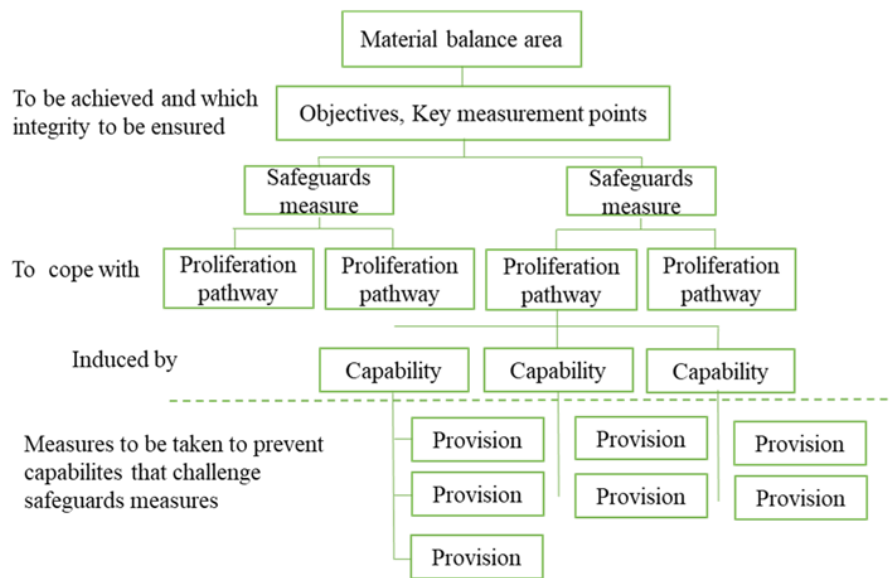


Figure 31. The interrelation between safeguards measures, challenges (proliferation pathways), and provisions for MBA.

Proliferation pathways within the MBA can be seen as challenges against which safeguards measures (‘fundamental safeguards functions’) are applied to ensure the integrity of the SA (objectives and KMPs within MBA). Proliferation pathways are induced by proliferator capabilities and preventive measures are established as provisions to ensure that the SA will remain efficient and effective.

4.7 Safeguards and security

Commonalities can be noticed between safeguards and security as they both share similar objectives and measures. Security aims to protect NPP from adversaries whose attempt is to steal NM, radioactive material, or other valuable goods (such as information, equipment, and components), to sabotage facility, or to commit other malicious acts which may influence facility operations. Safeguards aim to detect diversion of NM, facility misuse, and proliferation of equipment and information that could be used for weapon manufacture. Evident common objectives are associated with the prevention of theft (NM, equipment, components, and information). However, proliferation threats could be mainly considered to

progress outward from the facility; the intrinsic material barriers are the first ‘in-depth’ barrier and physical structures the last one (in case of NM).

Deterrence, detection, delay, and response are an analogy between safeguards and security. Safeguards make use of deterrence since effective and efficient SA is to deter proliferators and is achieved by the risk of early detection. Delay is not as an obvious common measure as other ones, however, containment and use of sealing systems may complicate and hinder attempts to gain access to NM.

An on-site response could aim to mitigate failures in SA such as significant MUF and involve immediate actions to clarify deviations or to correct any other failures. The response may also be initiated by SRA that has enforcement rights to non-compliance and uses measures such as warning letters, fines, or penalties, suspension or revocation licenses, removal of material, and criminal prosecution (IAEA 2018c, 28). IAEA may respond to non-compliance by calling for remedial actions and provide formal sanctions if corrections are not finished in a time that includes suspension of assistance, call for the return of materials and equipment and alerting Member States which may react to violation (e.g., refusal to provide material and equipment) (IAEA 1983, 23-24).

One synergy effect between safeguards and security could be detection and deterrence of insider threats as IAEA as an external observer could notice suspicious acts (such as protracted theft or sabotage attempt), that may otherwise remain unnoticed by the operator. IAEA response could also be viewed in the context of security as providing detection information to the operator on suspicious activities within the facility or deviations in NMA, that may initiate the response of security personnel, if necessary. It is worth noting that the use of RMSs and cooperation could facilitate this synergy effect.

An obvious contradiction also exists that is related to the objective of security to block intruders’ access to the NPP. To reach safeguards objectives, IAEA must be provided access to locations within the facility (such as vital areas). On-site verification activities may disrupt security operations as they tie resources since from a security point of view IAEA inspectors could be considered as threats until all necessary security procedures are finished (such as identification and equipment check). To successfully achieve safeguards and security objectives it is essential to consider these operations and strive to implement them in harmony.

4.8 Safeguards by design

Safeguards by design (SBD) is a concept which aims to have safeguards requirements in the facility's design process starting from the initial conceptual design through all phases of the facility life cycle including design modifications (figure 32). The SBD process has two essential objectives, to reduce costs of safeguards implementation by avoiding costly and time-consuming retrofits or redesigns, and to provide more efficient and effective SA at facilities. The benefits are the reduction of on-site activities needed for IAEA verification, which also decreases both the intrusiveness during operation and coordination activities that SRA is responsible for. (IAEA 2014b, 1-2; IAEA 2013c 1-4).

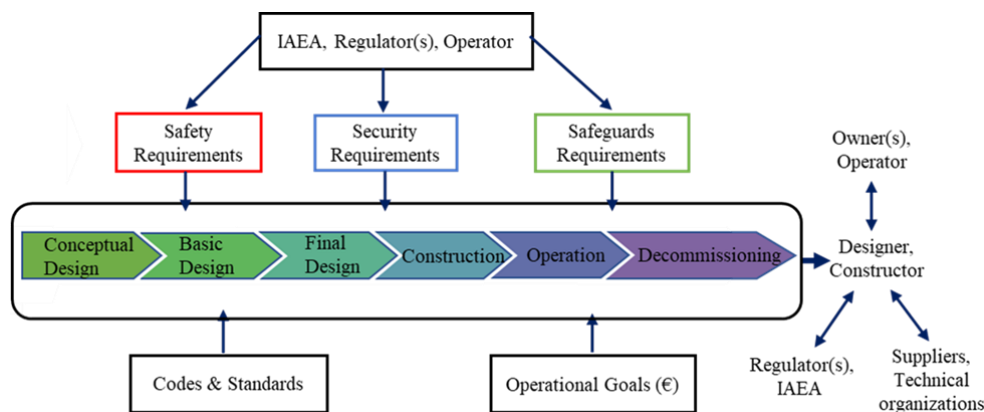


Figure 32. The design considerations through all life cycle phases of an NPP, and associated stakeholders. SBD refers to integrating safeguards requirements as part of NPP project starting from conceptual design phase (modified from IAEA 2013c, 2; IAEA 2014b, 12).

The SBD process needs to ensure that IAEA has sufficient knowledge regarding the design, operation, conditions, and any constraints of the facility or its process. Therefore, the development of an optimized SA is facilitated by a transparent interaction between stakeholders (constant dialogue and open information sharing). A common understanding of safeguards systems, goals, and objectives should be sought such that all stakeholders have contributed to the development of safeguards measures. (IAEA 2013c 1-8; IAEA 2014b, 1-2).

It is worth noting that SBD is an important concept as it supports the integrated design of safety, security, and safeguard. Currently, it is a requirement for NPP design that ‘the 3S’ shall be implemented in an integrated manner without compromises as it is stated in requirement 8 of SRS-1/2:

“Safety measures, nuclear security measures and arrangements for the State system of accounting for, and control of, nuclear material for a NPP shall be designed and implemented in an integrated manner so that they do not compromise one another.” (IAEA 2016a, 16)

Safeguardability is an essential issue for the SBD process. The facility and its technical features are assessed using facility safeguardability analysis (FSA) to support IAEA equipment installations and verification activities. PR assessment methods such as INPRO and GIF are related to SBD as both provide information for FSA. PR assessment methods are means for identifying and optimizing proliferation barriers and design features such that safeguards goals can be met with minimal interferences between other considerations (safety, security, and operations). For example, an intrinsic proliferation barrier such as a high radiation field may be effective for PR from a security point of view but complicates IAEA on-site activities and facility operations. It is beneficial to start such analyses early in facility design to support the development of SA. (IAEA 2014d, 6-8, 13-15). The facility safeguards design envelope can be summarized by combining all the relevant concepts introduced so far (figure 33).

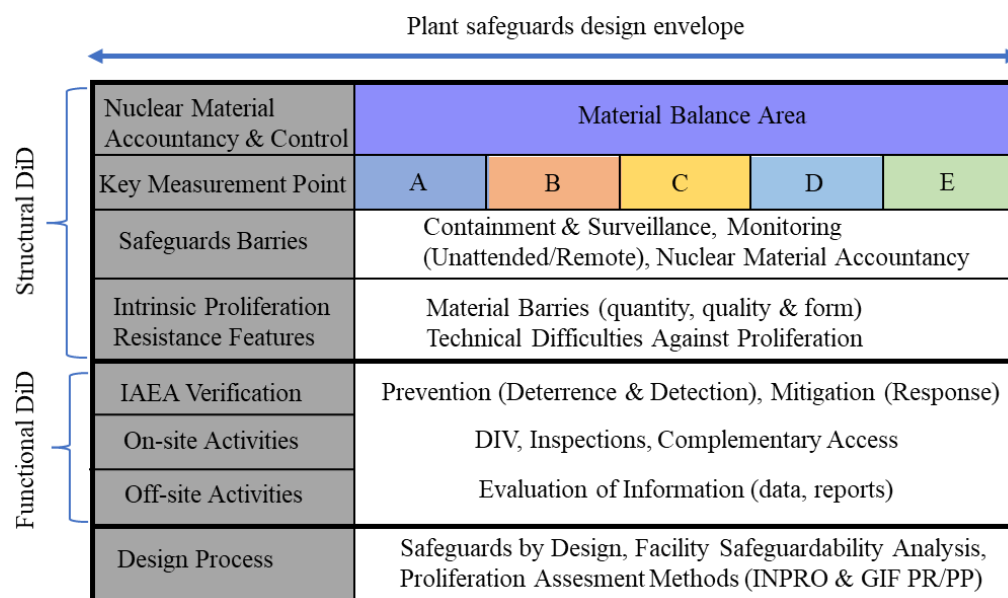


Figure 33. Plant safeguards design envelope.

5. Overall safety framework development

Hyvärinen et al. have developed an Overall safety conceptual framework (ORSAC), which aims to integrate safety, security, and safeguards into a single tool for the evaluation of '3S'. ORSAC is build based on DiD concept of safety and it enables placement of SSCs such as SFs, support systems and I&C systems on different defence levels. This kind of placement of SSCs provides means to evaluate dependencies between DiD levels regard to different systems in the design of NPP. Many other design requirements could also be placed at levels, and this is demonstrated for safety classes and reliability criteria in their study. In addition, it is discussed that hazards could be possible to lay on framework via event frequencies. Furthermore, ORSAC provides initial efforts to extend its use for both security and safeguards. (Hyvärinen et al. 2016, 70-71).

The first aim of this thesis has been to contribute to ORSAC framework development by considering security and safeguard related issues further in the theory part. Security can be integrated into the framework with safety if a similar DiD concept with progressive levels is applied. Such threat levels and corresponding security zones can be connected to the defences levels of safety by using acceptance criteria, so harmonized radiological doses for both plant events and threat levels. Security design aspects such as access controls, PPSs, and security response organizations could be placed on threat levels and their boundaries. In addition, cyber security is added into ORSAC by the inclusion of computer security levels and zones. Thus, computer systems can be also placed on such levels.

The integration of Safeguards into the ORSAC is not that evident as radiological doses cannot be used. Although commonalities with both security and safety can be identified, safeguards and security have more in common. The DiD concept of safeguards could be considered with progressive levels if a similar approach based on events is applied than it is for threat levels. The measure of severity for such proliferation events should correspond to proliferation risk and relevance of safeguards measures, thus amounts of SQs of material could be used. Therefore, 'proliferation levels' each of which corresponds to a quantity of NM lost (mistake or diversion) or produced (misuse) have been proposed. Safeguard design aspects such as barriers and on-site verification activities could be placed on these levels The developed ORSAC with such modifications is introduced in figure 34.

		10 ⁰ 1/a	10 ⁻² 1/a	10 ⁻³ 1/a	10 ⁻⁴ 1/a	10 ⁻⁵ 1/a	5·10 ⁻⁷ 1/a	
Safety	DiD Level	Level 1	Level 2	Level 3		Level 4		
	Plant State	NO	AOO	DBA Class I	Class II	DEC A (CCF)	Core melt accident	
	Subcriticality							
	Heat removal							
	Containment							
	Support systems							
	I&C systems							
	Hazards							
							DEC B (Multi-F), DEC C (Rare event)	
	Acceptance criteria	0,1 mSv/a	0,1 mSv/event	1 mSv	5 mSv	20 mSv	100 TBq (Cs-137)	
Security	Threat Level	Level 1	Level 2	Level 3		Level 4	Level 5	
	Security Zone	Restricted area	Plant area	Protected area		Vital area	Vital area	
	Access control							
	Physical protection systems							
	Security response organizations							
	Security Level	Level 5	Level 4	Level 3		Level 2	Level 1	
	Computer Zone	E	D	C		B	A	
	Computer systems							
Safeguards	"Proliferation Level"	Level 1	Level 2	Level 3		Level 4	Level 5	
	Quantity of nuclear material	None	< 1 SQ	1 SQ	x·SQ	SQ amount for Nuclear Weapon		
	Barriers (material, NMA, safeguards, physical)							
	On-site verification (DIV, inspections, CA)							
	Proliferation event	None	MUF error	Diversion sufficient for Nuclear Explosive Device		Misuse	Diversion sufficient for Nuclear Weapon	

Figure 34. The proposed Safety-Security-Safeguards ORSAC.

6. Case study SMRs in concern

The second aim of this thesis has been to provide insights on Safety, Security, and Safeguards (the '3S') in the context of SMRs. To achieve this, case study of four different designs has been used as methodology. Only LWRs have been considered. Designs have been chosen from four different categories: 1) SMR for multi-module plant (NuScale), 2) SMR for district heating (RUTA-70), 3) conventional NPP- like SMR (BWRX-300) and 4) SMR for floating nuclear power plant (FNPP) (KLT-40S). Open-source references, design information and secondary sources, have been reviewed for the study. The focus is to evaluate designs with respect to current requirements (Safety and Security) and safeguardability (Safeguards). The emphasis is on technical design; thus, the evaluation of organizational aspects is given less attention.

6.1 NuScale

The NuScale Power Module (NPM) is an integral pressurized water reactor (PWR) type SMR design for electricity production and process heat applications (figure 35). It is developed by the U.S company NuScale, LLC. The plant design enables scalable production, power can be increased in 60 MWe (single module) increments up to 720 MWe (twelve modules). The modules operate independently in a multi-module configuration and are managed from a single control room. The NuScale plant design with a twelve-module configuration has received design approval from U.S NRC in 2020. (IAEA 2020, 89; NuScale 2021). The main design parameters of NuScale are shown in table 2.

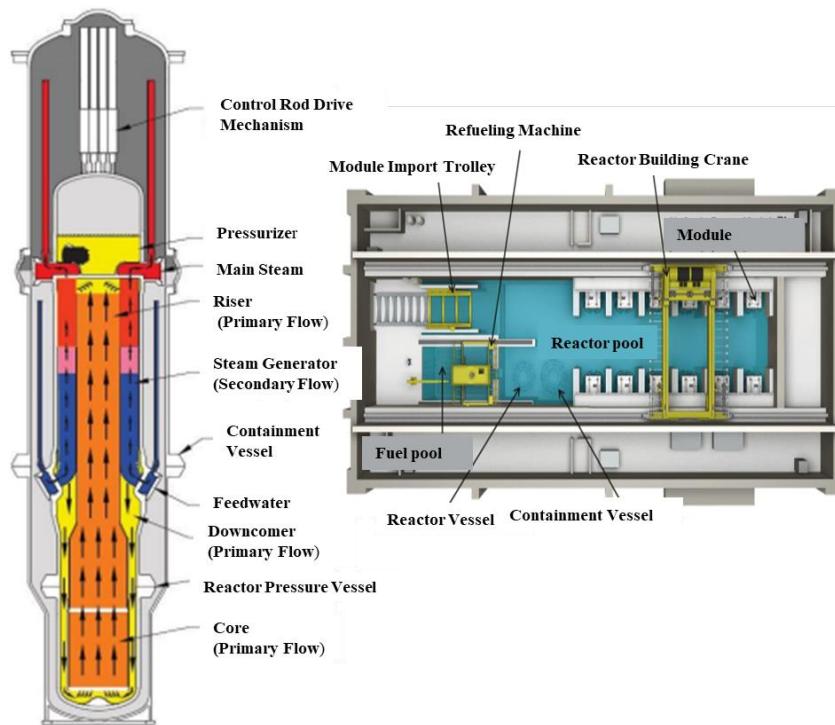


Figure 35. NuScale Power Module and the reactor hall layout (modified from NuScale 2020a, 11, 15).

Table 2. The main design parameters of NuScale (IAEA 2020, 89).

Parameter	Value
Coolant/moderator	Light water/Light water
Thermal/electrical power (MWth/MWe)	200/60 (gross)
Primary pressure (MPa)	13,8
Secondary pressure (MPa)	4,3
Core inlet/outlet temperature (°C)	265/321
Primary circulation	Natural circulation
Fuel type/assembly array	UO ₂ pellets/ 17x17 square
RPV height/diameter (m)	17,7/2,7
Number of FAs	37
Fuel enrichment	< 4,95 m%
Refueling cycle (months)	24
Average discharge burnup	> 30 MWd/kgU

6.2 RUTA-70

RUTA-70 is an integral pool-type LWR SMR design, that is to be used as a nuclear heating plant with thermal power of 70 MWth (figure 36). It is developed by the Russian NIKIET for multiple application areas such as district heating, seawater desalination, and radioisotope production for industrial and medical purposes. However, the primary aim has been the provision of district heating in isolated areas. The design is still in a conceptual phase. (IAEA 2020, 77). The main design parameters of RUTA-70 are shown in table 3.

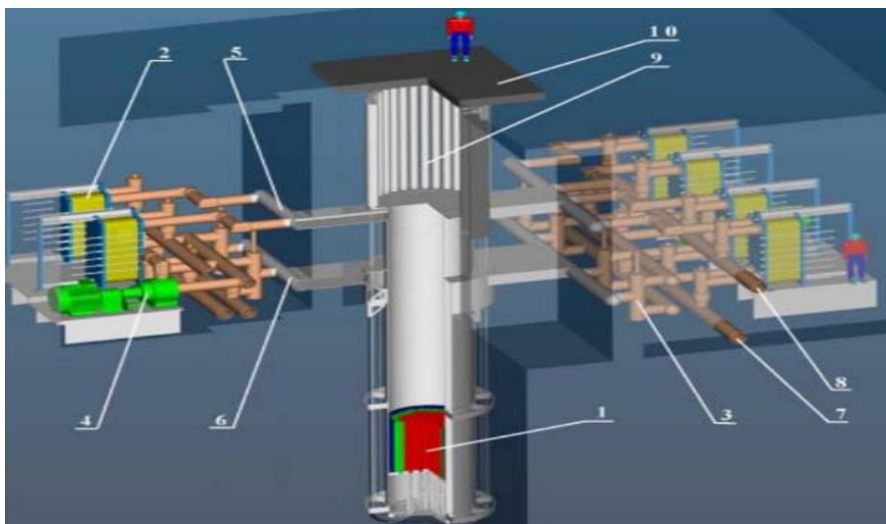


Figure 36. RUTA-70: 1) core, 2) primary heat exchanger (HX), 3) check valve, 4) pump, 5) distributing header, 6) collecting header, 7) secondary circuit supply line, 8) secondary circuit discharge line, 9) Control Rod Drive System (CRDS), 10) upper plate (Cherepnin et al 2007, 7).

Table 3. The main design parameters of RUTA-70 (IAEA 2020, 77).

Parameter	Value
Coolant/moderator	Light water/Light water
Thermal power (MWth)	70
Operating pressure (MPa)	Atmospheric pressure at reactor pool water surface
Core inlet/outlet temperature (°C)	75/102
Primary circulation	Natural circulation in 0 – 30 % of power Forced circulation in 30 – 100 % of power
Fuel type/assembly array	UO ₂ or Cermet (60% UO ₂ and 40% Al alloy) / hexagonal
RPV height/diameter (m)	17,25/3,2
Number of FAs	91
Fuel enrichment	3,0 m% (UO ₂), 4,2 m% (Cermet)
Refueling cycle (months)	36
Average discharge burnup	25 – 30 MWd/kgU

6.3 BWRX-300

BWRX-300 is the 10th generation boiling water reactor (BWR) developed by the US-Japanese GE-Hitachi Nuclear Energy (figure 37). It is 300 MWe reactor, which is an evolutionary design of NRC-licensed ESBWR. Such SMR is to be used in baseload electricity generation and load following within a power range of 50% - 100 %. In addition, the reactor is suitable for district heating and providing process heat. The design is under NRC regulatory review. (IAEA 2020, 93; GE-Hitachi 2021a). The main design parameters are shown in table 4.

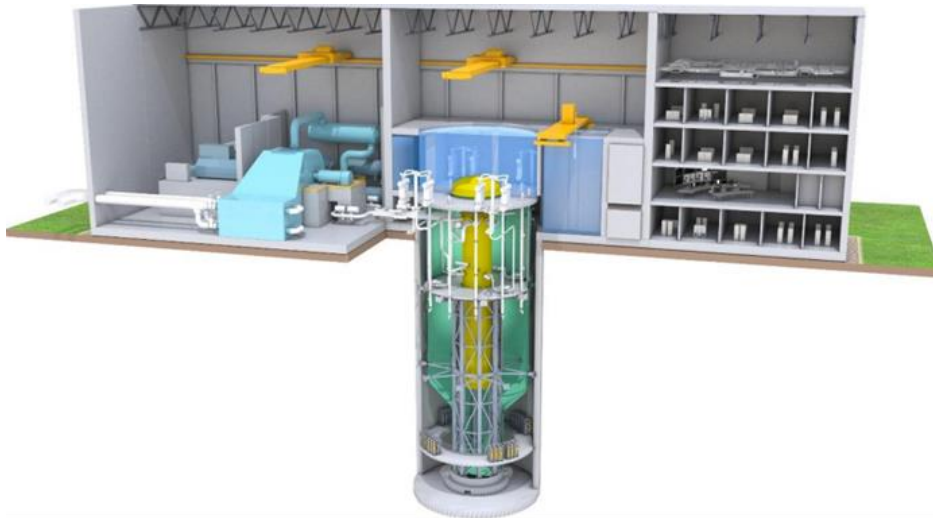


Figure 37. BWRX-300 in the reactor building, partially underground. Turbine building on the left. (GE-Hitachi 2019, 3).

Table 4. The main design parameters of BWRX-300 (IAEA 2020, 93).

Parameter	Value
Coolant/moderator	Light water/Light water
Thermal/electrical power (MWth/MWe)	870/270 – 290
Operating pressure (MPa)	7,2
Core inlet/outlet temperature (°C)	270/287
Primary circulation	Natural circulation
Fuel type/assembly array	UO ₂ / 10x10 array
RPV height/diameter (m)	26/4
Number of FAs	240
Fuel enrichment	3,40 (avg)/4,95 (max)
Refueling cycle (months)	12-24
Average discharge burnup	49,5 MWd/kgU

6.4 KLT-40S (Akademik Lomonosov)

The KLT-40S is a PWR, an advanced design of the KLT-40 that has provided long-term operation of nuclear icebreakers (figure 38). It is an SMR for a FNPP developed by the Russian JSC OKBM (figure 39). The plant unit has two reactors, 35 MWe per module. The FNPP can be manufactured, assembled, tested in shipyards, and then be delivered to the site for operation. The design is to be used for cogeneration and seawater desalination in isolated areas. The first FNPP (Akademik Lomonosov) has been in commercial operation since 2020. (IAEA 2020, 111). The main design parameters are shown in table 5.



Figure 38. KLT-40S: 1) isolation valves, 2) steam lines, 3) CRDS, 4) primary coolant pump, 5) steam generator (SG), 6) reactor, 7) pressurizer, 8) hydro accumulator (JSC OKBM 2021, 15).

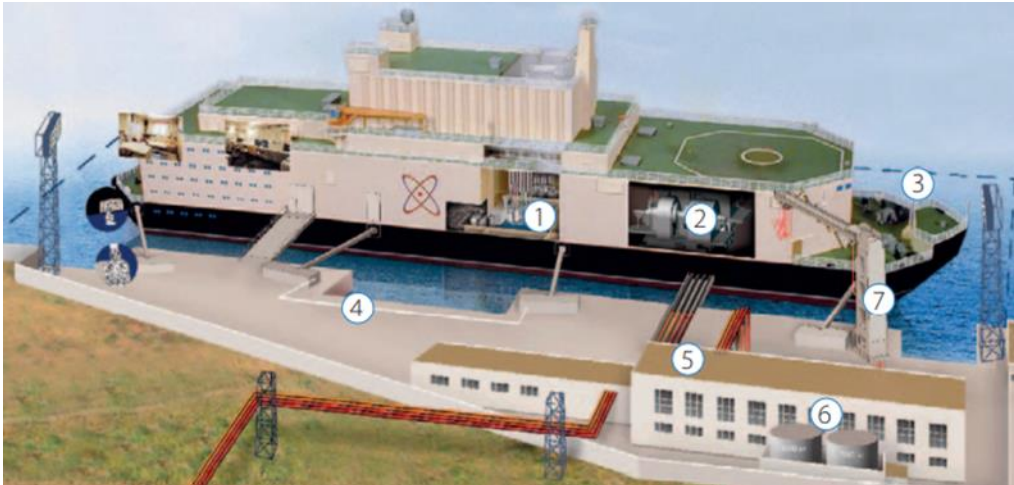


Figure 39. The FNPP: 1) reactor plants (RPs), 2) steam-turbine plants, 3) underwater trench, 4) water side structures, 5) heat point, 6) hot water tanks, 7) switch gear and electricity transmission/distribution devices (JSC OKBM 2021, 12).

Table 5. The main design parameters of KLT-40S (IAEA 2020, 111).

Parameter	Value
Coolant/moderator	Light water/Light water
Thermal/electrical power (MWth/MWe)	150/35
Primary pressure (MPa)	12,7
Core inlet/outlet temperature (°C)	280/316
Primary circulation	Forced circulation
Fuel type	UO ₂ in silumin matrix (Cermet)
RPV height/diameter (m)	4,8/2,0
Number of FAs	121
Fuel enrichment	14,1 (avg)/18,6 (max)
Refueling cycle (months)	30 – 36
Average discharge burnup	45,4 MWd/kgU

7. Safety results

This chapter presents results from the collection of safety information. The implementation of DiD has been evaluated for each SMR design. This has been done by placing Operational/Safety Systems performing fundamental SFs on ORSAC figure. The system descriptions have been used to justify placements at certain levels. However, such layout also reflects the author's considerations due to lack of information. Thus, it should be noted that all reasonings may not represent the view of the designer completely. The system descriptions and considerations on their level placements are included as appendices (3-6.) In addition, inherent and design features have been surveyed, and tentative evaluations of STUK's YVL B.1 requirements were done for all SMRs. The YVL B.1 evaluations only consider the implementation of DiD and Safety System requirements. It should be noted that acceptance considerations are partially indicative.

7.1 NuScale

Figure 40 presents systems of NuScale, performing fundamental SFs, on ORSAC. As it can be noticed, NuScale utilizes same non-safety related systems in first two defence levels for both NO and AOOs. However, at least some of these are operated differently when performing fundamental SFs. Decay Heat Removal System (DHRS) is Safety System, which is credited in first three levels (NO, AOOs and DBAs). This risks the independency of level 3 from level 2 and 1, that may introduce further challenges for level 4 as DECAs, if system failures were to occur in these two levels. Furthermore, DHRS is operated via SGs, that adds some functional dependency between systems performing non-safety related and safety related functions in multiple defence levels.

		10^0 1/a	10^{-2} 1/a	10^{-4} 1/a	10^{-5} 1/a	$5 \cdot 10^{-7}$ 1/a
		Operational States		Accident Conditions		
		Level 1	Level 2	Level 3	Level 4	
NuScale		Normal Operation	Anticipated Operational Occurrences	Design Basis Accidents	Design Extension Conditions	
					Without significant fuel damage	With core melting
Subcriticality	CVCS	CVCS	CVCS			
	CRA (Drive)	CRA (Drive/Drop)	CRA (Drop)			"N/A"
	Gadolinia					
	Soluble Boron					
Heat removal	SG → Condenser → CWS → Atmosphere	SG → Condenser → CWS → Atmosphere				
	RCCWS → SCWS → Atmosphere	RCCWS → SCWS → Atmosphere				
	SG → DHRS → Pool	SG → DHRS → Pool	SG → DHRS → Pool			
		ECCS → CNV → Pool	ECCS → CNV → Pool	ECCS → CNV → Pool		
Confinement				RPV → CNV → Pool	RPV → CNV → Pool	RPV → CNV → Pool
	Closed systems (RCPB)	Closed systems (RCPB)		RPV/CNV	RPV/CNV	
	RSVs → CNV	RSVs → CNV				
		CIVs	CIVs	CIVs	CIVs	

Figure 40. NuScale’s systems placed on DiD levels. The purple colour indicates shared systems between modules.

Other Safety Systems for heat removal are credited in both DBAs and DEC. Emergency Core Cooling System (ECCS) is also utilized during AOOs, which could be another dependency between Operational States and Accidents. CRDS is credited for subcriticality function in multiple levels (Operational States and DBAs), however different actuators are used to reliably perform criticality control functions. Confinement systems/subsystems have clear division between Operational States and ACs, though Containment Isolation Valves (CIVs) could also be credited in AOOs. Overall, despite of few dependencies between Operational States and ACs, NuScale seems to utilize DiD principle appropriately in its safety design.

NuScale includes only passive Safety Systems, which function by use of natural phenomena such as boiling and condensation, conduction, natural circulation, and gravity. The passive nature of Safety Systems could enhance reliability, since no external power supply, logics or operator actions are required to perform SFs. Furthermore, NuScale’s passive systems seem to have few components and are mainly based on structures such as reactor pressure

vessel (RPV), containment vessel (CNV), piping and water pools. This could also enhance reliability of safety design, due to fewer SSCs potentially capable to fail the system. In addition, there are quite few Safety Systems in total, this simplicity could enhance safety due to decreased number of connections between SSCs in the first place. Passive safety seems to provide control of DBAs and contribute to retain controlled state of plant.

Especially, large water inventory and steady heat removal from CNV to water pool is a great example of design provision to withstand DEC and mitigate consequences if severe accident would occur. In addition, the safety design aims to maintain the integrity of CNV during DEC by such a reliable and passive heat removal solution. Furthermore, NuScale design allows utilizing additional Safety Provisions such as make-up of pool water to ensure reliable transition to controlled state, if deemed necessary. NuScale follows in-vessel retention strategy for mitigation of severe accidents. Passive heat removal systems seem to contribute to this objective. However, from the system descriptions, it is evident, that NuScale aims to have severe accidents practically excluded, which could be justified due to low CDF of $4,1 \cdot 10^{-11}$ (internal events for multi modules) (NuScale 2020b, 126).

Table 6 presents safety features incorporated in NuScale design. In principle, reactor design includes inherent features (negative reactivity coefficients, large water inventory, small core inventory and power density), that support achieving better safety and reduce potential harmful consequences if they were to occur. One notable feature is inclusion of large water inventory, that provides sufficient timeframe for operator response and ensures safe transition to controlled or safe state. This feature is highly utilized in Safety Systems and contributes to DiD, especially for level 4, which can be already noticed from previous discussion. Another feature worth to highlight is the below-grade design of the reactor pool, that inherently enhances protection from external impacts.

In addition, NuScale takes benefit of many design features, which aim to prevent SSC failures, that could cause initiating events and subsequent accidents. This is mainly done by simplifying reactor design with compact Nuclear Steam Supply System (NSSS) and by utilization of passive Safety Systems. These design features provide protection against DBAs such as LOCAs. Overall, safety features seem to strengthen the principle of DiD in multiple defence levels and enhance safety of NuScale.

Table 6. Safety features included in NuScale design.

Name	Description	Safety benefit
Negative reactivity coefficients	Fuel temperature, coolant (moderator) temperature, moderator density (void) reactivity coefficients are negative.	Stabilizing reactivity feedbacks for reactor power.
Small core inventory	Module has 37 FAs and initial load of 811 kg U, that leads to small source term and less radioactivity.	Reduced potential radiological release in accidents. Less requirements for decay heat removal.
Low core power density	Module has core power density $47 \cdot 10^3 \text{ kW/m}^3$ (NuScale 2020a, 5)	Provides greater thermal hydraulic stability and enhances in-vessel retention.
Large water inventory	Pool water provides passive heat removal from CNV via conduction and enough water to remove heat from reactor core (s) by water boiling and evaporation. High thermal inertia allows slow progression of emergency conditions. Allows absorption of decay heat from a single module for over 30 days.	The high heat accumulating capability of water ensures reliable heat transfer from the FAs during transient and emergency conditions. Slow boiling and non-intensive evaporation inherently keep the fuel temperature in a safe range.
Natural circulation of primary coolant	Reactor core coolant flow by natural driving force due to temperature difference induced density changes and elevation difference between heat source and sink.	Eliminates the need for MCPs and associated failures. Allows passive reactor cooling without operator actions or power supply.
Below-grade layout	Reactor pool and modules situated below-grade. External impacts to critical SSCs are absorbed to surface area and damped. Low facility profile reduces vulnerabilities to malicious acts (external or internal).	Provides protection against external impacts (natural phenomena or terrorism). Additionally, provides protection against security threats due to harder accessibility of sabotage targets.
Compact NSSS	Integral NSSS that combines the reactor core, SGs, and pressurizer within the RPV.	Provides protection against LBLOCA scenarios due to elimination of large external piping
RPV inside CNV	Coolant lost from RPV stays within containment and is returned to RPV by natural circulation.	Protection against LOCA scenarios. Reduces the need for make-up water during DBAs.
Passive safety	SFs are maintained by passive means via natural phenomena such as conduction, convection, and natural circulation.	A safe state for the plant can be achieved and maintained entirely with passive Safety Systems without reliance on electrical power or operator actions.

Appendix 7 contains tentative evaluation of STUK YVL.B.1 requirements for NuScale Safety System design. It appears, that NuScale is likely to fulfil most of these requirements. Especially, passive Safety Systems and inherent features seem to contribute well to fulfil requirements pertaining to decay heat removal in DECAs. However, the design doesn't include diverse system for subcriticality control in accidents. Furthermore, RTS design

seems to only satisfy single-failure criterion. Although CRDS is capable to actuate scram passively and may be reliable system alone to ensure sufficient subcriticality, more information needs to be reviewed to make better evaluation for this system and its performance. Especially, it could be worthwhile to further research I&C systems and survey potential functional dependencies between SSCs in defence levels.

7.2 RUTA-70

Figure 41 presents systems of RUTA-70, performing fundamental SFs, placed on ORSAC.

	Operational States		Accident Conditions		
	Level 1	Level 2	Level 3	Level 4	
	Normal Operation	Anticipated Operational Occurrences	Design Basis Accidents	Design Extension Conditions	
				Without significant fuel damage	With core melting
RUTA-70					
Subcriticality	CRA (Drive) Gadolinia	CRA (Drive/Hydrodynamic insertion)	CRA (Hydrodynamic insertion/Drop)	CRA (Drop)	"N/A"
Heat removal	1-2 HX → 2-3 HX → DHN → Consumers 1-2 HX → SWSS → Atmosphere	1-2 HX → 2-3 HX → DHN → Consumers 1-2 HX → SWSS → Atmosphere 1-2 HX → ASEC → Atmosphere	1-2 HX → ASEC → Atmosphere RV → Pool → Concrete Vessel → Ground EMWS	RV → Pool → Concrete Vessel → Ground RV → Pool → Passive Condensers EMWS	RV → Pool → Concrete Vessel → Ground EMWS
Confinement	Closed systems (RCS) Closed systems (ICC)	Closed systems (RCS) Closed systems (ICC)	Concrete Vessel Containment Structure RPASOPS	Concrete Vessel Containment Structure RPASOPS	

Figure 41. RUTA-70's systems placed on DiD levels.

From figure 41, it is evident that RUTA-70 credits same two systems for heat removal function in first two defence levels (NO and AOOs). These systems provide diverse means for heat removal (normal heat removal and shutdown cooling) in Operational States. However, Passively Actuated Air Emergency Cooling System (ASEC), instead of solely

designed to control DBAs, is also credited for decay heat removal in AOOs. This dependency could risk the level 3 if system failures from level 2 propagate to further challenges in level 4 as DECAs. It also seems that all decay heat removal systems are somewhat connected to 1-2 HXs to transfer heat from reactor pool water to secondary circuit coolant. This could introduce functional dependencies between systems in Operational States and ACs. However, the design includes two cooling circuits, each having three HXs, that could provide enough reliability to perform heat removal functions.

The passive heat removal from concrete vessel and use of passive condensers to retain pool water inventory are safety features designed for level 4 in DECAs. It is stated that Emergency Make-up Water System (EMWS) is provided for ACs to recover primary/secondary coolant inventories, though, there is no information available for this system. EMWS might be implemented as single system credited in multiple levels, for both DBAs and DECAs. However, it could be reasonable to have separate make-up system for water pool inventory to provide better control of DECAs.

Furthermore, CRDS is credited in all levels for subcriticality, however it uses different actuators for criticality control related functions and for two diverse emergency shutdown systems. The gravity insertion of Control Rod Assemblies (CRAs) could be thought as design provision for DECAs. The confinement systems/subsystems seem to have a clear division between Operational States and ACs. There is little information about containment design available and it is unclear whether containment structure is included in current design concept. Nevertheless, steel-lined concrete pool with leak-tight protective slab is at least one structure to prevent potential radioactive releases. The containment design would likely incorporate CIVs also. All in all, despite dependencies mentioned, RUTA-70's Safety Systems are designed according to principle of DiD.

Despite of EMWS, all Safety Systems included in RUTA-70 design utilize passive, natural force driven mechanisms to perform SFs. This could enhance, its reliability to control DBAs. There are few Safety Systems in total incorporated in the design, due to inherently safe pool-type approach. Few SSCs utilized in implementation of safety and simplicity of the reactor is likely to benefit systems' reliability to perform their functions. The Safety System design incorporates features, that enhance prevention of DECAs and mitigation of their consequences. This is evident from those systems placed on defence level 4 in figure 41.

RUTA-70 also follows in-vessel retention strategy to mitigate consequences of severe accidents. However, the design aims to have core melt accidents ‘practically excluded’.

Tables 7 and 8 introduce principal safety features of RUTA-70 design. It is evident, that RUTA-70 incorporates inherent features (negative reactivity coefficients, large water inventory, non-pressurized primary circuit, small core inventory and power density), which highly benefit safety of this reactor concept.

Table 7. Safety features included in RUTA-70 design (part 1).

Feature	Description	Safety benefit
Negative reactivity coefficients	Fuel temperature, coolant (moderator) temperature, moderator density (void) reactivity coefficients are negative.	Stabilizing reactivity feedbacks for reactor power. Core remains in the self-control mode irrespective of the control rod positions and slow shutdown (subcriticality) can be achieved.
Small core inventory	Core has 91 FAs and initial load of 4165 kg U, that leads to small source term and less radioactivity.	Reduced potential radiological release in accidents. Less requirements for decay heat removal.
Low core power density	Core power density around $30\text{--}40 \cdot 10^3$ kW/m ³ (Cherepnin et al 2007).	Provides greater thermal hydraulic stability and enhances in-vessel retention.
No pressurization of primary circuit	Pool-type reactor with atmospheric pressure above water level. Pressure free state of primary coolant.	Provides protection against consequences of instantaneous LOCA events as coolant loss due to depressurization doesn't occur rapidly.
Large water inventory	Water inventory in reactor tank (250 m ³) and pool (450 m ³), provides enough water for core to remain covered. High thermal inertia leads to slow changing of coolant parameters.	The high heat accumulating capability of water in the reactor pool ensures reliable heat transfer from the FAs during transient and emergency conditions. Slow boiling and non-intensive evaporation of the coolant inherently keep the fuel temperature in a safe range. Gives an extended period during which automatic systems or plant operators can re-establish reactor inventory control.
Natural circulation of primary coolant	Reactor core coolant flow by natural driving force (below 30% of nominal power).	Allows passive reactor cooling during shutdown and emergency conditions without power supply or operator actions.
High thermal conductivity of the Cermet fuel	Effective heat conduction from fuel pellet.	Fuel temperature and stored energy are relatively low.

The non-pressurized primary circuit of reactor pool prevents events involving rapid coolant losses from the reactor. Furthermore, due to low pressure of primary circuit, ingress of radioactive water to secondary circuit, that is at higher pressure, is not possible. It is also

worth to mention, that negative reactivity coefficients alone can self-regulate the reactor in a safe state if CRDS would fail (Kozmenkov et al. 2012, 256).

Table 8. Safety features included in RUTA-70 design (part 2).

Feature	Description	Safety benefit
Passive heat conduction to ground	Accumulated decay heat in reactor pool water is removed passively by heat conduction from external surfaces to ground.	If all controlled trains of heat removal are lost, heat losses via the external surface of the reactor pool to the surrounding environment (ground) are considered as an additional safety train.
Below-grade layout	Reactor pool with core situated below-grade. External impacts to critical SSCs are absorbed to surface area and damped. Low facility profile reduces vulnerabilities to malicious acts (external or internal).	Provides protection against external impacts (natural phenomena or terrorism). Additionally, provides protection against security threats due to harder accessibility of sabotage targets.
Pressure differences between cooling circuits	Atmospheric pressure in primary circuit and higher secondary circuit pressure localizes primary coolant water in the reactor pool.	If the 1/2 HX is damaged and the physical barrier fails, the radioactive material will be kept in the primary circuit.
Passive safety	SFs are maintained by passive means via natural phenomena such as conduction, convection, and natural circulation.	A safe state for the plant can be achieved and maintained with passive Safety Systems without reliance on electrical power or operator actions.

The below-grade layout of reactor pool provides inherent protection against external impacts. In addition, high thermal conductivity of Cermet fuel enhances heat transfer from core and heat rejection from external surfaces of concrete pool could be seen as inherent, passive means for decay heat removal. Simple design and utilization of few safe systems with passive principles are design features, that contribute to the safety. All in all, safety features seem to strengthen DiD in multiple levels and enhance RUTA-70's safety.

Appendix 8 contains tentative evaluation of STUK YVL.B.1 requirements for RUTA-70 Safety System design. It appears, that RUTA-70 is likely to fulfil most of these requirements. Water-pool type design like research reactors takes benefit of many inherent safety features, which seems to be main contributor for RUTA-70 to have potential in satisfying requirements. This is prominent for decay heat removal requirements. However, the design doesn't include diverse reactor shutdown system apart from CRDS. Furthermore, there is little information available about Reactor Protection System (RPS) and associated I&C

systems. Still, RUTA-70 incorporates two diverse reactor scram systems, both of which can be actuated passively without operator actions if power supply is lost. Such design provision is promising for system reliability. Small thermal power and self-regulating capability of reactor core are inherent features, that provide additional support for ensuring sufficient subcriticality. RUTA-70 is still in conceptual design and more information will be available in future. It could be worthwhile to review information pertaining to containment/confinement design and I&C systems.

7.3 BWRX-300

Figure 42 presents BWRX-300's systems, performing SFs, placed on ORSAC.

	10^0 1/a	10^{-2} 1/a	10^{-4} 1/a	10^{-5} 1/a	$5 \cdot 10^{-7}$ 1/a
	Operational States		Accident Conditions		
	Level 1	Level 2	Level 3	Level 4	
BWRX-300	Normal Operation	Anticipated Operational Occurrences	Design Basis Accidents	Design Extension Conditions	
				Without significant fuel damage	With core melting
Subcriticality	CRA (Drive) FLCS Gadolinia	CRA (Drive/Hydraulic insertion)	CRA (Drive/Hydraulic insertion)	CRA (Drive/Hydraulic insertion (ARI)) SLC	"N/A"
Heat removal	Condenser → CCWS → PSWS → Sea/Atmosphere SDC → CCWS → PSWS → Sea/Atmosphere	Condenser → CCWS → PSWS → Sea/Atmosphere SDC → CCWS → PSWS → Sea/Atmosphere	SDC → CCWS → PSWS → Sea/Atmosphere	AIWAS PCCS → Reactor Pool → Atmosphere ICS → IC Pool → Atmosphere CRDSPs CFCs	AIWAS
Confinement	Closed systems (RCPB)	Closed systems (RCPB) RPIVs	RPV/PCV RPIVs CIVs CINS	RPV/PCV RPIVs CIVs CINS CFV	

Figure 42. BWRX-300's systems placed on DiD levels.

From figure 42, it can be noticed, that BWRX-300 credits two different systems for heat removal in first two defence levels (normal heat removal and shutdown cooling). In addition, there are other active systems performing containment cooling and RPV make-up for these levels. There is certain division between active systems used in Operational States and passive systems utilized in ACs. However, Shutdown Cooling System (SDC) is also credited in DBAs, which might risk the independence of level 3 from levels 1 and 2 if system failures in these levels propagate to further challenges in level 4 as DECs. Nevertheless, it seems that passive Isolation Condenser System (ICS) is the main system designed to control DBAs in level 3 and SDC is just thought to have additional contribution for decay heat removal as active system. Furthermore, ICS is also credited in level 2, which might risk the system's functions in ACs, if challenged significantly in AOOs. AC Independent Water Addition System (AIWAS) is credited in level 4, to recover water inventories of passive heat removal systems (ICS and Passive Containment Cooling System, PCCS) utilized in both levels 3 and 4.

CRDS is credited for subcriticality function in all four defence levels. However, the system performs different criticality control functions with separate actuators for control rod manoeuvring and fast reactor shutdown. Alternate Rod Insertion (ARI) is thought to be credited in DECs as alternative means for scram initiation. In addition, Standby Liquid Control System (SLC) as diverse system for reactor shutdown is provided in level 4 for DECs (Anticipated Transient Without Scram, ATWS). Thus, subcriticality function is systematically divided to separate defence levels. Confinement systems/subsystems seem to have a clear division between Operational States and ACs. However, Reactor Pressure Vessel Isolation Valves (RPIVs) are also credited in level 2 for AOOs to isolate RPV when ICS performs its decay heat removal function. Overall, it can be noticed that BWRX-300's Safety System design follows DiD principle very well.

BWRX-300's design relies on passive Safety Systems for heat removal function to control DBAs, to prevent DECs and mitigate their consequences. There are, just two systems (ICS and PCCS), which perform decay heat removal from the reactor and containment in ACs. The design involves few Safety Systems in total. From Safety System descriptions it is evident, that the design highly considers the capability to maintain the integrity of containment in DECs. This is achieved by isolation of the RPV and subsequent

pressurization control by decay heat removal via ICS. Furthermore, PCCS is utilized to protect containment from overpressure.

Passive Safety Systems for heat removal may enhance the reliability to perform necessary SFs. However, as the contradiction due to ICS piping external the Primary Containment Vessel (PCV) shows (appendix 5), these systems must be approved and licensed carefully. BWRX-300 systematically utilizes SSCs from other licensed BWRs of GE-Hitachi, that supports licensing process of systems. One of the systems already licensed is the CRDS, which has proven to be effective and reliable system due to vast operational experience from older BWRs. The hydraulic scram system of CRDS is also passive Safety System to some extent. Simplicity of design with few Safety Systems will likely benefit implementation of safety, but all restrictive circumstances that could risk fulfilment of SFs must be identified.

It seems that BWRX-300's safety design follows core melt prevention strategy. To achieve this, prolonged and reliable performance of passive heat removal systems must be ensured. The defence level 4 includes AIWAS to recover water pool inventories for ICS and PCCS during DEC. Unfortunately, there is no detailed information available for this system, but this is an evident design provision to maintain the performance of passive heat removal system to prevent core melt accidents. Furthermore, it stated that special 'diverse and flexible mitigation strategies' are planned to control severe accidents resulting from beyond design basis external events (GE-Hitachi 2019, 30). The objectives of these strategies are to prevent/ or mitigate fuel damage (reactor and spent fuel) and to maintain the integrity of the containment by providing additional water and power supply for important plant systems (GE-Hitachi 2019, 31). These can be seen as additional Safety Provisions in DEC. BWRX-300's CDF is expected to be lower than 10^{-7} (GE-Hitachi 2019, 8).

Tables 9 and 10 present inherent safety and design features of BWRX-300's design. From these results, it can be noticed, that BWRX-300 includes inherent features (negative reactivity coefficients, large water inventory, low core power density), which enhance its safety and support Safety System design. For example, large water inventory in RPV provides protection against LOCAs and decreases reliance on core make-up water. Another feature worth to highlight is partially below-grade layout of PCV, which protects reactor and associated SSCs from external impacts. This also provides additional decay heat removal passively by heat conduction from PCV external surfaces to surrounding ground.

Table 9. Safety features included BWRX-300 design (part 1).

Feature	Description	Safety benefit
Negative reactivity coefficients	Fuel temperature, coolant (moderator) temperature, moderator density (void) reactivity coefficients are negative.	Stabilizing reactivity feedbacks for reactor power.
Low core power density	Core power density $46 \cdot 10^3$ kW/m ³ (GE-Hitachi 2019, 6-7).	Provides greater thermal hydraulic stability and enhances in-vessel retention.
Large water inventory	Water inventory in RPV and tall chimney region provides enough water for core to remain covered. High thermal inertia leads to slow changing of coolant parameters.	Provides enough make up water in case of LOCAs transients such as feedwater flow interruption to cover the reactor core. Gives an extended period during which automatic systems or plant operators can re-establish reactor inventory control.
Natural circulation of coolant flow	Reactor core coolant flow by natural driving force due to temperature difference induced density changes and elevation difference between heat source and sink.	Eliminates the need for pumps and associated failures. Allows passive reactor cooling without operator actions or power supply.
Passive heat conduction to ground	Accumulated decay heat in RPV water is removed passively by heat conduction from PCV external surfaces to ground.	Heat losses via the external surfaces provides additional passive cooling.
Below-grade layout	Containment vessel situated mostly below-grade. External impacts to critical SSCs are absorbed to surface area and damped. Low facility profile reduces vulnerabilities to malicious acts (external or internal).	Provides protection against external impacts (natural phenomena or terrorism). Additionally, provides protection against security threats due to harder accessibility of sabotage targets.

In addition, BWRX-300 seem to include several design features, which aim to prevent those failures, that have been identified to be possible for conventional BWRs. One good example is utilization of RPIVs in all large diameter pipes, that provides prevention of LOCAs by isolation of RPV. Furthermore, RPIVs make it possible to exclude safety relief valves, which have been identified as most likely source for LOCAs in conventional BWRs. The design includes few nozzles with smaller diameters to prevent LOCAs. The containment protection is highly considered by exclusion of large bore high energy lines within containment. All these features in tables 9 and 10 evidently contribute to implementation of DiD in multiple defence levels and lead to better safety.

Table 10. Safety features included BWRX-300 design (part 2).

Reduced RPV pressurization rate	During RPV isolation event large RPV volume reduces pressurization rate. ICS provides decay heat removal to further mitigate pressurization.	Eliminates the need for Safety Relief Valves, which are most likely source of LOCA.
Exclusion of large diameter pipes outside containment	All fluid pipe systems > 50 mm diameter are equipped with double isolation valves which are integral the RPV. Reduced number and size of RPV nozzles.	Provides protection against LOCAs.
Exclusion of large bore high energy lines within containment	Sub compartments (volume below RPV, space between RPV and the biological shield, containment head area above the refueling bellows) do not include large bore high energy lines.	Line breaks both inside and outside the sub compartments do not create significant pressure differentials across sub compartment walls.
Passive Safety	SFs are maintained by passive means via natural phenomena such as conduction, convection, and natural circulation.	Safety Systems are designed such that no operator actions or power supply are needed to maintain safe, stable conditions following a DBA.

Appendix 9 contains tentative evaluation of STUK YVL.B.1 requirements for BWRX-300 Safety System design. It appears, that BWRX-300 has potential in fulfilling most of these requirements. This is understandable because the design is highly based on ESBWR that is already licensed by NRC. Especially, BWRX-300 seems to fulfil requirements pertaining to design of subcriticality control systems. Conventional Fine Motion Control Rod Drive (FMCRD) with two different initiators for hydraulic scram (RPS and ARI) is likely to have enhanced reliability. Furthermore, the design incorporates a diverse system for reactor shutdown (SLC). There is yet little information available for this system, but it could be somewhat similar than ESBWR design.

Passive systems may enhance reliability to maintain sufficient heat removal from core and containment. However, more review should be done for these systems so that their performance in multiple defence levels for both DBAs and DECAs is demonstrated. Some contradictions between containment/confinement and heat removal design have been identified by NRC. This points out, that it is also important to consider potential functional dependencies for passive Safety Systems. It could be worthwhile to further review that level 3b is not jeopardized if Safety Systems in level 3a are challenged.

7.4 KLT-40S (Akademik Lomonosov)

Figure 43 presents KLT-40S's systems performing SFs placed on ORSAC.

	10^0 1/a	10^{-2} 1/a	10^{-4} 1/a	10^{-5} 1/a	$5 \cdot 10^{-7}$ 1/a
	Operational States		Accident Conditions		
	Level 1	Level 2	Level 3	Level 4	
KLT-40S	Normal Operation	Anticipated Operational Occurrences	Design Basis Accidents	Design Extension Conditions	
				Without significant fuel damage	With core melting
Subcriticality	CRA (Drive)	CRA (Drive)	CRA (Spring insertion/Drop)	LAIS	"N/A"
	Gadolinia				
Heat removal	SG → Condenser → SCS → Sea	SG → Condenser → SCS → Sea	SG → ESCS → ESCS Tank → Atmosphere	SG → ESCS → ESCS Tank → Atmosphere	ERVCS
	SG → DH HX → DHN → Consumers	SG → DH HX → DHN → Consumers			
	PCS HX → SCS → Sea	PCS HX → SCS → Sea	PCS HX → SCS → Sea		
		SG → Auxiliary Condenser → SCS → Sea	SG → Auxiliary Condenser → SCS → Sea		
			ECPRS → ESCS Tank → Atmosphere	ECPRS → ESCS Tank → Atmosphere	
			Bubbling Tank	Bubbling Tank	
		LPSI (Pumps)	LPSI (Pumps)		
		HPSI (Pumps)	HPSI (Accumulators)		
Confinement	Closed systems (RCPB)	Closed systems (RCPB)	Containment Structure	Containment Structure	
			CWFS	CWFS	
		CIVs	CIVs	CIVs	
				Protective Enclosure	
				FVS	

Figure 43. KLT-40S's systems placed on DiD levels.

It can be noticed from figure 43, that KLT-40S seem to have a clear division between systems utilized in Operational States and Safety Systems credited in ACs. In addition, same systems are used in first defence levels for NO and AOOs. However, PCS is credited also for decay heat removal in level 3 for DBAs. This might risk the independency of level 3 to control DBAs if system failures from levels 1 and 2 propagate to further challenges. Still, PCS is one Safety System among others credited in DBAs for decay heat removal. It seems, that passive Emergency Shutdown Cooling System (ESCS) is the main system relied on to perform decay heat removal in DBAs and active PCS is thought to provide additional heat removal. Nevertheless, more design information is required to have precise conclusions.

Active heat removal by auxiliary condenser is credited for both AOOs and DBAs. There is little information available for this system and it is not clear, how it is credited in defence levels. This could be seen as system credited in both levels 2 and 3, but its significance for decay heat removal in DBAs is unclear. More information is required to review if there exist dependencies because of this system and whether it introduces risks for level 3. In addition, it seems that SGs are utilized in multiple defence levels, which may introduce functional dependency between systems. Also, ESCS pools are shared with ECPRS in ACs. More precise design information is required to assess significance of potential risks. Furthermore, figure 43 points out, that the design includes evident provisions for heat removal in level 4 to prevent and mitigate DECs.

The CRDS is credited in first three defence levels for subcriticality, though, separate subsystems are utilized with different actuators for normal reactivity control (control rod manoeuvring and normal shutdown) and fast reactor shutdown. Separate I&C systems are used to initiate subcriticality functions of CRDS. However, it is unclear whether scram is provided in AOOs and DBAs/DECs or only in DBAs/DECs. The level 4 includes Liquid Absorber Injection System (LAIS) as diverse shutdown system for DECs. The confinement systems/subsystems seem to have a clear division between Operational States and ACs, though, CIVs may be also credited in AOOs. All in all, it is prominent that principle of DiD has been applied in KLT-40S's Safety System design.

When compared to other three SMRs, KLT-40S doesn't only rely on passive Safety Systems but utilizes quite many active Safety Systems also in ACs. The design includes some conventional Safety Systems for High-Pressure and Low-Pressure Safety Injections (HPSI and LPSI), that are excluded from other three SMRs discussed in previous sections. This

seems to be possible, because new SMR designs incorporate safety features (inherent and design), which provide sufficient RPV water inventory in case of LOCAs. It can be also noticed that KLT-40S's passive Safety Systems for decay heat removal (ESCS) and containment heat removal (ECPRS) are quite similar solutions when compared to systems designed for other three SMRs.

It is evident from figure 43 that KLT-40S's safety design includes significantly more Safety Systems when compared to other three SMRs. The high number of Safety Systems adds more complexity in KLT-40S design and may increase necessary connections between SSCs. By reviewing more accurate design information, it could be possible to derive better insights regarding functional dependencies between SSCs. It is understandable that KLT-40S differs in this sense because it is the first SMR commercialized in operation (Akademik Lomonosov) and has long design history starting from 2000s.

From above results it can also be said that KLT-40S highly considers DEC's in Safety System design. It is evident from these systems, that they are designed to prevent core melt accidents in the first place and mitigate potential consequences if they were to occur. In addition, notable design provisions are included to provide overpressure protection for containment by use of passive systems, and thus fulfil one of the main objectives of level 4, to maintain the integrity of containment structure. Furthermore, KLT-40S follows in-vessel retention strategy to mitigate severe accidents with core melt. This is evident from External Reactor Vessel Cooling System (ERVCS) design that is credited in level 4. It is estimated that KLT-40S has CDF of less than 10^{-7} for internal events in full-power mode (Bylov 2013, 14-15).

Tables 11 and 12 present safety features incorporated in KLT-40S's design. It is prominent, that KLT-40S includes inherent features (negative reactivity coefficients, low core inventory and high heat accumulating capability), that enhance its safety by natural means. As typical for all LWRs, negative reactivity coefficients ensure stable power in operation due to reactivity feedbacks. Because of low core inventory, KLT-40S doesn't require as significant safety design provisions for decay heat removal as conventional PWRs do. Furthermore, radiological releases are low in potential accidents. The sufficiently large water inventory in primary circuit provides thermal inertia and enough time for operator response due to slow progression of events. One notable design feature is exclusion of possibility for inadvertent boron dilution since there is no reactivity control system based on soluble absorber in Operational States.

Table 11. Safety features included in KLT-40S design (part 1).

Feature	Description	Safety benefit
Negative reactivity coefficients	Fuel temperature, coolant (moderator) temperature, moderator density (void) reactivity coefficients are negative.	Stabilizing reactivity feedbacks for reactor power.
Small core inventory	Core has 121 FAs and initial load of 1273 kg U, that leads to small source term and less radioactivity.	Reduced potential radiological release in accidents. Less requirements for decay heat removal.
High heat accumulating capacity	Sufficiently large primary circuit water inventory provides thermal inertia and slow changing of coolant parameters.	Gives an extended period during which automatic systems or plant operators can react to transients and ACs. Water inventory in the tank ensures maintaining safe state for one day without operator actions.
Natural circulation capability for primary coolant	Reactor core coolant flow by natural driving force due to temperature difference induced density changes and elevation difference between heat source and sink.	Provides sufficient level of reactor cooling during MCP switch-off.
High thermal conductivity of Cermet fuel	Effective heat conduction from fuel pellet.	Fuel temperature and stored energy are relatively low.

It can also be noticed, that KLT-40s takes benefit of many design features in its modular and compact realization to prevent DBAs in the first place. For example, coaxial nozzles with low diameters in primary circuit and short connections between main equipment are design provisions to eliminate Large Break LOCAs (LBLOCAs) and Medium Break LOCAs (MBLOCAs). Furthermore, KLT-40S includes flow restrictors in nozzles connecting equipment with reactor to limit coolant outflow rate, which also provides protection against LOCAs. In addition, the reactor design aims to prevent certain failures of components. This is achieved, for example, by utilizing natural circulation for primary coolant (if MCPs fail) and by using external pressurizers and once-through SGs with low tube-side pressure in NO. Overall, it seems that these safety features contribute to implementation of DiD principle in multiple defence levels and lead to enhanced safety.

Table 12. Safety features included in KLT-40S design (part 2).

Feature	Description	Safety benefit
Low tube-side pressure in SGs in NO	Vertical coiled SGs with low tube-side pressure reduces the probability of inter-circuit leaks.	Provides prevention against abnormal conditions and failures.
Absence of soluble absorber reactivity control system	Liquid boron is not used for normal reactivity control.	Exclusion of inadvertent reactivity insertion resulting from boron.
Compact NSSS design	Short nozzles between main equipment connecting primary equipment (RPV, MCPs, SGs, Pressurizers).	Exclusion of long pipelines provides protection against MBLOCAs and LBLOCAs.
External gas pressurizers	Primary pressure is controlled by use of four external gas pressurizers, which excludes the need for electrical heaters.	Provides prevention against abnormal conditions and failures.
Primary circuit nozzle design	Sufficiently low pipe diameters in primary pipelines (< 50 mm). Use of coaxial nozzles for primary coolant circulation. Flow restrictors in the nozzles connecting primary circuit components with reactor to limit primary coolant outflow rate.	Provides protection against MBLOCAs and LBLOCAs.
Once-trough SGs	Use of once-trough SGs limits heat removal in secondary circuit.	Mitigates the effects of increased of secondary circuit heat removal during main steam pipeline break accident.
Partial passive safety	Subcriticality by gravity drop, ECCS HXs and containment HXs use natural circulation, bubbling tank for containment overpressure protection, passive external vessel cooling.	Partially safety related systems are designed such that no operator actions or power are needed to maintain safe, stable conditions following a DBA.

Appendix 10 contains tentative evaluation of STUK YVL.B.1 requirements for KLT-40S Safety System design. It appears, that it more tedious to evaluate KLT-40S system design when compared to other three SMRs. This is due to little information that is publicly available. However, it can be concluded that KLT-40S has potential to fulfil these requirements, since many of them are at least partially satisfied.

First challenging factor is high amount of different Safety Systems, both active and passive, that adds complexity in reactor design. There may exist functional dependencies between systems, that introduce risks for defence levels. It requires more detailed design information to make justified conclusions. Nevertheless, it should be highlighted that the many features incorporated in design provide prevention against failures in the first place.

Second is potential utilization of same Safety Systems in multiple defence levels. Especially, passive heat removal systems and possibly LPSI pumps may be credited in three level (3a, 3b and 4), that leads to increased dependency. Severe accident mitigation systems should be independent of those utilized to control DBAs. Furthermore, it should be demonstrated that level 3b is not jeopardized if same Safety Systems in level 3a are challenged. Although passive heat removal systems are likely to enhance reliability, design information needs to be reviewed further to evaluate their sufficient performance.

Third factor is lack of information pertaining to reactor control/protection systems and associated I&C. KLT-40S incorporates two different means for reactor shutdown and both can be actuated passively if external power supply is lost. However, without accurate design information it is difficult to justify acceptance for their sufficient performance. Further review of system design and analyses could lead to better evaluation.

8. Security results

This chapter presents results from the collection of security information. Only descriptions from public sources have been included because security information is highly confidential. The RUTA-70 has been excluded from this section since there was not enough information. Tentative evaluations of STUK's YVL A.11 requirements were done for NuScale and BWRX-300. These are included as appendices. Such evaluation wasn't done for KLT-40S due to a lack of information.

8.1 NuScale

8.1.1 Security descriptions

NuScale's PPS design is based on fundamental security functions, to provide detection, assessment, communication, delay, and response to protect against threats up to and including DBT. The NRC approved design certification includes descriptions for engineered PPS systems and credited design features, descriptions of security functions and performance requirements, design bases and other supportive technical information for further licensing. The information provided for design certification addresses security design elements and concepts that are within the scope of NuScale design (table 13). In addition, NuScale has identified security items, that license applicant must address during further licensing process to fulfil security requirements for site-specific considerations and operational activities. (NRC 2019, 1-5). Following results are based on NRC review of physical security.

Table 13. Security design elements and concepts within the scope of NuScale design.

Design element
Vital equipment
Vital areas
Protected area (plant area)
Intrusion detection systems for vital areas
Interior detection and assessment systems for vital areas
Communications
Central alarm station
Access control system
Physical barriers (vital areas)
Illuminations
Minimum safe standoff distances
Security computer system

NuScale has designated vital areas by identifying list of vital SSCs. Identification process was conducted by multidiscipline team, that utilized insights from different analyses (initiating event, accident scenario, human reliability, and system). In addition, Probabilistic Risk Assessment (PRA) results for postulated failure modes and internal hazard analyses were used to identify risk significant SSCs. NRC definition of vital equipment was used as criterion: *“Any equipment, systems, devices, or material, that failure, destruction, or release of which could directly or indirectly endanger the public health and safety by exposure to radiation”*. Furthermore, SSCs which would be required to remain operable to protect public health and provide safety in such failures were also considered to be vital. (NRC 2019, 8).

Vital areas include Main Control Room (MCR), CAS, Spent Fuel Storage, Secondary Power Supply Room, and other designated vital areas based on risk significant SSCs. NuScale has established specific boundaries of building that enclose risk significant SSCs and form vital areas within nuclear island and structures. In addition, exterior plant boundaries are mentioned to form certain vital areas. The designs and configurations of vital areas are stated to restrict access (access control) and limit pathways to SSCs (delay barriers). The site layout demonstrates separation of vital area boundaries from protected area (figure 44). However, physical barrier and access control designs for protected area perimeter are mentioned to be outside the scope of NuScale design certification. (NRC 2019, 9, 13).

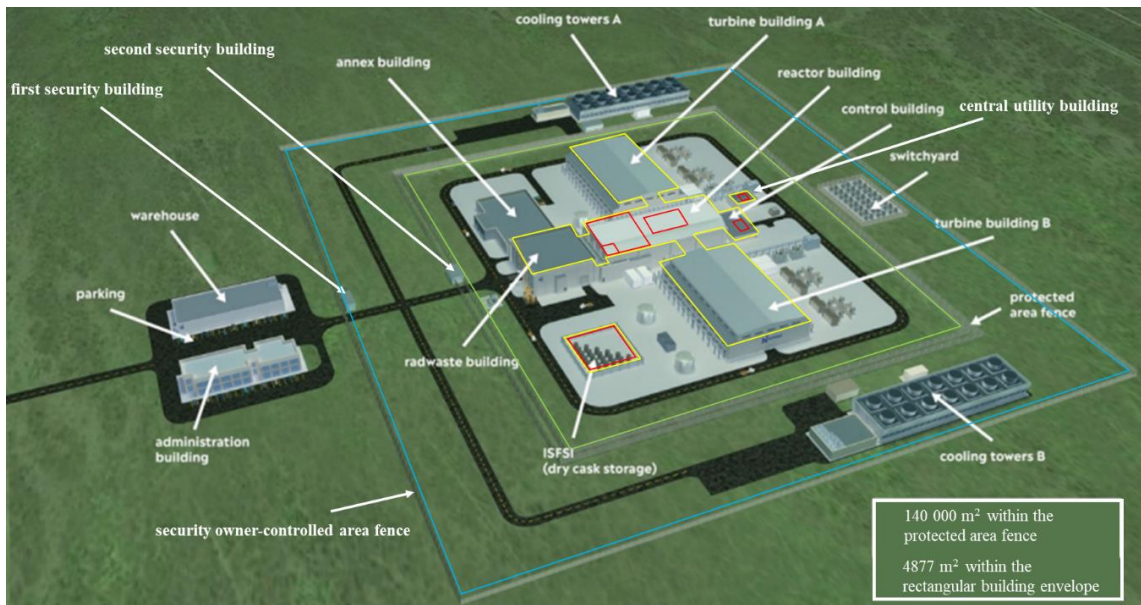


Figure 44. Conceptual NuScale site-lay out with demonstrative security zone boundaries using STUK’s implementation model. Blue (restricted area), green (plant area), yellow (protected area) and red (vital areas). Protected areas and vital areas are only representative assumptions. Note, that NRC uses the term ‘protected area’ for plant area (modified from NuScale 2019, 15, areas from NuScale 2020a, 4).

NuScale incorporates portal detection system, interior assessment and monitoring system (video cameras), intrusion detectors and associated alarm system for vital areas. The withheld design information describes requirements for systems and components that provide detection, assessment and communications functions. The redundancy requirement for detection (alarm transmission and assessment) is considered in the design descriptions by presenting system interfaces with two independent and physically separated alarm stations. Furthermore, vital area barrier openings also have dedicated security systems to detect unauthorized access (intrusion detectors, monitors and associated cabling). (NRC 2019, 10).

The CAS design description is included in NuScale design certification. NuScale incorporates intrusion detection systems that are independent and redundant of each other to allow both alarm stations to receive same information from field devices and components (intrusion detectors, door card readers, alarm devices and Closed-circuit television system CCTV). CAS is manned with security personnel to process and assess information from monitoring and alarm systems. Furthermore, CAS provides communication (radio, telephone, and microwave-transmitted two-voice communication) with response forces (on-site and off-site) and plant operators. CCTV consists of cameras that provide monitoring for designated areas and allow visual assessment for alarm actuation. (NRC 2019, 10-12; NuScale 2020c, 10).

The design information includes recommendations for cameras and locations that support selection of vendor-specific equipment by considering plant lightning system for illumination. The location and design details of SAS are outside of the scope for NuScale design certification. However, SAS that is independent and functionally equal to CAS is identified as one item to be provided by licensee to fulfil necessary redundancy requirements for detection and communications. (NRC 2019, 11-12, 20).

The description of vital area access control system is provided in NuScale design information. In addition, this information presents the design requirements for SSCs that are associated with locking, access control, and emergency egress. An automatic computer-based system is used to control personnel access in NuScale power plant. The system allows only authorized persons to enter areas (protected area, buildings, and vital areas) at specific access points. Access control system records data for access point activities such as unauthorized entry attempts, door status and alarm indications. In addition, detection systems such as CCTVs and intrusion detectors are part of the access control system. The access control system design allows functions for both alarm stations, which provides redundancy. (NRC 2019, 10-12).

NuScale describes the requirements for design and construction to delay forced entry and to provide secure locking mechanisms for vital area portal ingress and egress. Emergency exit is ensured by devices that allow for rapid egress. In addition, exit devices or locking hardware account for emergency and normal functions if power supply is lost. It is mentioned that locking devices comply with requirement to have unoccupied vital areas locked and alarmed. Furthermore, it is stated that locking system provides sufficient entry control to vital areas. The access control system is designed such that locking control cannot be deactivated without knowledge and concurrence of operators in both alarm stations. Likewise, status of a detection point cannot be changed without consensus. (NRC 2019, 12, 14-15).

NRC has concluded that vital area access control design provides protection to all access points and emergency exits. The exterior access control design for personnel, vehicles, and material (protected area and restricted area) and implementation of access authorization program with numbered identification badges are considered as required items for further licensing. (NRC 2019, 15-16, 20-21).

The barriers of protected area and vital areas along with access controls delay unauthorized person's attempt to enter vital areas and provide sufficient time for response forces to interrupt person before he/she reaches vital area. NuScale describes minimum construction design requirements for floors, walls, and ceilings to provide physical barriers that enclose vital areas within associated buildings (reactor building, control building and spent fuel storage). The design information includes locations for such barriers and drawings for recommended designs. (NRC 2019, 12-13).

The vital area design incorporates hardened doors with locking and alarming capabilities. The hardened doors provide delay against forced entry and resists explosive and mechanical breaching. In addition, vital area design includes hardened portal egress. Bullet-proof design of walls, roofs, ceilings, windows, and doors provide protective enclosures for CAS and MCR. Reinforced concrete with conservative thickness is credited to meet bullet-proof resistance requirement for structures. (NRC 2019, 12-14, 16).

Furthermore, NuScale presents descriptions of physical barriers to protect vital areas from openings such as HVAC penetrations (e.g., ducts, cable trays and ventilation fans). The design ensures that necessary penetrations do not enable pathways for a person and that the integrity of vital area barrier is not jeopardized. The design and integration of additional delay barriers for site-specific PPS is identified as one item to be addressed in further licensing. (NRC 2019, 14-15).

NuScale design incorporates two redundant, independent, and physically separated security computers, which provide plant security functions by access control, reporting and recording of alarm points, monitoring of doors and alarm detection. The security computers are connected to isolated network. Both these computers are located within vital areas with access controls. The design information presents functional diagrams with interfaces of security computer systems with devices performing detection, monitoring and access control. The network enables data communication between devices (e.g., computers, CCTV servers, graphic displays, video recording systems) and transmits information to alarm stations. Dedicated network that is independent from other network systems and includes redundancy is designed for computer systems that generate alarms from field detection systems. Vendor-specific descriptions of field devices and implementation of cyber security program are identified items to be addressed in further licensing. (NRC 2019, 11-12).

Furthermore, NuScale has provided preliminary information to support design of vehicle barrier system. It has assessed and documented minimum safe standoff distances (MSSDs) for protecting nuclear island and structures from maximum vehicle-born explosive derived from DBT. The design information provides required MSSDS for construction of a continuous vehicle barrier system. The design of defensive fighting positions for response forces to neutralize threats is mentioned to be outside the scope of NuScale design. Table 14 presents summary of security items, that NuScale has identified to be addressed in further licensing of NPP. (NRC 2019, 17-18).

Table 14. Security design elements and concepts identified by NuScale to be addressed in further licensing.

Design element
Secondary alarm station (design, location, and communication equipment)
Isolation zones (other security zones)
Illumination for isolation zones and protected area access
Physical barriers (outside nuclear island and structures)
Field security devices (intrusion detectors, cameras and other equipment)
Exterior access control portals (personnel, vehicle, and material)
Vehicle barrier system
Secondary power supply for communication system and security systems
Independent power supply (uninterrupted power supply batteries, in-line generators, or other power sources)
Inspections, tests, analyses, and acceptance criteria for site specific physical security SSCs
Physical security program (security plans, training, and qualification)
Cyber security program
Access authorization program
Insider mitigation program

8.1.2 Observations

From sections presented it can be noticed, that NuScale’s security design is based on risk-based approach in the first place. The safety-significant target SSCs has been surveyed by utilizing insights from safety analysis, reliability analysis and PRA. In addition, human factors seem to have been considered as part of this target evaluation. Furthermore, DBT is utilized as another basis for PP design to derive potential threats against which the NPP is to

be defended. The design information seems to focus on sabotage threats, but the PPS design will also protect against unauthorized access to nuclear/radioactive material.

In addition, NuScale's PPS design utilizes security zones surrounded by physical barriers and provides protection against threats by deterrence, detection, delay, and response. It is evident from the results that the design follows DiD concept of security. Though detailed descriptions of PPS have only been presented for vital areas in nuclear island, the design already facilitates implementation of DiD in further site-specific considerations. For example, the security computer network, access control system and recommendations for equipment locations support further PPS design.

Organizational security design considerations such as security plans and procedures, that are related to human/organizational activities are not considered as part of plant design. This is understandable since NPP organization is prerequisite to be able to design operative security provisions. Especially, organizational design features are crucial for PPS to be capable to provide sufficient response to interrupt and neutralize adversaries. Response plans and cooperation with local authorities should be highlighted when designing response measures. Furthermore, planning of organizational security activities are essential part of security implementation to provide access authorization, communication and guarding. Nevertheless, NuScale has identified security plans and procedures as important items to be addressed in further licensing process.

Appendix 11 contains tentative evaluation of STUK YVL A.11 requirements for NuScale security design. NuScale has potential to fulfil requirements pertaining to implementation of security zones and utilization of PP measures. Despite of lacking detailed design descriptions for security zones (other than vital areas) and their associated security devices, physical barriers, and access control portals, it seems that most technical security requirements have been well considered. It is worth to note, that NRC uses the term 'protected area' for plant area and doesn't consider plant buildings as one security zone that would be protected area in STUK's implementation model.

Furthermore, from the evaluation it can be yet again noticed that organizational security design is issue to be addressed to fulfil requirements for response measures (provision of command centres for on-site response forces and dedicated command room for police operations).

8.2 BWRX-300

8.2.1 Security descriptions

BWRX-300's PPS design is based on threats derived from the DBT and incorporates fundamental security functions to provide detection, assessment, communication, delay, and response (GE-Hitachi 2014a, 731). Although little information is yet presented for BWRX-300 security design, GE-Hitachi indicates NRC certified PPS design of ESBWR as applicable reference for security arrangements (GE-Hitachi 2019, 35-36). GE-Hitachi has introduced brief descriptions for basic design elements of PPS (table 15) and has identified items for site-specific considerations and operational security activities that must be addressed in the further licensing process. (GE-Hitachi 2014b, 15-22). The following sections are mainly based on ESBWR security design information.

Table 15. Security design elements and concepts within the scope of BWRX-300 preliminary design.

Design element
Vital equipment
Vital areas
Protected area (plant area)
Intrusion detection systems for vital areas
Interior detection and assessment systems for vital areas
Central alarm station (location, structure, equipment needs)
Access control system
Physical barriers (vital areas)
Illuminations

All vital equipment is in vital areas to which access is controlled and monitored. Many of these vital areas are within radiological control areas which are inaccessible in NO. The vital SSCs are located inside plant buildings and are enclosed within robust reinforced concrete structures that provide physical barriers against unauthorized access to vital areas. Some vital areas incorporate blast and bullet-resistant barriers. In addition, many components of vital systems remain in below-grade vital areas, thus protecting against external impacts. Furthermore, physical separation of redundant systems is utilized in plant design that multiple vital SSCs must be compromised before effective radiological sabotage could be

realized. The vital areas are located within the protected area surrounded by plant double-fence, that provides a separate physical barrier and access control (figure 45). (GE-Hitachi 2019, 35; GE-Hitachi 2014a, 731; GE-Hitachi 2014b, 16).

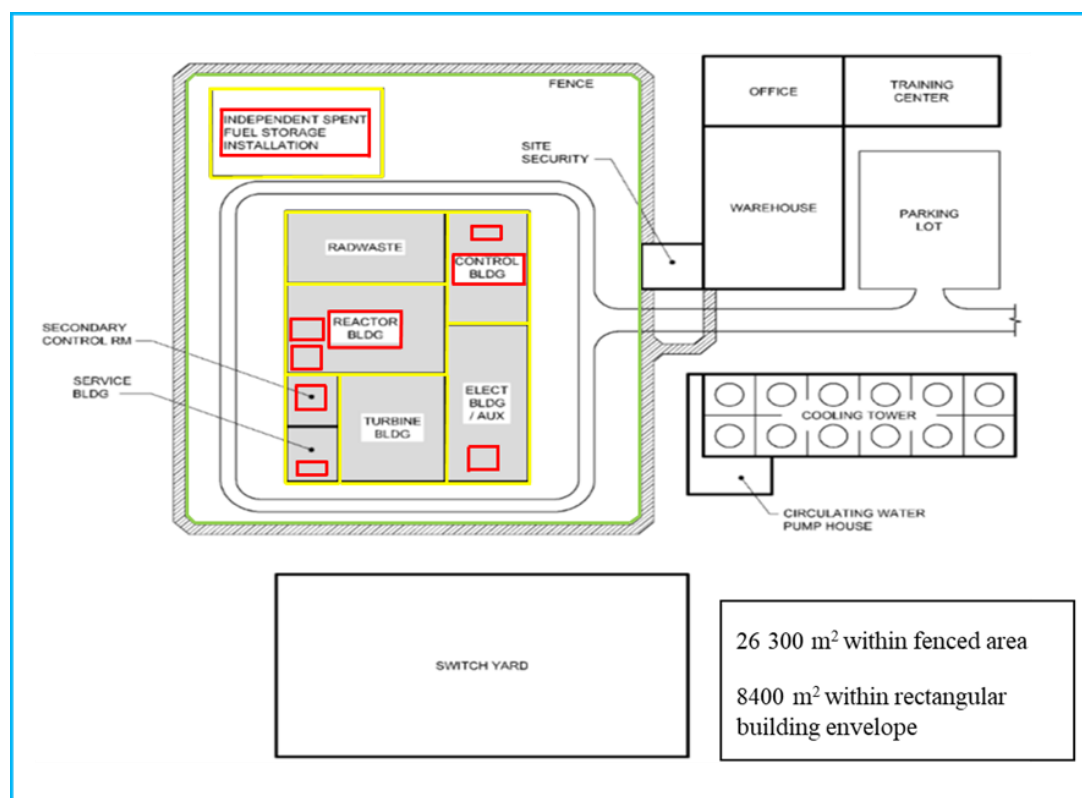


Figure 45. Conceptual BWRX-300 site layout with demonstrative security zone boundaries using STUK's implementation model. Blue (restricted area), green (plant area), yellow (protected area), and red (vital areas). Protected areas and vital areas are only representative assumptions (modified from GE-Hitachi 2019, 11, 5).

Vital areas that remain unoccupied in operation are locked and alarmed with intrusion detection systems. Access to vital areas is implemented through a minimal number of locked access points with entry portals, that are monitored (video camera system) and controlled (access control system) by the site PPS. Emergency conditions are considered by providing alarmed emergency exits with secure locking devices that allow prompt egress through the vital area boundaries. The intrusion attempts to the vital areas alarmed and assessed at the continuously manned CAS and SAS. Both alarm stations are located within buildings inside the protected area and constitute independent vital areas. The external walls, doors, floors, and ceilings of CAS and MCR are bullet resistant. (GE-Hitachi 2019, 35; GE-Hitachi 2014a, 731-732, GE-Hitachi 2014b, 16).

The site PPS will be designed to have physical barriers, intrusion detectors, alarm devices, monitoring systems, and controlled access to areas. An isolation zone is maintained around the protected area and is covered by an intrusion detection system. Detection of penetration attempts is provided on either side of the protected area barrier. The protected area surrounded by a plant fence encloses buildings required for plant operation. Alarmed exits are provided to allow sufficient emergency egress through the protected area barrier. Areas within the isolation zones and the protected area are equipped with lightning systems to provide sufficient illumination for observation of abnormal activity or presence of persons or vehicles. Detailed descriptions for site arrangement drawing and associated systems, that present the locations and designs of different zones, physical barriers, vehicle barriers, security devices and access control portals are items to be addressed in further licensing. (GE-Hitachi 2019, 35; GE-Hitachi 2014b, 15, 18, 21).

The intrusion detection and monitoring systems will be designed to be capable of detecting and alarming intrusion attempts into the protected area or any vital areas. The security alarm devices and associated transmission lines to annunciators are self-checking and tamper-indicating. These systems incorporate equipment to record on-site alarm annunciation including the type of alarm (intrusion alarm, emergency exit alarm, false alarm, alarm check, tamper indication), location, alarm circuit, date, and time. The systems provide audible alarms, visual display, and other data to two separate and redundant alarm stations for assessment. (GE-Hitachi 2014a, 731; GE-Hitachi 2014b, 17).

A computer-based access control system is provided to identify and verify personnel authorization to enter the protected area or vital areas at the controlled access points. Positive identification and authorization of personnel are based on numbered ID badges. Furthermore, similar means to control access of vehicles into the protected area is provided. In addition, access control measures involve means to verify the passage of materials into the protected area. The access points manned by security personnel provide detection of explosives, firearms, incendiary devices, or other prohibited material by detection equipment and both visual and physical searches of personnel, vehicles, and materials. (GE-Hitachi 2014b, 16-17).

Alarm stations are equipped with systems to monitor areas and evaluate data from security systems, perform an immediate assessment of alarms, provide command and control for alarm response. The communication systems are intended to allow continuous

communication between alarm stations, guard personnel, and the MCR. Furthermore, conventional communications such as telephone lines may be used to ensure communication between CAS/SAS and local law enforcement agencies. However, GE-Hitachi has identified the design of SAS (location and structure) and detailed descriptions of CAS/SAS systems as items to be addressed in the further licensing process. The design aspects of systems include communication equipment and type of signal transmission (e.g., radio, telephonic, site intercom), alarm central processing units, data gathering panels, alarm transmission technology (e.g., electronic data, fiber optic). (GE-Hitachi 2014b, 17, 19-20).

In the event of the loss of normal power, the continuous power supply for non-portable communication and alarm annunciator equipment is ensured by independent power sources of the secondary power supply system that is located within a vital area (GE-Hitachi 2014c, 731). The detailed descriptions of secondary power and remote uninterruptible power systems are addressed by the license applicant (GE-Hitachi 2014b, 19).

Table 16 presents summary of security items, that GE-Hitachi has identified to be addressed in further licensing of NPP.

Table 16. Security design elements identified be addressed in further licensing (GE-Hitachi 2014b 19-21).

Design element
Secondary alarm station (design and location)
Communication and alarm systems (CAS and SAS)
Physical barriers (outside nuclear island and structures)
Field security devices (intrusion detectors, cameras, alarm devices and other equipment)
Exterior access control portals (personnel, vehicle, and material)
Vehicle barrier system
External bullet-resistant enclosures (defensive positions for response forces)
Secondary power supply (communication system, security systems)
Independent power supply (uninterrupted power supply batteries, in-line generators, or other power sources)
Inspections, tests, analyses, and acceptance criteria for site specific physical security SSCs
Operational alarm response procedures
Operational response procedures to security events
Administrative control procedures (screening and vital area access)
Key control program
Cyber security program

As it can be noticed GE-Hitachi has identified organizational security design elements as items to be addressed by the license applicant. The security plan consisting of physical security plan, training and qualification, and contingency plan is to be provided. With respect to response measures, strategically placed defensive positions are to be provided for armed response forces in site arrangement drawing that indicates fields of fire from bullet-resistant enclosures. Furthermore, many procedures have considered to be relevant for plant security operations. Response procedures are utilized to include stepwise process for operators and security personnel to respond to alarm indications and security events. Policies and administrative procedures are implemented for screening personnel for access authorization. In addition, administrative control procedures are considered for vital areas and these include measures such as two-person rule and key control. (GE-Hitachi 2014b, 16-21; GE-Hitachi 2019, 35).

8.2.2 Observations

Although PPS design descriptions presented are mainly based on ESBWR design information, it can be noticed that GE-Hitachi has considered all necessary security design elements such as risk-based approach, DBT, security zones and provision of systems/organizational measures to provide PP functions. The information seems to focus on sabotage threats, but the PPS design will also protect against unauthorized access to nuclear/radioactive material. It could be stated that GE-Hitachi already has a conceptual PPS design for BWRX-300 that follows DiD concept of security. Appendix 12 presents a tentative evaluation of STUK YVL.A.11 requirements, this indicates that many technical design requirements have already been considered in conceptual design. However, detailed design descriptions for BWRX-300 are required to better evaluate fulfilment of these requirements.

In addition, it can be highlighted that GE-Hitachi has considered organizational security design aspects such as procedures and policies. These can be important for the implementation of operational security. By including clear and appropriate policies and procedures, it may be possible to execute organizational activities such as access control,

communication, and response in a more systematic manner. This emphasizes the importance of organizational design aspects because without efficient policies and procedures it is difficult to coordinate actions of personnel (security and others) towards desired outcomes, though technical security design would be robust. Some organizational procedures and policies (e.g two-person rule and key controls) also provide deterrence against insider threats.

Furthermore, GE-Hitachi considers design aspects pertaining to response such as hardened defensive positions for armed response forces. It seems that NRC requirements emphasize armed response and defensive strategies. However, it should be recalled that security design requirements are based on NTA. Thus, there are differences in provisions for forced response. These design provisions increase deterrence against external threats.

8.3 KLT-40S (Akademik Lomonosov)

The FNPP has a slightly different site layout design when compared to conventional land based NPPs. The site is essentially divided into two sections: the landward area and the seaward area. The plant requires a dedicated water area to be provided where the FNPP is safely installed and docked using waterside structures such as jetties, boom barriers, and sea walls. The sea area is to be enclosed as part of the PP. The coast has normal structures to transfer power and heat to the consumers and buildings associated with auxiliary, servicing, and protective functions. (JSC OKBM 2020, 9, 12; JSC OKBM 2013, 2, 22-23).

There is little information publicly available on security design of KLT-40S FNPP. However, a very short description of PP arrangements has been provided by JSC OKBM. The PPS design is stated to follow the concept of security zones, thus the implementation of DiD. The combined zone of the coastal and sea areas is mentioned to form one security zone and the boundaries of the FNPP comprise another. Two reactor units and storages for material (fresh fuel, spent fuel, and radioactive waste) are in the middle-ship compartments, which comprise some vital areas. The PPS design includes access control system and the access to the FNPP/the vital areas is highly controlled. (JSC OKBM 2013, 19-22). A simple illustration of the implementation of the security zones is presented in figure 46.

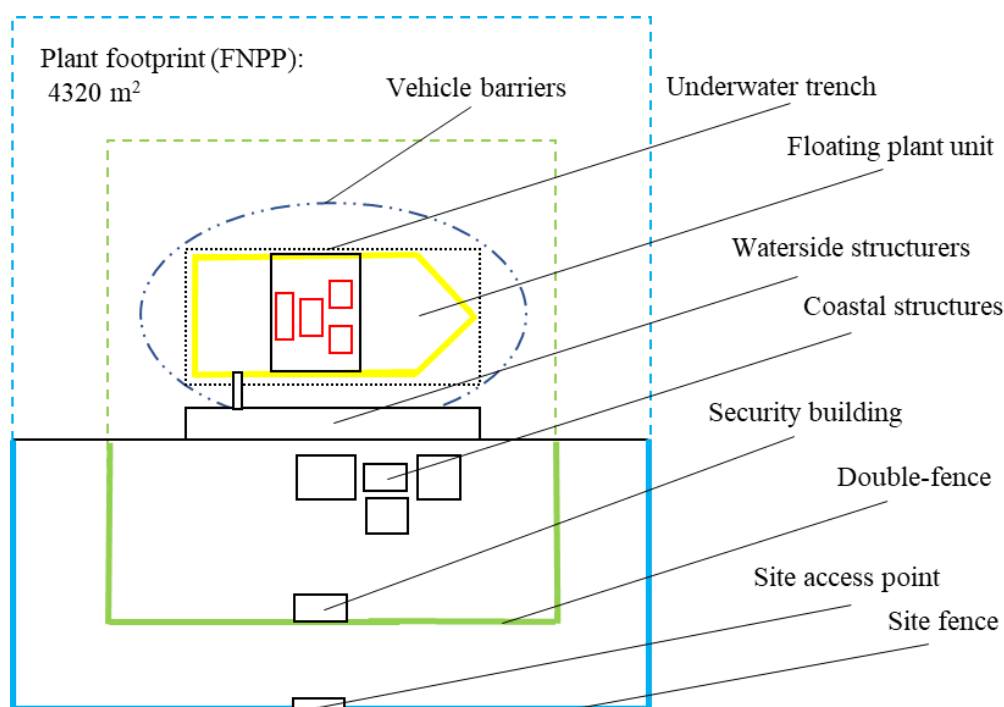


Figure 46. A simple illustration of the FNPP site and implementation of security zones using STUK's implementation model. Blue (restricted area), green (plant area), yellow (protected area) and red (vital areas).

Engineered security features are mentioned to be included for the PPS, which likely means physical barriers to provide delay at the security zone boundaries. The sea is to be bounded by breakwaters and dams, natural barriers such as a group of underwater rocks or cliffs are likely also utilized. Security devices such as alarms, TV-observation systems, and communications are included, which comprise design aspects for detection and response. The site likely incorporates two manned CASs, one could be on board and another at the coast. Organizational measures are included in PPS, which means guarding (land, sea, and the reactor compartment), communications at CASs, access control procedures and policies, and provision of response forces. (JSC OKBM 2013, 19).

The barge design includes features for protection against vehicle impacts. The anti-collision design is developed and refined from nuclear ice-breaker design requirements. The floors have been reinforced by thicker plating sheets and longitudinal framing with larger cross-sections is used. The board plating thickness has been increased, longitudinal stiffness ribs of the board are reinforced, the thickness of upper deck plating near the board is increased, the thickness of the first-tier superstructure deck plating near the board is increased and longitudinal stiffness ribs of the first-tier superstructure deck near the board are reinforced. Such reinforcements provide collision protection against other ships and crash of a helicopter

with a mass of 11 t. Organizational measures will be provided against aircraft crash. The FNPP is divided into watertight compartments and is mentioned to be unsinkable even if any two adjacent compartments would be flooded (the maximum static list is less than 3 degrees). (JSC OKBM 2013 22, 34; JSC OKBM 2020, 25).

Although differences exist when compared to land based NPPs, the realization of PPS is very similar and follows conventional security design principles of DiD. Norwegian Radiation Safety Authority (Statens strålevern) has already 2008 considered this by proposing an analogy of security arrangements between Atomflot and Akademik Lomonosov. Atomflot supplies and maintains nuclear icebreakers, thus its site is comparable to that of a FNPP. The site of Atomflot has a 2 km security zone around the facility. The eastern perimeter of the facility at the coast is provided with double-fence, intrusion detection/monitoring systems, and guard towers. In addition, the site is fenced and includes intrusion/monitoring systems. Russian Navy guard vessels patrol the northern and western seaward areas. In the long run, facility security has been enhanced by collaborative efforts between other countries such U.S, Norway, and Sweden. (Dowdall & Standing 2008, 51-54).

However, certain security challenges can be identified for FNPP design (table 17). The normal physical barriers such as walls and fences may not be applicable or at least are more difficult to build at the seaward areas, which could lead security zones to be open from the sea to some extent. This could make the site more vulnerable to intrusion, thus supporting adversaries' strategies to access the plant. Therefore, guard patrols at the sea would be essential mean to provide protection from such problem.

The FNPP design enables direct attacks from the sea and underwater attacks, which introduces challenges to PPS design when compared to land based NPPs. Security design elements important against such attacks could involve radar systems (detection) and vehicle barriers (delay). In addition, the movable plant makes it possible to have extreme threat scenarios involving the hijack of the FNPP. There are essentially two main scenarios, to steal the whole nuclear inventory of the plant for weapon production aims and to move the facility to a specified target area causing radiological consequences by sabotage.

Table 17. The identified security challenges of the FNPP.

Challenge	Description
Separation of security zones	The seaward location of the plant may make it difficult to set physical barriers for security zones (restricted and plant area). This could create potential pathways and benefit adversaries' strategies. For example, access to the plant could be attempted by swimming or diving.
Vulnerability to attacks from the sea	The FNPP enables direct attacks from the sea, such as a ship collision. In addition, scenarios involving underwater attack strategies are possible.
Extreme threat scenarios	The movability of the FNPP makes it possible to implement extreme threat scenarios. The adversaries may aim to hijack the FNPP to steal the whole nuclear inventory or move it to a target area and cause harm by sabotage.
Plant transports at sea	The security of FNPP transports at territorial/international waters likely necessitates comprehensive response forces. The response time for the arrival of reinforcements could be long. Such transports may not comply with the current international agreements and regulations.

As the plant is more vulnerable to such scenarios during transports, comprehensive response forces are likely required onboard to provide sufficient capability for defence against such attacks. This may introduce potential complexities with the international security legislation system. In general, the FNPP transports may not comply with the current international agreements and regulations pertaining to the security of nuclear and radioactive material transports. The time required for additional response forces to arrive at regional/international seas may be significant, thus enhanced cooperation between states and their authorities should be emphasized to ensure the protection of such transports.

9. Safeguards results

This chapter presents case study results for safeguards. No direct safeguards information was available for SMR designs. Only a trial FSA of NuScale by Pacific Northwest National Laboratory (PNNL) was found. The NuScale section is based on this publication. The same FSA tool of the authors was used to evaluate differences of RUTA-70 and KLT-40s when compared to conventional LWR plant. These all three are included as appendices. BWRX-300 has been excluded from this section due to lack of information. However, BWRX-300 plant is conventional-like, and safeguards implementation is likely the same as in operational BWR plants.

9.1 NuScale

NuScale Power Modules (NPM) are in a common below-grade pool inside the reactor building. Each NPM is in a bay surrounded by three walls and open pathway towards the centre of the pool. There are two rows at the ends of the pool each including up to six NPMs. A shield consisting of horizontal reinforced concrete slab (at the top of the bay) and vertical stainless steel tube framing with radiation panels (surrounds the bay) is provided for each module. The shield must be removed to access NPMs. To support refueling the design enables stacking of two shields. The central channel allows movement of NPMs between common refueling area and reactor pool bays. (NuScale, 2020a, 36).

The areas for fuel handling, storage, and reactor maintenance are located opposite the reactor pool. These include refueling pool, below-grade spent fuel pool, and dry-dock with equipment staging pool. By using a crane, the NPMs are transferred between reactor and refueling pools, which are directly connected. A fuel shuffler is used to move FAs between refueling pool and spent fuel pool. A weir with short channel for underwater fuel transfers is provided between refueling and spent fuel pools. The equipment staging pool includes an inspection rack for modules and space for new NPM components prior to assembly. It is separated from the refueling pool by a gate. The dry dock provides area for maintenance, inspection and testing for upper section of NPMs. Large equipment access door is connected

by rail to the dry dock. Fresh fuel receiving and staging area are located adjacent to the spent fuel pool. A jib-crane and elevator are used to transfer fresh FAs in spent fuel pool storage racks for temporary storage before refueling. (NuScale 2020d, 37; Coles et al. 2013, 14).

During refueling the lower CNV is removed and stored in the refueling pool using containment flange-stand (A in figure 47). Next, the crane is used to move upper CNV to RV flange-stand, where upper and lower RPV are separated (B in figure 47). The CNV and RPV containing upper reactor internals (e.g SGs and CRDS) are moved to staging pool. The lower RPV with core and control rods remains in RV flange-stand for refueling. Once refueling, maintenance and inspections are finished the NPM is reassembled in reverse order and transferred back to its own bay. The spent fuel pool provides storage for approximately 18 years of accumulated spent FAs. After sufficient cooling time, the FAs are loaded in spent fuel caskets and transferred to dry storage facility within plant area. (NuScale 2020d, 38; NuScale 2020a, 25).

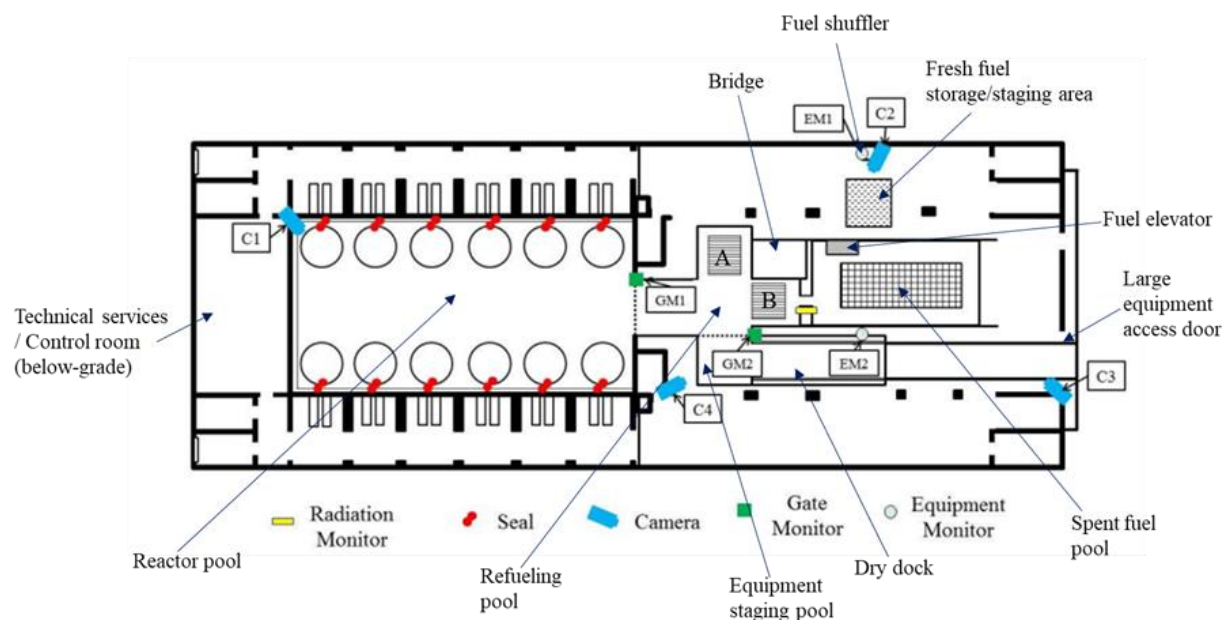


Figure 47. The layout of fuel handling and storage areas and proposed SA for NuScale design (modified from Coles et al. 2013, 14, 19).

9.2.1 Challenges and similarities

PNNL has applied an FSA tool for NuScale to evaluate differences when compared to conventional PWR (appendix 13). This has led to identification of safeguards challenges (table 18).

Table 18. Challenges of NuScale design when compared to conventional PWR safeguards.

Challenge	Description	Main cause
The design eliminates sealing system that would prevent/indicate removal of nuclear material from the RVs.	The locking and sealing of the fuel transfer canal are infeasible due to multiple modules that are in operation. This increases difficulty in maintaining CoK of the NM inventory of the RVs and the spent fuel pool.	Common refueling area for multiple modules.
Installation of C/S and monitoring equipment will be more difficult/expensive	Significantly large area with frequent activities is required to be monitored. C/S is required to be applied and maintained for multiple modules.	Common refueling area, presence of multiple modules.
Increased difficulty in maintaining CoK associated with DIV	Safeguards effectiveness is reduced due to multiple modules and DIV is challenging during the lifetime of the plant.	Common refueling area, frequent refueling of multiple modules.
PIT/PIV efficiency is reduced	There is no single point of time when all FAs are visually accessible at IKMPs. The double stacking of FAs limits/precludes visual checks, sampling, and NDA measurements. Inventory change/ movement between the time of the PIT and the PIV could occur if module reaches the refueling point.	Frequent refueling of multiple modules, the double stacking of FAs in the spent fuel storage pool.
Interim Inventory Taking (IIT)/Interim Inventory Verification (IIV) are more difficult	Executing shutdown of all modules to conduct physical inventory for all FAs in module cores during one IIT is infeasible. The design creates potential for Unmeasurable Inventory at the time of an IIV, since there is the likelihood of items that cannot be verified.	Differing refueling schedules.
The required collection of Other Strategic Points (OSPs) is more complex and expensive	The NuScale design is likely to require more OSPs compared to conventional PWR to effectively maintain CoK of NM and associated activities.	Common refueling area, frequent refueling of multiple modules.
Opportunities to conceal facility misuse	Module misuse could be disguised by swapping/duplicating operational records from other units that were operated as declared.	Presence of multiple modules.

The main design differences that introduce difficulties are the presence of multiple NPMs, common refueling area, staggered and frequent refuelings (24 month for one module) and double stacking of spent FAs in the spent fuel pool. Due to these challenges, CoK is difficult to maintain, more safeguards barriers are required, and IAEA on-site verifications become complicated during the lifetime of the plant. (Coles et al. 2013, 65-74).

As the fuel items and general PWR technology are essentially the same, it is possible to follow similar approaches for NMA. In addition, IAEA on-site verification activities can be conducted by using same equipment and measures. However, practical implementation of NMA and IAEA on-site verification can be difficult due to frequent refueling and associated material transfers. Particularly, physical inventory cannot be taken for all NPMs at a certain time, which results in uncertainty for the IAEA in the verification of all NMs. (Coles et al. 2013, 65-74).

9.1.2 Safeguards approach

PNNL has proposed a tentative SA for NuScale design based on their FSA. Practically same safeguards equipment can consider to be utilized for containment, surveillance, and monitoring (figure 47). However, the layout with 12 NPMs is likely to require more such safeguards barriers in carefully designed OSPs to maintain efficient CoK. Furthermore, sealing may be an issue because attaching/detaching seals during refueling (pool lids or canals), and transfers (fresh fuel containers and spent fuel caskets) requires more frequent IAEA inspector presence. It could be possible that SA relies more on utilization of RMSs if sealing cannot be appropriately implemented. The results of their simple diversion pathway analysis (table 19) indicate that basic scenarios remain the same for NuScale. However, the presence of multiple NPMs may support concealment strategies, for example in falsification of operational records (duplicating or swapping records from other NPMs to disguise misuse/diversion). In addition, multiple modules make it possible to have several core inventories, from which few FAs (four fresh FA or six spent FA) for SQ can be diverted. (Coles et al. 2013, 18-21, 34).

Table 19. Results of simple diversion pathway analysis for NuScale design based on proposed SA.

Diversion pathway	Description	IAEA safeguards to defend
Removal of fuel rods/FAs from the fresh fuel storage	Fuel items are substituted with dummy rods/assemblies and associated facility records are falsified to conceal diversion.	Sealing of fresh fuel shipping containers/FAs at dry fresh fuel storage area, surveillance of dry fresh fuel storage area, surveillance of spent fuel storage pool.
Removal of FAs from a module core	Fuel items are substituted with dummy rods/assemblies and associated facility records are falsified. Is possible from multiple modules. Reactor pool and refueling pool are two different areas where this scenario could be implemented.	Sealing of removable module lids, surveillance of reactor pool, surveillance of refueling pool, surveillance of spent fuel storage pool, gate monitors, radiation monitor between refueling and spent fuel pools, equipment monitors (fuel transfer/handling equipment).
Irradiation of undeclared material and removal from the facility	Undeclared FAs or other target material are irradiated in one of the modules at reactor hall and associated facility records are falsified to conceal misuse.	Sealing of removable module lids, surveillance of reactor hall, surveillance of refueling pool, surveillance of spent fuel storage pool, gate monitors, radiation monitor between refueling and spent fuel pools, equipment monitors (fuel transfer/handling equipment).
Removal of fuel rods/assemblies from the spent fuel storage pool	Fuel items are substituted with dummy rods/assemblies and associated facility records are falsified. The double-stacking of FAs impedes detection of diversion from the fuel on lower level.	Surveillance of spent fuel storage pool, surveillance of fuel transfer/handling equipment, radiation monitor between refueling and spent fuel pools.
Removal of fuel rods/assemblies from a consignment	Fuel items are substituted with dummy rods/assemblies during unloading (fresh fuel) or loading of shipping containers (spent fuel). Associated facility records are falsified.	Sealing of fresh fuel containers/spent fuel caskets, surveillance of receipt/shipment areas.

9.2 RUTA-70

The reactor core of RUTA-70 is small and consists of 91 hexagonal FAs each having 120 fuel rods. The FA design is similar to VVER-440 in the radial direction. However, the FAs have a different dimension in the axial direction (height 1400 or 1530 mm) when compared to VVER-440 (height 2420 mm). Two fuel rods options have been considered, either UO₂ fuel like in VVER-440 or Cermet (60% UO₂ and 40% Al alloy). The Cermet fuel consists of UO₂ granules in a silumin matrix which leads to benefits such as high thermal conductivity (low fuel temperature) and enhanced fission product retention. (Kozmenkov et al 2012, 2; Romenkov 2009, 394; NEA/CSNI 1998, 11).

The core inventory is located at the lower part of the pool in a vault. The design doesn't include a conventional pressure vessel, however, the metal-lining of the pool at the vault section can be considered to constitute a RV. The chimney barrel as a shell surrounds the core and extends out of the RV. The supplying plenum is connected to the upper part of the chimney barrel, whereas the collecting plenum is connected to the upper section of the RV. These constitute a closed structure inside which the core resides. The reactor pool includes a lid that consists of layers of protective slabs thus the nuclear inventory is inside a closed pool. (IAEA 2005b, 381-383, 385, Cherepnin et al. 2007, 6-7, 14).

The interim spent fuel storage pool is arranged in a separate compartment adjacent to the reactor pool. It includes space for the full core, one third of the core and a margin for damaged assemblies (total of 126 FAs). The refueling cycle is every three years. The spent fuel is to be cooled for three years before transfer to the spent fuel storage. The average and maximum discharge burnups for UO₂ fuel are mentioned to be 28,7 and 37 MWd/kgU, however these values consider 3% enrichment (UO₂) instead of recent 4,2 % (Cermet). The design considers reprocessing of spent nuclear fuel; thus, the spent fuel caskets are not to be remain stored on-site for long time periods. (IAEA 2005b, 383, 386, 388-389; Romenkov 2009, 393-394).

An underwater canal connects the spent fuel pool and the reactor pool, through which the FAs (fresh and spent) are transferred during refueling. Refueling is mentioned to be similar to research reactors. Little information is available about refueling operations, but the reactor hall includes at least fuel handling and transfer equipment such as refueling machine and crane along with reactor bridge. Plans for automatic verification and registration of indexed FAs to facilitate NMA and IAEA verification during fuel transfers has been considered. Fresh fuel receiving and storage areas are located adjacent to reactor compartment. It is likely that fresh FAs are transferred to the spent fuel pool storage racks before refueling. The design information doesn't mention a separate pool for fuel handling operations and loading of spent fuel caskets. (Romenkov 2009, 394; IAEA 2005b, 391, 393, 402-403).

RUTA-70 reactors are to be utilized in the industrial sector for district heat production, seawater desalination, or both purposes, especially in isolated locations. Thus, design considerations have been made for extended fuel cycle length using Cermet fuel with below 20% U-235 enrichment and discharge burnup of 100 MWd/kg. The core inventory would remain closed for a longer period and the frequency of fuel handling and transfer operations

associated with refueling would be reduced. Thus, the aim is to increase PR by minimizing fuel storage inventories (spent or fresh) and refueling operations, which comprise significant paths for diversion. (Kozmenkov et al 2012, 4).

Furthermore, the application of RUTA-70 as a neutron source for research and material production has been considered. The design descriptions introduce different kinds of irradiation channels and associated handling/transfer equipment for target insertion/removal. The irradiation channels are located above the core in tube structures which are lowered into the core. In addition, external irradiation devices with horizontal neutron beam channels have been designed for radiation therapy and to produce track membranes. (Romenkov 2009, 395-396; Cherepnin et al 2007, 12-15).

9.2.1 Challenges and similarities

Appendix 14 presents PNNL FSA tool results for RUTA-70. From this evaluation potential safeguards challenges (table 20) and similarities have been identified when compared to conventional LWR. In addition, insights related to research reactor design have been considered.

The pool-type reactor design that is typical for research reactors may be feasible for target irradiation. The reactor thermal power (70 MW) is over minimum required for plutonium production (25 MW); thus, it is suitable for undeclared production from fertile targets (Pan et al. 2012, 15-18). The design has already considered the use of RUTA-70 as a neutron source for irradiation purposes by incorporating irradiation channels and associated handling/transfer equipment. This could indicate the ease of modifications of such design to achieve facility misuse aims.

The planned multi-use of RUTA-70 for both commercial district heat production and research activities is problematic for safeguards implementation. The research facilities alone may support a range of flexible uses, which can decrease the transparency of facility operations (Pan et al. 2012, 18-19).

Table 20. Challenges of RUTA-70 design when compared to conventional LWR safeguards.

Challenge	Description	Main cause	Possible solution
Reactor design feasible for facility misuse	The pool-type reactor design that consists of a reactor core immersed in a closed reactor pool is typical for research reactors. The design has already considered features such as irradiation channels and chambers that would be incorporated to allow research reactor use. Such design provisions indicate the ease of technical modifications that could be implemented to facilitate irradiation of target material for undeclared material production.	Research reactor design	The SA should highly consider detection of facility misuse.
The sealing of core	The design doesn't include a conventional pressure vessel. The RV seems to consist of metal-lining of the reactor pool (vault section). The chimney barrel is within the vessel and extends out from it at the upper section. Distributing header is connected to upper chimney barrel and collecting header to upper vessel section. From the design descriptions it remains uncertain whether reactor core could be appropriately sealed.	RV configuration	If the sealing is not applicable, the SA could consider the sealing of the pool.
Double stacking of spent FAs	The FAs are around half-height when compared to VVER-440. This may allow double stacking of spent FAs in the storage racks. It would make verification measures such as visual checks and NDA measurements more difficult because the upper-level assemblies must be moved to gain access to the FAs on the lower level.	Short FAs	The double stacking should not be used. Otherwise, the lower layers could be sealed.
Potential to conceal facility misuse	If both district heating production and research activities are conducted simultaneously, it could ease the concealment of facility misuse. Verification would be more complicated due to a vast number of different operations. Furthermore, it could be easier to falsify operational records.	Incorporation of features for research use	The reactor should be used in only one application area.

Simultaneous research activities further complicate NMA and verification, especially if they involve NM such as uranium and plutonium as loose items (Pan et al. 2012, 15). The baseload district heat production at stable power level along with simultaneous research use would provide favourable circumstances for misuse of irradiation channels and concealment. Thus, such an arrangement requires a complex SA that would increase the burden of IAEA verification.

The FSA tool results indicate that, there are no significant differences in NMA and verification. RUTA-70 utilizes similar fuel that is used in VVER-440 reactors or slightly different Cermet fuel, both permit conventional item accountability. The pool-type reactor design is somewhat familiar to IAEA since SAs have already been implemented to similar

research reactors. The general plant process and characteristics are same when compared to conventional LWR. The single MBA approach with conventional IKMPs and FKMPs is suitable. The implementation of measures to provide NMA records and associated reports are essentially the same. Furthermore, IAEA verification relies on the use of similar measures and equipment. However, it should be noted that detailed design information must be reviewed to have more precise evaluation.

9.3.1 Safeguards approach

A rough SA based on insights from the literature has been presented in table 21 for RUTA-70. The access points in the containment, NM storage areas, and other shielded structures in which fuel transfers occur should be minimized to simplify the application of C/S and monitoring. If the limited fuel transfer routes in the facility have been planned appropriately, safeguards equipment such as surveillance cameras and radiation monitors can be set in strategic points to maintain CoK for fuel transfers. Such transfers include fresh fuel to the spent fuel pool and spent fuel caskets to the shipment area. The sealing of containers during transfers could be utilized if applicable. (Pan et al. 2012, 22; Reid et al. 2016, 15).

The fuel transfer canal can be equipped with a radiation monitor to indicate fuel transfers between the reactor pool and the spent fuel pool. In addition, sealing can be applied to the transfer canal for tamper-indication. The sealing of the RV or reactor pool lid could be done if possible. An indexing system along with underwater surveillance cameras can be utilized to monitor fuel transfers between spent fuel storage racks and the core. In addition, surveillance cameras should be mounted in storage rooms (fresh fuel and spent fuel), reactor hall, and above spent fuel pool. A surveillance camera could be attached to the refueling machine to monitor individual FA insertions/removals and to verify fuel items by their index numbers. The fresh FAs/containers and spent fuel caskets/containers could be sealed in storage areas. The sealing of storage room openings and doors may also be beneficial. (Pan et al. 2012, 22-28).

Table 21. A rough SA for RUTA-70.

Location/pathway	Safeguards equipment
Fresh fuel storage	Surveillance cameras, radiation monitors, sealing of fresh fuel containers/assemblies, sealing of access openings, sealing of door
Transfer pathway from fresh fuel storage to spent fuel pool	Surveillance cameras and radiation monitors at limited access points, equipment monitoring, sealing of equipment
Spent fuel storage pool	Surveillance cameras (above pool and underwater), sealing of low-layer FAs (if double stacked)
Fuel transfer canal	Radiation monitor, sealing of canal gate
Reactor hall	Surveillance cameras (hall area and refueling machine), equipment monitors, sealing of equipment (crane, refueling machine)
Reactor pool/vessel	Surveillance cameras (underwater), sealing of RV, sealing of reactor pool lid
Transfer pathway from spent fuel storage to shipment area	Surveillance cameras and radiation monitors at limited access points, equipment monitors, sealing of spent fuel caskets, sealing of equipment
Spent fuel storage	Surveillance cameras, radiation monitors, sealing of spent fuel containers/caskets, sealing of access openings, sealing of door.

The use of equipment monitors to indicate on-power state and usage of fuel handling /transfer equipment could be considered. Equipment monitors could be simple power indicators that would log when power was turned on/off or a combination of measures that would also log equipment position. For example, such a monitor could be attached to a refueling machine and a reactor hall crane. Equipment monitors with surveillance cameras could be attached to transport containers or equipment to maintain CoK for fresh fuel container/spent fuel casket transfers in or out of the plant, if applicable. Furthermore, the sealing of handling/transfer equipment could be an option. (Coles et al. 2013, 19; IAEA 2012, 20-21; Pan et al. 2012, 27; Raid et al. 2016, 15).

The RV design should be further reviewed for potential problems associated with the sealing. Another approach could be to consider the sealing of the reactor pool; however, it is uncertain whether this can be appropriately implemented.

9.3 KLT-40S (Akademik Lomonosov)

KLT-40S has a small reactor core that consists of 121 hexagonal FAs, each having a variable amount of fuel rods (68, 72, or 75). The core design is based on the KLT-40 reactor, which is used in nuclear icebreakers. Fuel rods are structurally the same as those of KLT-40 and burnable absorber rods are similar in design. The fuel is Cermet, which consists of UO_2 particles dispersed in an aluminium alloy (Al + Si) matrix. The average U-235 enrichment is mentioned to be 14,1 m% and a maximum below 20 m%. Several core studies have considered a maximum value of 18,6 m%. The core is designed with a closely packed cassette structure to maximize the number of fuel rods and fuel volume for increased fuel cycles. The FA's total height is 1600 mm, and the active core height is 1200 mm. The initial uranium load in the core is 1273 kg. (JSC OKBM 2013, 6-7,10, 30; Faisal et al. 2020, 1775-1776; Beliaevskii et al. 2020, 3; Baybakov et al 2016, 185).

The midship of the barge incorporates a fresh fuel storage room, fuel handling compartment, reactor compartment, spent fuel and radioactive waste storages. Two reactor units are in the reactor compartment inside their own containment structures. The interim spent fuel storage includes three wet storage tanks, each of which can store a full inventory of one core. The dry spent fuel storage comprises four dry containers each capable of holding an inventory from one reactor core in ChT-14 type spent fuel canisters. (JSC OKBM 2013, 8-9, 21-22).

The barge incorporates onboard fuel handling complex, that is designed to perform the entire technological cycle of fuel handling and transfers. Such operations involve loading onboard and transfers to fresh fuel storage, loading of fresh fuel from storage into core, unloading of spent fuel from the reactor, their transfers and placement into wet storage tanks, subsequent transfers into dry storage containers, preparation and unloading of spent fuel caskets out of the barge. The reloading system is mentioned to be standard, automated and includes monitoring. It consists of individual units transferred into the equipment room as operations are completed. The design is the first integrated complex onboard but is based on technology used in nuclear-powered vessels. (JSC OKBM 2013, 8-9; Dushev et al. 2020, 84-85; Fadeev 2011, 14). Figure 48 demonstrates the fuel handling process of KLT-40S.

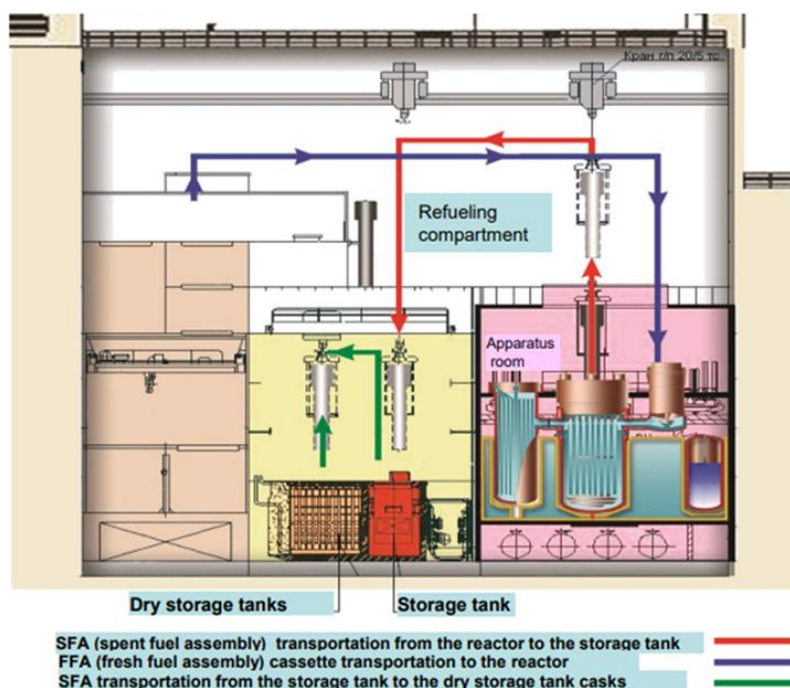


Figure 48. The fuel handling diagram of KLT-40S (Fadeev 2011, 14).

The FNPP is intended to be used as an autonomous unit in isolated areas for cogeneration or sea water desalination. For this purpose, the barge is loaded with fresh fuel inventory to achieve completion of four fuel cycles per reactor unit. The refuelling cycle is 2,5 – 3 years and single loading with replacement of all FAs is applied. The refuelling is done in turns for two RPs. The average discharge burnup is mentioned to be 45,4 MWd/KgU. The discharge of spent FAs is done after 13 days of shutdown, when the decay heat generation is still high. In addition, maintenance is done onboard using in-house equipment and doesn't require coastal power supply. (JSC OKBM 2020 11-12, 20; JSC OKBM 2013, 8-10; Faisal et al. 2020, 1775).

The barge is transported to a specialized maintenance centre after four fuel cycles and 10-12 years of operation. The plant goes through a complete overhaul that takes up to 1 year. All spent fuel is unloaded from the barge, reactors are refuelled, and fresh fuel storage is loaded with a total inventory of six fuel cycles. The spent fuel is planned to be reprocessed in a similar manner as it is done in existing factories for fuel from naval reactors. (Belyaev et al. 2020, 28-29; Faisal et al 2020, 1775; JSC OKBM 2013, 21).

JSC OKBM has proposed a build-own-operate scheme to commercialize FNPPs in other countries. For this operation scheme, the plant will be under the jurisdiction of the Russian Federation all the time and it will be serviced by Russian personnel only. The barge will be

always refuelled in maintenance centres provided by Russia, which aims to enhance PR. The spent fuel is unloaded from the barge to the supplier country and maintenance is performed at these centres. This kind of approach may lead to the exclusion of the fuel handling complex and storage. Such arrangement necessitates negotiations for agreements about physical security, safeguards, and plant operation between Russian Federation and the buyer state. Such agreements deal with the inviolability of the plant, PP, conduction of IAEA verifications, and guarantees of services not related to ownership rights for the plant. (JSC OKBM 2020, 27; JSC OKBM 2013, 17-18).

9.3.1 Challenges and similarities

Appendix 15 presents a trial FSA for KLT-40S that is done using the tool provided by PNNL. From this evaluation potential safeguards challenges (table 22) and similarities have been identified when compared to conventional PWR. The challenges are associated with design aspects such as movable, barge-type design, onboard fuel handling complex, and operational plans.

The barge-type design allows movable plant, which can be towed at sea. This makes it possible to have extreme diversion scenarios where all physical barriers will be eliminated and the whole NM inventory is promptly diverted. However, it is easy to detect such scenarios if the FNPP is under surveillance.

Onboard fuel handling complex provides capabilities to handle and transfer FAs. The system is essentially important for spent fuel that is radioactive and generates decay heat. The proliferator may take benefit of such a system to achieve diversion aims. Such a complex combined with movable design and potential to have the plant in remote difficult to access areas supports diversion scenarios. The PR would be improved if the fuel handling complex and storages are excluded from the design. Therefore, centralizing refuelling and maintenance in specified docks could be a good option.

The FNPP is to be loaded with nuclear inventory corresponding to a total of eight fuel cycles. Six core inventories of fresh fuel (7 638 kg U) are at storage, and two inventories (2546 kg U) are loaded in reactor units. As the average enrichment is 14,1 m%, around 1436 kg U-235 is onboard. Such amount corresponds to 19 SQ for U-235.

Table 22. Challenges of KLT-40S design when compared to conventional PWR safeguards.

Challenge	Description	Main cause	Possible solution
Extreme diversion scenarios	The FNPP is movable, thus eliminating all physical barriers at IKMPs. This creates a potential for extreme scenarios where the whole nuclear inventory can be promptly diverted.	The barge-type design	SA should consider measures to maintain CoK for the barge. Such measures could involve surveillance cameras at coastal and sea areas.
Capability to handle/transfer fuel onboard	The capability to handle and transfer FAs onboard supports proliferation aims.	Onboard fuel handling complex	Exclusion of fuel handling complex and storage areas. Centralized refueling at maintenance centers.
Large NM inventory onboard	The barge is intended to be loaded with fresh fuel inventory to complete a total of 8 fuel cycles (two reactors). A high amount of spent fuel with Pu and U-235 is stored at the facility.	Operating scheme	Exclusion of fuel handling complex and storage areas. Centralized refueling at maintenance centers.
Potential to have a site in remote, difficult access area	The barge-type design is suitable to be used in remote, difficult access areas. It can be difficult for inspectors to access the site for on-site verification such as DIV and inspections. This could reduce the transparency of plant operations and detection of diversion/misuse.	The barge-type design	Unannounced inspections should be emphasized in remote areas. An effective SA that utilizes RMSs should be designed.
Safeguards/security agreements	JSC OKBM has proposed a build-own-operate scheme for barge-type plants with KLT-40S reactors. Such arrangement necessitates both safeguards and security agreements between the owner state (Russia) and the buyer state. This can be difficult to achieve due to differences in national nuclear security legislation and safeguards agreements.	Build-own-operate-scheme	Harmonization of national nuclear security legislation and the use of cooperative safeguards agreements could support this aim.

The spent fuel likely contains a quite high fraction of U-235 due to the enrichment level, and plutonium that is produced during operation. The plant incorporates a large spent fuel inventory which also corresponds to dozens of SQs. Several SQs can be transported via barge, which is a challenge.

The benefit of a FNPP is flexible siting, especially to have cogeneration in isolated areas. For example, Far-East areas in Russia are such locations. However, IAEA on-site verification such as DIV and inspections may be challenging to implement. To have frequent access to the site may necessitate much effort in arrangements such as travels and equipment transports. It may not be possible to conduct short-notice inspections. If the on-site verification is impeded due to remote, difficult access location, the transparency of plant operations is reduced. Unannounced inspections and RMSs should be emphasized.

The build-own-operate scheme requires agreements between the owner state (Russia) and the buyer state on PP and IAEA safeguards. Each state has its own nuclear security legislation and safeguards agreements with the IAEA, which complicates arrangements. In addition, the transport of FNPPs in regional and international sea areas may not comply with current agreements and guidelines. Such a scheme requires legal and contractual reviews at both national and international levels. The harmonization of security/transport requirements and the use of cooperative safeguards agreements could support the realization of the scheme.

The Cermet fuel likely not introduces significant differences when compared to conventional ceramic UO₂ fuel. The general plant design and technology of the KLT-40S plant is similar to conventional PWR plants. The reactor design is based on KLT-40 and fuel handling complex utilizes similar technologies that are used in nuclear-powered vessels. Thus, the KLT-40S doesn't involve significantly new technology that would increase efforts of IAEA. However, the FNPP as a concept differs from conventional NPPs and necessitates further reviews, especially due to movability of the plant.

The item accountability is utilized like in conventional PWRs, thus similar nuclear inventory records are maintained. The NMA and reporting are essentially the same as in conventional plants. The single MBA approach can be used and the same IKMPs. The operation schemes may lead to exclusion of FKMPs associated with receptions and shipments. This could possibly simplify NMA and ICRs. The IAEA verification is based on similar equipment, activities, and associated measures.

9.3.2 Safeguards approach

No detailed information is publicly available on the KLT-40S plant design. Despite this, a rough SA is proposed in table 23 based on open-source information. The onboard fuel handling complex covers all fuel transfers and is likely a compact system due to limited space. The system is standard, automated, and includes monitoring, which may facilitate the incorporation of IAEA equipment. An effective safeguards system could be assumed to be possible to implement for verification of storage inventories and fuel transfers. However, the compact design may also make it difficult to install verification equipment.

Normal sealing approaches could be used for storage rooms, FAs, RPV and equipment. If the fuel handling complex equipment are stored in rooms, they could be sealed. RMSs with surveillance cameras, radiation detectors, and equipment monitors would indicate transfers and maintain CoK of the inventory and operations. The coastal and sea areas should have specified locations for surveillance cameras to maintain CoK of the barge.

Table 23. A rough SA for KLT-40S.

Location/pathway	Safeguards equipment
Fresh fuel storage	Surveillance cameras, radiation monitors, sealing of fresh fuel containers/assemblies, sealing of access openings, sealing of door
Transfer from fresh fuel storage to core	Surveillance cameras and radiation monitors
Wet spent fuel storage	Surveillance cameras, sealing of wet storage tanks (if applicable)
Equipment storage(s)	Surveillance cameras, sealing of fuel handling complex equipment, sealing of door
Fuel handling compartment	Surveillance cameras, equipment monitors
Reactor compartment	Surveillance cameras, radiation monitors, sealing of containment openings
Reactor core	Sealing of RV, underwater surveillance cameras in caisson pool
Transfer from core to wet spent fuel storage	Surveillance cameras and radiation monitors
Transfer from wet spent fuel storage to dry spent fuel storage	Surveillance cameras and radiation monitors
Dry spent fuel storage	Surveillance cameras, radiation monitors, sealing of spent fuel containers/caskets, sealing of access openings, sealing of door
Coastal and sea areas	Surveillance cameras at specified locations to maintain CoK for the barge

10. Discussion

The systematic implementation of DiD has been emphasized in the safety designs of studied SMRs. The systems performing the three fundamental SFs (subcriticality, heat removal, and confinement) have been clearly separated between Operational States (Level 1 and 2) and ACs (Level 3 and 4). It is common that the latter tend to be passive Safety Systems and the former are active Operational Systems. Dependencies between defence levels can be noticed for heat removal systems.

Often safety-related systems for decay heat removal (passive or active) have been credited in both level 2 (AOOs) and 3 (DBAs). In addition, passive Safety Systems for reactor and containment heat removal/depressurization tend to be utilized in accidents in both levels 3 and 4 (DECs). Safety Systems in multiple defence levels could be justified due to more reliable performance of passive Safety Systems, however functional dependencies may still exist between SSCs and should be carefully evaluated to ensure the strength of individual levels. The subcriticality and confinement systems are more evidently separated into different levels, however, other plant systems such as I&C should be reviewed for possible functional dependencies. KLT-40S includes many Safety Systems for heat removal and some are credited for both DBAs and severe accidents, which is problematic. The defence levels should be as independent as reasonable is achievable.

From all safety designs the endeavour to enhance and strengthen the defence level 4 can be noticed. The combination of passive Safety Systems, inherent and design features is utilized to control DECs and mitigate consequences if were to occur. This is achieved by maintaining reliable decay heat removal, subcriticality control, and containment integrity. Especially, such improvement can be perceived in decay heat removal. Some designs (NuScale and RUTA-70) aim to practically exclude severe accidents, which may be justified due to inherently safe designs with large water inventories and reliable passive heat removal from structures. Common to three SMR designs (NuScale, RUTA-70 and KLT-40S) is, that they follow in-vessel retention strategy to control severe accidents with core melt, although such events are unlikely to occur. The basic concept is the same; the prolonged passive cooling of the RV is maintained by ensuring sufficient water inventories at pools, and additional

make-up water is provided if deemed necessary (equipment and organizational strategies). The reactor designs are suitable to realize such a strategy.

The utilization of inherent safety features such as low core inventory, low power density, large water inventory, and effective heat conduction is evident, and it has provided enhancements in reactor safety. Especially, NuScale and RUTA-70 (non-pressurized primary circuit) take benefit of the above-mentioned inherent features, and these can be considered to have a significant contribution to their safety designs. KLT-40S also utilizes such inherent features, excluding low power density, but the safety design is not as distinctly based on them. It should be noted that BWRX-300 is quite similar to conventional BWR designs, core inventory and thermal power are much higher when compared to the other three SMR designs. Nevertheless, BWRX-300 includes conventional inherent features such as negative reactivity coefficients, high thermal inertia, and low core power density. In addition, heat conduction from containment to the surrounding ground may be considered an inherent feature for BWRX-300.

The safety of SMRs has been enhanced when compared to conventional LWRs by incorporation of design features such as integral/compact NSSS, short/coaxial pipelines, reduced number of RPV nozzles with smaller diameters, RPV inside CNV, large diameter pipelines inside PCV with double isolation valves. The aim has been to preserve coolant inventory and prevent events that could lead to LOCAs (DBAs). In addition, design improvements have been implemented to prevent system failures, that could cause AOs. Thus, strengthening of both defence levels 2 and 3 have been aimed. Especially such design improvements have been utilized in BWRX-300 and KLT-40S safety implementation. The passive Safety Systems and other design features have made it possible to exclude some systems such as ECCS HPSI/LPSI, hydro accumulators, containment sprinklers, relief/safety valves, and suppression pools (BWR). However, the KLT-40S includes some conventional PWR Safety Systems, understandable as it has been a pioneer LWR SMR design.

The passive Safety Systems utilize natural phenomena such as natural circulation, convection, conduction, boiling and evaporation, gravity, pressure differences. Such principles simplify systems designs and may reduce functional dependencies if appropriately designed. Thus, the number of Safety Systems has been reduced when compared to conventional LWRs. The passive systems likely enhance reliability, since they do not require external power supply, logic, operator interventions, and they fail-safe to actuate SFs. KLT-

40S has also many active Safety Systems credited in ACs, which makes it a more complex design when compared to the other three SMRs. It can be noticed that fundamental principles of passive reactor/containment heat removal systems are somewhat the same for all designs, which indicates maturation of safety design. The larger water inventories/inherent features of the other three SMRs have prolonged the operation time without additional make-up water when compared to the KLT-40S design.

The four SMR designs have the potential to fulfilling requirements associated with Safety System design. Many requirements of YVL B.1, originally have drawn up for conventional LWRs are likely to be fulfilled. Especially, inherent features and passive Safety Systems seem to support the accomplishment of requirements on decay heat removal. However, some Safety System requirements demand the inclusion of certain technical systems such as diverse subcriticality control system, which may not be considered necessary due to improved safety. This could apply to designs such NuScale and RUTA-70 if it has been appropriately justified. BWRX-300 as a similar design when compared to conventional BWR follows current Safety System requirements, the higher thermal power and larger core inventory could demand this if not demonstrated otherwise. The lack of information and several Safety Systems make it difficult to evaluate KLT-40S, the systems could be further reviewed for potential functional dependencies between systems in different defence levels. Nevertheless, the commissioning of Akademik Lomonosov could indicate, that current safety requirements have been met.

The security design of the three SMRs (NuScale, BWRX-300, and KLT-40S) follows the same DiD concept as has been utilized for conventional NPPs. The PPS design comprises threat evaluations derived from the DBT, target evaluations based on safety analyses, and the use of security zones within one another. The protection against threats is provided by technical and organizational measures to fulfil fundamental security functions of deterrence, detection, delay, and response. The technical design aspects involve security systems such as surveillance, detection, communication/assessment, access control systems, and physical barriers/structures. The detailed technical descriptions have been provided for systems within the plant and associated vital areas. Conceptual design has been included for site-specific PP considerations. Organizational security design aspects such as plans, procedures, policies, and provision of response forces/security organization have been highlighted but

are to be provided by the license applicant. As the information is highly confidential, detailed descriptions of security design could not be reviewed.

A notable feature of all three land-based SMR designs is to have safety-relevant SSCs placed underground. Such inherent feature can be considered to provide enhanced protection against external impacts such as security threats involving a terrorist attack (e.g. airplane crash). The security design of a FNPP such as KLT-40S is not much different when compared to land-based ones but requires consideration of challenges associated with movable barge-type design (physical barriers at sea, attacks from the sea, extreme threat scenarios, transports). Especially transport security of such plant is an issue to be solved. The potential remote location of the plant and capability to provide sufficient response against attack scenarios could be relevant for organizational security design, which is also a challenge for safeguards. In addition, the movability of the KLT-40S design introduces both security and safeguards challenges by facilitating threat and diversion scenarios.

The PPSs of three SMRs have been designed based on current security requirements that is evident for NuScale and the BWRX-300 as both follow NRC security requirements of conventional NPPs. The tentative evaluations of YVL A.11 for NuScale and BWRX-300 indicate the fulfilment of most technical security requirements. The technical side of plant security is not a concern for SMRs. However, the technical system is not sufficient alone, organizational security design has an essential significance in implementing successful security. The evaluation of requirements on organizational security would necessitate information from SMR projects, which have been progressed towards the construction phase. Akademik Lomonosov with KLT-40S reactors could provide such insights since it has already been commissioned. The organizational design would be an important aspect to be considered for SMRs as some designs are to be operated near the public (RUTA-70) and others in remote areas (KLT-40S) for district heating / cogeneration. Between these extremes are plants for electric production (NuScale and BWRX-300) that can be sited at sufficient distances from the public as conventional NPPs. In addition, the potential spread of multiple SMRs in many areas may also require further evaluation of organizational security such as the provision of response forces, guarding, and assessment of monitors.

An interesting issue between safety and security is whether the improved inherent safety of SMR designs such as RUTA-70 and NuScale (single modules) could justify amendments in nuclear security requirements. For example, could organizational security requirements on

the provision of guarding, response forces, assessment of security systems, and defensive arrangements such as command centers be relaxed to some extent when compared to conventional NPPs. The SMRs utilized for district heating are to be sited near the consumers, thus local authorities or private security services could provide such security arrangements. However, the variation in the designs is somewhat considerable, BWRX-300, KLT-40S, and multimodule NuScale likely require security arrangements of current regulatory practice. To justify such amendments careful safety/security evaluations and demonstrations within the risk-based graded approach would be required. Thus, it would be useful to study the influence of organizational security aspects on PPS and SMR plant safety in depth.

The implementation of safeguards for LWR SMRs can be based on similar technical equipment and follow the same approaches of NMA and IAEA verification. Such is not surprising since similar fuel items are used in conventional LWRs, and general plant design or process is not significantly different. However, more in-depth evaluation of technical SA necessitates detailed design information and may reveal differences in implementation of safeguards barriers between plant designs. One issue to consider would be to map out the design differences that make on-site verification activities difficult.

Safeguards challenges can be identified for three SMRs in concern. These are both technical design and operational-related issues. The presence of multiple modules with staggered refueling times in a common area causes challenges for NuScale. Its SA must be able to maintain CoK of all nuclear inventories and verify frequent operational activities related to refueling. The large area and frequent activities likely necessitate many OSPs with safeguards equipment. The nuclear inventory is not applicable to be verified for all modules within a certain time interval due to different refueling schedules, thus emphasizing the significance of NMA records and measures for maintaining CoK. The conventional sealing approaches necessitate the increased presence of inspectors and make both on-site verification and plant operations more difficult.

The potential safeguards challenges of RUTA-70 are associated with facility misuse. The pool-type reactor design may be more feasible for design modifications, that allow undeclared material production by target irradiation. The proposed plans of simultaneous research use of the reactor decrease the transparency of plant operations and makes verification more complex. The incorporation of irradiation channels would allow capability for misuse aims, which could be concealed during district heating production.

The movability of FNPP is a main safeguards challenge for KLT-40S. A large nuclear inventory is to be stored in such barge and fuel handling/transfer capability is provided onboard. Dozens of SQs could be transported and unloaded from the barge in remote areas, that makes extreme diversion scenarios possible. Such challenges could be eliminated, and PR improved if refueling and maintenance is to be done in specified docks. The remote, difficult to access location of the barge may be an issue for on-site verification.

Furthermore, the case study has provided some insights on SBD. It seems that safeguards aren't yet prominent in design, since there is little information available in plant descriptions. This could be because safeguards seem to lack common requirements and guidelines of technical designs relevant for safeguardability. Confidentiality may also be reason for this.

The development work of ORSAC indicates, that it is possible to integrate 'the 3S' in such a representative framework. Many analogies and commonalities between safety, security and safeguards can be found. It seems that connections can be found between all these three. The DiD can be used as basis for integration of all '3S', and similar concepts can be proposed for both security and safeguards. Barrier thinking forms the structural DiD, though these are not always considered to be individual physical structures. The functional DiD is the measures for prevention and mitigation along with progressive levels. Concerning security, maintaining the integrity of barrier (security zone/threat level and associated PP measures) is achieved by security systems and organizational measures. For safeguards, maintaining the integrity of barrier (SA) is by the NMA (operator) and verification activities (IAEA). The levels and associated events with acceptance criteria (dose/SQ) makes it possible to connect such concepts.

The ORSAC should be developed further by using detailed information on both plant security and safeguards. The use could be demonstrated for security by placing technical systems and organizational measures on ORSAC. Organizational aspects such as security arrangements, NMA, and on-site verification should be emphasized more since the technical design is highly related to them. This is because both PPS and SA necessitate human activities (guarding, communication, assessment, response, verification activities). The in-depth study of security and safeguards could provide more insights into overall safety. Such aspects as cyber security and cooperation between IAEA and the operator (joint use of equipment) could be worth studying.

11. Summary

The first aim of this master's thesis has been to contribute to ORSAC framework development by considering Security and Safeguard related issues further in the theory part. The second aim of this thesis has been to provide insights on Safety, Security, and Safeguards (the '3S') in the context of SMRs. The focus has been to evaluate designs with respect to current requirements and safeguardability

The development work of ORSAC indicates, that it is possible to have the '3S' in such a representative framework. The DiD is the basis for integration of all '3S', and similar concepts can be proposed for both security and safeguards using 'barrier thinking'. The levels and associated events with acceptance criteria (dose/SQ) makes it possible to connect such concepts.

The systematic implementation of DiD has been emphasized in the safety designs of studied SMRs. The endeavour to improve the defence level 4 can be noticed. The utilization of inherent safety features is evident and has provided enhancements in safety. The number of Safety Systems has been reduced when compared to conventional LWRs using passive Safety Systems, which utilize natural phenomena and could be more reliable. Designs have the potential to fulfilling requirements of YVL B.1 associated with Safety System design.

The security design of the three SMRs (NuScale, BWRX-300, and KLT-40S) follows the same DiD concept as has been utilized for conventional NPPs. A notable feature of all three land-based SMR designs is to have safety-relevant SSCs placed underground. The PPS design of a FNPP such as KLT-40S is not much different when compared to land-based ones. The tentative evaluations of YVL A.11 for NuScale and BWRX-300 indicate the fulfilment of most technical security requirements.

The implementation of safeguards for LWR SMRs can be based on similar technical equipment and follow the same approaches of NMA and IAEA verification. The presence of multiple modules with staggered refueling times in a common area causes challenges for NuScale. The potential safeguards challenges of RUTA-70 are associated with facility misuse. The movability of FNPP is a main safeguards challenge for KLT-40S. Common requirements or guidance for technical implementation would benefit safeguards

References

- Baybakov, D.F., A.V. Godovikh, A.V, Martynov, I.S, Nesterov, V.N. 2016. The dependence of the nuclide composition of the fuel core loading on multiplying and breeding properties of the KLT-40S nuclear facility. Nuclear Energy and Technology. Vol 2. No. 3. National Research Tomsk Polytechnic University. Institute of Physics and Technologies. Tomsk. Russia.183-190 pp.
- Beliaev, V & Polunichev, V. 2000. Basic Safety Principles of KLT-40C Reactor Plants. XA0056266. OKB Mechanical Engineering. Nizhny Novgorod. Russia. 29-39 pp.
- Beliavskii, Sergei V., Nesterov, Vladimir N., Laas, Roman A., Alexei V. Godovikh, Alexei V., Bulakh, Olga I. 2020. Effect of fuel nuclide composition on the fuel lifetime of reactor KLT-40S. Nuclear Engineering and Design. Vol. 360. Division of Nuclear-Fuel cycle. School of Nuclear Science & Engineering. National Research Tomsk Polytechnic University. Tomsk. Russia. 1-7 pp.
- Belyaev, V.M., Bol'shukhin, M.A., Pakhomov, A.N., Khizbullin, A.M, Lepekhin, A.N., Polunichev, V.I. Veshnyakov, K.B, Sokolov, A.N, Turusov, A. Yu. 2020. The World's First Floating NPP: Origination and Direction of Future Development. Atomic Energy. Vol. 129. No. 1. 27-34 pp.
- Coles, G.A, Hockert, J., Gitau, E.T, Zentne, M.D. 2013. Trial Application of the Facility Safeguardability Assessment Process to the NuScale SMR Design. PNNL-22000. Rev. 1. Pacific Northwest National Laboratory. Richland. Washington. 96 pp.
- Dowdall, Mark & Standring, William J.F. 2008. Floating Nuclear Power Plants and Associated Technologies in the Northern Areas. StrålevernRapport 2008:15. ISSN 0804-4910. Norwegian Radiation Protection Authority (Statens strålevern). Østerås. Norway. 61 pp.
- Dushev, S.A., Timofeev, A.V., Ermakov, A.V., Danilov, S.D., Plotnikov, I.V., Abrosimov, A.D. 2020. Refueling Complexes and Equipment for Civilian and Naval Ship Reactor Installations: Creation and Development. Atomic Energy. Vol. 129. No. 2. 80-86 pp.

- Fadeev, Yuru P. 2011. KLT-40S reactor plant for the floating CNPP FPU. In Proceedings of the IAEA Interregional Workshop on Advanced Nuclear Reactor Technology for Near-Term Deployment. Vienna. Austria. 4–8 July 2011. JSC “Afrikantov OKBM”. Russian Federation. 58 pp.
- Faisal, Dhirar. Agung, Alexander. Harto, Andang Widi. 2020. The Study of Floating Nuclear Power Plant Reactor Core Neutronic Parameters Using Scale 6.1 Code. International Journal on Advanced Science Engineering and Information Technology. Vol.10. No.5. 1774-1783 pp.
- Finnish Government. 2008. Government Decree (733/2008) on the Safety of Nuclear Power Plants. Decree. Helsinki 27.11.2008. 7 pp.
- GE-Hitachi. 2011. ESBWR Plant General Description. GE-Hitachi Nuclear Energy. 201 pp.
- GE-Hitachi. 2014a. ESBWR Design Control Document - Tier 1. 26A6641AB. Rev.10. GE-Hitachi Nuclear Energy Americas LLC. 853 pp.
- GE-Hitachi. 2014b. ESBWR Design Control Document - Tier 2. Chapter 13 - Conduct of Operations. 26A6642BL. Rev.10. GE-Hitachi Nuclear Energy Americas LLC. 22 pp.
- GE-Hitachi. 2014c. ESBWR Design Control Document - Tier 2. Chapter 4 Reactor. 26A6642AP. Rev. 10. GE-Hitachi Nuclear Energy Americas, LLC. 180 pp.
- GE-Hitachi. 2019. Status Report – BWRX-300. IAEA ARIS Database. GE-Hitachi and Hitachi-GE Nuclear Energy. United States of America. 38 pp.
- GE-Hitachi. 2021a. GE Hitachi Nuclear Energy Advances Efforts to License BWRX-300 Small Modular Reactor. [Website]. [updated 23.2.2021, cited 25.11.2021]. Available: <https://www.ge.com/news/press-releases/ge-hitachi-nuclear-energy-advances-efforts-to-license-bwrx-300-small-modular-reactor>
- GE-Hitachi. 2021b. Licensing Topical Report - BWRX-300 Reactivity Control. NEDO-33912-A. Rev.1. ML21060B579. GE-Hitachi Nuclear Energy Americas, LLC. 87 pp.
- GE-Hitachi. 2021c. Licensing Topical Report - BWRX-300 Reactor Pressure Vessel Isolation and Overpressure Protection. NEDO-33910-A. Rev.2. ML21183A262. GE-Hitachi Nuclear Energy Americas, LLC. 219 pp.

- GE-Hitachi. 2021d. Licensing Topical Report - BWRX-300 Containment Performance. NEDO-33911-A. Rev.2. ML21118A015. GE-Hitachi Nuclear Energy Americas, LLC. 210 pp.
- GIF. 2011. Evaluation Methodology for Proliferation Resistance and Physical Protection of Generation IV Nuclear Energy Systems. PR&PP Evaluation Methodology Report (Rev.6). the Generation IV International Forum (GIF). 94 pp.
- Hyvärinen, Juhani. Kauppinen, Otso-Pekka. Vihavainen, Juhani. 2016. Overall Safety Conceptual Framework – ORSAC. Revision 1. Lappeenranta University of Technology. Lappeenranta. 78 pp.
- Hyvärinen, Juhani. 2021. 7th Overall Safety Seminar. Presentation. SAFIR2022. 3.9.2021.
- IAEA. 1983. IAEA Safeguards: Aims, Limitations, Achievements. IAEA Safeguards Information Series. No.4. ISBN 92-0-179283-2. International Atomic Energy Agency (IAEA). Vienna. 42 pp.
- IAEA. 2002. IAEA Safeguards Glossary - 2001 Edition. International Nuclear Verification Series. No. 3. ISBN 92-0-111902-X. International Atomic Energy Agency (IAEA). Vienna. 218 pp.
- IAEA. 2005a. Assessment of defence in depth for nuclear power plants. IAEA Safety Report Series (SRS), No. 46. ISBN 92-0-114004-5. International Atomic Energy Agency (IAEA). Vienna. 120 pp.
- IAEA. 2005b. Optimization of the coupling of nuclear reactors and desalination systems Final report of a coordinated research project 1999–2003. IAEA TECDOC-1444. ISBN 92-0-102505-X. International Atomic Energy Agency (IAEA). Vienna. 327 pp.
- IAEA. 2006a. Fundamental Safety Principles. IAEA Safety Standard Series. Safety Fundamentals (SF) No. SF-1. ISBN 92-0-110706-4. International Atomic Energy Agency (IAEA). Vienna. 21 pp.
- IAEA. 2006b. Amendment to the Convention on the Physical Protection of Nuclear Material. IAEA International Law Series. No.2. ISBN 92-0-110806-0. International Atomic Energy Agency (IAEA). Vienna. 158 pp.

IAEA. 2006c. Status of innovative small and medium sized reactor designs 2005 - Reactors with conventional refuelling schemes. IAEA TECDOC-1485. ISBN 92-0-101006-0. International Atomic Energy Agency (IAEA). Vienna. 703 pp.

IAEA. 2009a. Deterministic safety analysis for nuclear power plants. IAEA Safety Standards Series. Specific Safety Guide (SSG) No. SSG-2. ISBN 978-92-0-113309-0. International Atomic Energy Agency (IAEA). Vienna. 62 pp.

IAEA. 2009b. Development, Use and Maintenance of the Design Basis Threat. IAEA Nuclear Security Series. Implementing Guide. No.10. ISBN 978-92-0-102509-8. International Atomic Energy Agency (IAEA). Vienna. 30 pp

IAEA. 2009c. Design Features to Achieve Defence in Depth in Small and Medium Sized Reactors. IAEA Nuclear Energy Series. No. NP-T-2.2. ISBN 978-92-0-104209-5. International Atomic Energy Agency (IAEA). Vienna. 264 pp.

IAEA. 2010. Development and Application of Level 1 Probabilistic Safety Assessment for Nuclear Power Plants. IAEA Safety Standard Series. Specific Safety Guide (SSG). No. SSG-3. ISBN 978-92-0-114509-3. International Atomic Energy Agency (IAEA). Vienna. 192 pp.

IAEA. 2011a. Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5). IAEA Nuclear Security Series. Recommendations. No.13. ISBN 978-92-0-111110-4. International Atomic Energy Agency (IAEA). Vienna. 55 pp.

IAEA. 2011b. Nuclear Security Recommendations on Radioactive Material and Associated Facilities. IAEA Nuclear Security Series. Recommendations. No.14. ISBN 987-92-0-112110-3. International Atomic Energy Agency (IAEA). Vienna. 27 pp.

IAEA. 2011c. Computer Security at Nuclear Facilities – Reference Manual. IAEA Nuclear Security Series. Technical Guidance. No.17. ISBN 978-92-0-120110-2. International Atomic Energy Agency (IAEA). Vienna. 69 pp.

IAEA. 2011d. Safeguards Techniques and Equipment: 2011 Edition. International Nuclear Verification Series. No. 1 (Rev. 2). ISBN 978-92-0-118910-3. International Atomic Energy Agency (IAEA). Vienna. 146 pp.

- IAEA. 2012. INPRO Collaborative Project: Proliferation Resistance: Acquisition/Diversion Pathway Analysis (PRADA). IAEA-TECDOC-1684. ISBN 978-92-0-130310-3. International Atomic Energy Agency (IAEA). Vienna. 41 pp.
- IAEA. 2013a. Objective and Essential Elements of a State's Nuclear Security Regime. IAEA Nuclear Security Series. Nuclear Security Fundamentals. No.20. ISBN 978-92-0-137810-1. International Atomic Energy Agency (IAEA). Vienna. 15 pp.
- IAEA. 2013b. Establishing the Nuclear Security Infrastructure for a Nuclear Power Programme. IAEA Nuclear Security Series. Implementation Guide. No.19. ISBN 978-92-0-138010-4. International Atomic Energy Agency (IAEA). Vienna. 83 pp.
- IAEA. 2013c. International Safeguards in Nuclear Facility Design and Construction. IAEA Nuclear Energy Series. No. NP-T-2.8. ISBN 978-92-0-140610-1. International Atomic Energy Agency (IAEA). Vienna. 22 pp.
- IAEA. 2014a. International Conference on Topical Issues in Nuclear Installation Safety: Defence in Depth — Advances and Challenges for Nuclear Installation Safety. IAEA-TECDOC-CD-1749. ISBN 978-92-0-158214-0. International Atomic Energy Agency (IAEA). Vienna. 340 pp.
- IAEA. 2014b. International Safeguards in the Design of Nuclear Reactors. IAEA Nuclear Energy Series. No. NP-T-2.9. ISBN 978-92-0-106514-8. International Atomic Energy Agency (IAEA). Vienna. 50 pp.
- IAEA. 2014c. Safeguards Implementation Practices Guide on Facilitating IAEA Verification Activities. IAEA Service Series. No. 30. ISSN 1816-9309. International Atomic Energy Agency (IAEA). Vienna. 96 pp.
- IAEA 2014d. Options to Enhance Proliferation Resistance of Innovative Small and Medium Sized Reactors. IAEA Nuclear Energy Series. No. NP-T-1.11. ISBN 978-92-0-145510-9. International Atomic Energy Agency (IAEA). Vienna. 63 pp.
- IAEA. 2016a. Safety of Nuclear Power Plants: Design. IAEA Safety Standard Series. Specific Safety Requirements (SSR) No. SSR-2/1 (Rev.1). ISBN 978-92-0-109315-8. International Atomic Energy Agency (IAEA). Vienna. 71 pp.

IAEA. 2016b. Considerations on the Application of the IAEA Safety Requirements for the Design of Nuclear Power Plants. IAEA-TECDOC-1791. ISBN 978-92-0-104116-6. International Atomic Energy Agency (IAEA). Vienna. 71 pp.

IAEA. 2016c. Safeguards Implementation Practices Guide on Provision of Information to the IAEA. IAEA Service Series. No.33. ISSN 1816-9309. International Atomic Energy Agency (IAEA). Vienna. 169 pp.

IAEA. 2016d. Guidance for States Implementing Comprehensive Safeguards Agreements and Additional Protocols. IAEA Service Series. No.21 (Rev.3). ISSN 1816-9309. International Atomic Energy Agency (IAEA). Vienna. 88 pp.

IAEA. 2017. Safety of Nuclear Fuel Cycle Facilities. IAEA Safety Standard Series. Specific Safety Requirements (SSR) No. SSR-4. ISBN 978-92-0-103917-0. International Atomic Energy Agency (IAEA). Vienna. 135 pp.

IAEA. 2018a. Regulations for the Safe Transport of Radioactive Material. IAEA Safety Standard Series. Specific Safety Requirements (SSR) No. SSR-6 (Rev.1). ISBN 978-92-0-107917-6. International Atomic Energy Agency (IAEA). Vienna. 71 pp.

IAEA. 2018b. Physical Protection of Nuclear Material and Nuclear Facilities (Implementation of INFCIRC/225/Revision 5). Nuclear Security Series. Implementing Guide. No. 27-G. ISBN 978-92-0-111516-4. International Atomic Energy Agency (IAEA). Vienna. 120 pp.

IAEA. 2018c. Safeguards Implementation Practices Guide on Establishing and Maintaining State Safeguards Infrastructure. IAEA Services Series. No. 31 (Rev.1). ISSN 1816-9309. International Atomic Energy Agency (IAEA). Vienna. 114 pp.

IAEA. 2019a. Site Evaluation for Nuclear Installations. IAEA Safety Standard Series. Specific Safety Requirements (SSR) No. SSR-1. ISBN 978-92-0-108718-8. International Atomic Energy Agency (IAEA). Vienna. 34 pp.

IAEA. 2019b. Nuclear Security Assessment Methodologies for Regulated Facilities Final Report of a Coordinated Research Project. IAEA-TECDOC-1868. ISBN 978-92-0-101719-2. International Atomic Energy Agency (IAEA). Vienna. 134 pp.

IAEA. 2020. Advances in Small Modular Reactor Technology Developments - A Supplement to: IAEA Advanced Reactors Information System (ARIS). 2020 Edition. International Atomic Energy Agency (IAEA). Vienna. 343 pp.

IAEA. 2021a. National Nuclear Security Threat Assessment, Design Basis Threats and Representative Threat Statements. IAEA Nuclear Security Series. Implementing Guide. No. 10-G (Rev.1). ISBN 978-92-0-131020-0. International Atomic Energy Agency (IAEA). Vienna. 35 pp.

IAEA. 2021b. Handbook on the Design of Physical Protection Systems for Nuclear Material and Nuclear Facilities. IAEA Nuclear Security Series. Technical Guidance. No. 40-T. ISBN 978-92-0-105419-7. International Atomic Energy Agency (IAEA). Vienna. 183 pp.

IAEA 2021c. IAEA Safeguards Overview. [Website]. [cited 28.6.2021]. Available: <https://www.iaea.org/publications/factsheets/iaea-safeguards-overview>

INSAG. 1996. Defence in depth in nuclear safety. A report by the International Nuclear Safety Advisory Group (INSAG). INSAG series No. INSAG-10. ISBN 92-0-103295- 1. International Atomic Energy Agency (IAEA). Vienna. 33 pp.

INSAG. 1999. Basic safety principles for nuclear power plants 75-INSAG-3 rev. 1. A report by the International Nuclear Safety Advisory Group (INSAG). INSAG series No. INSAG-12. ISBN 92-0-102699-4. International Atomic Energy Agency (IAEA). Vienna. 97 pp.

JSC OKBM. 2013. KLT-40S. Status Report. IAEA ARIS Database. JSC “Afrikantov OKB Mechanical Engineering” (OKBM). Nizhny Novgorod. Russia. 35 pp.

JSC OKBM 2021. KLT-40S - The KLT-40S Reactor Plants for Small-Sized Nuclear Power Plants. JSC “Afrikantov OKB Mechanical Engineering” (OKBM). Nizhny Novgorod. Russia. 28 pp.

Kozmenkov Y., Rohde U. Baranaev Yu., Glebov A. 2012. Simulations of RUTA-70 Reactor with Cermet Fuel Using DYN3D/ATHLET and DYN3D/RELAP5 Coupled Codes. Kerntechnik Vol.77. No 4. Institute of Safety Research. Forschungszentrum Dresden-Rossendorf. Dresden. Germany. SSC Institute of Physics and Power Engineering. Obninsk. Russia. 249-257 pp.

NEA/CSNI. 1998. VVER-specific Features Regarding Core Degradation. Organisation for Economic Co-operation and Development. Status Report. NEA/CSNI /R(98)20. Nuclear Energy Agency (NEA), Committee on the Safety of Nuclear Installations (CSNI), Organisation for Economic Co-operation and Development (OECD). 36 pp.

NRC. 2019. NuScale Standard Plant Design Certification Application – Chapter 13.6 - Physical Security – Safety Evaluation with No Open Items. NRC document database. www.nrc.gov/docs/ML19182/ML19182A241. [updated 16.12.2019, cited 4.10.2021]. The U.S. Regulatory Commission (NRC).

NuScale. 2019. NuScale Small Modular Reactor (SMR) Overview. Presentation for INPRO Dialogue Forum on Opportunities and Challenges in Small Modular Reactors. Held by Keng Langdon. 2.7.2019 – 5.7. 2019. Ulsan. Republic of Korea. 33 pp.

NuScale. 2020a. Status Report – NuScale SMR (NuScale Power, LLC). 2020/05/28. 28 pp.

NuScale 2020b. NuScale Standard Plant Design Certification Application. Chapter Nineteen Probabilistic Risk Assessment and Severe Accident Evaluation. Part 2 – Tier 2. Rev. 5. 424 pp.

NuScale 2020c. NuScale Standard Plant Design Certification Application. Chapter Thirteen Conduct of Operations. Part 2 – Tier 2. Rev. 5. 12 pp.

NuScale. 2020d. NuScale Standard Plant Design Certification Application. Introduction and General Description of the Plant. Part 2 – Tier 2. Rev.5. 352 pp.

NuScale. 2020e. NuScale Standard Plant Design Certification Application. Chapter Four Reactor. Part 2 – Tier 2. Rev. 5. 202 pp.

NuScale. 2020f. NuScale Standard Plant Design Certification Application. Chapter Seven Instrumentation and Controls. Part 2 – Tier 2. Rev.5. 304 pp.

NuScale. 2020g. NuScale Standard Plant Design Certification Application. Chapter Nine Auxiliary Systems. Part 2 – Tier 2. Rev.5. 806 pp.

NuScale. 2020h. NuScale Standard Plant Design Certification Application. Chapter Ten Steam and Power Conversion System. Part 2 – Tier 2. Rev.5. 151 pp.

NuScale. 2020i. NuScale Standard Plant Design Certification Application. Chapter Five Reactor Coolant System and Connecting Systems. Part 2 – Tier 2. Rev.5. 160 pp.

NuScale. 2020j. NuScale Standard Plant Design Certification Application. Chapter Six Engineered Safety Features. Part 2 – Tier 2. Rev. 5. 162 pp.

NuScale. 2021. NRC INTERACTION. Website. [updated 1.7.2021, cited 23.11.2021]. Available: <https://www.nuscalepower.com/technology/licensing>

Pan, Paul. Boyer, Brian. Murphy, Chantell. 2012. Safeguards by Design (SBD): Safeguards Guidance for Research Reactors and Critical Assemblies. LA-UR-12-26349. Los Alamos National Laboratory. 31 pp.

Polin, Roman. 2020. Technical Feasibility Assessment of RUTA-70 Nuclear Pool-Type Reactor as a Heat-Only Energy Source for District Heating Systems in Finland. Master's Thesis. Department of Energy Technology. School of Energy Systems. Lappeenranta-Lahti University of Technology (LUT University). Lappeenranta. 105 pp.

Reid, Bruce. Anzelon, George. Budlong-Sylvester, Kory. 2016. Strengthening IAEA Safeguards for Research Reactors. PNNL-25885. Pacific Northwest National Laboratory. Richland. Washington. Lawrence Livermore National Laboratory. Livermore. California. Los Alamos National Laboratory. Los Alamos. New Mexico. 59 pp.

Romenkov, A. 2009. Practical application of the RUTA safe pool-type nuclear reactor to demonstrate the advantages of atomic energy use. Int. J. Nuclear Desalination. Vol. 3. No. 4. N.A. Dollezhal Research and Development Institute of Power Engineering (NIKIET). Moscow. Russian. 390-400 pp.

STUK. 2019a. Guide YVL B.7/15.12.2019. Provisions for Internal and External Hazards at a Nuclear Facility. Regulatory Guides on Nuclear Safety (YVL). Radiation and Nuclear Safety Authority (STUK). 40 pp.

STUK 2019b. Guide YVL B.1/15.06.2019. Safety Design of a Nuclear Power Plant. Guides on Nuclear Safety (YVL). Radiation and Nuclear Safety Authority (STUK). 51 pp.

STUK. 2019c. Guide YVL D.1/24.05.2019. Regulatory Control of Nuclear Safeguards. Guides on Nuclear Safety (YVL). Radiation and Nuclear Safety Authority (STUK). 65 pp.

STUK. 2020a. Design basis threat for the use of nuclear energy and use of radiation. Memorandum 1/Y42217/2020. Radiation and Nuclear Safety Authority (STUK). 9 pp.

STUK. 2020b. Regulation STUK Y/3/2020. Radiation and Nuclear Safety Authority (STUK). Helsinki 29.12.2020. 11 pp.

STUK. 2021. Guide YVL A.11/12.02.2021. Security of a Nuclear Facility. Regulatory Guides on Nuclear Safety (YVL). Radiation and Nuclear Safety Authority (STUK). 55 pp.

Turunen, Mikko. 2020. Overall Safety of Small Modular Reactors. Master's Thesis. Department of Energy Technology. School of Energy Systems. Lappeenranta-Lahti University of Technology (LUT University). Lappeenranta. 87 pp.

WENRA. 2009. Safety objectives for new power plants. Study by the WENRA Reactor Harmonization Working Group (RHWG). Western European Nuclear Regulators' Association (WENRA). 30 pp.

Zrodnikov, A.V. Poplavsky, V.M. Baranaev, Yu.D. Sozonyuk, V.A. Gabaraev, B.A. Kuznetsov, Yu.N. Romenkov, A.A. Mishanina, Yu.A. 2004. The use of pool type nuclear reactor RUTA for municipal district heating or desalination of seawater. IAEA-CN-114/B-2. State Scientific Center of Russian Federation – Institute for Physics and Power Engineering. Moscow. Russia. Research and Development Institute of Power Engineering. Obninsk. Russia. 8 pp.

Appendix 1: The Fundamental Safety Principles (IAEA 2006a)

Principle	Description
1: Responsibility for safety	The prime responsibility for safety must rest with the person or organization responsible for facilities and activities that give rise to radiation risks.
2: Role of government	An effective legal and governmental framework for safety, including an independent regulatory body, must be established and sustained.
3: Leadership and management for safety	Effective leadership and management for safety must be established and sustained in organizations concerned with, and facilities and activities that give rise to, radiation risks
4: Justification of facilities and activities	Facilities and activities that give rise to radiation risks must yield an overall benefit
5: Optimization of protection	Protection must be optimized to provide the highest level of safety that can reasonably be achieved.
6: Limitation of risks to individuals	Measures for controlling radiation risks must ensure that no individual bears an unacceptable risk of harm.
7: Protection of present and future generations	People and the environment, present and future, must be protected against radiation risks.
8: Prevention of accidents	All practical efforts must be made to prevent and mitigate nuclear or radiation accidents.
9: Emergency preparedness and response	Arrangements must be made for emergency preparedness and response for nuclear or radiation incidents.
10: Protective actions to reduce existing or unregulated radiation risks	Protective actions to reduce existing or unregulated radiation risks must be justified and optimized.

Appendix 2. INPRO PR evaluation table for material barriers (IAEA 2012)

Basic Principle: PR intrinsic features and extrinsic measures shall be implemented throughout the full life cycle for INS to help ensure that INS will continue to be an unattractive means to acquire fissile material for a nuclear weapons programme. Both intrinsic features and extrinsic measures are essential, and neither shall be considered sufficient by itself.								
User requirement UR2: The attractiveness of nuclear material and technology in an INS for a nuclear weapons programme should be low.								
Indicators IN	Evaluation Parameter EP		Evaluation Scale*					Acceptance Limit (AL)
			VW	W	M	S	VS	
IN 2.1: Material quality	EP2.1.1: Material type/ category		UDU	IDU	LEU	NU	DU	AL2.1: Attractiveness considered in design of INS acceptably low based on expert judgment (EJ)?
	EP2.1.2: Isotopic composition	²³⁹ Pu/Pu (wt %)		(59.9) > 50		< 50		
		²³² Ucontam. for ²³³ U (ppm)	< 400	400~1000	1000~2500	2500~25000	> 25,000	
	EP2.1.3: Radiation field	Dose (mGy/hr) at 1 metre	< 150	150~350 (150mGy/hr γ)	350 ~ 1000	1000~10000	> 10000	
	EP2.1.4: Heat generation	²³⁸ Pu/Pu (wt %)		(1.7) < 20		> 20		
EP2.1.5: Spontaneous neutron	²⁴⁰ Pu+ ²⁴² Pu / Pu (wt %)		(~30)**					
IN 2.2: Material quantity	EP2.2.1a: Mass of an item (kg)		10	10~100 (17.64 kg)	100~500	500~1000	>1000	AL2.2: Attractiveness considered in design of INS acceptably low based on expert judgment (EJ)?
	EP2.2.1b: Mass of bulk material for SQ (dilution) (kg)		10	10~100	100~500	500~1000	>1000	
	EP2.2.2: No. of items for SQ		1	1~10	10~50 (49)	50~100	>100	
	EP2.2.3: No. of SQs (material stock or flow)		>100	50~100	10~50	10~1	< 1	
IN 2.3: Material classificati on	EP2.3.1: Chemical/ physical form	U	Metal	Oxide/ Solution	U compounds	Spent fuel	Waste	AL 2.3: Attractiveness considered in design of INS acceptably low based on expert judgment (EJ)?
		Pu	Metal	Oxide/ Solution	Pu compounds	Spent fuel	Waste	
		Thorium	Metal	Oxide/ Solution	Th compounds	Spent fuel	Waste	
IN 2.4: Nuclear technology	EP2.4.1: Enrichment			Yes		No		AL2.4: Attractiveness of technology considered in design and found acceptably low on basis of expert judgment?
	EP2.4.2: Extraction of fissile material			Yes		No		
	EP2.4.3: Irradiation capability of undeclared fertile material			Yes		No		

* VW = Very Weak, W = Weak; M = Moderate, S= Strong, VS = Very Strong; It was determined that the mixture of 5-column and 2-column headings within the Evaluation Scale assessment is confusing to the first-time user, and perhaps could be clarified in future revisions of the INPRO PR Manual.

** The Pu-238, Pu-240, and Pu-242 content depends strongly on Pu-239 content (see EP 2.1.2).

Appendix 3: System descriptions for NuScale

A.3.1 Subcriticality control

NuScale's CRDS consists of 16 CRAs within 37 FAs, each containing 24 control rods. It has both safety and non-safety related functions. During NO Regulating Bank provides control of excess reactivity and rapid reactivity changes, and radial power shaping. The Shutdown Bank is used in normal plant shutdown. Control rod maneuvering is via electromechanical drive system, which moves the control rods in and out of the core and holds them at elevation within their range of travel. For AOOs and DBAs reactor trip is provided by releasing all 16 CRAs via gravity drop in case of loss of power to the reactor trip breaker (operator initiated or due to loss of power). Reactor Trip System (RTS) includes two divisions of circuitry and trip breakers to satisfy single-failure criterion. Manual actuation by non-digital signals provides diversity for RTS initiation. The design ensures shutdown margin with highest worth rod stuck out of core. (NuScale 2020d, 30; NuScale 2020e, 86, 191-194, NuScale 2020f, 15-16).

Chemical and Volume Control System (CVCS) has a variety of operational functionalities along with reactivity control. Each NPM is equipped with independent CVSC. It controls and maintains boron concentration of the primary coolant for normal reactivity changes and minor transients. In addition, CVCS provides reactor coolant makeup water to primary circuit. The system includes two make up pumps, one in operation and other in stand-by. Although CVCS is a non-safety related system it includes two isolation valves for demineralized water, which are classified as safety related. These valves prevent operation that could accidentally dilute the boron concentration of the primary coolant. CVCS is operated to adjust boron concentration for sufficient shutdown margin during AOOs. Burnable absorber rods (Gd_2O_3 in certain FAs) are credited only in NO for partial excess reactivity control. Furthermore, gadolinia is used to prevent positive Moderator Temperature Coefficient (MTC) at Beginning-Of-Life (BOL) that would occur if soluble boron were used alone. (NuScale 2020e 9-10, 70-72, 85-86; NuScale 2020g, 205, 211, 214).

A.3.2 Heat removal

Normal heat removal is via two helical-coil SGs which are inside the RPV and part of RCPB. Primary coolant flows through the core, removes heat, and flows upward the central hot leg riser. Secondary water is supplied from Feed Water System (FWS) to SGs. Heat is removed from primary coolant as feed water flows through SG tubes that wrap the riser. Feed water is generated to steam and is superheated. In the secondary side steam exits SGs and drives the Turbine-Generator (TG). The heat is rejected to Circulating Water System (CWS) as steam from the turbine is condensed by Main Condenser (MC). CWS rejects the heat to the Ultimate Heat Sink (UHS) via cooling towers (Atmosphere). Primary coolant flow is due to natural circulation. Secondary water flow is provided by feedwater pumps. During AOOs heat removal is achieved by dumping steam directly to the condenser through turbine by-pass system. Each NPM has its own power conversion system. CWS is a shared, non-safety related system consisting of two subsystems which both serve six MCs. The steam and power conversion system is not required to function in ACs. (NuScale 2020d, 28; NuScale 2020h 7, 32, 70-71).

Reactor Component Cooling Water System (RCCWS) is a closed water-cooling loop, which removes heat from plant components (e.g CVCS HXs and CRDS) to Site Cooling Water System. (SCWS). It is a shared, non-safety related system consisting of two independent subsystems which both can serve up to six modules. SCWS is open loop that provides cooling water for RCCWS and other heat loads such as Reactor Pool Cooling System and Spent Fuel Cooling System. The heat is rejected from SCWS to Atmosphere (UHS) via cooling towers. SCWS is shared system between all modules and classified as non-safety related. Both RCCWS and SCWS are only required to provide heat removal during operational states. (NuScale 2020d, 35; NuScale 2020g 96-97, 136).

DHRS is classified as safety-related system. It provides passive heat removal via natural circulation in non-LOCA DBAs after reactor trip and when normal heat removal is unavailable. In addition, it provides decay heat removal during operational states to transit to safe shutdown conditions. Each of two redundant trains has 100 % capacity to remove decay heat. Once in operation, DHRS valves open and water from Decay Heat Removal

Condensers (DHRC) is generated to steam in SG tubes as heat is absorbed from primary coolant. Heat is rejected from steam via DHRCs immersed in reactor pool (UHS) and condensate flows back to the SGs. Feedwater and main steam lines are isolated when the system is actuated, and primary coolant continues to flow within RPV due to natural circulation. DHRS is connected to feed and steam piping of SGs, thus, SGs have a safety-related function during ACs. It could be justified that DHRS is not credited for DECAs, due to functional reliance on SGs. (NuScale 2020d, 40-41; NuScale 2020i, 11-12, 92, 106).

ECCS provides core heat removal in AOOs, DBAs and DECAs. It is especially designed for LOCAs during which the loss of coolant would otherwise exceed the make-up capability. ECCS consists of three Reactor Vent Valves (RVV) located on RPV head and two Reactor Recirculating Valves (RRV) mounted on the side of RPV. In NO all five valves remain closed and are part of RCPB. Once actuated the RVVs open and vent steam from RPV into CNV. Steam rejects heat on the CNV inner surfaces and condenses. Condensate flows back in the bottom of CNV and re-enters the RPV via RVVs. The system functions by natural circulation of primary coolant between RPV and CNV. Heat is removed by convection to CNV surfaces and from CNV to reactor pool (UHS) by conduction. The valves are actuated by stored energy, don't require external power or auxiliary systems, and fail safe (in open position). Two RVVs and one RRV are required to open. It is stated that no single failure event could prevent ECCS to perform its function. ECCS is not required to provide additional make-up water, because the coolant inventory released in LOCA events is retained inside the CNV. (NuScale 2020j, 107-108).

During all ACs heat is removed passively from RPV and CNV to water pool (UHS) by conduction. This safety feature is possible due to modular design of the reactor and CNV partially immersed in the pool. The UHS for ACs is combined borated water inventory consisting of reactor, spent fuel and refuelling pools. The pool is located below-grade and is a shared safety-related system between all modules. The large amount of water in the pool ensures sufficient decay heat removal from all 12 modules without operator actions or power supply and is capable to maintain the plant in a safe condition at least for 72 hours. For a single module the pool inventory is designed to provide core cooling for over 30 days, after which the long-term cooling is stated to be achieved by natural circulation of air inside the CNV. The pool includes a line for additional make-up water. In ACs the water begins to

boil, heat is removed by evaporating and boiling and is ultimately rejected to atmosphere (UHS). The design aims for in-vessel retention strategy for potential severe accidents, thus heat removal to the pool is essentially credited in DECAs. It stated that the design provides sufficient time for actions to restore pool inventory. (NuScale 2020g, 118-120, 125-126; NuScale 2020j, 39-42; NuScale 2020a, 21, 23-24).

A.3.3 Confinement

RCPB is formed by pressure containing components of the Reactor Coolant System (RCS) up to and including the outermost CIV in piping that penetrates the CNV, the Reactor Safety Valves (RSV), ECCS valves (RVVs and RRVs). Piping of RCPB penetrates both the RPV and the CNV up to the outermost CIV. The RPV that contains portion of the RCS is the primary component of RCBP. The integrity of closed piping and associated components of the RCPB can be thought to provide confinement of radioactive material in operational states. RSVs discharge steam directly to the CNV for overpressure protection of RCS components. There are two redundant, self-actuating (passive) pilot valves installed to the top of RPV upper head. These valves are credited during NO and AOOs. (NuScale 2020i, 19; NuScale 2020j, 21-22).

The CNV contains, supports, and protects the RPV from external impacts. It is a steel pressure vessel partially immersed in the below-grade pool. The nested design of RPV inside the CNV provides confinement in ACs. The containment boundary is formed by CIVs, the CNV and passive isolation barriers (piping) that close the containment penetrations. CIVs are used to isolate process lines penetrating the CNV to prevent or limit the releases of radioactive material in accidents. Secondary CIVs (Main Steam Isolation Valves and Feedwater Isolation Valves) are also credited in AOOs, because they must close for DHRS to perform. There are two CIVs in a single valve body for primary system, welded outside CNV, and single CIV are used for secondary system. These are designed to fail-safe (closed position) and power supply is not required for their isolation function. (NuScale 2020j, 18, 44-50; Turunen 2020, 71).

Appendix 4: System descriptions for RUTA-70

A.4.1 Subcriticality control

RUTA-70 has a Reactor Control and Protection System, which includes 42 control rods. It is divided to two diverse shutdown systems with different actuators. Mechanical drive actuated CRA system functions for normal reactivity control and shutdown during operational states. It includes a group of six automatic control rods (ACR) and four groups of manual control rods (MCR). MCRs compensate for fast reactivity changes (e.g., xenon poisoning of the core and heat up) and they are used to shape the radial power distribution. ACRs control slow reactivity changes (e.g., burn-up of fuel and absorber) with required MCRs. Hydrodynamically actuated CRA with 12 scam rods (SR) is used in emergency conditions (AOOs and DBAs). Additionally, MCRs and ACRs provide diversity for scam function as the load attached to rod clusters provides gravity-driven insertion if the power supply is lost (can be initiated by the operator). This, passive scam could be credited for DEC. Furthermore, gadolinia (Gd_2O_3) is used as integrated burnable absorber in NO. (IAEA 2006c, 395-398).

A.4.2 Heat removal

Normal heat removal is via three-circuit scheme. The primary coolant flows through the core via forced circulation, generated by two axial pumps. The heated coolant flows through chimney section and is supplied to primary-secondary heat exchangers (1-2 HXs) via pipelines connected to distributing header. There are two cooling circuits, and each have three plate-type HXs. At the outlet of each HX coolant is supplied to the intake header of the reactor downcomer via pipeline. The intermediate cooling circuit (ICC) acts as barrier between primary and tertiary circuit, to isolate contaminated coolant from water used for district heating. During NO secondary coolant is actively circulated by feedwater pumps. Heat is transferred from secondary circuit water to third circuit (district heating network, DHN) via secondary-tertiary heat exchangers (2-3 HXs). The heat consumers of the DH circuit are the main UHS in NO. The design includes Service Water Supply System (SWSS),

an open water-cooling loop, to remove heat via cooling towers to atmosphere (UHS) if heat rejection to DH circuit isn't applicable. (IAEA 2006c, 381-382; Romenkov 2009, 394-395).

The design provides natural circulation of primary coolant below 30% of nominal power, thus during shutdown heat removal is by passive means. Switching from one circulation mode to another occurs automatically by means of passive closing and opening of the check valves, that normally isolate the RV from the pool. During natural circulation mode the reactor coolant and pool water are mixed. Furthermore, natural circulation of secondary coolant provides decay heat removal from primary circuit. (Polin 2020, 46; Romenkov 2009, 398; IAEA 2005b, 56).

ASEC is designed for AOOs and DBAs to remove heat from shutdown reactor. Decay heat is removed from the core by natural circulation in reactor pool. Heat from primary coolant is transferred to secondary circuit via 1-2 HXs. Both secondary circuit loops include an ASEC subsystem, which consists of water-air convectors located in their own compartments at elevations sufficient for natural circulation. Heat is removed from secondary coolant to atmosphere (UHS) by active ventilation and passive natural circulation of air in compartments. Air louvers of ASEC are passively actuated by direct-acting devices. Furthermore, it stated that active EMWS is included in design to recover primary and secondary water inventories in ACs. (IAEA 2006c, 390, 400; Romenkov 2009, 398).

An additional train for heat removal is via external surfaces of the concrete vessel if all controlled heat transfer loops are lost during DEC. The decay is accumulated to large water inventory in the reactor pool and heat is removed passively by conduction from pool surfaces to surrounding ground (UHS). It takes several days before the pool water starts to boil and evaporate. After this, the heat is also removed by boiling and evaporating. The reactor cover has rupture devices to allow steam release to the reactor hall. Steam is condensed by passive condensers and is returned to the pool inventory via gravity. It is stated that a reactor boil-off takes 18-20 days without addition of water. Furthermore, self-regulating effect of the negative reactivity coefficients on reactor power and moderate fuel temperatures contribute controlling DEC. (IAEA 2006c, 393, 401).

A.4.3 Confinement

RUTA-70 doesn't have actual RCPB, because the primary system isn't pressurized and lacks pressure containing components. However, the leak-tight surfaces of primary circuit HXs, closed piping and associated components of the RCS provides confinement of radioactive material in operational states. In addition, the intermediate circuit with closed piping and leak tight HX surfaces, is a barrier, which prevents ingress of radioactive material to tertiary circuit water. The below-grade, steel-lined concrete vessel (reactor pool) and its leak-tight cover made of protective slabs, confine radioactive material in ACs. Reactor Pool Airspace Overpressure Protection System (RPAOPS) is included to decrease pressure in airspace above the reactor pool. The plant concept includes an above-grade containment structure that is credited in accidents, however recent documents provide little information about its design. It is stated that its leak-tight enclosures and primary circuit connections prevent releases of radioactive material. (IAEA 2006c, 385, 398-399; Romenkov 2009, 397-399; Zrodnikov et al, 2004, 4).

Appendix 5: System descriptions for BWRX-300

A.5.1 Subcriticality control

BWRX-300 includes a standard (FMCRD that has been utilized in older GE-Hitachi BWRs with broad operational experience accumulated from many reactors. Total of 57 FMCRDs are used for both normal reactivity control and emergency shutdown with different actuators. During NO electro-mechanical drive is used to insert and withdraw control rods in fine increments to position them for reactivity control (all rods) and to flatten power distribution in the core (counter-balance steam voids at the top of the core with a group of rods). In emergency situations fast reactor shutdown is provided by hydraulic insertion of control rods. The system includes 29 Hydraulic Control Units (HCU), each provide high-pressure water to scram two FMCRDs. (GE-Hitachi 2021b, 35-37; GE-Hitachi 2014c, 14, 83).

Once initiated, scram valves are opened by spring action (normally closed by pressurized air control) and high-pressure nitrogen via piston forces water to flow through accumulator discharge line. Inside CRDs high-pressure water lifts piston and drives the attached control rod into the core. Scram is actuated automatically by signal from Reactor Protection System, manually by operator action, or passively when pilot valve solenoids are de-energized (in case of loss of power). Diversity for scram function is provided by automatic electric motor run-in of FMCRDs that occurs simultaneously with hydraulic insertion. ARI pilot valves are included in design, which open scram valves for hydraulic insertion of all control rods, if HCU actuation fails (ATWS). Both ARI valves and automatic run-in of FMCRDs are credited in DECs. Furthermore, SLC, which injects highly borated water to RPV is provided as additional means to ensure reactor shutdown in case of ATWS. (GE-Hitachi 2021b, 37,46, 76-80; GE-Hitachi 2019, 17).

Second independent system for reactivity control in NO is the Feedwater Level Control System (FLCS). The system controls downcomer water level, which affects the reactor power by varying natural circulation flowrate in the core (via reactivity feedback effects). FLCS functions quite similarly as reactivity control by varying forced flow rate of

recirculation pumps that is done in conventional BWRs. In addition, integral burnable absorbers (Gd_2O_3) are used for slow reactivity control. (GE-Hitachi 2021b, 20, 56).

A.5.2 Heat removal

During NO heat removal is via MC. Condensate and feedwater system supplies water to reactor downcomer and coolant flows through the core removing heat. Natural circulation of coolant water in the core is provided by tall RPV with chimney section above the top of the core. Generated steam is separated from re-circulating coolant water (steam separator) and dried (steam dryer) before its supply via Main Steam Lines (MSLs). Steam rejected from the turbine is condensed and heat is transferred to non-safety related Component Cooling Water System (CCWS). CCWS consists of two 100% redundant, intermediate, closed cooling loops, which provide cooling for plant components. Heat is removed from CCWS water to non-safety related Plant Service Water System (PSWS) via HXs. PSWS consists of two 100% redundant, open cooling loops, which eventually reject heat from CCWS to Atmosphere or Sea (UHS). Turbine by-pass valves allow steam dumping directly to MC in NO and AOs to remove heat and control reactor pressure. (GE-Hitachi 2019, 15-16, 19; GE-Hitachi 2011, 67-68, 105, 144-145).

SDC with two 100% redundant trains is provided to remove decay heat in shutdown modes during NO. Following AOs and DBAs it has capability to remove decay heat in conjunction with ICS. The system includes pumps with adjustable speed motor drives. Heat is removed via non-regenerative HXs to CCWS. SDC is part of the Reactor Water Clean Up/Shutdown Cooling System, which performs both shutdown cooling and water clean-up functions. (GE-Hitachi 2019, 8; GE-Hitachi 2011, 59-63).

Passive ICS ensures decay heat removal in RPV isolation event during AOs and ACs. In addition, it provides overpressure protection as heat removal limits pressurization rate of isolated RPV. Once actuated, condensate return valve opens and water drains into the core. Heat is removed and generated steam flows to the Isolation Condenser (IC), which is immersed in water pool above the PCV. Steam condenses in tube-side and flows back to the core; heat is transferred to pool water on the shell-side of the IC. Once pool water begins to

boil and evaporate, heat is rejected to Atmosphere (UHS) via vent. The system is actuated automatically, even if power supply is lost. Furthermore, the condensate return valve can be manually opened by operator. Flow is due to natural circulation. There are three independent ICs in total and water pool has an inventory for seven days of decay heat removal. The system is mentioned to remain in service for at least 72 hours. In addition, indefinite cooling is possible by recovering IC pool inventory. (GE-Hitachi 2021c, 47-48; GE-Hitachi 2019, 28-29; GE-Hitachi 2021d, 20).

PCCS removes decay from PCV and maintains its pressure within design limits in ACs, such as LOCAs. It includes several independent low-pressure HXs, which are closed loop and integral part of the containment boundary. PCCS is always in stand-by since there are no CIVs between HXs and the drywell. The heat from the containment is transferred to Reactor Pool above the PCV as steam flows through HXs. Ultimately, boiling and evaporating of pool water rejects heat to the atmosphere (UHS) via vent. Steam and condensate flow is due to natural circulation. PCCS doesn't require I&C, power supply or any operator actions to perform its SFs. During operational states Containment Fan Coolers (CFCs) perform containment cooling. (GE-Hitachi 2019, 29; GE-Hitachi 2021d, 63).

Furthermore, high-pressure makeup water is provided via Control Rod Drive Supply Pumps (CRDSP). CRDSPs have other functions also as part of the Control Rod Hydraulic Subsystem. The system includes two pumps (supply pump and a stand-by pump), which supply water from condensate storage tanks or condensate treatment system. Both pumps are simultaneously in operation for make-up water function to deliver required flow capacity to the RPV. The high-pressure make-up mode of operation is initiated automatically due to signal indicating low reactor water level. CRDSPs are used to control events in which feedwater system is unable to maintain the core water level (AOOs). In addition, AIWAS is included for DECAs. However, there is no information yet available for this system. (GE-Hitachi 2014c, 83, 94, 96; GE-Hitachi 2019, 27, 29).

A.5.3 Confinement

RCPB constitutes the RPV, its associated piping of RCS (e.g. main steam and feedwater lines), valve bodies and other connecting lines to it from systems (e.g. ICS and PCS) up to and including the first CIV. The lines penetrating PCV boundary are part of the RCPB. The integrity of closed piping and associated components of the RCPB can be thought to provide front-line confinement of radioactive material in operational states. (GE-Hitachi 2021d, 92, 150).

The PCV is stainless steel or reinforced concrete pressure vessel, which encloses and supports the RPV and its piping. It is mostly located below-grade. The containment design excludes suppression pool when compared to traditional BWRs, instead it has a leak-tight dry containment to confine radioactive material, steam, and water in LOCAs. It provides barrier against potential radioactive releases from RCS or associated systems connected to it that are inside the PCV. The confinement function of PCV can be thought to be mainly credited in ACs. CIVs are included in system piping inside the PCV and containment penetrations. The pipelines penetrating PCV to containment atmosphere have two CIVs. Penetrations for closed systems, which are neither part of the RCPB nor directly connected to PCV atmosphere have at least one CIV. These valves are either outside or both inside and outside the PCV depending on system. (GE-Hitachi 2021d, 10-12, 30-31, 178-179).

The RPV includes two integral RPIVs in all large (> 50 mm diameter) pipelines, which are capable to preserve coolant inventory and prevent releases of radioactive material in MBLOCAs and LBLOCAs. RPIVs are credited as inner CIVs for RCPB containment penetrations whereas automatic CIVs are provided outside containment. The ICS piping includes two redundant RPVs in serial on each end of the system. Since ICS requires open flow path to reliably provide emergency heat removal, there is no isolation valves in outer PCV piping for this system. Thus, confinement against potential radioactive releases relies on closed piping of ICS in outer PCV section. ICS pipelines have two different SFs, which are somewhat contradicted. (GE-Hitachi 2019, 23; GE-Hitachi 2021d, 29, 69, 150, 153-155).

Containment Inerting Nitrogen System (CINS) supplies nitrogen to containment atmosphere during operating modes. The inerted-containment provides protection against hydrogen combustion or detonation by dilution of oxygen and hydrogen released in ACs. Inerted PCV atmosphere mitigates dynamic effects of DBAs, and limits potential negative pressure to protect containment from external pressure in DECs. CINS is equipped with automatic, normally closed CIVs located both inside and outside PCV. It is stated that design doesn't require Combustible Gas Control System for DBAs, because the PCV atmosphere is well mixed and initially inerted. Furthermore, Containment Filtered Vent (CFV) is provided to confine radioactive releases in DECs. (GE-Hitachi 2021d, 63-64, 94, 110, 143; GE-Hitachi 2019, 29).

Appendix 6: System descriptions for KLT-40S

A.6.1 Subcriticality control

KLT-40S has an RPS, which includes two independent banks of CRAs with different actuators. Compensating Group Drive Mechanisms (CGDM) Bank is used to control normal reactivity changes in NO and minor transients in AOOs. It includes four peripheral, three middle and one central CRAs. Electro-mechanical drive consisting of step-motor and reduction gear screw mechanism is used to maneuver control rods. CGDM Bank is operated for normal shutdown, but the drive also seems to provide emergency insertion (with lowering speed of 4 mm/s) due to indication of trip signal (AOOs). Furthermore, it performs scram function by gravity drop of all CRAs, if the hold-up electromagnets of the control rod drives are de-energized (DBAs). The average lowering speed via gravity is mentioned to be 30 – 120 mm/s. The scram function can be actuated passively without power supply or operator actions. (JSC OKBM 2021, 18; Beliaev & Polunichev 2000, 32; JSC OKBM 2013, 12, 15).

Safety Rod Drive Mechanisms (SRDM) Bank is the main system credited in DBA to ensure reactor scram. It consists of three CRAs, each having two control rods and a drive. The electro-mechanical drive is a rack and pinion type mechanism with an asynchronous motor, electromagnet, and spring. The rods are released into the core by accelerating force of spring-action, when holding electromagnets of the drives are de-energized. The drop time is below 0,5 s and withdrawal time around 20 s. The system can passively perform its SFs. There are two systems (Preventive Reactor Protection System and Emergency Reactor Protection System) with different set-points for limiting parameters to initiate either preventive reactivity control or emergency shutdown (scram). (JSC OKBM 2021, 18, 23; JSC OKBM 2013, 15; Beliaev & Polunichev 2000; 32).

In addition, the design includes LAIS for DEC, which uses cadmium nitrate as soluble absorber (JSC OKBM 2021, 23; JSC OKBM 2013, 30). As usual, Gadolinia (Gd_2O_3) is utilized as burnable absorber to control slow reactivity changes and compensate for initial excess reactivity (Beliaev & Polunichev 2000, 30). It is worth to note, that KLT-40S design

doesn't include soluble neutron absorber (boron) for normal reactivity control (IAEA 2009c, 101).

A.6.2 Heat removal

KLT-40S has compact NSSS, all main components are connected by short pressure nozzles. The NSSS and its auxiliary equipment (e.g pressurizers and purification system) are arranged within metal tank's caissons filled with water. Normal heat removal is via four vertical once-through coil-type HXs. Primary coolant flows on shell-side and is supplied/removed through short co-axial nozzles. Steam is generated in secondary side within SGs tube system, which consists of cylindrical helical coils. The forced circulation of primary coolant is achieved by four centrifugal, canned, vertical, single-stage MCPs with asynchronous electric motor. The steam rejected from turbine is condensed in MC and heat is removed to Seawater Cooling System (SCS), which is an open cooling loop. The heat is ultimately rejected to sea (UHS) from SCS. Furthermore, steam extractions are taken from turbine and heat is removed via HXs to DHN. Thus, second UHS for NO are the heat consumers of DHN. The co-generation turbine includes a protection and control system, which can be used to dump steam directly to the MC through by-pass valves in operational states. (Beliaev & Polunichev 2000, 29, 32; JSC OKBM 2013, 4-6, 19-20; JSC OKBM 2021, 17, 19).

The design includes two active systems and one passive for emergency heat removal. Purification and Cooldown System (PCS) is likely credited in AOOs and DBAs as active Safety System for decay heat removal. Furthermore, PCS provides shutdown cooling in NO. The system includes two pumps, HX, filters, and associated piping with valves. Decay heat is removed via HX to SCS. PSC constitutes one train for decay heat removal with equipment redundancy, but it also has a function to maintain primary coolant water quality. The second active system credited in AOOs and DBAs is emergency heat removal by dumping steam through SGs to auxiliary condenser. The system constitutes one train for decay heat removal with equipment redundancy. Passive ESCS includes two 100% capacity trains, each having HX immersed in a water tank. The ESCS removes heat passively by natural circulation as steam flows to ESCS HX and condenses. The heat is transferred to water inventory in tank. Once water boils and evaporates heat is ultimately rejected to atmosphere via vent (UHS).

The passive ESCS can be thought to be credited in both DBAs and DECs. The water inventory in ESCS tanks is sufficient to ensure reactor cooling for over 24 hours. The primary circuit has natural circulation capability to provide sufficient coolant flow for core cooling if MCPs are off. (Beliaev & Polunichev 2000, 34; JSC OKBM 2013, 9, 11-15, 32-33; JSC OKBM 2021, 22; Bylov 2013, 6; IAEA 2009c, 89).

KLT-40S has two trains for emergency core cooling credited in ACs. ECCS train is divided to two subsystems, one performs HPSI whereas other provides LPSI. HPSI subsystem consists of active high-pressure pump system with 10 m³ water tank and passive hydro accumulator with 4 m³ water capacity. It is stated that the hydro accumulators are utilized during DECs to provide sufficient time margin to control accidents if the active systems fail. LPSI subsystem provides emergency core cooling by circulating condensate accumulated in containment into reactor core using low-pressure recirculation pump. The single-failure criterion is applied in the design of trains. (Beliaev & Polunichev 2000, 36-37; JSC OKBM 2013, 15; Bylov 2013, 7).

Containment heat removal and pressure reduction are implemented by passive principles. The Emergency Containment Pressure Reduction System (ECPRS) includes two channels, each having passive containment condensers connected to ESCS water tank. The system removes heat by condensing steam on HX surfaces. The heat is transferred to water inventory in tank and is ultimately rejected to atmosphere (UHS) by boiling and evaporating. The coolant flow in ECPRS piping is due to natural circulation. The suppression of increased pressure and containment heat removal is also provided by using bubbler tanks, in which steam flows and condenses. Furthermore, heat is removed passively by steam condensation on containment walls. These systems are credited in ACs, especially during DECs to maintain integrity of containment barrier. (Beliaev & Polunichev 2000, 37; Bylov 2013, 7; JSC OKBM 2013, 15-16).

The safety design follows in-vessel retention strategy to control severe accidents with core melt. Accident progression and mitigation of consequences is ensured by passive systems (ECPRS, bubbling tank and hydro accumulators) and incorporation of ERVCS. ERVCS functions to ensure retention of corium inside the RV by relocating core melt to the vessel

bottom and removing heat from outer surfaces of the bottom. The cooling water to reactor caisson is supplied from bubbling tank, condensate collector and tank's plating due to elevation difference. The water-filling of caisson functions passively by steam condensation on containment HXs and supply into caisson via gravity. It is likely, that ERVCS can also utilize recirculating pumps to actively supply water into caisson. (Beliaev & Polunichev 2000, 37; JSC OKBM 2013, 16-17; Bylov 2013, 10; JSC OKBM 2021, 22).

A.6.3 Confinement

The RCPB is formed by RPV and all pressure containing components (MCPs, SGs and Pressurizers) connected to it via short piping. Associated valve bodies and piping related to auxiliary systems such as PCS are also part of the RCPB. The leak-tight components and closed piping of the RCPB provide first-line confinement of radioactive material during operational states. The primary circuit overpressure protection is ensured by transition to shutdown cooling state by engineered protection systems. (JSC OKBM 2021, 13, 24; JSC OKBM 2013, 12).

The Reactor Compartment, which contains the RPs, is situated at midsection of the barge. Both RPs are enclosed in own parallelepiped steel containments. The containment has an internal design pressure of 0,5 MPa and it withstands depressurization of the primary circuit. To exclude containment destruction during barge sink, a special Containment Water Filling System (CWFS) is provided to fill the containment with water and subsequently seal it. The containment is credited in ACs, especially during DEC, to prevent potential radioactive releases. The design includes isolation system and normally closed 'localization valves' in primary circuit auxiliary systems and interfacing boundaries, which means provision of CIVs to prevent potential releases AOs and ACs. (Beliaev & Polunichev 2000, 34, 37; JSC OKBM 2013, 12, 15-16, 22, 32; JSC OKBM 2021, 13).

Containment and rooms adjacent to it are enclosed by leak-tight protective enclosure, that is credited in DEC as secondary containment. It consists of multi-layer ceilings of the superstructure roof, superstructure side rooms and machine room bulkheads. These structures constitute external protection of Reactor Compartment, capable to withstand

external impacts such as helicopter crash. The protective enclosure is intended to remove leaks of volatile radioactive material from rooms inside it, and direct them to Filtered Ventilation System (FVS) via ventilation channels. During DEC, FVS provides confinement function by restraining volatile radioactive material in filters. (Beliaev & Polunichov 2000, 35; JSC OKBM 2013, 12, 15-16, 22, 34; JSC OKBM 2021, 21).

Appendix 7: YVL.B.1 requirement evaluation for NuScale

Requirement	Description	Fulfilment	Acceptance
101	Safety functions shall be based on five successive levels according to DiD principle.	Systems performing fundamental SFs have been designed for different defence levels.	Yes
425/426	Levels shall be as independent as reasonably achievable. Systems shall have adequate functional isolation and diversity.	Division of systems between Operational States and ACs exists. However, same systems are credited in levels 1 – 2 and 3 – 3b. Subcriticality function is implemented separately for different levels. Some functional dependencies may exist between SSCs. Redundancy and diversity are utilized in system design.	Partially
431	Safety Systems of level 4 (severe accidents) shall be independent of other levels. These may be utilized to prevent core melt accidents in level 3b (DECs) if their primary functions are not jeopardized.	RPV/CNV/Pool decay heat removal is a system for level 4 (severe accidents). It is also credited in level 3a (DBAs) and level 3b (DECs), but its primary function is likely not jeopardized. Additional safety provisions exist (make-up water supply) to preserve operability of RPV/CNV/Pool system.	Yes
456b	Active components of level 4 systems shall satisfy N+1 failure.	RPV/CNV/Pool is a passive Safety System for level 4.	N/A
445	In AOOs subcriticality shall have N+1 criterion and fast shutdown by control rods.	CVCS includes two make-up pumps to fulfil N+1 criterion. Two different means for reactivity control (drive and gravity drop) to fulfil N+1 criterion. Passive reactor trip by gravity insertion of CRAs for fast shutdown.	Yes
445a	After AOOs and DBAs scram initiation shall have N+2 failure criterion and fast shutdown without reliance on external power. Shutdown shall be accomplished if any CRA fail to be inserted.	Passive reactor trip by gravity insertion of CRAs for fast shutdown. Design ensures shutdown margin with highest worth rod stuck out of core. RTS includes two divisions of circuitry and trip breakers to satisfy N+1 criterion. However, N+2 criterion for RTS initiation is not fulfilled.	Partially

446	Diverse shutdown system shall be provided for DECs initiated by AOOs. N+1 failure criterion shall be applied.	The design doesn't include diverse system for shutdown apart from CRAs in case of ATWS.	No
447	Sufficient subcriticality in DECs (B and C).	Passive scram by gravity insertion of CRAs is credited in DECs. This system alone may be demonstrated to ensure sufficient subcriticality in multiple failures or during severe external events. However, more design information needs to be evaluated. Especially I&C systems and potential functional dependencies should be highlighted.	Partially
448	Decay heat removal systems in AOOs shall satisfy N+1 criterion.	DHRS is utilized, it has two 100% redundant circuits to fulfil N+1 criterion. ECCS is utilized, it has N+1 criterion for RVVs and RRVs opening.	Yes
448a	Decay heat removal systems in DBAs shall satisfy N+2 criterion (N+1 for passive). 72h self-sufficiency shall be satisfied.	Passive DHRS is utilized, it has two 100% redundant circuits to fulfil N+1 criterion. Passive ECCS is utilized, it fulfils N+1 criterion for opening of RVVs and RRVs. 72h self-sufficiency for 12 modules is due to large water pool inventory.	Yes
449	Containment heat removal system shall apply diversity and satisfy N+1 and 72h self-sufficiency criteria. It can be counted for 448 if applicable.	Passive heat removal by conduction from RPV/CNV to pool. N+1 criterion and 72h self-sufficiency are fulfilled for this system. However, diversity principle is not applied.	Partially
450/450a	Sufficient heat removal from reactor to outside containment shall be ensured in DECs (B and C). There is no failure criterion.	In case of multiple failures for ECCS and DHRS, heat removal by conduction from RPV/CNV to pool remains operable. Below-grade layout of reactor pool may provide sufficient protection against severe external events. The system is self-sufficient.	Yes
455	Decay heat removal systems shall ensure transition from controlled to safe state in AOOs, DBAs and DEC As. N+1 criterion shall be satisfied.	Three decay heat removal systems (DHRS, ECCS and RPV/PCV/Pool) each fulfilling N+1 criteria are utilized. Inclusion of two passive Safety Systems may prevent CCFs in	Yes

		the first place. Safe state is likely to be achieved and maintained by use of these systems.	
455a	Decay heat removal systems shall ensure transition from controlled to safe state in DEC B and C. There is no failure criterion.	Two passive decay heat removal systems (ECCS and RPV/PCV/Pool) are utilized. Safe state is likely to be achieved by use of these systems without external power or operator actions. Additional safety provisions (make-up water supply) may be implemented if deemed necessary.	Yes
456e	Containment isolation function shall have N+1 failure criterion in DBAs and DEC As.	Two CIVs in series for primary circuit connections to fulfil N+1 criterion. Secondary circuit lines (main steam and feedwater) have a single CIV. These fail-safe to closed position and don't require external power to perform isolation.	Yes

Appendix 8: YVL B.1 requirement evaluation for RUTA-70

Requirement	Description	Fulfilment	Acceptance
101	Safety functions shall be based on five successive levels according to DiD principle.	Systems performing fundamental SFs have been designed for different defence levels.	Yes
425/426	Levels shall be as independent as reasonably achievable. Systems shall have adequate functional isolation and diversity.	Division of systems between Operational States and ACs exists. Subcriticality function is implemented separately for different levels. Diverse decay heat removal systems are credited in level 3a (DBAs) and level 3b (DECs). Heat removal from concrete vessel to ground seems to be reliable, though, it is credited in multiple levels (3a, 3b and 4). Functional dependencies must be studied further.	Partially
431	Safety Systems of level 4 (severe accidents) shall be independent of other levels. These may be utilized to prevent core melt accidents in level 3b (DECs) if their primary functions are not jeopardized.	Reactor/Pool//Concrete Vessel/Ground decay heat removal system might be credited for level 4. It is mainly credited for level 3b. There is not enough information yet available about severe accident management.	Partially
456b	Active components of level 4 systems shall satisfy N+1 failure.	Reactor/Pool/Concrete Vessel/Ground decay heat removal, if demonstrated to be applicable for level 4, is a passive system. There are no active components in this system.	N/A
445	In AOOs subcriticality shall have N+1 criterion and fast shutdown by control rods.	CRDS (mechanical drive) is used for normal reactivity control, and it fails safe if power supply is lost by releasing control CRAs into core via gravity drop. Hydrodynamic subsystem ensures fast shutdown by insertion of scram CRA into core.	Yes
445a	After AOOs and DBAs scram initiation shall have N+2 failure criterion and fast shutdown without reliance on external power. Shutdown shall be accomplished if any CRA fail to be inserted.	Fast shutdown is accomplished by hydrodynamic insertion of scram CRA. In addition, CRDS is capable to drop control CRAs via gravity if external power supply is lost. Furthermore, the core seems to be	Yes

		capable to inherently self-regulate criticality if control rod insertion fails, at least to some extent. However, there is yet little information available for RPS design. More information about I&C systems should be reviewed. All in all, requirement is likely to be fulfilled.	
446	Diverse shutdown system shall be provided for DECs initiated by AOOs. N+1 failure criterion shall be applied.	There is no diverse shutdown system apart from CRDS. However, the core seems to be capable to inherently self-regulate criticality, at least to some extent.	No
447	Sufficient subcriticality in DECs (B and C).	Two different means for scram (hydrodynamic insertion and gravity drop) and inherent self-regulation of reactor power. These could provide sufficient subcriticality.	Yes
448	Decay heat removal systems in AOOs shall satisfy N+1 criterion.	There are potentially two circuits for decay heat removal via 1-2 HXs to SWSS. In addition, each circuit includes ASEC subsystem that provides two redundant passive decay heat removal systems in AOOs.	Yes
448a	Decay heat removal systems in DBAs shall satisfy N+2 criterion (N+1 for passive). 72h self-sufficiency shall be satisfied.	Passive ASEC subsystem is credited in DBAs for decay heat removal. Both intermediate circuits include one, which provides two redundant trains. Heat conduction from concrete vessel surfaces to ground is additional train. It is stated that reactor pool boil-off takes 18-20 days without make-up. Requirement may be fulfilled.	Yes
449	Containment heat removal system shall apply diversity and satisfy N+1 and 72h self-sufficiency criteria. It can be counted for 448 if applicable.	If concrete vessel (pool) with protective lid is considered as containment, heat conduction from vessel surfaces provides its heat removal. Passive condensers in reactor compartment remove heat and condensate returns to pool via	Yes

		gravity. Pool boil-off takes 18-20 days without make-up. Requirement may be fulfilled.	
450/450a	Sufficient heat removal from reactor to outside containment shall be ensured in DECs (B and C). There is no failure criterion.	Reactor/Pool/Concrete Vessel/Ground decay heat removal system is credited for DECs. Pool boil-off takes 18-20 days without make-up. EMWS is utilized to supply water if deemed necessary. Requirement may be fulfilled.	Yes
455	Decay heat removal systems shall ensure transition from controlled to safe state in AOOs, DBAs and DEC As. N+1 criterion shall be satisfied.	ASEC provides two redundant trains for AOOs and DBAs. Heat conduction from concrete vessel surfaces to ground is credited for DEC A. While also considering quite low reactor thermal power (70 MW) and sufficiently large water inventory of reactor pool, this requirement is likely to be fulfilled.	Yes
455a	Decay heat removal systems shall ensure transition from controlled to safe state in DEC B and C. There is no failure criterion.	Heat conduction from concrete vessel surfaces to ground is credited for DEC A and EMWS is utilized to supply make-up water to reactor pool. While also considering quite low thermal power (70 MW), the reactor's inherent self-regulation of power and sufficiently large water inventory of reactor pool, this requirement is likely to be fulfilled.	Yes
456e	Containment isolation function shall have N+1 failure criterion in DBAs and DEC As.	There is no information available for containment/containment isolation design.	—

Appendix 9: YVL B.1 requirement evaluation for BWRX-300

Requirement	Description	Fulfilment	Acceptance
101	Safety functions shall be based on five successive levels according to DiD principle.	Systems performing fundamental SFs have been designed for different defence levels.	Yes
425/426	Levels shall be as independent as reasonably achievable. Systems shall have adequate functional isolation and diversity.	Division of systems between Operational States and ACs exists. Subcriticality function is implemented separately for different levels. Two same decay heat removal systems are credited for both level 3a (DBAs) and level 3b (DECs). Make-up water system is utilized for level 4 (severe accidents) but may also be credited in level 3b to prevent DECs. Additional mitigation strategies are planned for level 4 to cope severe accidents. Functional dependencies may exist between SSCs and these must be studied further.	Partially
431	Safety Systems of level 4 (severe accidents) shall be independent of other levels. These may be utilized to prevent core melt accidents in level 3b (DECs) if their primary functions are not jeopardized.	AIWAS is credited in level 4 but may also be utilized in level 3b to prevent core melt accidents. Severe accident mitigation strategies (to provide additional water and power supply) are planned for level 4.	Yes
456b	Active components of level 4 systems shall satisfy N+1 failure.	There is no information available for AIWAS.	—
445	In AOOs subcriticality shall have N+1 criterion and fast shutdown by control rods.	CRDS (electro-mechanical drive) is used to control minor transients and to provide normal shutdown. Fast shutdown is achieved by hydraulic insertion of control rods and is initiated by RPS. Automatic electric motor run-in of CRAs provides diversity for scram. Requirement is likely to be fulfilled.	Yes
445a	After AOOs and DBAs scram initiation shall have N+2 failure criterion and fast shutdown without reliance on external	RPS is capable to initiate hydraulic scram automatically, manually by operator action or passively if external power supply is lost. Simultaneous electric motor run-in of all CRAs provides diversity and ensures accomplishment of scram. The design includes ARI pilot valves as	Yes

	power. Shutdown shall be accomplished if any CRA fail to be inserted.	alternate means to actuate hydraulic scram if initiation by RPS fails. Design ensures appropriate shutdown margin with malfunctions such as rod stuck out of core. Requirement is likely to be fulfilled.	
446	Diverse shutdown system shall be provided for DECs initiated by AOs. N+1 failure criterion shall be applied.	The design includes SLC to inject highly borated water to RPV. There is no information yet available for this system. However, if similar system is used as for ESWBR, it consists of two separate trains with 50% injection capacity. This system includes two redundant injection valves for each train to satisfy N+1 criterion. Requirement may be fulfilled.	Yes
447	Sufficient subcriticality in DECs (B and C).	The hydraulic insertion of CRAs seem to be reliable with two different means to open scram air valves for initiation (RPS/ARI). Automatic run-in of CRAs by electric motor adds diversity and contributes to achieve reliable scram. SLC ensures maintaining subcriticality if scram fails. Requirement is likely to be fulfilled.	Yes
448	Decay heat removal systems in AOs shall satisfy N+1 criterion.	Active SDC has two 100% capacity redundant trains for decay heat removal. Passive ICS is credited in AOs and consists of three 100% capacity redundant trains. These systems fulfil N+1 criterion. In addition, Containment Cooling Fans provide active heat removal from PCV. Requirement is likely to be fulfilled.	Yes
448a	Decay heat removal systems in DBAs shall satisfy N+2 criterion (N+1 for passive). 72h self-sufficiency shall be satisfied.	Passive ICS with three 100% capacity redundant trains is credited in level 3a (DBAs). PCCS provides passive containment cooling by several low-pressure HXs. There is no information yet available for PCCS design. ICS remains in service at least for 72h without any need for power supply. Requirement is likely to be fulfilled.	Yes
449	Containment heat removal system shall apply diversity and satisfy N+1 and 72h self-sufficiency criteria. It can be counted for 448 if applicable.	Passive PCCS is utilized for containment heat removal. The system design is not finished and there is little information available. ICS is used to remove decay heat from RPV. Steam condensation of PCV walls provides additional containment heat removal. It is mentioned that these systems fulfil 72h self-sufficiency. Requirement is likely to be fulfilled.	Yes

450/450a	Sufficient heat removal from reactor to outside containment shall be ensured in DECAs (B and C). There is no failure criterion.	Passive ICS may ensure reliable decay heat removal from reactor to outside PCV. Passive PCCS is utilized for containment heat removal. ICS water pool has inventory for 7 days without additional make-up. AIWAS could be used to supply make-up water to ICS/Reactor pool. However, these systems are relied on in both level 3a (DBAs) and level 3b (DECAs). Further evaluation is needed to demonstrate reliable system performance in both levels.	Partially
455	Decay heat removal systems shall ensure transition from controlled to safe state in AOOs, DBAs and DECAs. N+1 criterion shall be satisfied.	The design includes two separate decay heat removal systems (active SDC and passive ICS), which both have redundancy. PCCS, if demonstrated to be robust, provides passive containment heat removal. Passive nature of systems may enhance protection against CCFs in the first place. However, further evaluations are needed to demonstrate system performance, especially in DECAs.	Partially
455a	Decay heat removal systems shall ensure transition from controlled to safe state in DEC B and C. There is no failure criterion.	Passive ICS and PCCS heat removal systems are credited in level 3b for DECAs (B and C). These systems together may ensure sufficient decay heat removal to achieve safe state. AIWAS could be used to supply make-up water to ICS Pool/Reactor Pool. However, further evaluations are needed to demonstrate system performance.	Partially
456e	Containment isolation function shall have N+1 failure criterion in DBAs and DECAs.	Two RPIVs in all large pipelines are considered as CIVs for RCPB piping. Two CIVs are included in penetrations to containment atmosphere. Penetrations which are neither part of the RCPB nor directly connected to PCV atmosphere have at least one CIV.	Yes

Appendix 10. YVL.B.1 requirement evaluation for KLT-40S

Requirement	Description	Fulfilment	Acceptance
101	Safety functions shall be based on five successive levels according to DiD principle.	Systems performing fundamental SFs have been designed for different defence levels.	Yes
425/426	Levels shall be as independent as reasonably achievable. Systems shall have adequate functional isolation and diversity.	Division of systems between Operational States and ACs exists. Subcriticality function is implemented separately for different levels. The design includes diversity for core decay heat removal systems. Two same passive containment heat removal systems (ECPRS and Bubbling Tank) and potentially one active system (LPSI pumps) are credited for level 3a (DBAs), level 3b (DECs) and level 4 (severe accidents). Functional dependencies may exist between SSCs in defence levels, and these must be studied further.	Partially
431	Safety Systems of level 4 (severe accidents) shall be independent of other levels. These may be utilized to prevent core melt accidents in level 3b (DECs) if their primary functions are not jeopardized.	ERVCS is credited in level 4 for severe accident mitigation. However, it utilizes systems credited in level 3b to refill reactor caisson water inventory. Both ECPRS and Bubbling Tank are passive systems. LPSI pumps may be used as active system. Furthermore, these systems are also credited in level 3a for DBAs. Further evaluations are needed to demonstrate reliable system performance in all levels. Sufficient independency of level 3a and level 4 should be demonstrated	No
456b	Active components of level 4 systems shall satisfy N+1 failure.	LPSI subsystem may be utilized to refill reactor caisson. There are two trains each having one LPSI pump to fulfil N+1 criterion. Other systems of ERVSC seem to be passive.	Yes
445	In AOOs subcriticality shall have N+1 criterion and fast shutdown by control rods.	CRDS (electro-mechanical drive) is used to control minor transients and to provide normal shutdown. Due to trip signal control CRAs are inserted with emergency speed. (4 mm/s). There is little information available about reactor scram in AOOs. It is stated that there are preventive reactor protection system and emergency protection system with respective setpoints. Emergency protection system initiates scram. More information needs to be reviewed.	Partially
445a	After AOOs and DBAs scram initiation shall have N+2 failure	The emergency reactor protection system initiates spring accelerated scram CRA insertion once	Partially

	<p>criterion and fast shutdown without reliance on external power. Shutdown shall be accomplished if any CRA fail to be inserted.</p>	<p>locking electromagnets of drives are de-energized. The system can be actuated passively if power supply is lost. Furthermore, control CRAs can provide scram by gravity drop, once holding electromagnets of drives are de-energized. This system also can be actuated passively if power supply is lost. There is little information available about design provisions to ensure shutdown in case of CRDS malfunctions. However, two different systems may ensure sufficient reliability. More information needs to be reviewed.</p>	
446	<p>Diverse shutdown system shall be provided for DECs initiated by AOOs. N+1 failure criterion shall be applied.</p>	<p>The design includes LAIS to inject cadmium nitrate to RPV. There is little information available for this system. More information needs to be reviewed.</p>	Partially
447	<p>Sufficient subcriticality in DECs (B and C).</p>	<p>The design incorporates two diverse scram systems (spring insertion and gravity drop). Both systems can actuate passively if external power supply is lost. However, more information is required to demonstrate their performance and research potential functional dependencies between SSCs. Especially, I&C systems should be highlighted. LAIS ensures maintaining subcriticality if scram fails.</p>	Partially
448	<p>Decay heat removal systems in AOOs shall satisfy N+1 criterion.</p>	<p>Active PSC and auxiliary condenser are two diverse trains for decay heat removal. There is little information available about these systems. However, two different systems may satisfy the requirement.</p>	Yes
448a	<p>Decay heat removal systems in DBAs shall satisfy N+2 criterion (N+1 for passive). 72h self-sufficiency shall be satisfied.</p>	<p>Passive ESCS with two 100% capacity redundant trains is credited in level 3a (DBAs). ECPRS provides passive containment cooling by two trains each having a condenser connected to ESCS pool. The two pools have water inventory to ensure core cooling for over 24 hours. Active systems provide additional decay heat removal. Though more information is needed, requirement is likely to be fulfilled.</p>	Yes
449	<p>Containment heat removal system shall apply diversity and satisfy N+1 and 72h self-sufficiency criteria. It can be counted for 448 if applicable.</p>	<p>Passive ECPRS with two trains is utilized for containment heat removal. In addition, both Bubbling Tank and steam condensation on containment surfaces provide diverse containment</p>	Partially

		heat removal. There is little design information available to evaluate 72h self-sufficiency.	
450/450a	Sufficient heat removal from reactor to outside containment shall be ensured in DECs (B and C). There is no failure criterion.	Passive ESCS may ensure reliable decay heat removal from reactor. Safety injection system (HPSI and LPSI) with two 100% capacity redundant trains is credited in DECs. Passive ECPRS and Bubbling Tank are utilized for containment heat removal, and these may ensure reliable performance. Two ESCS water pools have inventory for over 24 hours. However, some systems (ECPRS, Bubbling Tank and LPSI pumps) are credited in three levels (3a, 3b and 4), that may introduce challenges. More information is needed to demonstrate reliable performance in all levels.	Partially
455	Decay heat removal systems shall ensure transition from controlled to safe state in AOOs, DBAs and DEC As. N+1 criterion shall be satisfied.	The design includes two active decay heat removal systems (PCS and auxiliary condenser) and one passive system (ESCS). ECPRS and Bubbling Tank provide passive containment heat removal. Active safety injections systems (LPSI and HPSI pumps) and passive hydro accumulators are credited in DBAs and DECs. Inclusion of passive systems may prevent CCFs in the first place. Multiple systems in levels 3a and 3b may introduce challenges to these levels. More information is needed to demonstrate reliable performance in DEC As.	Partially
455a	Decay heat removal systems shall ensure transition from controlled to safe state in DEC B and C. There is no failure criterion.	Passive heat removal system (HPSI hydro accumulators, ESCS and ECPRS) are credited in level 3b for DECs (B and C). LPSI pumps may be utilized as active system. These diverse systems together may ensure reliable decay heat removal to achieve safe state. However, ECPRS and LPSI pumps are also credited in levels 3a and 4, which may introduce challenges. More information is needed to demonstrate system performance.	Partially
456e	Containment isolation function shall have N+1 failure criterion in DBAs and DEC As.	There is little information available for containment/containment isolation design.	—

Appendix 11. YVL.A.11 requirement evaluation for NuScale

Requirement	Description	Fulfilment	Acceptance
302	The planning of security arrangements shall be based on the DBT, the risk analyses of the activity to be secured, and the protection requirements assessed on the basis thereof.	The PP arrangements are based on DBT to protect against threats derived from it. The protection requirements of NPP are considered by risk analyses based on safety evaluations, system reliability and human factors.	Yes
303	SSCs important to safety and the storage locations of nuclear material and nuclear waste shall be designed to facilitate the appropriate implementation of security.	Multidiscipline team has identified vital SSCs from insights derived from risk-related analyses. Vital areas with sufficient detection, delay and access control are established to facilitate security response. However, it is uncertain whether only SSCs have been considered.	Partially
307a	Nuclear security related risk analyses shall utilize PRA.	PRA has been utilized in designating risk significant SSCs.	Yes
310	The planning of security arrangements shall take account of the various areas of PP: deterrence, detection, delay, and response.	The design provides detection (intrusion detectors, monitoring systems, alarm devices), delay (bullet-proof structures, hardened doors, locks, physical barriers) and access control. Detailed descriptions of security provisions for nuclear island and structures are presented. Security computer system to facilitate PP functions has been provided. However, site-specific details for physical barriers, access control portals, security devices and response (organization and plans) have not been considered yet.	Partially
311	The number of access openings and routes to the plant area shall be kept to a practicable minimum to enhance access control.	Opening penetrations of vital areas are provided with physical barriers and entry points to these areas are minimized. Access openings and routes to the plant area have not been considered yet.	No
324	For the implementation of nuclear security nuclear facilities shall form four security zones within one another.	The concept of security zones is utilized in the security design. Vital areas constitute areas within protected buildings in nuclear island and other structures. The plant buildings are inside protected area surrounded by double-fence. The plant area is within a controlled area surrounded by a fence. At least three zones are considered, however protected buildings could be credited as one security zone. Detailed descriptions for site-specific isolation	Yes

		zones (other security zones than protected area and vital areas) have not been considered yet.	
320	The security zones shall have arrangements in place to enable the detection of threats.	Intrusion detectors, alarm devices, video monitoring and access control data recording provides detection. Detailed design descriptions of systems are presented for vital areas. System descriptions for other security zones have not been considered yet. However, preliminary locations and recommendations for equipment are provided.	Partially
320a	The interfaces of security zones shall form obstacles to prevent or delay unauthorized access to provide the security organization and police authorities with sufficient time to undertake countermeasures.	The bullet-proof, hardened, and locked structures with access control prevent and delay unauthorized access to vital areas. The plant area is surrounded by double-fence. However, design details of physical barriers for security zones other than vital areas have not been considered yet.	Partially
321a	Security zones shall be separated appropriately.	The vital areas are enclosed within structures that are located inside buildings in nuclear island. These areas form boundaries, thus it is likely that they are separated. The vital area boundaries are separated from plant area boundary. For other security zones, there is no information yet available.	Partially
325a	Technical monitoring shall be implemented in all security zones.	Design description of video monitoring system (doors, interior area, and penetrations) for vital areas has been presented. Preliminary locations and recommendations for vendor-specific equipment have been considered for other security zones.	Partially
329	The plant area consists of a double-fenced area surrounding the buildings pertaining to the plant's operation and it shall be located inside the restricted area.	The plant area is surrounded by double-fence and constitutes all buildings pertaining to the plant operations. It is located inside the security owner-controlled area, namely restricted area.	Yes
331	The outer surfaces of buildings inside the protected area shall be heavily protected against unlawful action and other action that endangers nuclear or radiation safety as described in the DBT.	The reactor building is safety-related reinforced concrete structure (Seismic Category 1). The control building is structural steel with metal siding above-grade and remaining portion below-grade is safety-related concrete structure (Seismic Category 1). The radioactive waste building is Seismic Category 2. No information has been provided on dry storage for spent fuel. Other buildings are non-safety related structures. Safety significant buildings are heavily protected from threats.	Yes

333	Vital areas in their entirety shall be located inside the protected area.	The vital areas constitute areas within buildings in nuclear island and structures.	Yes
386	Inside the perimeter of the plant area, persons shall be monitored.	The design description of monitoring system has been presented for vital areas. For plant area detailed design have not been described. However, preliminary locations and recommendations for monitoring equipment have been considered.	Partially
387	Access control at the nuclear facility shall be implemented in a way enabling reliable establishment of who are, or have been, within the plant area, the protected area and the vital area.	The design description of access control system is presented. Access control is established by utilizing automatic computer-based system, which provides constant data records on access point activities. However, access authorization program with numbered id-badge system have not been considered yet.	Partially
393	A nuclear facility shall have a central alarm station and a stand-by alarm station. Both shall be capable of maintaining redundant and secure communication with the police, the nuclear facility's command centre and the nuclear facility's control room. The stand-by station shall be separated from the central alarm.	The design description of CAS and associated communication systems are presented. The secondary alarm station design, location and communication systems have not been considered yet.	Partially
395	A command centre equipped for threats and a stand-by command centre shall be in place. Both shall be capable of maintaining redundant and secure communication with the police, the nuclear facility's alarm station and the nuclear facility's control room. The stand-by command centre shall be separated from the command centre.	The security design of response forces and defensive plans have been identified as site-specific item to be addressed in further licensing.	No
396	A nuclear facility shall have a designated and appropriately equipped room for use by the police in commanding operations to prevent threats targeting the nuclear facility.	The security design of response forces and defensive plans have been identified as site-specific item to be addressed in further licensing.	No

Appendix 12. YVL.A.11 requirement evaluation for BWRX-300

Requirement	Description	Fulfilment	Acceptance
302	The planning of security arrangements shall be based on the DBT, the risk analyses of the activity to be secured, and the protection requirements assessed on the basis thereof.	The PP arrangements are based on DBT to protect against threats derived from it. The risk-based approach is likely to be utilized in security design.	Yes
303	SSCs important to safety and the storage locations of nuclear material and nuclear waste shall be designed to facilitate the appropriate implementation of security.	Vital areas with sufficient detection, delay and access control are established to facilitate security response. However, it is uncertain whether only SSCs have been considered.	Partially
307a	Nuclear security related risk analyses shall utilize PRA.	It is likely that PRA has been utilized in determining vital SSCs. However, there is little information to answer this requirement.	—
310	The planning of security arrangements shall take account of the various areas of PP: deterrence, detection, delay, and response.	The design considers detection (intrusion detectors, monitoring systems, alarm devices), delay (bullet-proof/hardened structures, locks, physical barriers) and access control. However, site-specific details for physical barriers, access control portals, security devices and response (organization and plans) have not been considered yet.	Partially
311	The number of access openings and routes to the plant area shall be kept to a practicable minimum to enhance access control.	Minimal access points to vital areas have been considered. Access openings and routes to the plant area have not been considered yet.	No
324	For the implementation of nuclear security nuclear facilities shall form four security zones within one another.	The concept of security zones is utilized in the security design. Vital areas constitute areas within plant buildings. Plant buildings are inside plant area surrounded by double-fence. The plant area is within isolation zone, namely restricted area. At least three zones are considered, however protected buildings could be credited as one security zone. Detailed descriptions for site-specific isolation zones (other security zones than plant area and vital areas) have not been considered yet.	Yes
320	The security zones shall have arrangements in place to enable the detection of threats.	Intrusion detectors, alarm devices, video monitoring and access control provides detection. System descriptions for other security zones than vital areas have not been considered yet.	Partially

320a	The interfaces of security zones shall form obstacles to prevent or delay unauthorized access to provide the security organization and police authorities with sufficient time to undertake countermeasures.	The bullet-proof, hardened, and locked structures with access control prevent and delay unauthorized access to vital areas. The plant area is surrounded by double-fence. However, design details of physical barriers for security zones other than vital areas have not been considered yet.	Partially
321a	Security zones shall be separated appropriately.	The vital areas are enclosed within structures that are located inside plant buildings. The vital area boundaries are separated from plant area boundary. For other security zones, there is no information yet available.	Partially
325a	Technical monitoring shall be implemented in all security zones.	Vital areas are monitored. Furthermore, monitoring has been considered to be relevant design aspect for other security zones. However, design details of monitoring system have not been provided yet.	Partially
329	The plant area consists of a double-fenced area surrounding the buildings pertaining to the plant's operation and it shall be located inside the restricted area.	The plant area is surrounded by double-fence and constitutes all buildings pertaining to the plant operations. It is located inside the isolation zone, namely restricted area.	Yes
331	The outer surfaces of buildings inside the protected area shall be heavily protected against unlawful action and other action that endangers nuclear or radiation safety as described in the DBT.	The reactor building is safety-related reinforced concrete structure (Seismic Category 1), and safety significant SSCs inside the building are located below-grade. Little information is yet available on other buildings.	Partially
333	Vital areas in their entirety shall be located inside the protected area.	The vital areas constitute areas within plant buildings, that is protected area.	Yes
386	Inside the perimeter of the plant area, persons shall be monitored.	Monitoring system has been considered to be relevant design aspect. However, detailed descriptions and locations for monitoring equipment have not been provided.	Partially
387	Access control at the nuclear facility shall be implemented in a way enabling reliable establishment of who are, or have been, within the plant area, the protected area and the vital area.	Access control is established by utilizing computer-based system with numbered id-badges for personnel identification and authorization. Administrative procedures will be implemented to provide screening of personnel and access control for vital areas (e.g. two-person rule). However, detailed descriptions have not been provided yet.	Partially

393	A nuclear facility shall have a central alarm station and a stand-by alarm station. Both shall be capable of maintaining redundant and secure communication with the police, the nuclear facility's command centre and the nuclear facility's control room. The stand-by station shall be separated from the central alarm.	The design description of CAS (structure and location) is presented. The secondary alarm station design (structure and location) and detailed descriptions of CAS/SAS communication/alarm systems have not been considered yet.	Partially
395	A command centre equipped for threats and a stand-by command centre shall be in place. Both shall be capable of maintaining redundant and secure communication with the police, the nuclear facility's alarm station and the nuclear facility's control room. The stand-by command centre shall be separated from the command centre.	The security design of response forces and defensive plans have been identified as item to be addressed in further licensing.	No
396	A nuclear facility shall have a designated and appropriately equipped room for use by the police in commanding operations to prevent threats targeting the nuclear facility.	The security design of response forces and defensive plans have been identified as site-specific item to be addressed in further licensing.	No

Appendix 13. Facility Safeguardability Analysis Tool for NuScale (Coles et al. 2013).

Question	Response	Reasoning
1. Does this design differ from the comparison design/process in ways that have the potential to create additional diversion paths or alter existing diversion paths?	Yes/No	Potential for new diversion paths associated with consolidation of refueling areas for multiple modules. More detailed diversion path analysis is required to assess the significance of this potential path. See answers to subsidiary questions
1.1. Does this design introduce nuclear material of a type, category, or form that may have a different significant quantity or detection time objective than previous designs/processes (e.g., mixed oxide rather than low enriched uranium, irradiated vs. unirradiated or bulk rather than items)?	Yes/No	
1.2. Does this design layout eliminate or modify physical barriers that would prevent the removal of nuclear material from process or material balance areas, e.g., circumventing a key measurement point (KMP)?	Yes/No	The NuScale design common refueling area for multiple modules reduces the safeguards effectiveness or renders infeasible the locking and sealing of the fuel transfer tube when modules are in operation. This makes it more difficult to maintain CoK of the inventory of the reactor vessels and the spent fuel pool. It may be possible to compensate by locking and sealing the removable pool lids and other monitoring approaches. However, it is not likely to be possible to have an inspector present every time these seals need to be broken and available to affix new seals after the module is refueled. Perhaps remote surveillance could be employed to compensate
1.3. Does this design obscure process areas or material balance area (MBA) boundaries making containment/surveillance or installation of verification measurement and monitoring equipment more difficult?	Yes/No	The need to transport NuScale reactor vessels to a common refueling area necessitates the monitoring of a significantly larger area. Thus installation of containment/surveillance or monitoring equipment will be more difficult and expensive.
1.4. Does this design introduce materials that could be effectively substituted for safeguarded nuclear material to conceal diversion?	Yes/No	Fuel material is similar, only differing in dimension, with PWR fuel.
Does this design differ from the comparison design in a way that increases the difficulty of design	Yes/No	See response to question 2.4.

information examination (DIE) and verification (DIV) by IAEA inspectors?		
2.1. Does the design incorporate new or modified technology? If so, does the IAEA have experience with the new or modified technology?	Yes/No	General technology is similar to conventional PWR technology. The difference in refueling associated with the removal of components additional to the PWR reactor head does not appear to make a significant difference.
2.2. Are there new design features with commercial or security sensitivities that would inhibit or preclude IAEA inspector access to equipment or information?	-	There is insufficient information in the description of the NuScale to answer this question. Need to know whether anything that could be seen with visual access to the NuScale removal pool, spent fuel storage area, and the unit transfer system is proprietary. These locations and activities within them would need to be monitored to maintain CoK.
2.3. Do aspects of the design limit or preclude inspector access to, or the continuous availability of, Essential Equipment for verification or testing?	Yes/No	There does not appear to be a significant difference in this area.
2.4. Are there aspects of the design that would preclude or limit IAEA maintenance of Continuity of Knowledge (CoK) associated with design verification during the life of the facility?	Yes/No	The NuScale design common refueling area for multiple modules and relatively frequent module refuelings (perhaps 6 per year) makes it more difficult to maintain CoK. (See notes in rationale for questions 1.2 & 2.2 for discussion of challenges of maintaining CoK of reactor core loading.)
3. Does this design/process differ from the comparison design/process in a way that makes it more difficult to verify that diversion has not taken place?	Yes/No	See answers to subsidiary questions.
3.1. Does this design lessen the efficiency of physical inventory taking (PIT) by the operator or the effectiveness of physical inventory verification (PIV) by the IAEA?	Yes/No	The multiple modules refueling makes a physical inventory more difficult because there is no time in normal operation when all fuel assemblies are visually accessible. Thus complete physical inventory must rely upon the use of C/S. The fuel assemblies in the operating reactor cores must be accepted on book value to be physically verified during their next refueling. The double stacking of NuScale fuel assemblies in the fuel storage pool also impedes PIV because the upper level assemblies must be moved to gain visual and NDA access to the fuel assemblies on the lower level.
3.1.1. Does the plant/process design evaluated reduce the measurement accuracy or otherwise impede the use of	Yes/No	The double stacking of NuScale fuel assemblies in the fuel storage pool also impedes PIV because the upper level assemblies must be moved to gain visual and NDA access to the fuel assemblies on the lower level. The inability to schedule PIV when the reactor core

Inventory Key Measurement Points (IKMP). If so, are there other well defined locations that could be considered by the IAEA as IKMPs.		assemblies are visually accessible for all reactor units impedes the ability to select an IKMP where all in-core fuel assemblies are visually accessible.
3.1.2. Does the plant/process design evaluated impede or preclude the collection/storage of inventory at IKMPs at the time of PIT/PIV?	Yes/No	See rationale for question 3.1.1.
3.1.3. Does the design preclude PIT/PIV measurements on some inventory? If so, does the new design include features to permit CoK to be maintained from a previous measurement and verification?	Yes/No	Refueling of multiple modules makes a physical inventory more difficult because there is no time in normal operation when all fuel assemblies are visually accessible. Thus the complete physical inventory cannot be 100% verified by visual inspection/NDA.
3.1.4. Does the design/process employ nuclear material types, categories, or forms that are more difficult to measure accurately at IKMP? If so, can the plant accountancy measurement systems meet International Target Values (ITV) for the PIT?	Yes/No	No significant difference. Both NuScale and PWR designs permit item accountability. Smaller fuel pins in the NuScale assemblies make accounting for damaged NuScale fuel pins less significant/more accurate than for PWR. (SFM inventory in damaged fuel pins is usually booked as an estimate based upon the physical configuration of the damaged fuel pin.)
3.1.5. Does the design preclude or limit the ability of the IAEA to take/analyze independent samples for the PIV?	Yes/No	The double stacking of NuScale fuel assemblies in the fuel storage pool also impedes PIT and PIV because the upper level assemblies must be moved to gain visual and NDA access to the fuel assemblies on the lower level.
3.1.6. Does the process design preclude controls to prevent inventory change or movement between the time of the PIT and the PIV? If so, does the design include measures to maintain CoK of the changed or moved inventory between the time of the PIT and the PIV?	Yes/No	Depending upon the lag time between the PIT and PIV, it is possible that a unit could reach the refueling point between the PIT and PIV. There are no design measure described that would maintain CoK under this circumstance. Perhaps remote monitoring of refueling operations could maintain CoK.
3.2. Does this design impair the ability of the operator to produce timely and accurate interim inventory declarations or for the IAEA to perform timely and	Yes/No	Like the PWR, the NuScale design can employ item accountability so interim inventory declarations should not be an issue.

accurate Interim Inventory Verification (IIV)?		
3.2.1 Does design impede or preclude shutdown of the process for an IIV?	Yes/No	Differing refueling schedules make it infeasible to conduct an IIV for all fuel assemblies in reactor unit cores.
3.2.2 Does the design impede or preclude the collection/storage of inventories at IKMP, which provide access for measurement and declaration by the operator and verification by the IAEA, at the interim inventory cut-off time (CoT)?	Yes/No	Differing refueling schedules make it infeasible to conduct a physical inventory for all fuel assemblies in reactor unit cores during one IIT.
3.2.3 Does design create the potential for Un-Measurable Inventory (UMI) at the time of an IIV in locations such as pipes, pumps, or evaporators? If so, can the UMI be accurately estimated by the operator and can the estimation method be verified by the IAEA?	Yes/No	Because there is no possible physical inventory of the assemblies in the reactor cores of units that are not shutdown at the time of the IIT, there is the likelihood of items that cannot be physically verified or NDA verified for SFM content (i.e., "measured").
3.2.4 Does the new plant/process design increase the time required for the operator to provide the IAEA with an Interim Inventory List (IIL) after the CoT	Yes/No	No significant difference because both the NuScale and PWR designs permit item accountability.
3.2.5 Does design increase the expected overall measurement uncertainty of the operator's interim inventory declaration?	Yes/No	No significant difference because both the NuScale and PWR designs permit item accountability.
3.2.6 If the comparison facility Safeguards Approach included short-notice or no-notice interim inspections, does the design include real time measurement and accounting systems that allow for almost immediate inventory declarations required to support such inspections?	Yes/No	The SDC development will consider the possibility of incorporating short-notice or no-notice interim inspections.
3.3. Does this design impede timely and accurate inventory change (IC) measurements and	Yes/No	Like PWRs, the NuScale design can employ item accountability so interim inventory change measurements and declarations should not be an issue. Using the single MBA approach, the receipt and

declarations by the operator and verification by the IAEA?		shipment item counts and verification, including NDA, should be similar for both designs.
3.3.1. Does this design reduce the accuracy of or otherwise impede the use of customary Flow Key Measurement Points (FKMPs). If so, are there other well defined locations that could be considered by the IAEA as FKMP?	Yes/No	No significant difference because both the NuScale and PWR designs permit item accountability.
3.3.2. Does the design increase the measurement uncertainties at FKMPs? If so, can the plant accountancy system meet International Target Values (ITV) for inventory change	Yes/No	No significant difference because both the NuScale and PWR designs permit item accountability. Smaller fuel pins in the NuScale assemblies make accounting for damaged NuScale fuel pins less significant/more accurate. (See discussion in the rationale for item 3.1.4.)
3.3.3. Does the new design impede or preclude IAEA verification of the IC declarations by sample taking, portable or installed measurements systems, or by joint-use of authenticated operator systems?	Yes/No	No significant difference because both the NuScale and PWR designs permit item accountability
3.3.4. Does the design impede or preclude IAEA verification of calculated IC declarations such as nuclear material loss and gain?	Yes/No	No significant difference because both the NuScale and PWR designs permit item accountability. The calculations of special fissionable material changes due to reactor “burnup” are subject to commensurate uncertainties
3.3.5. Does the design impede or preclude IAEA verification of IC declarations that are determined indirectly or based on historical measurement data (e.g., waste transfers to retained waste or measured discards), decrease the accuracy of the determinations, or limit the availability of the historical data	Yes/No	No significant difference because both the NuScale and PWR designs permit item accountability. Smaller fuel pins in the NuScale assemblies make accounting for damaged NuScale fuel pins less significant/more accurate so that damaged assembly/pin inventories have lower uncertainty. (See discussion in the rationale for item 3.1.4.)
3.3.6. Does the design increase the time required for the operator to measure, calculate, prepare, and approve the IC declarations?	Yes/No	No significant difference because both the NuScale and PWR designs permit item accountability.
3.3.7. Does the new design increase the expected overall	Yes/No	No significant difference because both the NuScale and PWR designs permit item accountability. Smaller fuel pins in the NuScale assemblies make accounting for damaged NuScale fuel

measurement uncertainty of the operator's IC declaration?		pins less significant/more accurate so that damaged assembly/pin inventories have lower uncertainty. (See discussion in the rationale for item 3.1.4.)
3.4. Does this design impede the introduction of or reduce the usefulness of Other Strategic Points (OSP) within a Material Balance Area (MBA)?	Yes/No	The use of an OSP in the fuel transfer canal to maintain an inventory of fuel assemblies in the reactor vessel for the PWR does not translate simply to the NuScale design. However, the designation of OSP in the NuScale removal pool, the unit transfer canal, and the spent fuel storage area will probably be part of the safeguards design concept for NuScale. (See the answers to the subsidiary questions).
3.4.1. Would OSP be less effective in providing CoK of measured/verified nuclear material (e.g., reduce the effectiveness of surveillance systems or containment devices; make installation of these systems/devices more difficult; impede or preclude access to or maintenance of these systems/devices; make interfaces [e.g., utility support or data transmission] more difficult)?	Yes/No	The required collection of OSP for NuScale would be more complex than the simple PWR configuration. As a result the use of OSP would be more difficult; but certainly still possible.
3.4.2. Would OSP be less effective in providing additional assurance for high uncertainty verifications done at KMPs (e.g., reduce opportunities for random short notice sampling by IAEA inspectors; reduce or eliminate opportunities for correlation with measurement data at related locations, reduce the scope or accuracy of Process Monitoring; or limit or preclude IAEA ability to authenticate plant PM systems or introduce independent systems)	Yes/No	No significant difference because both the NuScale and PWR designs permit item accountability. With item accountability, there are no KMPs that make high uncertainty verifications
4. Does this design differ from the comparison design in ways that create new or alter existing opportunities for facility misuse or make detection of misuse more difficult?	Yes/No	The presence of multiple units creates possible opportunities to disguise misuse of one unit by swapping/duplicating operating records with those from other units that were operated in accordance with declared activities. (See answers to subsidiary questions.)

4.1. Does this design differ from the comparison facility/process by including new equipment or process steps that could change the nuclear material being processed to a type, category, or form with a lower significant quantity or detection time objectives?	Yes/No	The production of plutonium by irradiation in the reactor core is essentially the same in both designs.
4.2. Should the comparison facility safeguards approach employ agreed upon short-notice visits or inspections, measurements, or process parameter confirmations, would this design preclude the use of or reduce the effectiveness of these measures?	Yes/No	There are no differences in design that would adversely affect the ability of IAEA inspectors to conduct effective Short-Notice or No Notice Random Inspections.
4.3. Do the design and operating procedures reduce the transparency of plant operations (e.g., availability of operating records and reports or source data for inspector examination or limited inspector access to plant areas and equipment)?	Yes/No	There may be opportunities to disguise unit misuse by swapping/duplicating operating records with those from other units that were operated in accordance with declared activities.

Appendix 14. Facility Safeguardability Analysis Tool for RUTA-70

Question	Response	Reasoning
1. Does this design differ from the comparison design/process in ways that have the potential to create additional diversion paths or alter existing diversion paths?	Yes/No	It is likely that RUTA-70 design doesn't include significant differences in refueling, fuel handling and storage when compared to conventional LWR. The SA utilizing standard safeguards equipment for C/S and monitoring have already been implemented for pool-type research reactors that are similar to RUTA-70. The diversion paths are essentially the same for both research reactors and RUTA-70. However, the research reactor type design is feasible for undeclared production of nuclear material (or other material for weapon production such as neutron sources) by target irradiation. Thus, the design may support facility misuse and diversion of undeclared nuclear material.
1.1. Does this design introduce nuclear material of a type, category, or form that may have a different significant quantity or detection time objective than previous designs/processes (e.g., mixed oxide rather than low enriched uranium, irradiated vs. unirradiated or bulk rather than items)?	Yes/No	RUTA-70 uses similar fuel as VVER-440 (UO ₂) with a difference of around half-height of FAs. In addition, another fuel option (Cermet with 0,4 Al and 0,6 UO ₂) doesn't introduce significant differences.
1.2. Does this design layout eliminate or modify physical barriers that would prevent the removal of nuclear material from process or material balance areas, e.g., circumventing a key measurement point (KMP)?	Yes/No	The reactor pool and interim spent fuel storage pool are located inside the reactor building. Both are situated below-grade and separated from each other. Fuel transfer canal connects these pools. The core is inside a reactor vessel. The reactor pool incorporates a lid that consists of protective slabs. The closed reactor pool and reactor vessel may be appropriate physical barriers against the removal of nuclear material. The design includes storage area for fresh FAs and on-site spent fuel storage facility for spent fuel caskets. However, the pool-type design that is typical for research reactors, may support reactor misuse aims by providing easier insertion of target materials in the core or around it. The design has already considered the research reactor use by the inclusion of irradiation chambers and channels, which indicates the ease of modifications to achieve misuse aims.
1.3. Does this design obscure process areas or material balance area (MBA) boundaries making containment/surveillance or installation of verification	Yes/No	Although little layout information is available, it is likely that there are no significant differences that would make the installation of safeguards equipment more difficult. The design is similar to pool-type research reactors for which SAs involving such equipment already exist. Provision of minimal access paths to fuel and associated transfer routes with safeguards equipment capable of

measurement and monitoring equipment more difficult?		detection should be highlighted. To maintain CoK appropriate sealing of the reactor pool should have further consideration. High priority should be given to safeguards provisions that would facilitate detection of misuse (e.g surveillance/monitoring of target removal/insertion)
1.4. Does this design introduce materials that could be effectively substituted for safeguarded nuclear material to conceal diversion?	Yes/No	The fuel is similar VVER-440 fuel (UO ₂) with a difference of around half-height of FAs. In addition, another fuel option (Cermet with 0,4 Al and 0,6 UO ₂) doesn't introduce significant differences.
Does this design differ from the comparison design in a way that increases the difficulty of design information examination (DIE) and verification (DIV) by IAEA inspectors?	-	IAEA has already conducted DIE/DIV for pool-type research reactor which may benefit such implementation for RUTA-70. However, it is difficult to answer this question because of the lack of detailed design descriptions.
2.1. Does the design incorporate new or modified technology? If so, does the IAEA have experience with the new or modified technology?	Yes/No	The design introduces LWR that is immersed in a closed water pool, thus general technology can be considered similar to conventional LWRs. Similar pool-type research reactors are already in operation and subject to IAEA safeguards. Although RUTA-70 is intended to be used for district heat production, it seems that design doesn't introduce significantly new or modified technology that would be safeguards relevant.
2.2. Are there new design features with commercial or security sensitivities that would inhibit or preclude IAEA inspector access to equipment or information?	-	There is insufficient information in the design descriptions of the RUTA-70 to answer this question.
2.3. Do aspects of the design limit or preclude inspector access to, or the continuous availability of, Essential Equipment for verification or testing?	-	There is insufficient information in the design descriptions of the RUTA-70 to answer this question
2.4. Are there aspects of the design that would preclude or limit IAEA maintenance of Continuity of Knowledge (CoK) associated with design verification during the life of the facility?	-	There is insufficient information in the design descriptions of the RUTA-70 to answer this question
3. Does this design/process differ from the comparison design/process in a way that makes it more difficult to verify that diversion has not taken place?	Yes/No	Overall, there are no significant differences that would make verification more difficult when compared to conventional LWR design.

3.1. Does this design lessen the efficiency of physical inventory taking (PIT) by the operator or the effectiveness of physical inventory verification (PIV) by the IAEA?	Yes/No	The design doesn't seem to include characteristics, that would make it difficult to conduct annual PIT by the operator and subsequent PIV by the IAEA. Although the refueling cycle is once every 3 years, it could be possible to conduct PIT/PIV in periods during which there is no need for district heating and the plant is not in operation. However, short FAs make it possible to double stack FAs in spent fuel storage racks, which impedes inspector access to lower layers of fuel if done so. The design characteristics such as platforms (e.g refueling bridge) that would support inspectors access to conduct nuclear material verification directly from above the FAs should be considered.
3.1.1. Does the plant/process design evaluated reduce the measurement accuracy or otherwise impede the use of Inventory Key Measurement Points (IKMP). If so, are there other well defined locations that could be considered by the IAEA as IKMPs.	Yes/No	The IKMPs are essentially the same as they are for conventional LWRs (fresh fuel storage, reactor core, spent fuel storage pool, on-site spent fuel storage facility). The fuel is similar to VVER-440 which doesn't cause differences in the measurements and their accuracy. It is likely that Cermet as another fuel option would not cause significant differences either. However, if double stacking of FAs in spent fuel storage racks is done, it could impede NDA measurements
3.1.2. Does the plant/process design evaluated impede or preclude the collection/storage of inventory at IKMPs at the time of PIT/PIV?	Yes/No	The IKMPs are essentially the same as they are for conventional LWRs. Collection/storage of inventory at the time of PIT/PIV can be done.
3.1.3. Does the design preclude PIT/PIV measurements on some inventory? If so, does the new design include features to permit CoK to be maintained from a previous measurement and verification?	Yes/No	It seems that PIT/PIV measurements can be conducted for all inventory. However, the possible double stacking of FAs in spent fuel storage could impede NDA measurements.
3.1.4. Does the design/process employ nuclear material types, categories, or forms that are more difficult to measure accurately at IKMP? If so, can the plant accountancy measurement systems meet International Target Values (ITV) for the PIT?	Yes/No	The fuel is similar to VVER-440 which doesn't cause differences in the measurements and their accuracy. It is likely that Cermet as another fuel option would not cause significant differences either. Furthermore, smaller fuel rods in the FAs may make accounting for damaged fuel rods less significant/ more accurate than for conventional LWR (nuclear material in damaged fuel rods is usually booked as an estimate).
3.1.5. Does the design preclude or limit the ability of the IAEA to take/analyze independent samples for the PIV?	-	The potential double stacking of FAs in the spent fuel storage pool impedes PIT and PIV because the upper-level assemblies must be moved to gain visual and NDA access to the FAs on the lower level. However, it is uncertain whether this will be done.

3.1.6. Does the process design preclude controls to prevent inventory change or movement between the time of the PIT and the PIV? If so, does the design include measures to maintain CoK of the changed or moved inventory between the time of the PIT and the PIV?	Yes/No	The nuclear material inventory is stored at defined IKMPs like it is for conventional LWRs. It is likely that access to these locations and associated fuel transfer paths can be minimized and controlled to prevent inventory change and movement. Detailed design information should be reviewed to confirm this. Containment, surveillance, and RMSs can be utilized to maintain CoK for fuel transfers and storage at these locations and pathways.
3.2. Does this design impair the ability of the operator to produce timely and accurate interim inventory declarations or for the IAEA to perform timely and accurate Interim Inventory Verification (IIV)?	Yes/No	Like the conventional LWR, the RUTA-70 design can employ item accountability so interim inventory declarations should not be an issue.
3.2.1 Does design impede or preclude shutdown of the process for an IIV?	Yes/No	The shutdown of the process could be done for an IIV. However, as RUTA-70 is intended to provide baseload district heating this is not feasible during cold periods when there is demand for heat.
3.2.2 Does the design impede or preclude the collection/storage of inventories at IKMP, which provide access for measurement and declaration by the operator and verification by the IAEA, at the interim inventory cut-off time (CoT)?	Yes/No	Although there is little detailed design information available, it seems that there are no differences at IKMPs that would impede measurements, declarations, and verification. Physical inventory and verification can be done for all nuclear inventory during IIT/IIV.
3.2.3 Does design create the potential for Un-Measurable Inventory (UMI) at the time of an IIV in locations such as pipes, pumps, or evaporators? If so, can the UMI be accurately estimated by the operator and can the estimation method be verified by the IAEA?	Yes/No	The NMA and verification are based on fuel items, which all are accessible for counting, sampling and measurements at the time of an IIV. It is not likely that the design could create a potential for UMI.
3.2.4 Does the new plant/process design increase the time required for the operator to provide the IAEA with an Interim Inventory List (IIL) after the CoT	Yes/No	No significant difference because both the RUTA-70 and conventional LWR designs permit item accountability.
3.2.5 Does design increase the expected overall measurement	Yes/No	No significant difference because both the RUTA-70 and conventional LWR designs permit item accountability and similar measurements.

uncertainty of the operator's interim inventory declaration?		
3.2.6 If the comparison facility Safeguards Approach included short-notice or no-notice interim inspections, does the design include real time measurement and accounting systems that allow for almost immediate inventory declarations required to support such inspections?	-	There is insufficient information in the design descriptions of the RUTA-70 to answer this question. However, short-notice and no-notice interim inspections along with real-time measurement and accounting systems should be essential issues to be considered when developing SA.
3.3. Does this design impede timely and accurate inventory change (IC) measurements and declarations by the operator and verification by the IAEA?	Yes/No	Like conventional LWRs, the RUTA-70 design can employ item accountability so interim inventory change measurements and declarations should not be an issue. Using the single MBA approach, the receipt and shipment item counts and verification, including NDA, should be similar for both designs.
3.3.1. Does this design reduce the accuracy of or otherwise impede the use of customary Flow Key Measurement Points (FKMPs). If so, are there other well defined locations that could be considered by the IAEA as FKMP?	Yes/No	The accuracy of FKMPs is not reduced and their use is not impeded. There are no significant differences because design permits item accountability and similar measurements than are used for conventional LWR fuel items.
3.3.2. Does the design increase the measurement uncertainties at FKMPs? If so, can the plant accountancy system meet International Target Values (ITV) for inventory change	Yes/No	The measurement uncertainties are not increased at FKMPs because the design permits item accountability and similar measurements than are used for conventional LWR fuel items. Smaller fuel rods in the RUTA-70 assemblies may make accounting for damaged fuel rods less significant/more accurate.
3.3.3. Does the new design impede or preclude IAEA verification of the IC declarations by sample taking, portable or installed measurements systems, or by joint-use of authenticated operator systems?	Yes/No	There are no significant differences on verification measures when compared to conventional LWRs because similar fuel items are used.
3.3.4. Does the design impede or preclude IAEA verification of calculated IC declarations such as nuclear material loss and gain?	Yes/No	There are no significant differences on because similar fuel items are used and calculation basis for plutonium production and fuel depletion are essentially the same. The calculation of special fissionable material changes due to reactor burnup are subject to commensurate uncertainties
3.3.5. Does the design impede or preclude IAEA verification of IC declarations that are determined	Yes/No	There are no significant differences between RUTA-70 and conventional LWR because similar fuel items are used which allow the same practices. However, smaller FAs may make accounting

indirectly or based on historical measurement data (e.g., waste transfers to retained waste or measured discards), decrease the accuracy of the determinations, or limit the availability of the historical data		for damaged fuel rods less significant/more accurate so that damaged assembly/rod inventories have lower uncertainty.
3.3.6. Does the design increase the time required for the operator to measure, calculate, prepare, and approve the IC declarations?	Yes/No	There is no significant difference because RUTA-70 uses similar fuel items to conventional LWRs. Same measures and approaches can be utilized for declarations. The efforts pertaining to NMA and reporting are likely to be the same.
3.3.7. Does the new design increase the expected overall measurement uncertainty of the operator's IC declaration?	Yes/No	There is no significant difference because RUTA-70 uses similar fuel items to conventional LWRs. However, smaller FAs may make accounting for damaged fuel rods less significant/more accurate so that damaged assembly/rod inventories have lower uncertainty.
3.4. Does this design impede the introduction of or reduce the usefulness of Other Strategic Points (OSP) within a Material Balance Area (MBA)?	Yes/No	Although little information is available about detailed design, it seems that there are no significant characteristics that would reduce/impede OSPs. SAs with OSPs have already been implemented for pool-type research reactors of similar kinds.
3.4.1. Would OSP be less effective in providing CoK of measured/verified nuclear material (e.g., reduce the effectiveness of surveillance systems or containment devices; make installation of these systems/devices more difficult; impede or preclude access to or maintenance of these systems/devices; make interfaces [e.g., utility support or data transmission] more difficult)?	Yes/No	Although little information is available about detailed design, it is likely that effective OSPs can be implemented to provide CoK for nuclear material inventory and associated transfers. The design is similar to pool-type research reactors, for which IAEA already has SAs with equipment such as video cameras, sealing systems, and radiation monitors at OSPs. However, if the design incorporates irradiation chambers and channels for research use, at least sealing of these is difficult to maintain.
3.4.2. Would OSP be less effective in providing additional assurance for high uncertainty verifications done at KMPs (e.g., reduce opportunities for random short notice sampling by IAEA inspectors; reduce or eliminate opportunities for correlation with measurement data at related locations, reduce the scope or accuracy of Process Monitoring; or	Yes/No	No significant difference because both the RUTA-70 and conventional LWR designs permit item accountability. With item accountability, there are no KMPs that make high uncertainty verifications.

limit or preclude IAEA ability to authenticate plant PM systems or introduce independent systems)		
4. Does this design differ from the comparison design in ways that create new or alter existing opportunities for facility misuse or make detection of misuse more difficult?	Yes/No	The pool-type reactor design typical for research reactors may ease modifications that would facilitate undeclared production of nuclear material or other material for weapon production. The misuse could be difficult to detect during baseload district heat production. The design considers potential simultaneous research use along with heat production, which may reduce safeguards efficiency.
4.1. Does this design differ from the comparison facility/process by including new equipment or process steps that could change the nuclear material being processed to a type, category, or form with a lower significant quantity or detection time objectives?	Yes/No	When compared to conventional LWR the pool-type reactor design typical for research reactors may be more feasible for target irradiation. The design has already considered irradiation channels and chambers to be used for research purposes. This indicates the ease of design modification for target insertion/removal that could facilitate undeclared production of nuclear material or other material for weapon production.
4.2. Should the comparison facility safeguards approach employ agreed upon short-notice visits or inspections, measurements, or process parameter confirmations, would this design preclude the use of or reduce the effectiveness of these measures?	Yes/No	The on-site verification measures for similar fuel items are essentially the same. It is likely that there are no design characteristics that would adversely affect the ability of IAEA inspectors to conduct effective Short-Notice or No-Notice Random Inspections. However, detailed design descriptions should be reviewed to confirm this.
4.3. Do the design and operating procedures reduce the transparency of plant operations (e.g., availability of operating records and reports or source data for inspector examination or limited inspector access to plant areas and equipment)?	Yes/No	RUTA-70 is intended to be used for district heat production and if the design incorporates features for research reactor use it will reduce the transparency of plant operations and complicate IAEA verification. The simultaneous district heating operations and research activities would support concealment of facility misuse due to the complexity of IAEA verification and increased potential to falsify operational records.

Appendix 15. Facility Safeguardability Analysis Tool for KLT-40S

Question	Response	Reasoning
1. Does this design differ from the comparison design/process in ways that have the potential to create additional diversion paths or alter existing diversion paths?	Yes/No	The KLT-40S may have technically a bit different refueling operations when compared to conventional PWRs due to the barge-type design. However, the basic process for fuel handling, transfer and storage remains the same. The onboard fuel handling complex likely requires a compact system that may facilitate surveillance/monitoring of activities. The CoK for inventories and equipment can be maintained using conventional C/S. However, the barge type design makes it possible to have extreme diversion scenarios, where the whole nuclear material inventory is diverted. Periodical sea transports between site and maintenance center, onboard fuel handling/transfer equipment, and potential to have the plant located in remote areas, are issues that may support the implementation of these scenarios. The nuclear material inventory onboard is quite large because the intention is to complete four fuel cycles before overhaul. Furthermore, the barge-type design allows diversion scenarios that involve underwater transfers, which may introduce challenges.
1.1. Does this design introduce nuclear material of a type, category, or form that may have a different significant quantity or detection time objective than previous designs/processes (e.g., mixed oxide rather than low enriched uranium, irradiated vs. unirradiated or bulk rather than items)?	Yes/No	KLT-40S FAs use Cermet fuel, that is UO ₂ fuel particles dispersed in an aluminum alloy (silumin) matrix. Average U 235 enrichment is 14,1 % and maximum value of 18,6 % is below 20 %, thus the category remains as low enriched uranium. The metallic matrix enhances PR since nuclear material is more difficult to reprocess
1.2. Does this design layout eliminate or modify physical barriers that would prevent the removal of nuclear material from process or material balance areas, e.g., circumventing a key measurement point (KMP)?	Yes/No	The barge includes IKMPs (two cores, fresh fuel storage, three spent fuel wet storage tanks, four spent fuel dry storage canisters), that are in the center of the deck in the reactor compartment. The core is inside a closed RPV followed by a containment structure. The fresh FAs, wet storage tanks, and dry storage canisters are likely in closed storage rooms. The wet storage tanks and dry storage canisters themselves may act as physical barriers. However, the barge is movable, thus in the extreme case the physical barriers will be eliminated and the whole nuclear inventory could be diverted.
1.3. Does this design obscure process areas or material balance area (MBA) boundaries making containment/surveillance or	Yes/No	Although little layout information is available on the reactor compartment, there are likely no differences that would make the installation of safeguards equipment significantly more difficult. The fuel handling complex comprises automatic systems and

installation of verification measurement and monitoring equipment more difficult?		monitoring for transfers and handling, that provides feasible conditions for the safeguards equipment. A likely compact system is required to execute all operations onboard, which may ease the verification via equipment installations (e.g. limited transfer routes and smaller areas to be monitored). However, the incorporation of safeguards equipment to already compact design may introduce challenges. The sealing of fuel handling/transfer equipment, fresh FAs, wet storage tanks, and spent fuel canisters is likely feasible. Additional safeguards equipment could be utilized to maintain CoK for the barge, if applicable. Surveillance cameras can be utilized to provide a view of the coastal areas. Detectors at sea areas could be used to indicate undeclared material transfers, if possible.
1.4. Does this design introduce materials that could be effectively substituted for safeguarded nuclear material to conceal diversion?	Yes/No	Hexagonal FAs with fuel rods are used. The fuel is UO ₂ dispersed in a silumin matrix (Cermet.) The design doesn't introduce differences.
2. Does this design differ from the comparison design in a way that increases the difficulty of design information examination (DIE) and verification (DIV) by IAEA inspectors?	Yes/No	The reactor design is like conventional PWR. The facility design that is a floating nuclear power unit on a barge is a difference. However, the main safeguards relevant design issues are likely the same as they are in conventional PWR plants. The DIE has already been done for the Akademik Lomonosov and IAEA inspectors conduct continuous DIV for the plant. It is likely, that the difficulty of DIE/DIV is not significantly increased.
2.1. Does the design incorporate new or modified technology? If so, does the IAEA have experience with the new or modified technology?	Yes/No	The reactor design, plant technology, and general process are similar to conventional PWR plants. In addition, the reactor design is derived from KLT-40 that has been utilized for nuclear icebreakers. Overall, it seems that the design doesn't introduce significantly new or modified technology that would be safeguards relevant.
2.2. Are there new design features with commercial or security sensitivities that would inhibit or preclude IAEA inspector access to equipment or information?	-	There is insufficient information in the design descriptions of the KLT-40S to answer this question.
2.3. Do aspects of the design limit or preclude inspector access to, or the continuous availability of, Essential Equipment for verification or testing?	-	There is insufficient information in the design descriptions of the KLT-40S to answer this question. The barge-type facility design introduces some differences in plant layout, which could be relevant for inspector access provision.
2.4. Are there aspects of the design that would preclude or limit IAEA maintenance of Continuity of	Yes/No	There is insufficient information available to answer regarding the technical design of the plant/layout. However, the potential remote, difficult access location of the floating power plant at

Knowledge (CoK) associated with design verification during the life of the facility?		least makes it more difficult to conduct DIV during the lifetime of the plant.
3. Does this design/process differ from the comparison design/process in a way that makes it more difficult to verify that diversion has not taken place?	Yes/No	Overall, there are no significant differences that would make verification more difficult when compared to conventional PWR design.
3.1. Does this design lessen the efficiency of physical inventory taking (PIT) by the operator or the effectiveness of physical inventory verification (PIV) by the IAEA?	Yes/No	The design doesn't seem to include characteristics, that would make it difficult to conduct PIT by the operator and subsequent PIV by the IAEA. The refueling cycle is once every 2,5 - 3 years, it could be possible to conduct PIT/PIV during these periods. The onboard fuel handling complex and quite large nuclear inventory could necessitate yearly PIT/PIV. However, if it is justified that the implemented SA utilizing C/S and monitoring maintains sufficient CoK, inspections may be enough until refueling. The refueling and associated PIT/PIV are done in turns for two reactor cores. In addition, the fresh fuel and spent fuel inventories are verified.
3.1.1. Does the plant/process design evaluated reduce the measurement accuracy or otherwise impede the use of Inventory Key Measurement Points (IKMP). If so, are there other well defined locations that could be considered by the IAEA as IKMPs.	Yes/No	The IKMPs are essentially the same as they are for conventional PWRs (fresh fuel storage, two reactor cores, wet spent fuel storage, dry spent fuel storage). The Cermet fuel doesn't cause differences in the measurements and their accuracy. There is little information available on storage area tank/canister designs, but likely wet storage tanks and dry canisters are accessible for inspectors and nuclear material can be verified by NDA measurements and visual checks.
3.1.2. Does the plant/process design evaluated impede or preclude the collection/storage of inventory at IKMPs at the time of PIT/PIV?	Yes/No	The IKMPs are essentially the same as they are for conventional PWRs. Collection/storage of inventory at the time of PIT/PIV can be done. Two reactor inventories are verified in turns. It seems, that the barge has spent fuel storage capacity for three fuel cycles, thus the fourth core inventories are discharged at the maintenance center.
3.1.3. Does the design preclude PIT/PIV measurements on some inventory? If so, does the new design include features to permit CoK to be maintained from a previous measurement and verification?	Yes/No	It seems that PIT/PIV measurements can be conducted for all inventory. Two reactor inventories are verified in turns.
3.1.4. Does the design/process employ nuclear material types, categories, or forms that are more difficult to measure accurately at	Yes/No	The Cermet fuel likely doesn't cause differences in the measurements and their accuracy. Furthermore, smaller fuel rods in the FAs may make accounting for damaged fuel rods less

IKMP? If so, can the plant accountancy measurement systems meet International Target Values (ITV) for the PIT?		significant/ more accurate than for conventional PWR (nuclear material in damaged fuel rods is usually booked as an estimate).
3.1.5. Does the design preclude or limit the ability of the IAEA to take/analyze independent samples for the PIV?	-	There is insufficient information to answer this question. The detailed design descriptions should be reviewed.
3.1.6. Does the process design preclude controls to prevent inventory change or movement between the time of the PIT and the PIV? If so, does the design include measures to maintain CoK of the changed or moved inventory between the time of the PIT and the PIV?	Yes/No	The nuclear material inventory is stored at defined IKMPs like it is for conventional PWRs. It is likely that access to these locations and associated fuel transfer paths can be minimized and controlled to prevent inventory change and movement. Detailed design information should be reviewed to confirm this. Containment, surveillance, and RMSs can be utilized to maintain CoK for fuel transfers and storage at these locations and pathways.
3.2. Does this design impair the ability of the operator to produce timely and accurate interim inventory declarations or for the IAEA to perform timely and accurate Interim Inventory Verification (IIV)?	Yes/No	Like the conventional PWR, the KLT-40S design can employ item accountability so interim inventory declarations should not be an issue.
3.2.1 Does design impede or preclude shutdown of the process for an IIV?	Yes/No	The shutdown of the process could be done for an IIV, if deemed necessary. There are two reactor units in operation for co-generation.
3.2.2 Does the design impede or preclude the collection/storage of inventories at IKMP, which provide access for measurement and declaration by the operator and verification by the IAEA, at the interim inventory cut-off time (CoT)?	Yes/No	Although there is little detailed design information available, it is likely that there are no differences at IKMPs that would impede measurements, declarations, and verification. Physical inventory and verification can be done for all nuclear inventory during IIT/IIV.
3.2.3 Does design create the potential for Un-Measurable Inventory (UMI) at the time of an IIV in locations such as pipes, pumps, or evaporators? If so, can the UMI be accurately estimated by the operator and can the estimation method be verified by the IAEA?	Yes/No	The NMA and verification are based on fuel items, which all are accessible for counting, sampling and measurements at the time of an IIV. It is not likely that the design could create a potential for UMI.
3.2.4 Does the new plant/process design increase the time required for the operator to provide the IAEA with an Interim Inventory List (IIL)	Yes/No	No significant difference because both the KLT-40S and conventional PWR designs permit item accountability.

3.2.5 Does design increase the expected overall measurement uncertainty of the operator's interim inventory declaration after CoT?	Yes/No	No significant difference because both the KLT-40S and conventional PWR designs permit item accountability and similar measurements.
3.2.6 If the comparison facility Safeguards Approach included short-notice or no-notice interim inspections, does the design include real time measurement and accounting systems that allow for almost immediate inventory declarations required to support such inspections?	-	There is insufficient information in the design descriptions of the KLT-40S to answer this question. However, short-notice and no-notice interim inspections along with real-time measurement and accounting systems should be essential issues to be considered when developing a SA. Especially, if the plant is planned to be sited in remote, difficult to access areas.
3.3. Does this design impede timely and accurate inventory change (IC) measurements and declarations by the operator and verification by the IAEA?	Yes/No	Like conventional PWRs, the KLT 40S design can employ accountability so interim inventory change measurements and declarations should not be an issue. Using the single MBA approach, the receipt, and shipment item counts and verification, including NDA, should be similar for both designs.
3.3.1. Does this design reduce the accuracy of or otherwise impede the use of customary Flow Key Measurement Points (FKMPs). If so, are there other well defined locations that could be considered by the IAEA as FKMP?	Yes/No	The intention is to have fresh fuel inventory for four fuel cycles onboard, thus inventory changes pertaining to fresh fuel reception and spent fuel shipment may occur only during complete overhaul. This practice would eliminate some conventional FKMPs. However, if such transfers/shipments are done, the accuracy of FKMPs is neither reduced nor their use impeded. This is because the design permits item accountability and similar measurements that are used for conventional PWR fuel items.
3.3.2. Does the design increase the measurement uncertainties at FKMPs? If so, can the plant accountancy system meet International Target Values (ITV) for inventory change	Yes/No	The measurement uncertainties are not increased at FKMPs because the design permits item accountability and similar measurements than are used for conventional PWR fuel items. Smaller fuel rods in the KLT-40S assemblies may make accounting for damaged fuel rods less significant/more accurate.
3.3.3. Does the new design impede or preclude IAEA verification of the IC declarations by sample taking, portable or installed measurements systems, or by joint-use of authenticated operator systems?	Yes/No	There are no significant differences on verification measures when compared to conventional PWRs because somewhat similar fuel items are used.
3.3.4. Does the design impede or preclude IAEA verification of calculated IC declarations such as nuclear material loss and gain?	Yes/No	There are no significant differences because somewhat similar fuel items are used and the calculation basis for plutonium production and fuel depletion are essentially the same. The calculation of special fissionable material changes due to burnup are subject to commensurate uncertainties

3.3.5. Does the design impede or preclude IAEA verification of IC declarations that are determined indirectly or based on historical measurement data (e.g., waste transfers to retained waste or measured discards), decrease the accuracy of the determinations, or limit the availability of the historical data	Yes/No	There are no significant differences between KLT-40S and conventional PWR because somewhat similar fuel items are used which allow the same practices. However, smaller FAs may make accounting for damaged fuel rods less significant/more accurate so that damaged assembly/rod inventories have lower uncertainty.
3.3.6. Does the design increase the time required for the operator to measure, calculate, prepare, and approve the IC declarations?	Yes/No	There is no significant difference because KLT-40S uses somewhat similar fuel items to conventional PWRs. Same measures and approaches can be utilized for declarations. The efforts pertaining to NMA and reporting are likely to be the same.
3.3.7. Does the new design increase the expected overall measurement uncertainty of the operator's IC declaration?	Yes/No	There is no significant difference because KLT-40S uses somewhat similar fuel items to conventional PWRs. However, smaller may make accounting for damaged fuel rods less significant/more accurate so that damaged assembly/rod inventories have lower uncertainty.
3.4. Does this design impede the introduction of or reduce the usefulness of Other Strategic Points (OSP) within a Material Balance Area (MBA)?	Yes/No	Although little information is available about detailed design, it seems that there are no significant characteristics that would reduce/impede OSPs. Such points should be defined at coastal and sea areas to maintain CoK.
3.4.1. Would OSP be less effective in providing CoK of measured/verified nuclear material (e.g., reduce the effectiveness of surveillance systems or containment devices; make installation of these systems/devices more difficult; impede or preclude access to or maintenance of these systems/ devices; make interfaces [e.g., utility support or data transmission] more difficult)?	Yes/No	Although little information is available about detailed design, it is likely that effective OSPs can be implemented to maintain CoK for nuclear material inventory and associated transfers. The fuel handling complex design is likely to be compact and may support this aim.
3.4.2. Would OSP be less effective in providing additional assurance for high uncertainty verifications done at KMPs (e.g., reduce opportunities for random shortnotice sampling by IAEA inspectors; reduce or eliminate opportunities for correlation with measurement data at related locations,	Yes/No	No significant difference because both the KLT-40S and conventional PWR designs permit item accountability. With item accountability, there are no KMPs that make high uncertainty verifications.

reduce the scope or accuracy of Process Monitoring; or limit or preclude IAEA ability to authenticate plant PM systems or introduce independent systems)		
4. Does this design differ from the comparison design in ways that create new or alter existing opportunities for facility misuse or make detection of misuse more difficult?	Yes/No	The potential remote, difficult access location of the floating power plant at least makes it harder to conduct IAEA on-site verifications during the lifetime of the plant. In these circumstances, the detection of misuse may reduce if the inspector's access to the site is difficult to arrange. From a technical point of view, there are likely not significant capabilities that would make the design more feasible for undeclared production and its concealment.
4.1. Does this design differ from the comparison facility/process by including new equipment or process steps that could change the nuclear material being processed to a type, category, or form with a lower significant quantity or detection time objectives?	Yes/No	When compared to conventional PWR design there are no equipment or process steps that would introduce differences.
4.2. Should the comparison facility safeguards approach employ agreed upon short-notice visits or inspections, measurements, or process parameter confirmations, would this design preclude the use of or reduce the effectiveness of these measures?	Yes/No	The on-site verification measures for somewhat similar fuel items are essentially the same. However, if the plant is sited in a remote, difficult access area the accessibility of inspectors to the site may be an issue for such inspections.
4.3. Do the design and operating procedures reduce the transparency of plant operations (e.g., availability of operating records and reports or source data for inspector examination or limited inspector access to plant areas and equipment)?	Yes/No	If the plant is sited in remote, difficult access areas the accessibility for inspectors to conduct on-site verification activities such as inspections and DIV may be an issue. In that case, the transparency of plant operations may be reduced.