

Charting Safe Waters for Nuclear Shipping

Risk Based Design Framework for Nuclear Powered Commercial Vessels

MSc Marine Technology - Thesis
Sofoklis Mougis



This page is left blank intentionally.

Thesis for the degree of Master of Science (MSc) in Marine Technology in the specialization of Ship
Design and Marine Engineering

Charting Safe Waters for Nuclear Shipping

Risk Based Design Framework for Nuclear Powered Commercial Vessels

by

Sofoklis Mougis

Performed at

C-Job Naval Architects

25th of September 2026

This thesis (MT.25/26.059.M) is classified as confidential in accordance with the general conditions for
projects performed by the TU Delft.

Company supervisors

Responsible Supervisor: ir. N. de Vries

Responsible Supervisor: ir. R. J. Berendschot

Thesis exam committee

Chair/Responsible Professor: dr. ir. A. A. Kana

Staff Member: dr. ir. H. Polinder

Company Member: ir. R. J. Berendschot

Author Details

Student Number: 6287816

Cover design: Elisavet Mougi

An electronic version of this thesis is available at <http://repository.tudelft.nl/>.



This page is left blank intentionally.

Preface

As I am writing this, I am approaching the end of my academic journey, and I would like to take this opportunity to look back at where it all started.

Five years ago, I left home and moved to the United Kingdom to pursue a dream of combining a bachelor's degree in Mechanical Engineering with competitive swimming. At the time, I could never have imagined that five years later I would be sitting in Delft, finishing an MSc in Marine Technology.

During my time in the UK, I do not think I fully understood the importance of studying or the career that could follow from it. After some difficult decisions and, perhaps more importantly, some important realizations, I decided during the second year of my bachelor's degree to stop competitive swimming. At that point, I knew that I needed a change. I wanted a new wind to sail with.

At the end of my bachelor's studies, I decided to leave the UK and move to the Netherlands to pursue my MSc at TU Delft. Looking back, I can say that this was probably the best decision I have made in my life so far. I am certain that, if I read this again many years from now, I will still feel the same way. Perhaps someone else reading it might also be reminded that sometimes making a difficult change can lead somewhere completely unexpected.

Delft brought its own challenges. For the first time in my life, I was away from competitive swimming for an extended period, which meant changing something that had been a major part of my identity for most of my life. I had always known that there was more to life than swimming, but apparently I had to turn 23 and move to the Netherlands to truly understand that.

In Delft, I met some wonderful people who never knew me primarily as a swimmer. They became an important part of my life and played a significant role in the personal growth I have experienced over the past few years. I would like to take this opportunity to thank them from the bottom of my heart.

None of what I have achieved would have been possible without the support of my parents and my sister. When they were young, they had dreams of their own, some they were able to achieve and others perhaps not. I consider myself extremely fortunate that, despite the difficulties they have faced in their own lives, they have always tried to make mine easier. Whatever decision I make, I know they will stand beside me, even when they may not completely agree with it. That means more to me than I can properly express. I would also like to thank the rest of my family back home and my friends. Each person has influenced my life in a different way and, in their own small or large way, helped shape the person I am today.

Regarding this thesis, I would first like to thank my supervisors at C-Job, Niels de Vries and Robin Berendschot, who each contributed to this project in different ways. Niels taught me many new things and greatly expanded my knowledge in this field, while Robin and I had many long discussions about the topic that often helped me clear my mind, reconsider problems from another perspective, and find a way forward. Finally, I would like to thank my TU Delft supervisor, Austin Kana, for making sure that I remained on track throughout the project and for helping me find a way forward at moments when it seemed that I had reached a dead end. Each of them contributed to this thesis in their own way, and I am extremely grateful for their guidance and support.

I am proud to have reached the end of this chapter and excited to discover what comes next. The future is uncertain, and perhaps that is exactly what makes it exciting. Who knows what comes next? I cannot wait to find out.

And, just for my ego: I know I am probably not the smartest person to graduate with an MSc from TU Delft, but I would like to think I am at least one of the fittest and most aesthetic ones.

Sofoklis Mougis
Hoofddorp, September 2026

This page is left blank intentionally.

*“A ship in harbor is safe,
but that is not what ships are built for.”*

— John A. Shedd

This page is left blank intentionally.

Disclosure of AI Tool Usage

DECLARATION OF GENERATIVE AI AND AI-ASSISTED TECHNOLOGIES IN WRITING

During the preparation of this work the author used OpenAI in order to improve the readability of the paper. After using this tool/service, the author reviewed and edited the content as needed and takes full responsibility for the content of the publication.

This page is left blank intentionally.

Abstract

The global transition towards more sustainable energy systems is placing increasing pressure on the maritime industry to reduce its greenhouse gas emissions. In response, the International Maritime Organization (IMO) has set the ambition of reaching net zero greenhouse gas emissions by/or around 2050. Achieving this objective requires the development and adoption of alternative propulsion technologies capable of supporting the energy demands of commercial shipping. Nuclear propulsion represents an attractive candidate, particularly for long distance shipping, because it can provide continuous high density energy, long operational endurance, and very low operational greenhouse gas emissions during onboard operation. However, its application introduces safety and integration challenges.

Existing maritime, nuclear, and classification requirements provide relevant safety principles, but they remain fragmented and do not provide a single modern methodology for assessing nuclear and maritime hazards together and translating the resulting findings into ship design decisions. To address this problem, the work was divided into two distinct phases.

The first phase established the technical, regulatory, and methodological basis of the study through a literature review. It examined the fundamentals of marine nuclear propulsion, the shipboard systems required to support nuclear safety, relevant safety frameworks and representative accident scenarios, and available risk assessment methods. From this review, Hazard Identification Study (HAZID) and Bow-tie analysis were selected within a Formal Safety Assessment (FSA)-informed structure, supported by Defence-in-Depth (DiD) and an As Low As Reasonably Practicable (ALARP) approach.

The second phase applied this methodology to a reference nuclear powered bulk carrier. A HAZID identified and ranked 95 scenarios across five functional nodes, after which three representative top events were examined in greater detail using Bow-tie analysis. The assessment identified weaknesses related to barrier dependencies, system segregation, release management, electrical support, heat rejection, and severe condition mitigation. These findings were translated into six concept level design recommendations and implemented in a second design iteration.

Twenty scenarios affected by the recommendations were reassessed. Following the second design iteration, no High- or Extreme-risk scenarios remained within this subset, while the number of Medium-risk scenarios decreased and the number of Low-risk scenarios increased. The study concludes that the methodology proposed in this research provides a structured and traceable framework for linking hazard identification, barrier assessment, design improvement, and reassessment. A key finding is that the nuclear installation and the vessel should be developed as one integrated safety system rather than as separate design domains.

This page is left blank intentionally.

Contents

Preface	iii
Disclosure of AI Tool Usage	vii
Abstract	ix
Nomenclature	xix
1 Introduction	1
1.1 Background & Problem Description	1
1.2 Research Objective and Scope	2
1.3 Research Approach	2
1.4 Research Questions and Report Structure	3
2 Fundamentals of marine nuclear propulsion	5
2.1 Fission principles & energy generation	5
2.2 Reactivity & criticality	5
2.3 Radiation	6
2.3.1 Radiation hazards	6
2.3.2 Exposure and contamination	6
2.3.3 Penetration & shielding	7
2.4 Heat generation and removal	7
2.5 Control & protection systems	8
2.6 Core lifetime and refueling strategy	8
2.7 Radioactive waste	9
2.8 Marine nuclear application review	9
2.9 Chapter 2 Conclusion	10
3 Nuclear propulsion operational profiles & system integration	11
3.1 Operational states	11
3.2 Marine operational demand	11
3.3 Nuclear system design	13
3.3.1 Heat transfer	13
3.3.2 Power conversion	13
3.4 Nuclear auxiliary systems	13
3.4.1 Decay heat removal and emergency cooling	14
3.4.2 Electrical power, emergency power and distribution	14
3.4.3 Instrumentation & Control (I&C) and safety systems	14
3.4.4 Heating, Ventilation, and Air Conditioning (HVAC)	15
3.4.5 Fuel handling, spent fuel and radioactive waste systems	15
3.5 Nuclear Ship Arrangement	16
3.5.1 Reactor location	16
3.5.2 Compartmentalization and zoning	17
3.5.3 Segregation of safety pathways	17
3.5.4 Control room and emergency control	17
3.5.5 Integration with propulsion and cargo	18
3.5.6 Port interface and emergency response	18
3.6 Chapter 3 Conclusion	18
4 Regulatory and safety basis and representative accident scenarios	19
4.1 Regulatory and safety basis for nuclear powered commercial vessels	19
4.1.1 Class society guidance	19

4.1.2	Statutory maritime basis (IMO Nuclear Code, INF Code, SOLAS interfaces) . . .	21
4.1.3	Nuclear safety basis from the International Atomic Energy Agency (IAEA)	23
4.2	Representative initiating events and accident scenarios	24
4.2.1	Internal plant events	24
4.2.2	Internal shipboard hazards	25
4.2.3	Maritime initiated events	25
4.2.4	Representative accident scenario set	25
4.3	Chapter 4 Conclusion	26
5	Risk assessment methods	27
5.1	Foundations of risk assessment and risk based design	27
5.1.1	Risk assessment	27
5.1.2	Risk based design	27
5.2	Principles	28
5.2.1	Defence-in-Depth (DiD)	28
5.2.2	As Low As Reasonably Practicable (ALARP)	29
5.3	Criteria for method selection	30
5.4	Qualitative & Quantitative approaches to risk assessment	31
5.5	Assessment frameworks	32
5.5.1	Deterministic & Probabilistic safety analysis (DSA & PSA)	32
5.5.2	Formal Safety Assessment (FSA)	33
5.6	Analytical methods	34
5.6.1	Hazard Identification Study (HAZID) & Hazard and Operability Study (HAZOP) .	34
5.6.2	Bow-tie method	35
5.6.3	Failure Modes and Effects Analysis (FMEA) & Failure Modes, Effects and Criti- cality Analysis (FMECA)	36
5.7	Comparison & Selection	36
5.7.1	Selection rationale	38
5.8	Chapter 5 Conclusion	38
6	Reference Vessel Concept and Assessment Basis	39
6.1	Reference vessel and system design	39
6.1.1	Vessel mission and operating profile	39
6.1.2	Principal vessel dimensions	40
6.1.3	Nuclear heat source	40
6.1.4	Power conversion system	40
6.1.5	Seawater heat rejection system	41
6.1.6	Electrical power and propulsion system	41
6.1.7	Nuclear and machinery space arrangement	41
6.2	Assessment objectives	41
6.2.1	Nuclear and ship safety objectives	41
6.2.2	Defence-in-Depth (DiD) objective	44
6.2.3	As Low As Reasonably Practicable (ALARP) objective	44
6.3	Assessment scope, constraints and assumptions	44
6.3.1	Ship design constraints	44
6.3.2	Assessment scope and system boundaries	44
6.3.3	Assessment assumptions	46
6.4	Risk ranking method	46
6.4.1	Severity Index	46
6.4.2	Frequency Index	47
6.4.3	Risk Index and risk categories	47
6.4.4	Initial and residual risk	47
6.4.5	Safeguard classification	48
6.4.6	DiD assignment	48
6.5	Design iteration and evaluation structure	48
6.5.1	REV0: Initial concept	48
6.5.2	REVA: First design iteration configuration	49

6.5.3	REVB: Safety driven second iteration	49
6.5.4	Traceability between assessment and design	49
6.6	Chapter 6 Conclusion	49
7	Risk Assessment and First Design Iteration	51
7.1	Application sequence for the first design iteration	51
7.2	HAZID application	52
7.2.1	Node and boundary definition	52
7.2.2	Guidewords and deviations	53
7.2.3	Scenario construction	53
7.2.4	Initial risk assessment	53
7.2.5	Existing safeguard assessment	53
7.2.6	Data processing and visualization	54
7.3	First iteration HAZID results	54
7.3.1	Initial risk picture	54
7.3.2	Risk picture after existing safeguards	55
7.3.3	Interpretation of the HAZID results	55
7.4	Selection of representative top events for Bow-tie analysis	56
7.5	Bow-tie construction and assessment	56
7.5.1	Bow-tie structure	57
7.5.2	HAZID traceability	58
7.5.3	Barrier classification	58
7.5.4	DiD assessment	59
7.6	Bow-tie results and escalation path analysis	59
7.6.1	Loss of primary helium circuit pressure boundary integrity	59
7.6.2	Loss of steam generator tube integrity	60
7.6.3	Loss of ship service electrical power	61
7.6.4	Cross-cutting barrier findings	63
7.7	Synthesis of first iteration findings	63
7.8	Implementation of the first design iteration	64
7.9	Chapter 7 Conclusion	66
8	Design Recommendations and Second Design Iteration	67
8.1	Translation of assessment findings into design recommendations	67
8.2	Design recommendations	69
8.2.1	REC-1: Segregated seawater cooling and condensing trains	70
8.2.2	REC-2: Controlled handling of potentially contaminated relief flow	70
8.2.3	REC-3: Controlled turbine side pressure relief	71
8.2.4	REC-4: Segregated electrical distribution	73
8.2.5	REC-5: Seawater discharge monitoring and isolation	74
8.2.6	REC-6: Normally unmanned nuclear compartment and controlled manned intervention	75
8.3	Implementation in the second design iteration	76
8.4	Second iteration assessment results	79
8.4.1	Selection of scenarios affected by the recommendations	79
8.4.2	Risk reassessment after design recommendations	80
8.4.3	Effect on Defence-in-Depth (DiD)	82
8.4.4	ALARP-oriented evaluation	83
8.5	Evaluation and discussion	84
8.5.1	Evaluation of the combined methodology	84
8.5.2	General ship design implications	84
8.5.3	Limitations of the second iteration	85
8.6	Chapter 8 Conclusion	86
9	Conclusion	87
9.1	Conclusions	87
9.1.1	Summary and Answer to the Main Research Question	87
9.1.2	Design considerations derived from this study	88

9.2 Research limitations and recommendations for further work	89
9.3 Personal Reflection	90
References	93
A Supplementary Literature and Method Material	99
B Reference Design and Drawing Revisions	105
C HAZID Register first iteration	111
D First Iteration Bow-tie Analysis	133
E Design Recommendation Traceability and Second Iteration Results	137

List of Figures

2.1	Example of fertile to fissile. [11]	6
2.2	Simplified comparison of the penetration and shielding of different types of ionizing radiation. [12]	7
2.3	Heat transfer mechanisms in fuel rods and Pressurized Water Reactor (PWR) systems.	8
3.1	HTGR module section. [16]	15
3.2	Nuclear ship protection concept illustrating radioactivity containment, radiation shielding, the reactor compartment boundary, and collision protection structures. [21]	16
3.3	Reactor placement. [21]	17
3.4	Example of 4 module HTGR plan. [16]	17
3.5	Simplified Example Arrangement of Nuclear Power Service Vessel. [6]	18
4.1	Classification of representative initiating events	24
5.1	Tolerability of risk used to explain ALARP decisions, adapted from [39].	30
5.2	Comparison of the reviewed approaches and assessment frameworks against the criteria.	37
5.3	Method–criteria applicability matrix.	37
6.1	Reference REV0 vessel arrangements used to define the machinery space locations for the risk assessment.	42
6.2	Reference nuclear reactor and REV0 principal system interfaces for the risk assessment.	43
6.3	Functional HAZID nodes and their interfaces	45
7.1	Applied risk based design workflow used in the first design iteration.	52
7.2	Global Hazard Identification Study (HAZID) risk distribution before and after crediting the existing safeguards.	55
7.3	Simplified Bow-tie for loss of primary helium circuit pressure boundary integrity	58
7.4	Simplified Bow-tie for loss of steam generator tube integrity	61
7.5	Simplified Bow-tie for loss of ship service electrical power	62
7.6	Comparison of the REV0 and REVA nuclear island arrangements.	65
7.7	Comparison of the REV0 and REVA general arrangements.	66
8.1	Second iteration workflow showing how first iteration findings are translated into Safety driven second design iteration (REVB) design changes and reassessed.	68
8.2	Comparison of the REVA and REVB nuclear compartment arrangements showing the controlled relief routing introduced in the second design iteration.	71
8.3	Comparison of the REVA and REVB turbine-generator arrangements showing the additional turbine side pressure relief provision introduced in REVB.	72
8.4	Comparison of the REVA and REVB electrical distribution arrangements showing the increased physical and functional segregation introduced in the second design iteration.	74
8.5	Comparison of the REVA and REVB seawater cooling arrangements showing the additional discharge monitoring and isolation provision introduced in REVB.	75
8.6	Comparison of the REVA and REVB nuclear island arrangements.	78
8.7	Comparison of the REVA and REVB general arrangements.	79
8.8	Risk matrix development for the scenarios affected by the design recommendations across the three assessment states.	81
A.1	FSA process structure per IMO FSA Guidelines [36]	101
A.2	Standardized Qualitative Risk Assessment (QIRA) workflow used in HAZID & Hazard and Operability Study (HAZOP) workshops [41].	101

A.3	Risk matrix structure and indexing used for HAZID & HAZOP with frequency categories Extremely remote (1) to Frequent (7), adapted from [41].	102
A.4	Generic Bow-tie structure.	102
A.5	Typical Failure Modes and Effects Analysis (FMEA) & Failure Modes, Effects and Criticality Analysis (FMECA) workflow. [47], [48]	103
B.1	Reference design drawing of nuclear island	105
B.2	Reference design drawing of general arrangement	106
B.3	First iteration design drawing of nuclear island	107
B.4	First iteration design drawing of general arrangement	108
B.5	Final design drawing of nuclear island	109
B.6	Final design drawing of general arrangement	110
D.1	Detailed first iteration Bow-tie for loss of primary helium circuit pressure boundary integrity.	133
D.2	Detailed first iteration Bow-tie for loss of steam generator tube integrity.	134
D.3	Detailed first iteration Bow-tie for loss of ship service electrical power.	135
E.1	HAZID scenarios affected by the design recommendations and their risk ranking development across the three assessment states.	137
E.2	Updated second iteration Bow-tie for loss of primary helium circuit pressure boundary integrity, including the applicable design recommendations.	138
E.3	Updated second iteration Bow-tie for loss of steam generator tube integrity, including the applicable design recommendations.	139
E.4	Updated second iteration Bow-tie for loss of ship service electrical power, including the applicable design recommendations.	140

List of Tables

3.1	Representative reactor and vessel operating modes considered in this thesis.	12
4.1	Comparative summary of the main contributions of the class societies to the safety of nuclear powered commercial vessels [7, 6, 5, 8]	21
4.2	How situations are defined as PPCs based on their occurrence frequency. [3].	22
4.3	Comparative summary of the main contributions of the IMO statutory instruments to the safety basis of nuclear powered commercial vessels [3, 32, 33].	22
4.4	Comparative summary of the main contributions of the IAEA safety sources to the safety basis of nuclear powered commercial vessels [29, 34].	23
4.5	Representative initiating events and accident conditions carried forward into the assessment.	25
5.1	Summary of the five levels of DiD [28]	28
5.2	Comparison of qualitative and quantitative risk assessment approaches.	32
5.3	Comparison of Deterministic Safety Analysis (DSA) and Probabilistic Safety Analysis (PSA) for uncertainty management and safety decision support [43], [44], [34].	33
5.4	Method-selection criteria used in the comparison	37
6.1	Principal dimensions of the reference vessel	40
6.2	Reference reactor parameters	40
6.3	Functional nodes used in the HAZID.	45
6.4	Main assumptions used in the risk assessment	46
6.5	Definition of the Severity Index, adapted from [36].	47
6.6	Definition of the Frequency Index [36].	47
6.7	Risk Index categories used in the HAZID	48
7.1	Initial HAZID risk distribution before existing safeguards.	55
7.2	Top events selected for Bow-tie analysis	57
7.3	Main findings from the first iteration Bow-tie assessment	63
8.1	Design recommendations derived from the first iteration assessment	69
8.2	Main safety related differences between First design iteration configuration (REVA) and REVB	77
8.3	Risk development for the scenarios affected by design recommendations	80
8.4	Principal Defence-in-Depth (DiD) contribution of the recommendations	83
8.5	Evaluation of the applied methodology against the selection criteria	84
A.1	Civilian nuclear powered vessels. [9]	99
A.2	Key characteristics of advanced reactor concepts [9], [56].	100
A.3	PSA levels: scope, modelling focus, and typical outputs [44].	100
A.4	Bow-tie layout notation and symbol explanation	103

This page is left blank intentionally.

Nomenclature

ABS American Bureau of Shipping.

ALARP As Low As Reasonably Practicable.

DiD Defence-in-Depth.

DNV Det Norske Veritas.

DSA Deterministic Safety Analysis.

ETA Event Tree Analysis.

FMEA Failure Modes and Effects Analysis.

FMECA Failure Modes, Effects and Criticality Analysis.

FSA Formal Safety Assessment.

FTA Fault Tree Analysis.

GFR Gas-Cooled Fast Reactor.

HAZID Hazard Identification Study.

HAZOP Hazard and Operability Study.

HTGR High Temperature Gas Reactor.

HVAC Heating, Ventilation, and Air Conditioning.

I&C Instrumentation & Control.

IAEA International Atomic Energy Agency.

IMO International Maritime Organization.

LFR Lead-Cooled Fast Reactor.

LOCA Loss of Coolant Accident.

LR Lloyd's Register.

MIT Massachusetts Institute of Technology.

MSR Molten Salt Fast Reactor.

MTF Maritime Technologies Forum.

NPP Nuclear Power Plant.

NSSS Nuclear Steam Supply System.

PPC Power Plant Condition.

PSA Probabilistic Safety Analysis.

PWR Pressurized Water Reactor.

QIRA Qualitative Risk Assessment.

QnRA Quantitative Risk Assessment.

REV0 Initial vessel and nuclear island concept.

REVA First design iteration configuration.

REVB Safety driven second design iteration.

RMRS Russian Maritime Register of Shipping.

SFR Sodium-Cooled Fast Reactor.

SMR Small Modular Reactor.

SOLAS Safety of Life at Sea.

ToR Terms of Reference.

This page is left blank intentionally.

1

Introduction

Nuclear propulsion is being reconsidered for commercial shipping because of its potential to provide low operational greenhouse gas emissions, high energy density, and long endurance. Its application to commercial vessels, however, introduces safety challenges that extend beyond the reactor installation itself. Nuclear safety functions must be maintained within a moving and space constrained vessel exposed to maritime hazard.

This chapter defines the problem addressed by the research, establishes the research objective and scope, presents the research approach and questions, and outlines the structure of the thesis.

1.1. Background & Problem Description

The maritime sector is exploring alternative energy systems to reduce greenhouse gas emissions and support long term decarbonization. Nuclear propulsion represents one possible pathway because it can provide continuous, high energy density power with low direct greenhouse gas emissions during onboard operation. The investigation of its safe application to commercial shipping is therefore relevant to the wider maritime decarbonization and technology-development objectives reflected in the Dutch Sectoragenda Maritieme Maakindustrie and the European Green Deal [1, 2].

Despite this potential, safety, regulation, operation, and public acceptance remain major barriers to the commercial adoption of nuclear propulsion. A nuclear powered commercial vessel combines two safety domains that have traditionally been addressed separately. Nuclear safety requires continued control of reactivity, removal of reactor heat, and confinement of radioactive material. Maritime safety must additionally consider ship motions, structural damage, machinery space fire and flooding, loss of propulsion, loss of electrical power, and the limited availability of external emergency support while at sea.

No modern and universally accepted framework currently provides a complete safety basis for civilian nuclear powered commercial vessels. Conventional ships operate within a mature statutory and classification framework governed principally through the International Maritime Organization (IMO), conventions such as Safety of Life at Sea (SOLAS), flag administrations, and class societies. Nuclear installations are governed through a separate body of safety principles, regulatory practices, and assessment methods developed mainly for land based facilities.

The principal international maritime reference for nuclear propulsion remains the IMO Code of Safety for Nuclear Merchant Ships, adopted as Resolution A.491(XII) in 1981 [3]. The Code predates modern Small Modular Reactor (SMR) concepts, contemporary International Atomic Energy Agency (IAEA) safety assessment practices, and current commercial ship system designs. Military nuclear vessel standards and land based nuclear regulations are also not directly transferable because they are based on different operating objectives, institutional arrangements, emergency provisions, and design assumptions.

The resulting problem is therefore not simply an absence of individual safety requirements. Relevant

principles are available across maritime regulations [3], nuclear safety standards [4], and classification guidance [5, 6, 7, 8], but they remain fragmented. In particular, there is no generally prescribed concept level methodology showing how hazards involving the reactor, supporting ship systems, and maritime operating environment should be assessed and how the resulting safety findings should be translated into ship design decisions.

To address this methodological gap, the present thesis adopts a structured risk based design approach. The approach identifies credible nuclear and maritime hazards, examines how failures may escalate across system boundaries, assesses the function and independence of the available safeguards, and uses the resulting risk insights to guide development of the vessel arrangement and supporting system design.

1.2. Research Objective and Scope

The objective of this research is to develop and apply a structured risk based design methodology for the concept level safety assessment of a nuclear powered commercial vessel.

The methodology is intended to connect hazard identification, risk ranking, accident pathway analysis, barrier assessment, and ship design development within one traceable process. Its purpose is not only to identify and categorize hazards, but also to determine where system design, arrangement, segregation, supporting services, or mitigation functions require further development.

The methodology is applied to a reference nuclear powered bulk carrier fitted with a High Temperature Gas Reactor (HTGR), an indirect steam Rankine power conversion system, all electric propulsion, and seawater heat rejection. The assessment focuses on the interaction between the reactor, primary helium circuit, steam-water system, seawater cooling system, electrical distribution, machinery space arrangement, and representative maritime hazards.

The work is conducted at concept design level. Detailed reactor physics calculations, thermal hydraulic simulations, structural accident calculations, radiological consequence modeling, component level reliability analysis, human reliability analysis, security assessment, port emergency planning, and formal cost effectiveness analysis are outside the detailed scope.

The research therefore supports an As Low As Reasonably Practicable (ALARP)-oriented design process, but it does not constitute a formal ALARP demonstration, a licensing level safety case, or quantitative proof that the reference vessel has achieved a level of safety equivalent to that of conventional ships.

1.3. Research Approach

The objective of the study is addressed through an iterative risk based design process consisting of the following stages:

1. Establish the technical basis of marine nuclear propulsion and identify the principal shipboard systems and operational functions required to support nuclear safety, as presented in Chapters 2 & 3;
2. Review the relevant maritime, classification, and nuclear safety frameworks and define representative accident conditions for nuclear powered commercial vessels, as presented in Chapter 4;
3. Compare available risk assessment principles, frameworks, and analytical methods against the concept level requirements of the study, as presented in Chapter 5;
4. Define a reference vessel, assessment boundaries, assumptions, risk ranking method, and design iteration structure, as presented in Chapter 6;
5. Apply the selected risk assessment methodology to the reference vessel and use the resulting insights to inform the design process, as presented in Chapter 7;
6. Translate the assessment findings into concept level design recommendations, implement them in a second design iteration, and reassess the affected scenarios, as presented in Chapter 8.

The selected analytical methods are applied in a complementary manner to support the structured assessment of the reference vessel. Together, they provide a basis for identifying relevant safety sce-

narios, examining the adequacy of the existing protection measures, and informing the subsequent stages of the design process.

1.4. Research Questions and Report Structure

To support the research objective, the following main research question is addressed:

‘How can risk based design be applied to the safety assessment for nuclear powered commercial vessels, and what ship design implications follow from this approach?’

The main research question is supported by the following sub-questions:

1. *Chapter 2: What are the fundamental principles of marine nuclear propulsion?*
2. *Chapter 3: What are the main shipboard systems and operational functions that must be considered when integrating a nuclear power system into a vessel?*
3. *Chapter 4: What nuclear, maritime, and classification safety frameworks are relevant, and what limitations exist for commercial ship concepts?*
4. *Chapter 5: What risk based assessment principles and methods can be used to support the safety evaluation of nuclear powered commercial vessels?*
5. *Chapter 6: How can a reference vessel concept be established to provide a consistent basis for risk assessment?*
6. *Chapter 7: How can a structured risk based methodology be applied to assess safety events and identify safeguard limitations?*
7. *Chapter 8: What design and safety recommendations follow from the risk assessment of the selected safety events?*

The first four questions establish the technical, regulatory, and methodological basis of the study. Chapter 2 introduces the fundamental principles of marine nuclear propulsion. Chapter 3 examines reactor operating conditions, supporting shipboard systems, and nuclear plant integration. Chapter 4 reviews the applicable maritime, classification, and nuclear safety basis and defines representative accident scenarios. Chapter 5 compares the available risk assessment approaches and justifies the selected methodology.

The research phase begins in Chapter 6, which establishes the reference vessel and the assessment basis. Chapter 7 presents the application of the selected methodology to the vessel concept. Chapter 8 describes how the assessment outcomes are used to support further design development and evaluation. Chapter 9 summarizes the main conclusions, discusses the broader implications and limitations of the research, and identifies areas for further work.

This page is left blank intentionally.

2

Fundamentals of marine nuclear propulsion

What are the fundamental principles of marine nuclear propulsion?

This chapter establishes the nuclear engineering principles most relevant to marine propulsion and shipboard safety. It examines controlled fission, reactivity, radiation protection, heat and decay heat removal, reactor control, fuel life, radioactive waste, and the main lessons from previous civilian marine applications. The purpose is to provide the technical foundation required for the later assessment of ship integration and accident scenarios.

2.1. Fission principles & energy generation

Nuclear propulsion is based on controlled fission in the reactor core. In power reactors, the most important fissile nuclides are uranium-235 ($^{235}\text{U}_{92}$) and, in some concepts, plutonium-239 ($^{239}\text{Pu}_{94}$). When a fissile nucleus absorbs a neutron, it becomes unstable and splits into lighter fission products, releasing additional neutrons and a large amount of energy. Most of this energy appears first as kinetic energy of the fission fragments and neutrons and is then rapidly converted into heat within the fuel. This heat forms the basis of the ship's propulsion and electrical power supply. [9]

For the purposes of this study, the key distinction is between fissile and fertile material. Fissile material can sustain the fission chain reaction directly under suitable neutron conditions [10], whereas fertile material does not normally fission under thermal neutrons but can be converted into a fissile isotope through neutron absorption and radioactive decay. Uranium-238 ($^{238}\text{U}_{92}$) and thorium-232 ($^{232}\text{Th}_{90}$) are the most common fertile materials discussed in reactor technology [11]. An example of this conversion is shown in Figure 2.1 where thorium-232 ($^{232}\text{Th}_{90}$), after absorbing a neutron, decays into protactinium-233 ($^{233}\text{Pa}_{91}$), which similarly then decays into uranium-233 ($^{233}\text{U}_{92}$). Their relevance here is not to compare complete fuel cycles in detail, but to show that reactor type, fuel management strategy, core lifetime, and waste characteristics are all influenced by the choice of fuel and conversion pathway. [9]

2.2. Reactivity & criticality

A reactor can operate safely only if its neutron population and resulting power level remain controlled. In many thermal reactor concepts, fast neutrons produced by fission are slowed by a moderator to energies at which the probability of inducing further fission in uranium-235 is higher. At the same time, neutrons may be absorbed by the fuel, moderator, coolant, structural materials, and control materials, while others may leak from the core. Reactor behavior is therefore governed by the balance between neutron production, absorption, and leakage [9].

This balance is quantified using the effective neutron multiplication factor, k_{eff} , defined as the ratio between the neutron populations in two successive generations:

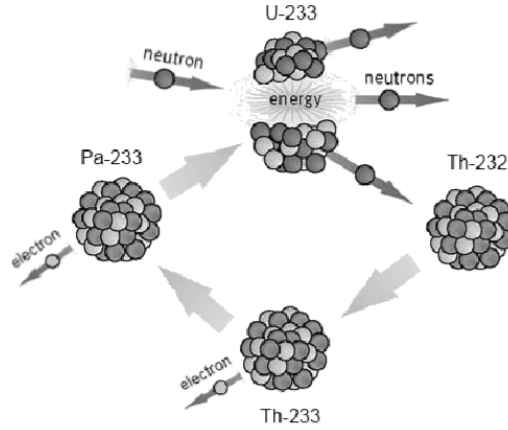


Figure 2.1: Example of fertile to fissile. [11]

$$k_{\text{eff}} = \frac{N_{n+1}}{N_n},$$

where N_n and N_{n+1} represent the neutron populations in successive generations.

- If $k_{\text{eff}} < 1$, the reactor is subcritical and the neutron population decreases;
- if $k_{\text{eff}} = 1$, the reactor is critical and the neutron population remains stable; and
- if $k_{\text{eff}} > 1$, the reactor is supercritical and the neutron population increases.

Reactivity expresses the departure of the reactor from the critical condition and is controlled through mechanisms such as control rods, inherent feedback effects, and, in some reactor concepts, soluble neutron absorbers. For this thesis, the main significance of reactivity control is its role in regulating reactor power, responding safely to operational transients, and bringing the reactor to a subcritical condition when shutdown is required. Changes in propulsion demand are managed by the wider integrated energy system, while reactivity control ensures that the reactor itself remains within its permitted operating limits.

2.3. Radiation

In [10], radiation refers to energy emitted from nuclei or produced by nuclear processes, which is then transported through matter either as particles or as electromagnetic waves. The distinction that matters for safety is whether the radiation is ionizing. Ionizing radiation is radiation that can deposit enough energy in matter to produce ions. The most relevant ionizing radiation types for nuclear fundamentals are alpha, beta, gamma, and neutrons.

2.3.1. Radiation hazards

Ionizing radiation is dangerous because it can ionize atoms and molecules in living tissue and thereby disrupt normal biological function. At the cellular level, ionisations and excitations can produce harmful effects depending on what structures are affected. The severity of harm depends mainly on the dose received and the conditions of exposure. [10]

2.3.2. Exposure and contamination

Exposure¹ is about receiving dose from a radiation field, such as being near a source emitting gamma rays. Contamination² however, is different; it is the presence of radioactive material itself. This distinc-

¹Exposure refers to being subjected to ionizing radiation. In practical terms, when a person is exposed and absorbs some radiation energy, the person receives a radiation dose.

²Contamination refers to radioactive material being present where it is not wanted, for example, on a surface, in a fluid, or within the body. It can keep producing exposure until it is removed, contained, or decays.

tion is important because exposure can often be reduced by shielding, distance, and time management, whereas contamination requires controlling the spread of radioactive material and removing it where necessary. [10]

2.3.3. Penetration & shielding

A key difference between radiation types is their penetrating power, which directly determines the kind of shielding and operational controls required. Figure 2.2 provides a simple qualitative comparison [10]:

- Alpha (α) particles are stopped by very thin barriers such as paper;
- Beta (β) particles penetrate further but can be blocked by relatively thin metal, such as aluminum;
- Gamma (γ) rays are far more penetrating and require thick, dense shielding such as lead to attenuate the field.
- Neutrons (n) can penetrate deeply, and effective shielding relies on hydrogen-rich materials like water and bulk shielding such as concrete, which reduce neutron energy and intensity.

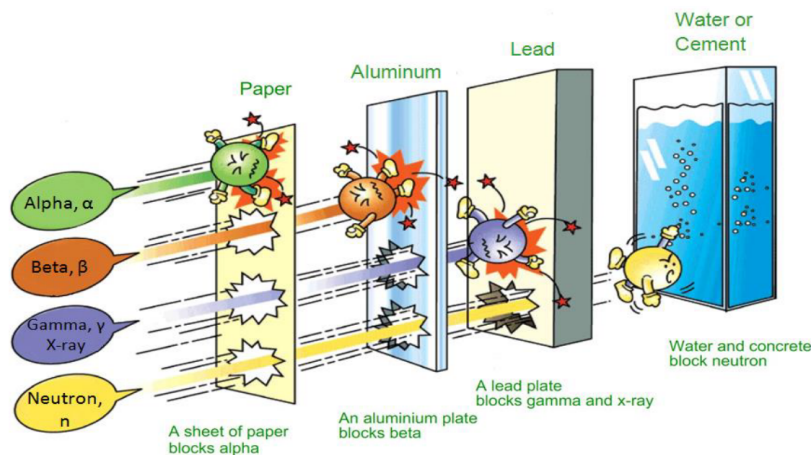


Figure 2.2: Simplified comparison of the penetration and shielding of different types of ionizing radiation. [12]

2.4. Heat generation and removal

The primary function of a nuclear reactor is to generate heat through controlled fission, while the cooling system transfers this heat away from the fuel and towards the power conversion system. The detailed heat transfer path depends on the reactor concept, fuel form, coolant, and system configuration.

In conventional water cooled reactors, heat is transferred by conduction from the fuel pellets, across the fuel-cladding gap, and through the cladding, before being transferred by convection to the coolant, as illustrated in Figure 2.3a. This represents a typical fuel rod arrangement and should not be interpreted as a universal configuration for all reactor technologies [13].

Different reactor concepts employ different fuel configurations, coolants, and pressure-temperature regimes. PWRs use high pressure liquid water to prevent bulk boiling within the core, while boiling water reactors permit controlled boiling. The heat-transfer chain of a typical PWR is shown in Figure 2.3b. By contrast, an HTGR transfers heat from coated fuel particles embedded within a graphite structure to a helium coolant. The helium may then transfer heat through a steam generator or intermediate heat exchanger, depending on the selected power conversion arrangement. Other advanced reactor concepts may use coolants such as liquid sodium or lead.

For the present study, the most important common requirement is that heat removal must continue after reactor shutdown. Although the fission chain reaction is terminated, radioactive fission products continue to generate decay heat. Shutdown therefore does not eliminate the need for cooling. In a marine application, this creates a continuing requirement for reliable decay heat removal, supporting electrical power where required, and an available ultimate heat sink under both normal and accident conditions.

This requirement forms the direct link between the reactor fundamentals discussed in Chapter 2 and the auxiliary system and ship integration considerations examined in Chapter 3.

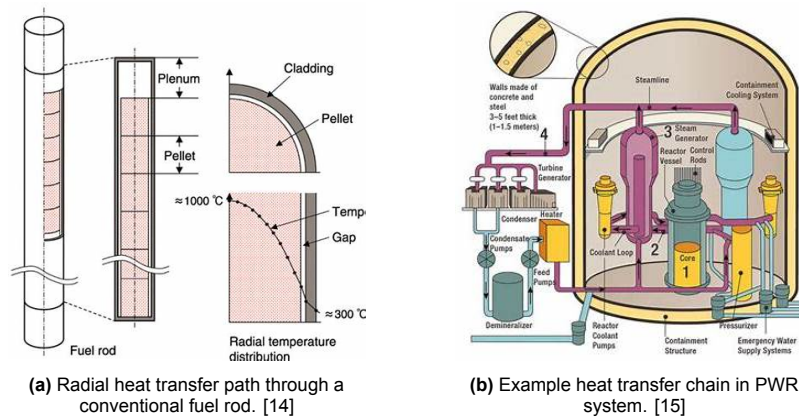


Figure 2.3: Heat transfer mechanisms in fuel rods and PWR systems.

2.5. Control & protection systems

Control and protection systems regulate reactor power, maintain key plant parameters within their permitted operating limits, and initiate protective actions when predefined limits or set points are exceeded. Reactivity is commonly controlled by mechanical devices such as control rods and, in some water cooled reactor designs, by soluble neutron absorbers within the coolant. Instrumentation continuously monitors parameters such as neutron flux, reactor power, coolant temperature, pressure, and flow rate to support both normal control and protective functions [13].

A key feature of reactor control is the presence of delayed neutrons, which are emitted by certain fission products following fission. Although they represent only a small fraction of the total neutron population, delayed neutrons slow the response of reactor power sufficiently for reactivity to be controlled using engineered mechanical systems. They are therefore fundamental to the stable and controllable operation of a power reactor. After shutdown, radioactive fission products also continue to generate decay heat, which must be removed even though the self sustaining fission chain reaction has ended [13].

In a marine application, the integrated nuclear energy system must accommodate changes in propulsion and ship service demand without exceeding reactor, thermal, electrical, or mechanical limits. Depending on the selected Nuclear Power Plant (NPP), mismatches between reactor heat production and electrical demand may be managed through reactor load following, turbine control, controlled heat rejection, electrical energy storage, or other load buffering arrangements. The control and protection systems must also remain reliable under shipboard conditions, including vibration, motion, humidity, temperature variation, and the effects of fire or flooding [7, 6].

2.6. Core lifetime and refueling strategy

For marine nuclear propulsion, core lifetime refers to the operating period between refueling or major fuel related core interventions, rather than to the physical lifetime of the ship or reactor vessel [9]. Long core lifetimes are attractive for commercial shipping because nuclear refueling is infrequent and requires specialized infrastructure, radiological controls, regulatory oversight, and extended periods out of service. A longer interval between refueling can therefore reduce logistical dependence, limit operational disruption, and improve endurance, particularly for vessels operating on long distance or regular routes. These benefits must, however, be balanced against constraints associated with fuel enrichment, achievable burn up, core power density, reactivity management, and reactor size [7].

An important design question is whether the core lifetime should approach or match the intended service life of the vessel. For some marine reactor concepts, a long life or ship life core could reduce the need for routine refueling and allow major fuel related intervention to coincide with reactor module replacement, a major refit, or end of life dismantling [6, 16]. Achieving such a lifetime is nevertheless

strongly dependent on the selected reactor and fuel design. Within the applicable fuel enrichment and regulatory constraints, it may require lower specific power, increased fuel inventory, conservative operating margins, and careful management of reactivity over the full operating period. These requirements may increase core dimensions, reactor mass, shielding demand, and capital cost, although the resulting trade offs are concept specific rather than universal. [9]

For this thesis, the main implication is that core lifetime is not solely a fuel cycle consideration. It also affects ship arrangement, reactor module accessibility, maintenance philosophy, refit planning, decommissioning strategy, and commercial availability.

2.7. Radioactive waste

Nuclear power generation produces no direct CO_2 emissions during reactor operation, but it generates radioactive materials that require controlled handling, storage, and disposal. If radioactive material is not adequately contained and managed, it may result in environmental contamination and radiological exposure to workers or members of the public.

Radioactive waste is not a uniform category. The required management approach depends on characteristics such as activity concentration, radionuclide content, physical form, heat generation, and radioactive half life³. These characteristics determine the duration and magnitude of the radiological hazard and consequently influence the requirements for containment, shielding, storage, transport, and final disposal. Radioactive waste management must therefore be considered over the complete life cycle, from waste generation and characterization to treatment, storage, transport, and disposal. A commonly used broad classification distinguishes between [10]:

- low-level waste;
- intermediate-level waste; and
- high-level waste.

Spent nuclear fuel⁴ is a particularly important radioactive material requiring long term management. Following removal from the reactor, its radioactivity and decay heat generation decrease with time. This time-dependent behavior affects the required cooling, shielding, storage period, transport arrangements, and eventual disposal or reprocessing strategy. [10]

For a marine nuclear application, radioactive waste management also has direct ship design implications. Adequate space, shielding, containment, monitoring, handling routes, and temporary storage must be provided onboard, while arrangements are also required for transferring radioactive material to licensed shore facilities. These requirements affect compartment layout, maintenance planning, port interfaces, and the vessel's eventual decommissioning strategy.

2.8. Marine nuclear application review

Historical experience with civilian nuclear powered vessels remains limited compared with the extensive use of nuclear propulsion by naval vessels and submarines. The four merchant cargo vessels identified in the reviewed literature are listed in Table A.1: *Savannah*, *Otto Hahn*, *Mutsu*, and *Sevmorput*. Of these, *Sevmorput* is the only vessel shown as remaining in service, following its return to operation in 2016. The other operational civilian nuclear powered vessels included in the table are specialized icebreakers.

All of the historical vessels listed in Table A.1 used or continue to use PWRs. This historical preference is consistent with the technical maturity, accumulated operating experience, and established industrial basis of PWR technology. It should not, however, be interpreted as evidence that a PWR is necessarily the most suitable reactor concept for every future commercial marine application.

Lessons from historical civilian marine applications

From the historical vessel projects reviewed above, three recurring implementation challenges can be identified. Because these observations are derived from a small and diverse group of vessels, they

³Half life is the time required for the activity of a radionuclide to decrease to half of its initial value through radioactive decay.

⁴Spent fuel is nuclear fuel that has been irradiated in a reactor and subsequently removed from the core.

should be regarded as indicative lessons rather than universally applicable conclusions.

- **Commercial and economic challenges:** Several early commercial vessel projects combined commercial operation with technology demonstration objectives. Their commercial viability was constrained by high capital costs, specialized operating and support requirements, and competition with conventionally powered ships.
- **Regulatory and port access constraints:** The operation of some historical vessels was restricted by differences in national acceptance, the absence of a harmonized international approval framework, and concerns regarding nuclear powered vessels entering ports. This indicates that approval by the flag Administration alone may not provide unrestricted access to international trading routes.
- **Public acceptance and confidence:** The experience of *Mutsu*, including the radiation leakage identified during its early sea trials and the resulting public opposition and programme delays, demonstrates that public confidence and credible regulatory oversight are important in addition to technical safety performance [17].

Advanced reactor concepts applicable to ships

SMRs and Generation IV reactors represent related but distinct classifications. The term SMR primarily refers to reactor scale, modular construction, and deployment approach, whereas Generation IV refers to families of advanced reactor technologies. An SMR may therefore be based on either established or advanced reactor technology, while a Generation IV reactor is not necessarily small or modular [18].

Historical civilian marine nuclear applications listed in Table A.1 predominantly used PWRs. This reflects the technical maturity, accumulated operating experience, and established industrial basis of PWR technology at the time these vessels were developed. It should not, however, be interpreted as evidence that a PWR is necessarily the most suitable reactor type for every future commercial marine application.

The advanced reactor concepts compared in Table A.2 may offer characteristics that are potentially attractive for shipboard use, including lower system pressure, higher operating temperature, compact configurations, and inherent or passive safety features. The extent of these benefits depends on the specific reactor, fuel, coolant, power conversion system, and ship integration arrangement. Passive safety features can reduce reliance on active equipment, electrical power, and immediate operator action, but they do not imply that cooling or active supporting systems are unnecessary under all operating and accident conditions [18].

Consequently, advanced reactor concepts should be treated as potential candidates for marine application rather than as inherently superior solutions. Their suitability must be assessed against ship-specific requirements, including mass and volume, shielding, containment, decay heat removal, load response capability, maintainability, and survivability under maritime accident conditions.

2.9. Chapter 2 Conclusion

The fundamental principles of marine nuclear propulsion are controlled fission and reactivity management, continuous removal of operating and decay heat, protection against radiation and contamination, reliable reactor control and shutdown, and safe management of nuclear fuel and radioactive waste. In a marine application, these principles directly affect shielding, confinement, auxiliary system availability, maintenance, arrangement, and the ability of the vessel to maintain the reactor in a safe condition throughout its operating life. Chapter 3 examines how these nuclear safety requirements interact with vessel operation, supporting systems, and ship arrangement.

3

Nuclear propulsion operational profiles & system integration

What are the main shipboard systems and operational functions that must be considered when integrating a nuclear power system into a vessel?

This chapter examines the operational and ship integration requirements of marine nuclear propulsion. It considers reactor and vessel operating states, changes in propulsion and electrical demand, the main heat transfer and power conversion interfaces, the auxiliary systems required to maintain nuclear safety, and the arrangement measures needed to protect and segregate safety functions.

3.1. Operational states

The operating modes summarized in Table 3.1 provide a representative description of the interaction between reactor condition and vessel operation. They are not intended to reproduce a formal regulatory plant state classification. Instead, they establish the operating context within which plant performance, safety functions, supporting systems, and ship reactor interactions must be considered.

These operating modes demonstrate that the safety and availability of the nuclear plant depend not only on reactor condition, but also on the continued availability of electrical power, heat rejection, monitoring, control, and other supporting ship systems.

3.2. Marine operational demand

Marine operational demand is one of the principal factors distinguishing a shipboard nuclear plant from a land based nuclear installation. A nuclear powered commercial vessel must produce and convert heat safely while remaining compatible with propulsion demand, ship service electrical loads, voyage phase, maneuvering requirements, and port operating constraints. The nuclear plant must therefore be considered as part of an integrated marine energy system rather than as an isolated reactor [7, 20].

For many commercial ship types, including container ships, bulk carriers, and tankers, propulsion demand during ocean passage is relatively steady. This operating profile may be favorable for nuclear propulsion because it requires less frequent power variation than some other marine applications. The design basis cannot, however, be limited to steady cruising. The integrated plant must also accommodate changes in demand during port entry and departure, maneuvering, collision avoidance actions, and transitions between propulsion dominated and ship service load dominated operation. Dynamic positioning may introduce additional rapid load variation where it forms part of the vessel's operating profile.

The relevant design question is therefore not only whether sufficient power can be produced, but also whether mismatches between reactor heat production and electrical demand can be managed without exceeding reactor, thermal, mechanical, electrical, or control system limits. Depending on the selected

Table 3.1: Representative reactor and vessel operating modes considered in this thesis.

Operating mode	Reactor and vessel condition	Principal integration considerations
Cold shutdown	The reactor is subcritical and maintained at sufficiently low temperature and pressure for extended shutdown, inspection, or maintenance. Depending on the reactor concept and maintenance scope, selected systems may be depressurized, isolated, or placed in a maintenance condition.	Decay heat removal, radiation monitoring, confinement, and essential electrical support remain necessary despite reactor shutdown [7, 19].
Hot shutdown	The reactor is subcritical but remains at elevated temperature and in a condition permitting a comparatively rapid return to power.	Residual heat must be removed through normal or dedicated shutdown heat removal systems, while the supporting services required for monitoring and control remain available [7, 19].
Startup and heat up	Reactivity and reactor power are increased progressively while the required temperature, pressure, coolant-flow, and power conversion conditions are established.	Reactor, thermal, electrical, and ship support systems must remain coordinated throughout the transition without exceeding their operating limits [7, 19].
Power operation and cruising	The reactor is critical and supplies thermal energy to the power conversion system for propulsion and ship service electricity. Propulsion demand during ocean passage is relatively steady for many commercial cargo vessels.	The integrated energy system must retain sufficient load following or load buffering capability to accommodate gradual demand changes and operational transients [7, 19].
Transient and maneuvering operation	Propulsion and electrical demand may change rapidly during port entry, departure, collision avoidance, speed changes, or the connection and disconnection of large consumers.	Heat production and electrical demand mismatches may be managed through reactor load following, turbine control, controlled heat rejection, electrical energy storage, or other load-buffering arrangements [7, 19].
Port stay mode	Depending on the vessel licensing basis and port state requirements, the reactor may operate at reduced power, remain in hot shutdown, or remain in cold shutdown while shore power or auxiliary generation supplies the vessel.	Essential cooling, monitoring, protection, confinement, and emergency power functions must remain available under the selected port configuration [20].

design, these mismatches may be accommodated through reactor load following, turbine generator control, controlled heat rejection, electrical energy storage, or other load-buffering arrangements [7, 20].

Marine operational demand also interacts with nuclear and ship safety. Changes in propulsion or electrical demand affect the power conversion system, electrical distribution, heat rejection requirements, and the availability of supporting functions during abnormal conditions. Port operation introduces a further interface because the permitted reactor condition may depend on the vessel's licensing basis, the flag Administration, port-State policy, and port requirements. Depending on these conditions, the vessel may operate the reactor at reduced power, place it in shutdown, or rely on shore power or auxiliary generation.

Marine operational demand should therefore be treated not solely as a propulsion consideration, but as an input to the vessel's energy system design, operating philosophy, port interface, and subsequent accident and safety assessment [7, 20].

3.3. Nuclear system design

At ship level, nuclear system integration is strongly influenced by the selected heat transfer arrangement and power conversion cycle. These choices affect plant mass, volume, machinery space requirements, heat-rejection demand, maintainability, weight distribution, and the interfaces between the reactor, propulsion system, and ship service systems. For a nuclear powered commercial vessel, they therefore influence not only thermal efficiency but also arrangement, stability, survivability, and the availability of safety functions [9, 21].

3.3.1. Heat transfer

The heat transfer system must remove heat reliably during normal operation and after reactor shutdown while maintaining separation between the nuclear plant and the marine environment. Depending on the reactor concept, decay heat removal may rely on active circulation, passive natural circulation, or a combination of active and passive functions. Passive arrangements can reduce dependence on electrical power and immediate operator action, but their performance remains dependent on the availability of the heat transfer path and ultimate heat sink.

The surrounding seawater may provide an effective ultimate heat sink for a marine reactor concept. However, using seawater for this purpose requires suitable intermediate heat exchangers and system boundaries that prevent direct interaction between the reactor coolant and the marine environment. The design must also account for corrosion, fouling, blockage, seawater temperature, and damage to external or hull integrated heat transfer components. The seawater cooled passive residual heat removal system examined by [22] represents one possible application of this principle rather than a universal arrangement for marine SMRs.

3.3.2. Power conversion

The power conversion cycle affects the mass, volume, thermal efficiency, heat rejection requirement, load response characteristics, and maintainability of the balance of plant. These characteristics are important for machinery arrangement, weight distribution, propulsion integration, and seawater cooling demand. Historical civilian nuclear powered merchant vessels predominantly combined PWRs with steam Rankine cycle power conversion systems [9].

Steam Rankine cycle

The steam Rankine cycle is a mature and well established power conversion solution for water cooled reactors and can also be coupled to other reactor concepts through a steam generator or intermediate heat exchanger. Its marine integration requires sufficient space and mass allowance for the steam generator, turbine generator, condenser, feedwater system, and associated heat rejection equipment. The condenser and seawater cooling systems can impose particularly important arrangement and survivability requirements because they form the final heat rejection path from the power conversion system [9].

Brayton cycle

Closed Brayton cycles have been investigated as alternative power conversion systems for high temperature and other advanced reactor concepts. Supercritical carbon dioxide (sCO_2) is of interest because its relatively high fluid density may permit more compact turbomachinery and, under suitable temperature conditions, competitive thermal efficiency. The study by [23] examines this potential for an advanced reactor application. These findings should not, however, be interpreted as showing that an sCO_2 Brayton cycle is automatically superior for all marine reactors, since its suitability depends on reactor outlet temperature, system pressure, component maturity, transient behavior, maintenance requirements, and ship integration constraints.

3.4. Nuclear auxiliary systems

For a nuclear powered commercial vessel, auxiliary systems are not just supporting services. They are the systems that enable the fundamental safety functions to be maintained during normal operation, shutdown, and abnormal conditions [18]. In a shipboard context, their importance is amplified by limited space, marine motion, vibration, saltwater exposure, and the possibility of accident conditions such as fire, flooding, or blackout. The purpose of this section is therefore to identify the auxiliary systems that

are central to safe shipboard nuclear operation and to explain why they become major drivers of ship integration.

3.4.1. Decay heat removal and emergency cooling

Following reactor shutdown, decay heat continues to be generated and must be removed to prevent excessive fuel temperatures and potential fuel damage. Depending on the reactor design, shutdown cooling may rely on active systems using pumps and heat exchangers, passive systems based on natural circulation, or a combination of both. In several proposed marine nuclear concepts, seawater or hull integrated heat exchangers are considered as the ultimate heat sink. Such arrangements require careful design to preserve the relevant safety boundaries while accounting for corrosion, fouling, blockage, and other marine environmental effects. Passive arrangements can reduce dependence on AC electrical power and immediate operator action during accident conditions. [6, 24]

The main implication for this thesis is that decay heat removal is not solely a reactor system issue. It is a ship design requirement that affects system redundancy, compartment arrangement, electrical support, heat rejection availability, and survivability under blackout or damaged-ship conditions. Consequently, decay heat removal requirements must be considered during the early development of the ship arrangement and supporting auxiliary systems.

3.4.2. Electrical power, emergency power and distribution

The electrical design of a nuclear powered vessel depends on the selected reactor, power conversion, and propulsion arrangement. Several proposed commercial concepts use integrated electric propulsion, in which the reactor supplies heat to a power conversion system and the resulting turbo generator provides electricity to propulsion motors and ship service loads. However, an all electric configuration is one possible arrangement rather than a universal characteristic of nuclear powered ships. [7, 6, 20]

In addition to propulsion and conventional ship service loads, electrical power is required for reactor protection, instrumentation, monitoring, control, communication, valve actuation, ventilation, and selected cooling auxiliaries. Independent emergency sources are therefore required to support essential functions following loss of the main electrical supply. These may include emergency diesel generators and battery backed DC systems capable of supplying reactor protection, monitoring, control, and other essential auxiliaries during a blackout. [25, 3, 26]

Where redundant or independent electrical sources are credited, their generators, switchboards, distribution branches, and cable routes should be physically and functionally segregated. This reduces the possibility that a single electrical fault, fire, flooding event, or other common cause failure simultaneously disables conventional ship service systems and safety related functions. [6, 25, 27]

For the reference vessel developed later in this thesis, an all electric propulsion arrangement is adopted. The key implication is that electrical segregation and continuity of emergency supply must be treated as core ship integration requirements, because the progression of later accident scenarios depends directly on whether shutdown support, monitoring, control, and cooling functions remain available following loss of normal electrical power.

3.4.3. Instrumentation & Control (I&C) and safety systems

The Instrumentation & Control (I&C) design supports both normal plant control and safety related protection functions. Normal control systems regulate reactor power and plant parameters during operation, while the reactor protection system independently monitors safety significant variables and initiates automatic reactor shutdown or actuation of required safety functions when predefined limits or set-points are exceeded. [3, 6, 26]

Redundancy provides tolerance against random equipment failures and supports the single failure criterion. Redundancy alone does not, however, prevent common cause failures. These risks are reduced through independence, physical and functional separation, and, where appropriate, diversity. For example, an alternative shutdown system may use a different actuation principle, equipment technology, or signal processing pathway from the primary shutdown system. [6, 26, 28]

Safety related I&C systems should also be appropriately separated from non-safety ship automation and conventional machinery control networks. Digital systems introduce additional requirements con-

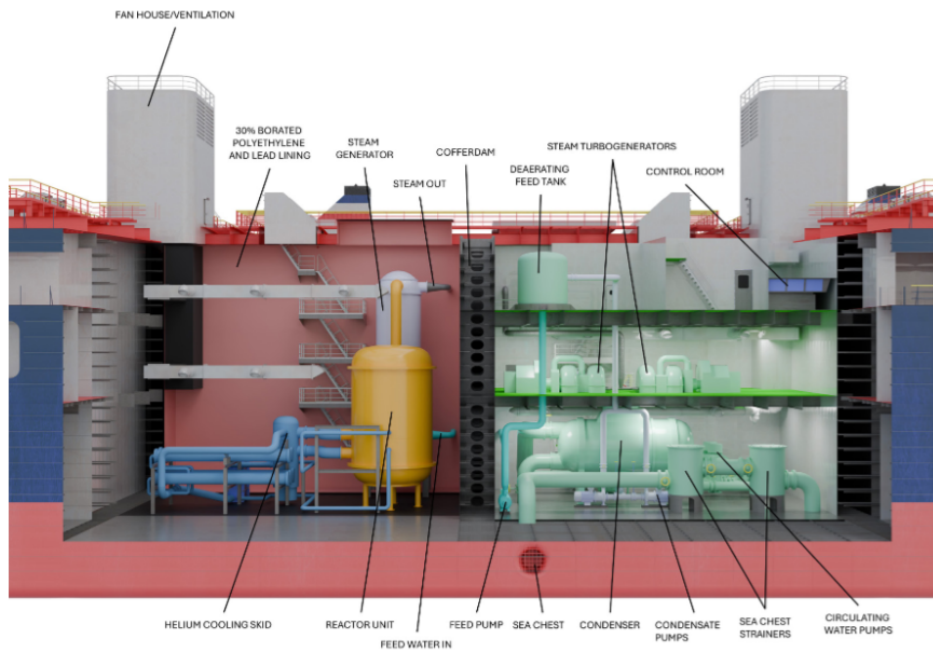


Figure 3.1: HTGR module section. [16]

cerning cybersecurity, data communication independence, software assurance, and controlled access. Equipment and associated cabling must also be qualified for the relevant marine and nuclear environmental conditions, including vibration, vessel motion, temperature variation, humidity, electromagnetic interference, and radiation [7, 6, 26].

3.4.4. Heating, Ventilation, and Air Conditioning (HVAC)

Heating, Ventilation, and Air Conditioning (HVAC) systems support equipment environmental conditions, personnel habitability during access, and radiological confinement. Ventilation serving nuclear or potentially contaminated spaces should be appropriately separated from accommodation spaces, control rooms, and conventional ship service ventilation systems. Where pressure zoning is applied, differential pressures should direct leakage airflow from areas of lower contamination potential towards areas of higher contamination potential. [29, 30]

Air extracted from potentially contaminated spaces should be monitored and, where required, filtered or otherwise treated before controlled discharge. The required treatment depends on the expected radioactive material, since high efficiency particulate filtration primarily controls radioactive aerosols and does not remove all gaseous contaminants. [30, 31]

The ventilation arrangement should also include suitable isolation dampers and be coordinated with fire and smoke control functions. Fan shutdown, damper actuation, or pressure changes during a fire should not unintentionally spread contamination or compromise the required confinement function. [3, 6, 26]

3.4.5. Fuel handling, spent fuel and radioactive waste systems

Marine SMR concepts with a sealed lifetime core eliminate routine onboard refueling and associated spent fuel handling during service. Auxiliary systems are therefore required for infrequent but high-consequence life cycle operations, like initial core installation and end-of-life removal, including controlled transfer interfaces, shielding and confinement boundaries (Figure 3.2), radiological monitoring, and arrangements to maintain sub-criticality and heat removal as required. In parallel, radioactive waste management systems handle liquid, gaseous, and solid radioactive waste through collection, treatment, conditioning, and shielded interim storage. Recent American Bureau of Shipping (ABS) rules [6] for floating nuclear plants and nuclear power barges require robust radioactive waste management and well defined interfaces with port facilities.

For the thesis, this matters because even when routine refueling is avoided, life cycle fuel and waste handling still create arrangement, shielding, logistics, and port interface requirements that must be reflected in the overall safety case.

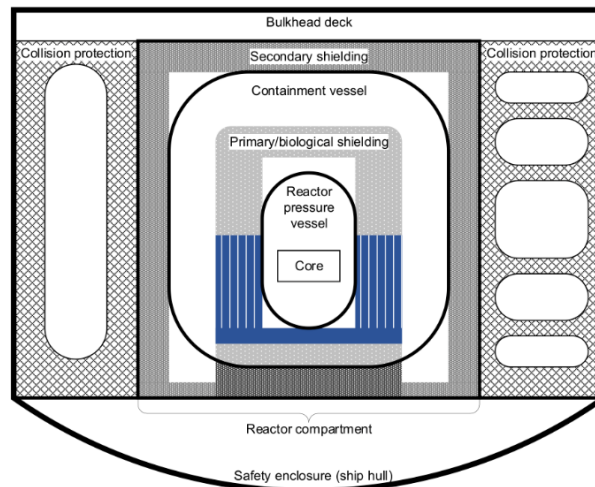


Figure 3.2: Nuclear ship protection concept illustrating radioactivity containment, radiation shielding, the reactor compartment boundary, and collision protection structures. [21]

3.5. Nuclear Ship Arrangement

Ship arrangement is one of the clearest areas in which nuclear propulsion departs from conventional commercial ship design. The arrangement must protect the reactor and its safety systems against collision, grounding, internal hazards, and radiological release, while also preserving cargo function, habitability, maintainability, and emergency access. For that reason, nuclear ship arrangement is one of the main means by which shielding, survivability, segregation, and consequence limitation are achieved onboard. [3, 6, 20]

3.5.1. Reactor location

The location of the reactor compartment is concept dependent and must be considered together with the vessel arrangement, subdivision, damage stability, shielding, accessibility, and maintenance requirements. Positioning the reactor within the central region of the hull can reduce its exposure to vessel motions and increase its separation from the ship side and bottom, thereby improving protection against collision and grounding.

Figure 3.3 illustrates one possible arrangement in which the reactor compartment is located in a protected region near midship. In this concept, the compartment is surrounded by a double hull, local structural reinforcement, and energy absorbing structures intended to limit the transfer of collision loads to the reactor containment [20]. This arrangement should be regarded as a representative design solution rather than a universal requirement for nuclear powered vessels.

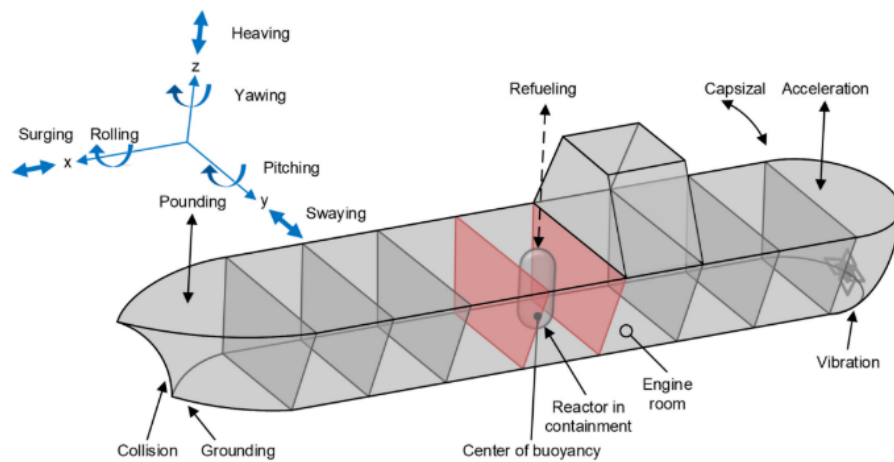


Figure 3.3: Reactor placement. [21]

3.5.2. Compartmentalization and zoning

Radiological zones, including the reactor, primary coolant loop, spent fuel, and radioactive waste spaces, are grouped into a nuclear compartment that is separated from accommodation, cargo spaces, and conventional machinery by multiple watertight bulkheads and substantial shielding. Functional zoning is also applied, distinguishing the nuclear compartment, turbine-generator and power conversion spaces, conventional engine-room systems, cargo holds, and accommodation blocks. [3]

3.5.3. Segregation of safety pathways

Redundant safety systems for cooling, electrical power, and I&C are arranged in separate (Figure 3.4), physically distinct working pathways. These are often located on opposite sides or on different decks to ensure that a single failure/damage cannot disable all of them. Cable routes and pipe trunks are designed to minimize common routes and shared spaces as usual, but where common routing is unavoidable, additional protection measures are applied. [6]

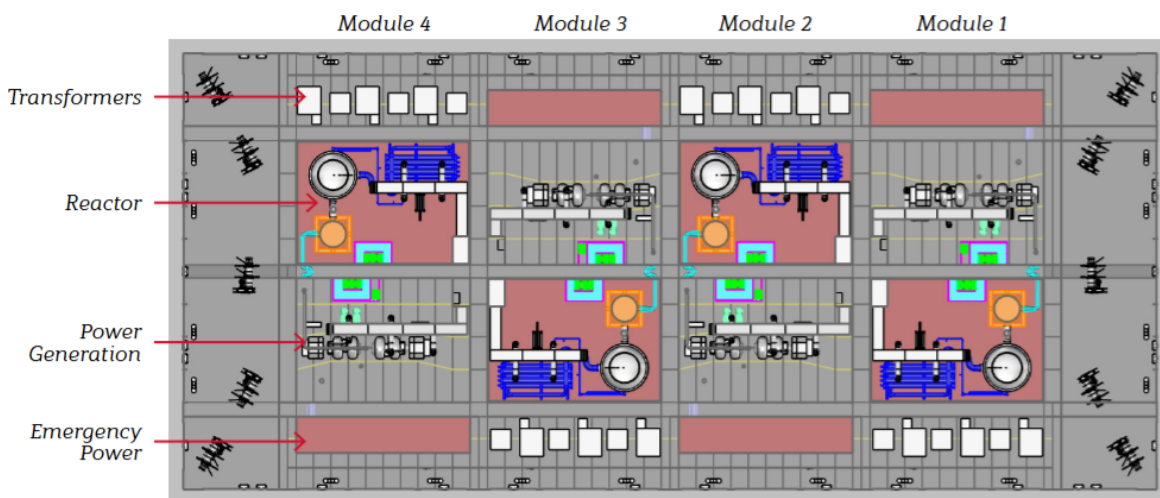


Figure 3.4: Example of 4 module HTGR plan. [16]

3.5.4. Control room and emergency control

The location of the main control room is concept dependent. In the example arrangement shown in Figure 3.5, it is positioned above and aft of the reactor compartment and protected by substantial shielding [20]. The main control room provides centralized monitoring and control of the nuclear plant and its interfaces with the propulsion and ship service systems.

Current guidance also considers a physically and functionally separated emergency control station capable of bringing the reactor to, and maintaining it in, a safe shutdown state if the main control room becomes inaccessible or inoperable [6].

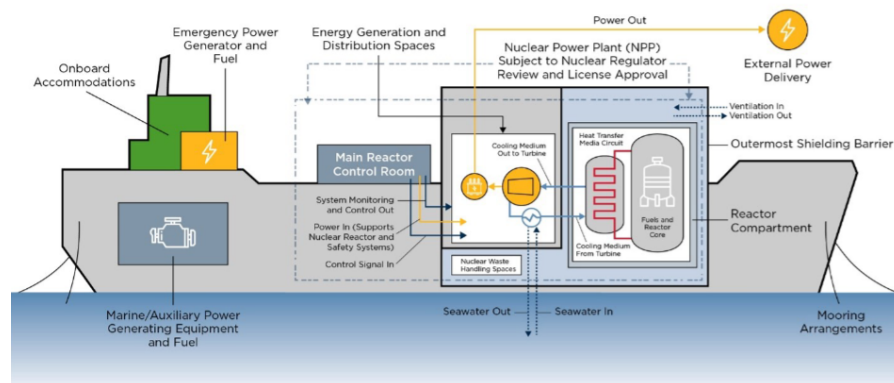


Figure 3.5: Simplified Example Arrangement of Nuclear Power Service Vessel. [6]

3.5.5. Integration with propulsion and cargo

For cargo ships, layouts are being developed such that the nuclear compartment occupies a central block of hull volume while minimizing disruption to cargo operations. Example arrangements in Det Norske Veritas (DNV) [7] and Massachusetts Institute of Technology (MIT) [20] publications show container vessels with the nuclear compartment amidships, and conventional cargo holds forward and aft. The general trend is towards modular “nuclear power blocks” that can, in principle, be integrated into different hull types with minimal re-design, while preserving required separations and safety margins.

3.5.6. Port interface and emergency response

Layout planning also explicitly considers operations in port and emergency management. Dedicated access routes, hatches, and handling spaces are provided for bringing fuel and waste casks on and off the vessel without routing them through accommodation or cargo areas. The arrangement must support the establishment of exclusion zones around the ship, emergency access for port authorities, and effective deployment of monitoring and decontamination equipment in the unlikely event of an incident [20].

3.6. Chapter 3 Conclusion

Integrating a nuclear power system into a vessel requires consideration of the complete operating envelope rather than the reactor alone. The principal requirements include managing changes in propulsion and electrical demand, maintaining operating and decay heat removal, providing reliable emergency electrical power, instrumentation, control, ventilation, confinement, radiation monitoring, and radioactive material handling.

These functions must be supported by an arrangement that provides structural protection, shielding, compartmentalization, segregation of redundant safety pathways, protected control locations, and suitable access and port interfaces. Chapter 4 examines how these integration requirements are reflected in the applicable maritime, classification, and nuclear safety frameworks and in the representative accident scenarios carried forward into the assessment.

4

Regulatory and safety basis and representative accident scenarios

What nuclear, maritime, and classification safety frameworks are relevant, and what limitations exist for commercial ship concepts?

This chapter establishes the regulatory and safety basis for the assessment. It reviews the relevant class society guidance, IMO statutory instruments, and IAEA safety standards, and identifies the limitations of applying these sources to modern nuclear powered commercial vessels. The resulting safety expectations are then translated into a representative set of plant, shipboard, and maritime initiating events for the later risk assessment.

4.1. Regulatory and safety basis for nuclear powered commercial vessels

No single modern framework provides a complete contemporary regulatory basis for nuclear powered commercial vessels. Instead, the safety basis used in this study is assembled from three source groups: class society guidance, statutory maritime requirements, and the IAEA nuclear safety framework. Class rules translate nuclear safety needs into ship design and survivability expectations, the IMO layer provides the statutory maritime approval context and ship level safety functions, and the IAEA framework provides the modern safety assessment principles that underpin later methodology development. Port-state and local emergency planning issues are considered as cross-cutting interfaces within this basis rather than as a separate regulatory layer. Accordingly, this section does not aim to identify one complete ready made code, but to define the combined regulatory and safety basis for the later risk assessment methodology.

4.1.1. Class society guidance

Although class societies do not provide a complete modern regulatory and safety basis for nuclear powered commercial ships, the reviewed sources show broad agreement on the main ship-level safety expectations. Across DNV, Lloyd's Register (LR), Russian Maritime Register of Shipping (RMRS), and ABS, several themes are consistent: the reactor installation must remain protected against ship accidents and severe environmental conditions; essential safety functions such as shutdown, cooling, shielding, confinement, control, and electrical support must be preserved under abnormal conditions; and the ship arrangement must provide sufficient structural integrity, segregation, and survivability. The importance of class guidance in this study is therefore not that it offers a full regulatory framework, but that it translates nuclear safety concerns into practical ship design expectations. The individual class sources then add different emphases, which are summarized below and in Table 4.1.

Det Norske Veritas (DNV)

DNV [7] is valuable because it highlights issues that affect the wider feasibility and integration of a commercial nuclear fleet, rather than only the reactor itself. In particular, it emphasizes the importance of the back end of the fuel cycle, including spent fuel handling, interim storage, and disposal, and notes that ship operational profiles can influence spent fuel characteristics and burn-up. DNV also highlights reactor configuration trade-offs, showing that single reactor, dual reactor, and multi module arrangements involve different balances between redundancy, power, space, weight, cost, availability, and crew demands. In the same context, shielding is treated as a major ship design driver, while passively safe and lower pressure concepts are presented as very attractive for civil marine use.

Lloyd's Register (LR)

LR [5] is useful because it connects ship structural design and the marine operating environment directly to nuclear safety expectations. LR treats meteorological and oceanographic conditions as inputs to the safety basis rather than as background marine data only, and therefore links safe operation and safe shutdown to representative ship motions, accelerations, inclinations, and severe environmental loads. It also emphasizes that accident loads such as collision, explosion, dropped objects, capsizing, and sinking may need to be addressed explicitly in the design basis. In addition, LR highlights potential incompatibilities between marine material choices and radioactive service, and it stresses the need to plan for temporary onboard radioactive waste storage and handling as part of the overall ship safety strategy.

Russian Maritime Register of Shipping (RMRS)

RMRS [8] is especially valuable because it provides a more prescriptive example of how nuclear-specific requirements can be translated directly into ship rules. Compared with the other class sources, RMRS gives clearer rule-based treatment of reactor compartment structural protection, including controlled load transfer between the protected compartment and the surrounding hull after major ship accidents. It also distinguishes shielding more clearly from containment and introduces strong fire protection and fuel segregation requirements around the reactor zone. For this reason, RMRS is useful in this chapter as a source of concrete ship design implications for compartment protection, barrier definition, and segregation.

American Bureau of Shipping (ABS)

ABS [6] is particularly useful because it makes the safety implications of ship operating conditions and accident environments more explicit and directly links them to the need for structured safety assessment. ABS gives clear attention to marine specific initiating conditions that can challenge reactor safety functions, including sinking, extreme weather, severe ship motions, shock loading, vibration, and damage to the outer shielding boundary. It also emphasizes structural and mechanical accident effects, including wave slamming, collision, grounding, and explosion, and notes that containment-related structures should be designed with sufficient margin against brittle failure and rapid fracture. Finally, ABS is important for this thesis because it explicitly recognizes that additional structured analyses such as HAZID, HAZOP, FMEA, FMECA, and quantitative risk studies may be required to support design approval.

Table 4.1: Comparative summary of the main contributions of the class societies to the safety of nuclear powered commercial vessels [7, 6, 5, 8]

Class society	Main emphasis
DNV	Maritime nuclear fuel cycle, reactor configuration trade-offs, shielding as a ship design driver, and preference for passively safe lower-pressure concepts.
LR	Meteocean conditions as safety-basis inputs, structural accident loads, materials compatibility, and onboard radioactive waste storage.
RMRS	Prescriptive nuclear-ship rules, severe environmental conditions, reactor compartment structural protection, shielding-barrier definition, and fire/fuel segregation around the reactor zone.
ABS	Marine accident effects, extreme motions, shock, vibration, shielding-boundary damage, and explicit expectation for further structured analysis.

4.1.2. Statutory maritime basis (IMO Nuclear Code, INF Code, SOLAS interfaces)

The statutory maritime layer remains centered on the IMO Code of Safety for Nuclear Merchant Ships and its interfaces with SOLAS and related IMO instruments. Although this framework remains the principal formal maritime reference for nuclear powered commercial vessels, it predates modern SMR concepts and does not fully reflect contemporary nuclear safety principles. For the present study, its value lies less in providing a complete modern design basis and more in identifying the statutory approval logic, shipboard safety functions, radiological controls, and port related considerations that a future nuclear powered commercial vessel would still need to address.

The Nuclear Code supplements rather than replaces the conventional maritime safety framework established by SOLAS. Requirements relating to subdivision and stability, fire safety, machinery and electrical installations, life saving appliances, and emergency arrangements therefore remain relevant to a nuclear powered vessel. Nuclear requirements add further expectations concerning reactor shutdown, decay heat removal, confinement, radiation protection, radioactive material control, and nuclear safety assessment. The interface is therefore two directional, the nuclear installation must not compromise conventional ship safety, while shipboard hazards such as fire, flooding, collision, grounding, and loss of electrical power must be assessed for their potential effects on nuclear safety functions.

IMO Code of Safety for Nuclear Merchant Ships

The IMO Code of Safety for Nuclear Merchant Ships [3] remains the principal statutory maritime reference for nuclear powered commercial vessels because it defines the formal approval and operational assurance framework expected by an Administration. The Code establishes two overarching objectives, protecting people and the environment against radiation hazards and radioactive releases, and protecting the ship against hazards arising from interactions between the NPP and the remainder of the vessel. It also translates these objectives into approval documentation and life cycle assurance requirements, including the preparation of a Safety Assessment, implementation of a Quality Assurance Programme, and continuing survey oversight. In this respect, the Code is useful to the present study as a framework for understanding what a maritime nuclear safety case would need to demonstrate, even though it predates modern SMR-based ship concepts.

A further important contribution of the Code is its classification of operating and accident conditions into Power Plant Conditions (PPCs), which relate event frequency and consequence expectations to required plant behavior and radiological limits, as shown in Table 4.2. Across these conditions, the Code defines safety criteria and associated safety functions relating to reactor shutdown, cooling, containment, shielding, and safe ship operation. It also establishes radiological protection expectations, including the application of the ALARP principle in design, the designation of controlled and supervised areas, protection of occupied spaces during accident conditions, and provisions for radioactive waste storage and controlled discharge. For the present chapter, this is valuable because it demonstrates how statutory maritime requirements connect ship arrangement, safety functions, radiological zoning, and accident condition planning within a single formal approval framework.

Table 4.2: How situations are defined as PPCs based on their occurrence frequency. [3].

PPC	General description	Likelihood of occurrence	Consequence class
1	Normal operation	Continuous or frequent	1
2	Minor occurrences	Infrequent	2
3	Major occurrences	Remote	3
4	Severe accident	Extremely remote	4

The PPC framework is used in this thesis as regulatory context rather than as a direct classification system for the later HAZID. The risk assessment is not restricted to the most severe accident category. It also considers deviations, equipment failures, and initiating events that may correspond conceptually to minor or major occurrences and that could escalate if the available safeguards fail. Accident scenarios are not assigned formal PPC classifications because this would require plant specific event frequencies, system response analyses, and radiological acceptance criteria that are not available at the present concept design stage.

IMO INF Code for the Safe Carriage of Nuclear Cargo

The IMO INF Code is relevant to this study not because it governs nuclear propulsion directly, but because it provides a useful statutory benchmark for how IMO already regulates ships carrying highly radioactive material [32]. The Code classifies ships according to the permitted activity of irradiated nuclear fuel, plutonium, and high-level radioactive waste, and then links those classes to requirements for damage stability, fire protection, structural strength, and cargo securing. In doing so, it shows that the IMO framework already recognizes the need for stronger survivability, protection, and segregation measures when ships carry high consequence radioactive material.

For the present study, the value of the INF Code is therefore indirect but important. It does not provide a propulsion safety code, yet it demonstrates how statutory maritime regulation can impose graduated ship requirements based on radiological hazard, survivability expectations, and fire and stability performance. This makes it useful as a reference point for thinking about how future statutory treatment of nuclear powered commercial ships might also need to combine reactor related risks with ship safety requirements in an integrated way.

As summarized in Table 4.3, the principal IMO instruments contribute to the safety basis of nuclear powered commercial vessels in different but complementary ways. The Nuclear Code provides the core ship-specific framework, while the INF Code indicates how broader maritime safety requirements would still shape design, survivability, and operational arrangements.

Table 4.3: Comparative summary of the main contributions of the IMO statutory instruments to the safety basis of nuclear powered commercial vessels [3, 32, 33].

IMO instrument	Main emphasis
IMO Nuclear Code	Formal statutory approval basis for nuclear commercial ships. Defines the overarching safety objectives, required safety assessment and quality assurance documentation, life cycle oversight, and the ship-level safety functions that must be demonstrated, including shutdown, cooling, containment, shielding, and radiological protection. Also introduces the PPC framework linking operating and accident conditions to expected plant behavior and radiological limits.
INF Code	Indirect but important for how IMO regulates ships carrying high-consequence radioactive material. Links radiological hazard level to survivability related requirements such as damage stability, fire protection, structural strength, and cargo securing, thereby illustrating how statutory maritime requirements can scale with hazard severity.

4.1.3. Nuclear safety basis from the International Atomic Energy Agency (IAEA)

While the IMO framework provides the main statutory maritime reference point, the IAEA safety standards provide the more modern nuclear safety logic for how safety should be assessed and demonstrated. For the present study, the IAEA material is important because it introduces the core concepts that later shape the methodology, including safety assessment across the full life cycle, graded assessment, safety function demonstration, Defence-in-Depth (DiD), and the complementary use of DSA and PSA. In this sense, the IAEA sources are valuable not as ship rules, but as the clearest basis for structuring the safety case of a nuclear powered commercial vessel.

International Basic Safety Standards

The IAEA International Basic Safety Standards [29] provides the internationally recognized baseline requirements for radiation protection and safety that national regulators transpose into regulation. For this chapter, its main value is that it requires safety assessment across the full design life cycle and makes clear that the assessment must consider external events, failure modes, and factors that could lead to releases of radioactive material. It is also directly relevant to ship arrangement, because it defines controlled and supervised areas, their boundaries, their physical delineation, and the need for appropriate access control and signage. For a nuclear powered commercial vessel, these requirements map closely to radiological zoning, access control, and the physical arrangement of reactor and support spaces on board.

As shown in Table 4.4, the IAEA sources contribute mainly through radiation protection requirements and the methodological basis for safety assessment. Together, they help translate high level nuclear safety expectations into design, layout, and assessment requirements relevant to marine application.

Assessment for Facilities and Activities

The IAEA Safety Assessment for Facilities and Activities [34] is important because it explains how safety should be demonstrated through a structured assessment that is documented, verified, and maintained as part of authorization. A central contribution is the graded approach, under which the scope and level of detail of the assessment should be proportionate with the magnitude of the radiation risk. The standard also requires identification of possible radiation risks, specification and assessment of safety functions across all plant states, including severe accidents, and evaluation of the reliability attributes needed to deliver those functions, such as redundancy, diversity, segregation, independence, and qualification. In addition, it requires assessment of DiD, attention to internal and external events that may defeat multiple barriers, and the complementary use of DSA and PSA, together with explicit safety criteria and uncertainty analysis. For the present study, this makes the document important as the main methodological bridge between the regulatory review in Chapter 4 and the risk assessment framework developed in Chapter 5.

Table 4.4: Comparative summary of the main contributions of the IAEA safety sources to the safety basis of nuclear powered commercial vessels [29, 34].

IAEA source	Main emphasis
International Basic Safety Standards	Provides the baseline international requirements for radiation protection and safety. Requires consideration of external events, failure modes, and release pathways across the full life cycle, and is relevant to ship arrangement through its expectations for controlled and supervised areas, access control, physical delineation, and radiological zoning.
Safety Assessment for Facilities and Activities	Provides the main methodological basis for how safety should be demonstrated and maintained as part of authorization. Emphasizes a documented and verified safety assessment, graded approach, identification of radiation risks, assessment of safety functions in all plant states including severe accidents, and consideration of redundancy, diversity, segregation, independence, DiD, and the complementary use of DSA and PSA.

4.2. Representative initiating events and accident scenarios

This section identifies representative initiating events and accident conditions relevant to a nuclear powered commercial vessel. The objective at this stage is scenario identification rather than detailed sequence modeling or formal regulatory classification. The identified events provide the basis for the later construction of cause-consequence scenarios and evaluation of the safety functions and safeguards associated with them.

The scenario taxonomy follows the IMO Nuclear Code, which requires both nuclear power plant accidents and ship accidents to be considered within the safety assessment [3]. For the present study, the initiating events are organized into three domains: internal plant events, internal shipboard hazards, and maritime initiated events. Their relationship to the principal safety functions is summarized in Figure 4.1.

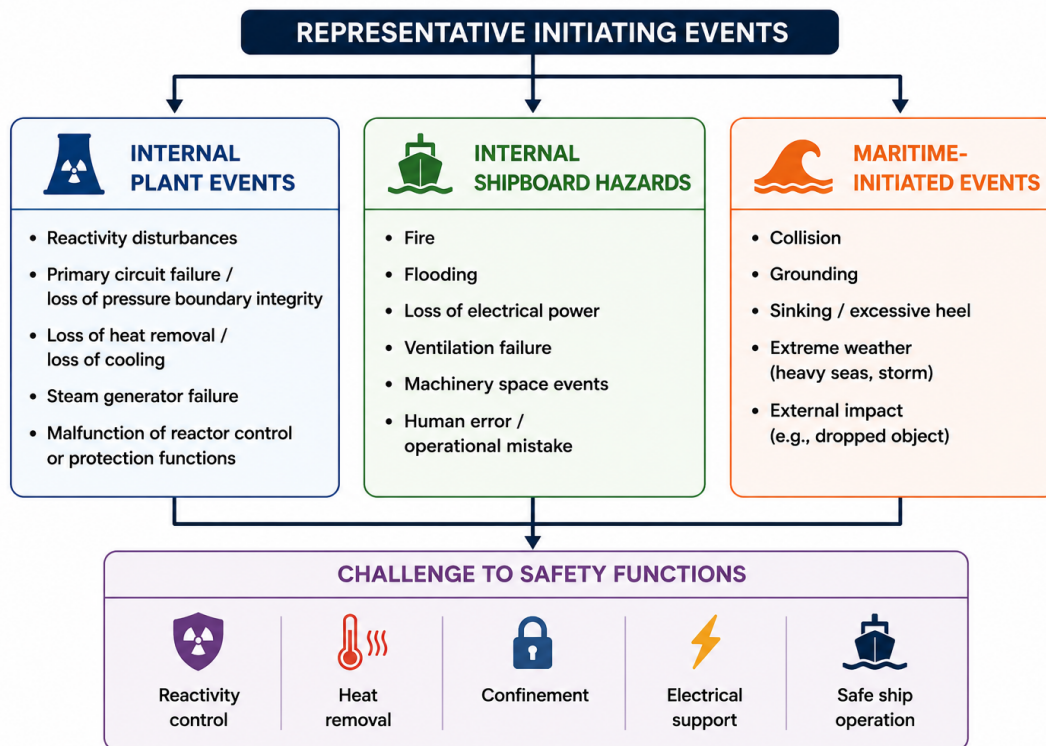


Figure 4.1: Classification of representative initiating events and the principal safety functions they may challenge. Author's illustration based on [3, 6, 20].

External port interface, security, and malicious action hazards are acknowledged but excluded from the detailed assessment because they require additional port specific, security related, and operational interface assumptions.

4.2.1. Internal plant events

Internal plant events originate within the Nuclear Steam Supply System (NSSS), power conversion system, or associated nuclear safety systems. Rapid load rejection or turbine trip may produce a mismatch between reactor heat production and electrical demand, requiring controlled power reduction, heat rejection, or reactor shutdown. Loss of heat removal is particularly important because it directly challenges the continued removal of reactor and decay heat.

Failures of the primary pressure boundary or coolant inventory, including a Loss of Coolant Accident (LOCA), may challenge core cooling and confinement. Steam-generator leakage or rupture may also create an interface between the primary and secondary circuits and provide a pathway for contamination transfer. Reactivity disturbances, malfunction of reactor control or protection functions, and

anticipated transients without scram¹ are also retained because they are explicitly recognized within nuclear safety guidance as conditions requiring analysis [3, 20].

4.2.2. Internal shipboard hazards

Internal shipboard hazards originate within the vessel but outside the nuclear plant itself. They are important because they may disable several systems simultaneously through common spaces, cable routes, ventilation paths, supporting services, or restricted access.

Representative hazards include fire, flooding from non-collision sources, loss of electrical power, ventilation failure, machinery space events, local structural shock, and dropped loads. Human or operational error may also initiate or worsen these conditions. Such events may challenge physical and functional segregation, disable redundant equipment, compromise confinement, or reduce the availability of cooling, monitoring, control, and emergency response functions [3, 6].

4.2.3. Maritime initiated events

Maritime initiated events arise from the vessel's external operating environment and may impose structural damage, flooding, abnormal motions, or loss of essential supporting functions on the nuclear plant.

Collision may cause local penetration, crushing, structural shock, compartment flooding, or damage to cables and supporting systems. Grounding may breach the double bottom, impair seawater-intake or heat rejection arrangements, and initiate progressive flooding. Severe weather and heavy sea operation may produce high accelerations, slamming loads, green-water impact, abnormal heel, or temporary loss of essential services. External impacts, including dropped or swinging objects during cargo or maintenance operations, may similarly challenge safety-significant equipment or compartment boundaries [3, 20, 5].

Loss of propulsion and maneuvering capability is retained as a ship level functional loss scenario because it may increase exposure to collision, grounding, severe weather, or loss of safe positioning. It is therefore treated as a potential contributor to accident escalation rather than solely as an external initiating event.

4.2.4. Representative accident scenario set

The representative initiating events and accident conditions carried forward into the subsequent assessment are summarized in Table 4.5.

Table 4.5: Representative initiating events and accident conditions carried forward into the assessment.

Domain	Representative scenarios	Principal references
Internal plant events	Rapid load rejection or turbine trip; loss of heat removal; primary pressure boundary failure or LOCA; steam generator leakage or rupture; reactivity disturbance; malfunction of reactor control or protection functions; and anticipated transient without scram.	[3, 20]
Internal shipboard hazards	Internal fire; internal flooding from non collision sources; loss of electrical power; loss of essential support services; ventilation failure; machinery space events; local structural shock; dropped loads; and human or operational error.	[3, 6]
Maritime initiated events	Collision; grounding; severe weather and heavy-sea loading; external impact; and loss of propulsion or maneuvering capability.	[3, 20, 5]

¹A scram is a rapid reactor shutdown achieved by inserting sufficient negative reactivity to terminate the self-sustaining fission chain reaction.

Capsize and sinking are acknowledged as potential accident states but are not assessed as separate initiating events within the present study. Reaching such states would already require substantial escalation of preceding maritime accidents, with severe consequences having occurred before capsize or sinking itself is reached. The relevant initiating events and escalation mechanisms leading towards these conditions are addressed through the accident scenarios considered in the assessment.

The selected scenario set combines the principal nuclear plant initiators identified in nuclear ship safety guidance with the dominant internal and external hazards associated with commercial ship operation. It therefore provides the literature based starting point for the more detailed risk assessment applied to the reference vessel in Chapter 7 [3, 6, 20, 5].

4.3. Chapter 4 Conclusion

The safety basis for a nuclear powered commercial vessel must be assembled from complementary maritime and nuclear sources. Class society guidance translates nuclear safety concerns into ship design expectations, the IMO framework provides the statutory maritime approval and ship safety context, and the IAEA standards provide the modern principles for safety assessment, radiation protection, and DiD.

No single source provides a complete contemporary framework for modern commercial ship concepts, particularly those using SMRs. The combined review therefore supports a representative accident set covering internal plant events, internal shipboard hazards, and maritime initiated events, with capsize and sinking acknowledged as potential extreme accident end states but not assessed separately. Chapter 5 evaluates which risk-assessment principles and methods are suitable for examining these scenarios at concept-design level.

5

Risk assessment methods

What risk based assessment principles and methods can be used to support the safety evaluation of nuclear powered commercial vessels?

This chapter evaluates the risk assessment principles, frameworks, and analytical methods applicable to the concept level safety assessment of a nuclear powered commercial vessel. The reviewed approaches are compared against the requirements of the study, including limited design maturity and reliability data, the need to examine barrier dependencies and accident escalation, and the ability to translate safety findings into ship design measures.

5.1. Foundations of risk assessment and risk based design

Before comparing specific frameworks and analytical methods, it is useful to clarify the two central concepts that underpin this chapter: risk assessment and risk based design. These terms are closely related, but they are not the same. Risk assessment is the process used to identify, analyze, and evaluate risk. Risk based design is the design approach that uses those risk insights to guide design decisions and justify risk reduction measures. In the context of nuclear powered commercial vessels, this distinction is important because the present study is not only concerned with analyzing hazards, but also with using the resulting risk insights to support safer ship integration and a structured review of further practicable risk reduction measures.

5.1.1. Risk assessment

Risk assessment is a structured process used to identify hazards, examine how unwanted events may occur, evaluate their potential consequences, and support judgments about the acceptability of the resulting risk. Depending on the maturity of the design and the availability of data, this may be done qualitatively, quantitatively, or through a combination of both. In all cases, the core purpose is the same: to provide a transparent basis for understanding what can go wrong, how it can escalate, what barriers exist, and where additional risk controls may be needed. [35, 36, 37]

For the present study, risk assessment should be understood broadly rather than as a single method. It includes the selection and application of principles, assessment frameworks, and analytical tools that together help evaluate representative accident scenarios for a nuclear powered commercial vessel. This is important because the thesis is conducted at concept and ship integration level, where complete failure data and fully detailed system definitions are not yet available. As a result, the assessment must rely primarily on system logic, structured hazard identification, barrier analysis, and reasoned comparison of design measures rather than on fully quantified proof alone. [36, 37]

5.1.2. Risk based design

Risk based design is a design approach in which safety relevant design decisions are guided by the results of risk assessment rather than by prescriptive compliance alone. Instead of asking only whether a design satisfies a set of fixed rules, risk based design asks whether the design adequately reduces

the likelihood and consequences of hazardous events, whether key safety functions are preserved under those events, and whether further reasonably practicable risk reduction measures should be adopted. In that sense, risk based design links hazard analysis directly to design choice, arrangement, segregation, redundancy, and other safety-relevant features of the vessel. [35, 36]

In this thesis, risk based design does not mean performing a complete quantitative optimization of the ship. Rather, it means using representative accident scenarios and a selected combination of assessment methods to derive ship design implications that improve safety in a structured and defensible way. The aim is to move from hazard recognition to design action by identifying where layout, system design, barrier placement, segregation, or auxiliary support arrangements should be strengthened and by examining whether further concept level risk reduction is reasonably practicable. [36, 38]

5.2. Principles

DiD and ALARP provide the principal safety concepts used to structure and interpret the assessment. DiD is applied to examine the presence, function, and independence of the protective layers. ALARP is used in an orienting role to support the systematic consideration of further practicable risk reduction measures. The study does not undertake the quantitative, economic, or regulatory analysis required for a formal ALARP demonstration.

5.2.1. Defence-in-Depth (DiD)

DiD is one of the fundamental principles of nuclear safety and forms a central basis for the development and assessment of nuclear installations [28]. Its importance lies in the fact that safety must not depend on any single provision, component, human action, or line of defense. Instead, protection is achieved through multiple, consecutive, and as far as practicable independent layers of prevention, control, and mitigation. For this reason, DiD is highly relevant to nuclear powered commercial vessels, where reactor safety must be maintained not only against plant internal failures, but also against ship specific hazards.

The five levels of DiD, reproduced from INSAG-based guidance (Table 5.1), provide a useful structure for organizing the safety case and tracing how the design prevents abnormal operation, controls accidents, and mitigates potential radiological consequences. [28]

Table 5.1: Summary of the five levels of DiD [28]

Levels of DiD	Objective	Essential means
Level 1	Prevention of abnormal operation and failures	Conservative design and high quality in construction and operation
Level 2	Control of abnormal operation and detection of failures	Control, limiting and protection systems and other surveillance features
Level 3	Control of accidents within the design basis	Engineered safety features and accident procedures
Level 4	Control of severe plant conditions, including prevention of accident progression and mitigation of the consequences of severe accidents	Complementary measures and accident management
Level 5	Mitigation of radiological consequences of significant releases of radioactive materials	Off-site emergency response

An important feature of DiD is that the different levels should remain sufficiently independent, such that the degradation or failure of one level does not automatically disable the others. DiD therefore goes beyond simple redundancy. A design may contain several nominally redundant systems, but if these systems share the same location, support service, cable routing, environmental exposure, or common

vulnerability, the intended protection can be lost during a single initiating event. In that sense, DiD is closely linked to segregation, separation, diversity, and the avoidance of common cause failures. [28]

This principle is important in the present study because one of the main challenges of nuclear powered commercial vessels is the interaction between reactor safety functions and maritime accident conditions. External or ship originating events may challenge several protective layers simultaneously, meaning that the effectiveness of DiD cannot be assumed and must instead be examined explicitly. For this reason, examining whether DiD remains effective under representative initiating events will form an important part of the later assessment methodology.

5.2.2. As Low As Reasonably Practicable (ALARP)

In formal risk based assessments, ALARP¹ is the principle that risk reduction measures should be implemented unless the associated sacrifice, in terms of cost, time, or effort, would be grossly disproportionate to the additional safety benefit achieved. The principle therefore requires a structured examination of whether further reasonably practicable risk reduction remains available, rather than the complete elimination of risk. It is also reflected in IMO guidance for alternative design and equivalency assessments [38].

ALARP regions

In risk based safety assessment, ALARP is used to justify that residual risk has been reduced to a level at which any further reduction would require a sacrifice, in terms of cost, time, or effort, that is grossly disproportionate to the additional safety benefit achieved [38]. Its importance lies in the fact that it does not demand absolute elimination of risk, but instead requires a structured and defensible demonstration that all reasonably practicable risk reduction measures have been identified, considered, and implemented where justified. [36]

ALARP is commonly illustrated using a three region tolerability framework, shown in Figure 5.1. At the upper end lies the unacceptable region, where risk is intolerable and the activity or design cannot be accepted unless further risk reduction is achieved. At the lower end lies the broadly acceptable region, where risk is sufficiently low that no additional reduction is required beyond accepted good practice. Between these two lies the tolerable region, often referred to as the ALARP region, where risk may be accepted only if it can be demonstrated that all reasonably practicable risk reduction measures have been implemented and that any rejected measures have been excluded on defensible grounds. [38]

In formal practice, ALARP is often supported through cost effectiveness analysis (CEA)², particularly in the maritime domain where risk control options are compared against the safety benefit they are expected to provide [36]. However, a full cost effectiveness-based ALARP demonstration is outside the scope of the present research. As noted later in the report, this thesis is constrained by limited data, limited time, and concept level system definition, and therefore does not attempt a full quantified demonstration of risk reduction. Instead, ALARP is used here as a guiding decision principle, where the selected assessment methods should support the identification of hazards, the testing of barrier performance, the comparison of possible design measures, and the derivation of justified risk reduction implications for ship design.

In this thesis, these regions are used to support qualitative screening and design review, assignment to a risk matrix category does not by itself demonstrate formal risk acceptability or satisfaction of the ALARP principle.

¹The guidance from the HSE and ONR [35] expresses the relevant legal duty as reducing risk “so far as is reasonably practicable” (SFAIRP). The term ALARP is commonly used to describe how this duty is demonstrated in practice, and both formulations apply the same gross-disproportion test. The related term “as low as reasonably achievable” (ALARA) is principally used in radiation protection. Although ALARA similarly requires continued optimization of protection, it is not treated in this thesis as a substitute for a system-level ALARP demonstration.

²Cost effectiveness analysis (CEA): in ALARP compares candidate risk control options by relating cost (CAPEX, OPEX, downtime, and operational impacts) to the expected reduction in risk.

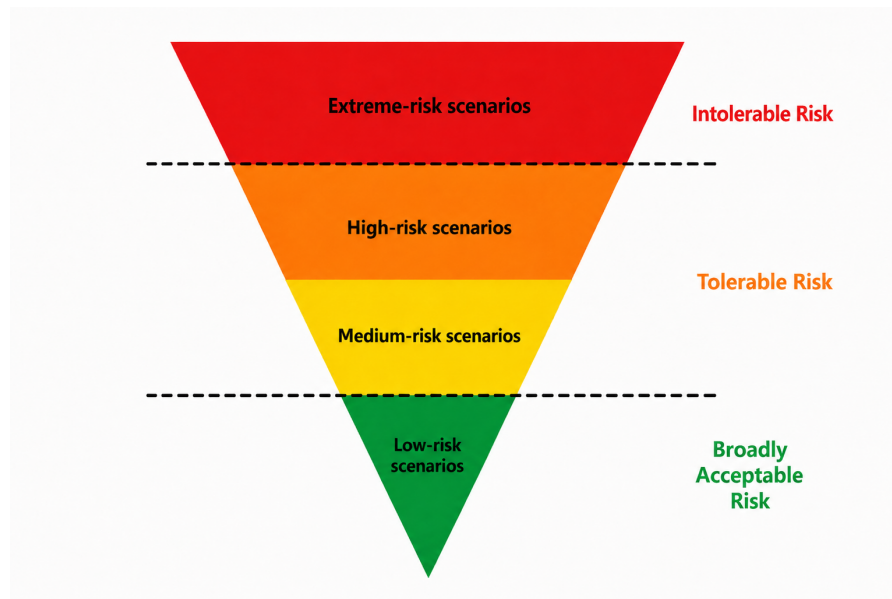


Figure 5.1: Tolerability of risk used to explain ALARP decisions, adapted from [39].

5.3. Criteria for method selection

The representative accident scenario set defined in Section 4.2, together with the main research question introduced in Section 1.4, are used to derive the criteria for selecting the most suitable risk assessment methods for this study. These criteria are shaped not only by the technical problem itself, but also by the practical boundary conditions of the present research. This thesis is conducted as an individual Master's project, within limited time, with limited access to detailed failure data, and without the multi-disciplinary specialist support that normally accompanies a nuclear safety assessment. In addition, the work is carried out at the concept design stage and ship integration level, rather than at the level of a fully defined reactor plant or vessel design. Accordingly, the preferred methods are those that can provide meaningful insight when the design is defined mainly in terms of vessel concept, major systems, safety functions, shipboard interfaces, general arrangement, and representative accident scenarios.

The criteria should therefore not be interpreted as universally representative of all possible safety assessments for nuclear powered commercial vessels. In a different context, where more detailed design information, validated reliability data, specialist nuclear expertise, and a larger assessment team are available, the relative suitability of the methods could change.

C-1: Suitability for concept design stage assessment. The method should be applicable when the design is defined only at the level of vessel concept, major systems, safety functions, shipboard interfaces, and general arrangement. It should not require detailed component definitions, or a complete system schematic. This is important because the present study evaluates nuclear ship integration at an early design stage and seeks to derive design relevant insights rather than perform a complete reactor safety case.

C-2: Ability to reveal common cause failures and false redundancy. The method should be able to identify dependencies, common cause failures, and false redundancy. This is important in a shipboard setting, where supposedly redundant safety systems may still be vulnerable to the same hazard because they are located close together, rely on the same supporting systems, follow the same routing, or are exposed to the same local conditions.

C-3: Ability to examine layered barrier performance across representative accident scenarios. The method should be able to test whether multiple safety barriers remain effective when the system is challenged by representative hazard conditions or accident scenarios. In this way, the selected

method can support assessment of whether DiD is meaningfully preserved, rather than considering only isolated failures in separation.

C-4: Ability to produce outputs that can be translated into ship integration measures. The method should be capable of producing findings that can be translated into concrete design improvements, rather than identifying or categorizing risks. Because the thesis aims not only to assess the safety of the basic concept but also to guide the development of a safer overall design, the selected methods must provide outputs that inform decisions on safety relevant design features.

C-5: Limited dependence on quantified reliability data. The method should be capable of producing meaningful results without requiring detailed failure frequencies, validated component reliability databases, or extensive probabilistic inputs. This criterion is distinct from C-1, since C-1 concerns the level of design definition, whereas C-5 concerns the level of data and evidence required by the method. Both matter in the present study because the concept is only partially defined and the available quantitative inputs are limited.

Each criterion will later be addressed through the most suitable framework logic and analytical method, as summarized in Figures 5.2b & 5.3. The purpose is not to identify a universally best method, but to justify a combination of methods that is credible, executable, and aligned with the scope and constraints of this research.

5.4. Qualitative & Quantitative approaches to risk assessment

Risk assessment can be conducted using Qualitative Risk Assessment (QIRA), Quantitative Risk Assessment (QnRA), or combined approaches. In qualitative risk assessment, risk is expressed through structured but non-numerical outputs, such as hazard registers, ordinal likelihood-consequence rankings, workshop findings, and scenario screening results. In quantitative risk assessment, risk is represented numerically, for example through event frequencies, probabilities, consequence estimates, or cost effectiveness metrics [37]. The distinction is therefore not only one of presentation, but also one of evidential depth, data requirements, and the type of decisions the assessment is intended to support.

In practice, safety assessments rarely rely on one form from the outset. Instead, a staged approach is commonly adopted, in which qualitative methods are first used to structure the hazard space, establish scope and assumptions, and identify the accident scenarios that merit further attention. Quantitative treatment is then introduced selectively where numerical comparison is needed, for example when competing design options must be evaluated, when tolerability or ALARP arguments depend on demonstrating the benefit of further risk reduction, or when cost effectiveness considerations form part of the decision basis. A clear maritime example of this staged approach is the IMO Formal Safety Assessment (FSA) [36], which begins with hazard identification and risk assessment, and only later introduces more explicit numerical comparison through cost benefit assessment, where the cost effectiveness of risk control options is evaluated using indices. A similar staged logic can also be seen in maritime concept studies [40], which used HAZID for a natural gas hydrate carrier to identify and rank hazards, then used the results to distinguish unacceptable and ALARP issues and to generate a Safety Action Register for designers, showing how an initially qualitative review can be used to screen the hazard space and direct later design action.

For the present research, this distinction is especially important because the thesis is carried out under concept level design conditions, limited failure data, and limited time. Under such conditions, a fully parameterized quantitative assessment would risk implying a level of precision that the available data does not support. A qualitative approach is therefore the appropriate starting point, since it allows hazard identification, scenario screening, and structured reasoning to proceed even where detailed inputs are unavailable. Qualitative assessment still requires a transparent and disciplined process so that assumptions, judgments, and uncertainties remain explicit and open to review [37]. In this study, qualitative methods provide the main basis for hazard completeness, traceability, and early design support, while limited and targeted quantitative logic may be introduced only where it strengthens the argument without overstating the quality of the available data. The two approaches should therefore be understood as complementary parts of a graded assessment strategy rather than as mutually exclusive alternatives. Table 5.2 summarizes the main differences between qualitative and quantitative risk

assessment approaches.

Table 5.2: Comparison of qualitative and quantitative risk assessment approaches.

Aspect	Qualitative	Quantitative
Typical outputs	Ordinal categories, risk registers, risk matrices [41]	Numerical frequency/probability, consequence distributions, cost effectiveness [36]
Primary purpose	Hazard discovery, scenario screening, early design decision support [41]	Support risk acceptance, ALARP arguments and trade studies [36]
Strengths	Fast, workshop-driven, effective under limited data [41]	Validity can be interrogated via sensitivity analysis
Limitations	Risk matrices may not represent aggregate risk, dependencies, or uncertainty well	Data quality can dominate results. Requires epistemic uncertainty and model limitations disclosure
Examples in safety cases	HAZID & HAZOP, structured checklists, risk matrices [41]	Fault tree & event tree quantification, Monte Carlo, Consequence modeling [42]

5.5. Assessment frameworks

This section reviews the broader assessment frameworks relevant to the study. These are not all applied here in their full formal sense. Instead, they are used selectively as guiding philosophies for structuring the safety argument, defining the type of evidence required, and clarifying when qualitative treatment is sufficient and when escalation toward more formal or quantitative analysis would be expected. In this way, the frameworks support method selection and interpretation without being treated as complete standalone applications within the present thesis.

5.5.1. Deterministic & Probabilistic safety analysis (DSA & PSA)

Safety assessment in the nuclear domain is generally built around two complementary approaches: DSA and PSA. The IAEA requires both approaches to be considered within the safety analysis because they provide different but mutually reinforcing types of evidence [43], [44]. DSA is used to demonstrate that the plant can withstand defined postulated initiating events while maintaining required safety functions and acceptable safety margins [43]. PSA, by contrast, is used to identify and quantify the dominant contributors to risk, including accident sequences, dependencies, common cause failures, and human contributions that may not be fully visible through deterministic analysis alone [44].

Deterministic Safety Analysis (DSA)

DSA is fundamentally scenario-based. Its main strength is that it provides a structured and defensible demonstration that the design can meet required safety functions, remain within prescribed limits, and tolerate specified accident conditions with adequate margins. In that sense, DSA is especially important for showing whether shutdown, cooling, confinement, shielding, and habitability assumptions remain valid under defined accident scenarios. It is therefore well suited to design-basis reasoning and to the establishment of clear success criteria. [43]

Probabilistic Safety Analysis (PSA)

PSA addresses a different question. Rather than asking whether the plant can withstand each postulated scenario with adequate margin, it asks how overall risk is structured, what accident sequences dominate it, and which failures or dependencies contribute most strongly to that risk. Its value lies in its ability to reveal interactions, weak points, and risk-significant contributors that may not be obvious in deterministic scenario analysis alone. For this reason, PSA is useful for identifying where redundancy is not truly independent, where common cause vulnerabilities exist, and where design improvements

may have the greatest risk reduction effect. [44]. PSA itself spans different levels of analysis, ranging from accident-sequence modeling to broader release and consequence assessment. Since the present thesis does not attempt a full multi-level PSA, the summary of PSA levels is provided in Table A.3, while the main discussion here focuses on the distinction between DSA and PSA that is most relevant to method selection.

Study relevance

For the present research, the importance of DSA and PSA lies mainly in their philosophy, rather than in their full formal application. DSA provides a useful structure for defining bounded cases, safety functions, and acceptance assumptions for representative accident scenarios. PSA provides a useful structure for thinking about initiating events, sequence development, dependencies, and dominant contributors to risk. However, because this thesis is conducted at concept level, under limited data and without the depth of design maturity required for a full plant-level probabilistic model, PSA is not adopted here as a primary applied method. Instead, its main value is conceptual, it informs the later use of Event Tree Analysis (ETA), Fault Tree Analysis (FTA), dependency analysis, and common cause failure treatment. DSA remains relevant as part of the reviewed nuclear safety literature, particularly for framing bounded cases and explicit safety assumptions, but it is not adopted as a primary element of the selected combination of methods for this thesis. Accordingly, DSA and PSA are not treated in this thesis as competing alternatives. They are better understood as complementary framework philosophies that help define what later analytical methods must demonstrate. The more important comparison for the present study is therefore between the roles of DSA and PSA in safety reasoning, as summarized in Table 5.3.

As a result, DSA and PSA contribute mainly to criterion C-3, since they provide the underlying logic for examining accident sequence development, dependencies, common cause vulnerabilities, and the maintenance of safety functions under representative accident conditions, but they are less suited to criterion C-5 in the present study because full formal application would require greater design maturity and more detailed data than are available at concept stage.

Table 5.3: Comparison of DSA and PSA for uncertainty management and safety decision support [43], [44], [34].

Aspect	DSA	PSA
Primary question	"Is the plant safe for each postulated scenario with an adequate margin?"	"How risky is the plant overall, and what dominates risk?"
Scenario-based	Postulated Initiating Event set with pre-defined rules and acceptance criteria.	Initiating events, sequence logic (event trees), system reliability (fault trees), and dependencies.
Outputs	Safety margins vs acceptance criteria; limiting cases; operational limits and conditions support.	Core damage and large early release frequencies.
Strengths	Clear compliance demonstration; defensible margins; strong for design-basis demonstration.	System-level prioritization; captures rare sequences, dependencies and human & organizational contributors quantitatively.
Limitations	Can miss risk-significant combinations if Postulated Initiating Event set and assumptions are incomplete.	Results depend on modeling quality and data; they can be sensitive to assumptions.

5.5.2. Formal Safety Assessment (FSA)

Formal Safety Assessment (FSA) is a structured and systematic framework developed by the IMO to support risk-informed decision making in maritime safety and environmental protection. Its importance lies in the fact that it does not treat hazard identification, risk analysis, and decision-making as separate exercises, but links them within a single traceable process [36]. For the purposes of this thesis,

FSA is particularly relevant because it provides a maritime-oriented structure for moving from accident scenarios to risk control options and, ultimately, to justified recommendations.

The IMO FSA Guidelines define a five-step process consisting of hazard identification, risk analysis, risk control options, cost-benefit assessment, and recommendations for decision making [36]. Taken together, these steps provide a clear pathway from the identification of relevant accident scenarios to the evaluation of candidate risk reduction measures. In that sense, FSA is especially valuable in studies such as the present one, where the objective is not only to describe hazards, but also to justify why certain design-oriented safety measures should be preferred over others. A summary of the IMO FSA process is provided in Figure A.1.

Study relevance

FSA is also relevant because it accommodates a staged approach rather than requiring a fully quantified analysis from the outset. The IMO guidance explicitly allows early screening and recognizes the need for sensitivity and uncertainty analysis in both the risk-analysis and cost benefit stages [36]. This is important in the present context, where the design is still at concept level and detailed reliability and consequence data are limited.

For this reason, FSA is not applied in this thesis as a full standalone regulatory assessment. Instead, it is adopted as the overarching maritime framework philosophy that helps organize the selected combination of methods later in the chapter. The value of FSA in this thesis is not that it replaces nuclear safety assessment logic, but that it provides a maritime-compatible decision structure within which the selected analytical methods can contribute to a traceable and risk based design argument.

As a result, FSA contributes strongly to criterion C-1, since it provides a system-level and ship-level structure for organizing the safety problem, and to criterion C-3, because its staged process supports the examination of accident development, safety functions, and risk-control logic under representative scenarios. It also contributes to criterion C-4, because it supports the translation of risk findings into traceable risk-control options and design-oriented recommendations, and to criterion C-5, since its staged logic remains usable under concept level conditions and limited data availability, even when full quantitative application is not yet justified.

5.6. Analytical methods

This section reviews the main analytical methods considered in this study. Unlike the broader assessment frameworks discussed in Section 5.5, these methods are the practical tools used to identify hazards, analyze accident sequences, examine failure mechanisms, and derive design relevant safety implications. Because each method addresses a different aspect of the problem, they are not treated here as interchangeable alternatives, but as complementary methods combined to support a concept level, limited data assessment. The aim of this section is therefore to clarify the role, strengths, and limitations of each method in relation to the criteria defined in Section 5.3 and the objective of the thesis.

5.6.1. Hazard Identification Study (HAZID) & Hazard and Operability Study (HAZOP)

HAZID and HAZOP are structured qualitative methods used to convert incomplete design knowledge into a traceable set of hazards, assumptions, safeguards, and follow-up actions. Their value lies in the fact that they impose discipline on early-stage uncertainty rather than requiring a mature quantitative evidence base from the outset. This makes them particularly relevant to the present research, where the study is conducted at concept and ship integration level, under limited data availability and without the depth of detailed system definition. Although the Maritime Technologies Forum (MTF) guidance used here was developed for alternative fueled ships, the methodological philosophy remains useful more broadly because it standardizes how qualitative risk workshops are prepared, conducted, recorded, and closed out. [41]

Hazard Identification Study (HAZID)

For this thesis, the main role of HAZID is early hazard discovery. HAZID is well suited to concept level studies because it can be applied before all system details are fixed, allowing to identify relevant

hazard categories, define the scope and boundaries of the assessment, and structure the initial accident scenario set.

A key strength of HAZID is that it helps reduce the risk of missing important scenarios when evidence is incomplete. The MTF workflow (Figure A.2) emphasizes preparation, hazard identification, consequence and likelihood evaluation, safeguard review, risk ranking³, and action tracking, thereby ensuring that the qualitative assessment remains structured and repeatable [41]. In particular, the guidance requires consequences to be considered without safeguards first, so that the full unmitigated escalation potential of a scenario is understood before preventive and mitigative measures are credited.

Hazard and Operability Study (HAZOP)

HAZOP serves a different, more detailed purpose. Whereas HAZID is primarily used to identify hazards broadly, HAZOP examines deviations from design intent at defined nodes and applies guidewords systematically to generate possible causes, consequences, safeguards, and required actions. It is therefore more suitable once the arrangement, system functions, and operating modes are sufficiently defined to support node-based analysis. In the present thesis, this means that HAZOP is potentially useful for later examination of deviations in cooling paths, auxiliary services, ventilation, confinement-related functions, electrical supply, or operational interfaces, but it is less suitable than HAZID as the main front-end method at concept level.

Study relevance

The distinction between the two methods is important for method selection. HAZID supports criterion C-1 strongly because it can be applied at system and architectural design level, and it also supports C-5 because it remains usable under limited data and limited design maturity. HAZOP contributes where design intent can be defined in sufficient detail, but it is more dependent on a clearer system description and therefore becomes more useful at a later stage of development. In the present study, neither HAZID nor HAZOP is used alone to assess barrier independence and common dependencies in detail. These aspects are examined through the subsequent Bow-tie analysis, which makes the position and relationship of the safeguards within the accident pathways more explicit.

5.6.2. Bow-tie method

The Bow-tie method is a barrier-based risk analysis tool used to represent, in a single integrated structure, how identified threats can lead to a central undesired event and how that event can then escalate into different consequences if further barriers fail. Its main value lies in the fact that it combines cause-side logic, consequence-side logic, and barrier placement in a format that is both analytical and visually transparent. [45]

Structure

In a Bow-tie structure, the top event is placed at the center of the diagram. To the left are the threats or causes that can lead to loss of control of the hazard, while to the right are the possible consequences that may follow if the top event occurs. Preventive barriers are positioned between the threats and the top event, and mitigative barriers are positioned between the top event and the consequences. In this way, the method makes barrier logic explicit and helps distinguish between controls intended to prevent occurrence and controls intended to limit escalation [45]. The method is closely related to the combined use of FTA and ETA, since the left-hand side is FTA-like and the right-hand side is ETA-like. The general structure of the Bow-tie method is shown in Figure A.4.

Study relevance

The Bow-tie method is valuable because it supports a barrier oriented interpretation of accident scenarios that aligns with DiD and contributes to an ALARP-oriented review of further risk reduction opportunities. In the case of nuclear powered commercial vessels, many of the relevant scenarios involve multiple interacting layers of protection, including design barriers, segregation measures, supporting services, operational controls, and emergency response functions. Bow-tie analysis provides a compact way to show how these barriers relate to one another and where accident escalation depends on their success or failure [45].

³The generic consequence–likelihood matrix used to support ranking and follow-up is shown in Figure A.3. Although the exact categorization must be adapted to the study context, the figure is useful here as a reference for how HAZID/HAZOP findings can be screened into acceptable, tolerable, and unacceptable bands to support further action and ALARP-oriented review.

Another strength of the Bow-tie method is that it remains useful even under limited data availability [46]. At concept stage, the method does not require a fully quantified probabilistic model in order to be informative. It can be used qualitatively to structure accident logic, identify barrier weaknesses, and support discussion of where additional design measures may be needed. Where greater detail is justified, the cause side and consequence side can later be developed using more formal FTA or ETA logic, but the Bow-tie itself already provides a traceable framework for organizing the scenario and control structure. [45]

As a result, the method contributes strongly to criterion C-2, since it helps expose dependencies and false redundancy, and to criterion C-3, since it allows layered barrier performance to be examined under representative initiating events. It also supports criterion C-4, because weaknesses identified in the barrier structure can be translated directly into design-oriented recommendations.

5.6.3. Failure Modes and Effects Analysis (FMEA) & Failure Modes, Effects and Criticality Analysis (FMECA)

FMEA and FMECA are inductive, bottom-up analytical methods used to examine how systems, sub-systems, functions, or components can fail, how those failures propagate, and what their effects are at higher levels of the system. Their value lies in the fact that they force the analyst to proceed systematically from function to failure mode, from failure mode to effect, and from effect to the need for controls, design changes, or further action. In marine and engineering practice, FMEA is used to identify possible failure modes, their effects on system performance and safety, and the corrective actions required to reduce vulnerability, while FMECA extends this process by adding a structured assessment of failure criticality. [47], [48]

Failure Modes and Effects Analysis (FMEA)

FMEA identifies the relevant failure modes associated with each item or function, the causes or mechanisms that may give rise to them, their local effects, their propagation to higher system-levels, the existing controls in place, and the actions required to reduce vulnerability. In this way, FMEA produces a structured catalogue of how a design may fail and what must be done to improve it. [47]

Failure Modes, Effects and Criticality Analysis (FMECA)

FMECA extends this logic by adding an explicit criticality assessment. The purpose of this additional step is not to change the underlying failure logic, but to prioritize the failure modes that are most significant in terms of severity, likelihood, or other selected decision criteria. FMECA therefore supports a more focused allocation of engineering effort by showing which contributors are most important and which actions deserve priority under constrained conditions [48]. A summary of the standard FMEA/FMECA workflow is provided in Figure A.5.

Study relevance

FMEA and FMECA are particularly useful because they translate higher-level accident concerns into concrete design-relevant vulnerabilities. Whereas HAZID and Bow-tie analysis are more useful for structuring hazards, accident scenarios, and barrier logic at system-level, FMEA and FMECA help identify which specific functions, support systems, interfaces, or items are most likely to undermine those barriers in practice.

These methods are also well suited to the boundary conditions of the present research. Since the study is conducted at concept and ship integration level, under limited data availability and without the depth of detail, a method is needed that can still generate structured and traceable outputs without implying false numerical precision. FMEA provides that structured basis by identifying failure modes, causes, effects, controls, and recommended actions, while FMECA adds the prioritization needed to focus attention on the most safety-significant contributors. This makes the methods relevant to criterion C-4, since they support the derivation of concrete design implications rather than only describing hazards in general terms.

5.7. Comparison & Selection

This section compares the reviewed approaches, frameworks, and analytical methods against the thesis-specific selection criteria defined in Section 5.3. The purpose is not to identify a single uni-

versally superior method, but to determine a combination of methods that is suitable for concept level safety assessment of a nuclear powered commercial vessel. Because the thesis is carried out under limited data availability, limited time, and limited design maturity, the selected combination of methods must remain executable in qualitative terms while still supporting accident scenario structuring, barrier assessment, and the derivation of design implications. The figures below summarize how the reviewed approaches (Figure 5.2a), frameworks (Figure 5.2b), and methods (Figure 5.3) perform against the criteria.

Some criteria are not fully met by all reviewed approaches, frameworks, and methods. This reflects differences in their intended scope rather than an inherent weakness. Methods suited to mature, data rich assessments may be less applicable under the concept level conditions of this thesis, while others are better suited to hazard identification, barrier analysis, or design development. The comparison is therefore used to identify complementary strengths rather than a single standalone method.

Table 5.4: Method-selection criteria used in the comparison

ID	Criterion
C-1	Suitability for concept design assessment
C-2	Ability to reveal common cause failure and false redundancy (<i>DiD</i>)
C-3	Ability to examine layered barrier performance (<i>DiD</i>)
C-4	Ability to produce ship integration measures (<i>ALARP-oriented</i>)
C-5	Limited dependence on quantified reliability data

Criteria	Approach	
	QIRA	QnRA
C-1	Strong	Moderate
C-2	Moderate	Weak
C-3	Moderate	Weak
C-4	Moderate	Weak
C-5	Strong	Moderate

(a) Approaches—criteria applicability matrix.

Criteria	Frameworks		
	DSA	PSA	FSA
C-1	Limited	Limited	Strong
C-2	Weak	Limited	Limited
C-3	Moderate	Strong	Strong
C-4	Moderate	Moderate	Moderate
C-5	Weak	Limited	Strong

(b) Frameworks—criteria applicability matrix.

Figure 5.2: Comparison of the reviewed approaches and assessment frameworks against the criteria.

Criteria	Methods				
	HAZID	HAZOP	Bow-tie	FMEA	FMECA
C-1	Strong	Limited	Moderate	Limited	Limited
C-2	Limited	Moderate	Strong	Limited	Moderate
C-3	Limited	Limited	Moderate	Limited	Limited
C-4	Strong	Moderate	Strong	Moderate	Moderate
C-5	Strong	Moderate	Strong	Moderate	Moderate

Figure 5.3: Method—criteria applicability matrix.

5.7.1. Selection rationale

This study adopts a combination of risk assessment methods rather than selecting a single universally superior method. The rationale is that the safety problem addressed in this thesis is multi-layered: hazards must first be identified, accident scenarios must then be structured, barriers and dependencies must be examined, and the resulting findings must support justified design-oriented recommendations. No single framework or method performs all of these functions equally well under the concept level constraints of the present research.

Although the reviewed frameworks and methods are separated analytically in this chapter, they are not fully independent in practice. There is important functional overlap between them. FSA includes hazard-identification and risk-analysis steps that overlap with the front-end role of HAZID, while Bow-tie overlaps with broader accident-sequence reasoning by linking causes, top events, consequences, and barriers in one traceable structure. HAZOP also overlaps partly with HAZID, but is more dependent on detailed node definition and design intent. The purpose of the present selection is therefore not to assign each criterion to one exclusive method, but to identify the combination that provides the most coherent and executable basis for this thesis.

For this reason, the selected combination of methods is centered on HAZID, Bow-tie analysis, and an FSA-informed decision structure. HAZID is selected as the principal front-end method because it is well suited to concept level studies, allows broad system and architectural hazards to be identified before full design maturity is reached, and remains usable under limited data availability. Bow-tie analysis is selected because it provides the clearest practical method for structuring how threats and escalation pathways may lead to top events and how these may escalate through barrier success or failure, which is particularly relevant for examining layered protection, dependencies, and false redundancy in shipboard nuclear safety. FSA is retained not as a standalone technical analysis method, but as the overarching maritime framework that organizes the transition from hazard identification to risk analysis, risk control options, and justified recommendations. Other reviewed approaches remain relevant but are not selected as primary elements of the combination of methods.

The selected combination addresses the thesis criteria more effectively than any of the reviewed methods used alone. HAZID contributes strongly to C-1 and C-5 because it operates at concept design stage and remains usable under incomplete information. Bow-tie contributes strongly to C-2 and C-3 because it exposes barrier dependencies, false redundancy, and escalation pathways under representative initiating events, while also contributing to C-4 by revealing where additional segregation, protection, or supporting design measures may be required. FSA contributes mainly by providing a structured maritime decision pathway that links the analytical results to risk control options and design-oriented recommendations. The combination is therefore suitable for the concept level and limited data conditions of this study.

5.8. Chapter 5 Conclusion

Concept level safety assessment of nuclear powered commercial vessels can be supported by using DiD and ALARP as guiding principles, an FSA-informed structure for risk based decision making, and a combination of HAZID and Bow-tie analysis as the principal analytical methods. The HAZID provides broad hazard identification and comparative risk ranking under limited design maturity, while Bow-tie analysis examines accident progression, barrier performance, dependencies, and false redundancy in greater detail.

This combination provides a practical basis for identifying hazards and translating safeguard limitations into design recommendations without implying unsupported quantitative precision. Chapter 6 therefore establishes the reference vessel and assessment basis required for its consistent application.

6

Reference Vessel Concept and Assessment Basis

How can a reference vessel concept be established to provide a consistent basis for risk assessment?

This chapter establishes the reference vessel and the assessment basis used in the risk assessment. It defines the vessel design, principal system interfaces, safety objectives, assessment boundaries, assumptions, and risk-ranking method. The distinction between Initial vessel and nuclear island concept (REV0), First design iteration configuration (REVA), and Safety driven second design iteration (REVB) is also introduced to provide a consistent basis for the assessment and design iterations presented in Chapters 7 & 8.

6.1. Reference vessel and system design

The reference vessel is a nuclear powered bulk carrier. An HTGR is used as the primary heat source. Reactor heat is transferred from the primary helium circuit through the steam generator to a separate steam-water Rankine cycle. Steam from this secondary circuit drives a turbine generator, which supplies electrical power to the propulsion motors and ship service systems.

A bulk carrier was selected because its normal ocean passage condition is associated with relatively stable propulsion demand. This operating profile is compatible with steady reactor operation. The assessment basis also considers abnormal conditions, including maneuvering, propulsion load changes, equipment failure, reactor shutdown, and loss of supporting services.

The vessel concept provides the compartment locations and main system interfaces required for the risk assessment. Detailed component design, control system design, thermal hydraulic analysis, and plant performance optimization are outside the scope of the study.

6.1.1. Vessel mission and operating profile

The vessel is intended for long distance cargo transport on fixed deep sea routes. It uses an all electric propulsion arrangement in which the nuclear plant supplies both propulsion and ship service electrical loads. The assumed design life is 30 years. The reactor is intended to use a long interval or ship life fuel strategy, although detailed fuel cycle analysis is not included.

The main operating condition is steady ocean passage. However, the assessment also covers maneuvering and abnormal operating conditions, and accident conditions involving loss of system function or loss of pressure boundary integrity.

Reduced power operation, startup, hot shutdown, cold shutdown, port reactor operation, refueling, and port emergency response arrangements are not assessed in detail. These activities would require additional assumptions concerning port state requirements, specialized facilities, operating procedures,

and external emergency support.

6.1.2. Principal vessel dimensions

The principal dimensions are derived from the reference general arrangement and are presented in Table 6.1.

Table 6.1: Principal dimensions of the reference vessel

Parameter	Reference value
Length overall, L_{OA}	310 m
Moulded breadth	50 m
Depth to main deck	40 m
Design draught	25 m

These dimensions establish the physical scale of the vessel and support the definition of machinery space locations, cargo arrangement, structural separation, double hull protection, and access routes. They are not used to calculate accident frequencies or structural response.

6.1.3. Nuclear heat source

The reference vessel is fitted with a Generation IV HTGR using TRISO¹-coated particle fuel in a pebble-bed core. Helium is used as the primary coolant. The assumed reactor parameters are summarized in Table 6.2.

Table 6.2: Reference reactor parameters

Parameter	Reference value
Reactor type	High Temperature Gas Reactor
Reactor configuration	Small modular reactor
Electrical output	25 MW _e
Fuel type	TRISO-coated particle fuel
Fuel form	Pebble bed
Fuel enrichment	Low-enriched uranium
Primary coolant	Helium

The reactor concept was selected because TRISO fuel, graphite moderation, helium cooling, and the thermal capacity of the core provide inherent and passive safety characteristics. Helium is chemically inert and remains in a single phase during normal operation. These characteristics reduce several chemical and phase change hazards associated with water cooled systems.

However, loss of helium inventory can reduce forced heat transport. Helium released from the primary circuit may also contain radioactive contamination. The integrity of the primary helium circuit is significant because the circuit must retain the pressurized coolant and limit its uncontrolled release. Reactor behavior is represented through the safety functions required to shut down the reactor, remove decay heat, and confine radioactive material.

6.1.4. Power conversion system

Reactor heat is transferred from the primary helium circuit through the steam generator to a separate steam-water Rankine cycle. Steam from this secondary circuit drives a turbine generator, which supplies electrical power for propulsion and ship service loads.

¹TRISO fuel consists of a uranium-bearing kernel surrounded by successive carbon and silicon-carbide coating layers. Each particle acts as an individual containment system, providing high temperature resistance and limiting the release of fission products.

The steam generator tube wall forms the physical interface between the primary helium circuit and the steam-water circuit. Loss of tube integrity may allow helium to enter the secondary circuit or water and steam to enter the primary circuit. Such a failure may affect primary circuit pressure and cooling, transfer radioactive contamination between the circuits, and disrupt electrical power generation. For this reason, steam generator tube integrity is treated as a system boundary in the subsequent risk assessment. Detailed component geometry and power conversion design are outside the scope of the concept level assessment.

6.1.5. Seawater heat rejection system

The condenser rejects waste heat through a seawater cooling circuit connecting the sea intake, seawater pumps, condenser, and overboard discharge.

This circuit provides the normal heat rejection path for the power conversion system. Loss of seawater flow or condenser cooling may increase condenser pressure and lead to turbine trip, loss of electrical generation, and reactor shutdown demand. The system also forms a direct interface with the marine environment, making its availability and discharge arrangement relevant to the subsequent risk assessment.

6.1.6. Electrical power and propulsion system

The vessel uses an all electric propulsion arrangement in which the main generator supplies both propulsion and ship service electrical loads.

Electrical distribution is treated as a safety supporting function because several reactor monitoring, control, cooling, isolation, and recovery functions depend on electrical power. Thus, a ship service blackout may affect both vessel operation and nuclear safety functions simultaneously. This is examined explicitly in the subsequent risk assessment.

6.1.7. Nuclear and machinery space arrangement

The nuclear installation is located low in the vessel and near the midship region, providing increased separation from the ship side and bottom and reducing exposure to vessel motions.

The reference arrangement separates the reactor and primary helium circuit from the turbine generator, seawater cooling, electrical distribution, cargo, and accommodation spaces. The reactor compartment is surrounded by structural separation, shielding, and a cofferdam.

The REV0 general arrangement and nuclear island arrangement are introduced in Figures 6.1 & 6.2, with the full size drawings provided in Appendix B.

6.2. Assessment objectives

The reference concept is assessed against the fundamental nuclear safety functions and the principles of DiD and ALARP. These objectives define which safety functions must be preserved during abnormal and accident conditions and how the adequacy of the available safeguards is evaluated. [34, 36, 4]

6.2.1. Nuclear and ship safety objectives

The assessment uses the three fundamental nuclear safety functions as its primary basis, control of reactivity, removal of heat from the reactor core, and confinement of radioactive material. These functions must remain available during normal operation, anticipated operational events, and accident conditions [34, 4].

At ship level, the nuclear safety functions depend on supporting systems. Reactor shutdown requires control and protection systems. Decay heat removal requires an available heat transfer path. Confinement depends on pressure boundaries, ventilation control, isolation, filtration, and structural protection. Monitoring and recovery require electrical power and access to control equipment [30, 50].

The design must maintain reactor shutdown capability, decay heat removal, pressure boundary integrity where practicable, isolation of failed sections, contamination control, radiation protection, and essential monitoring. A single local event should not disable all redundant safety provisions, in line with DiD implementation guidance that seeks to avoid single failures leading directly to harmful effects [28, 4].

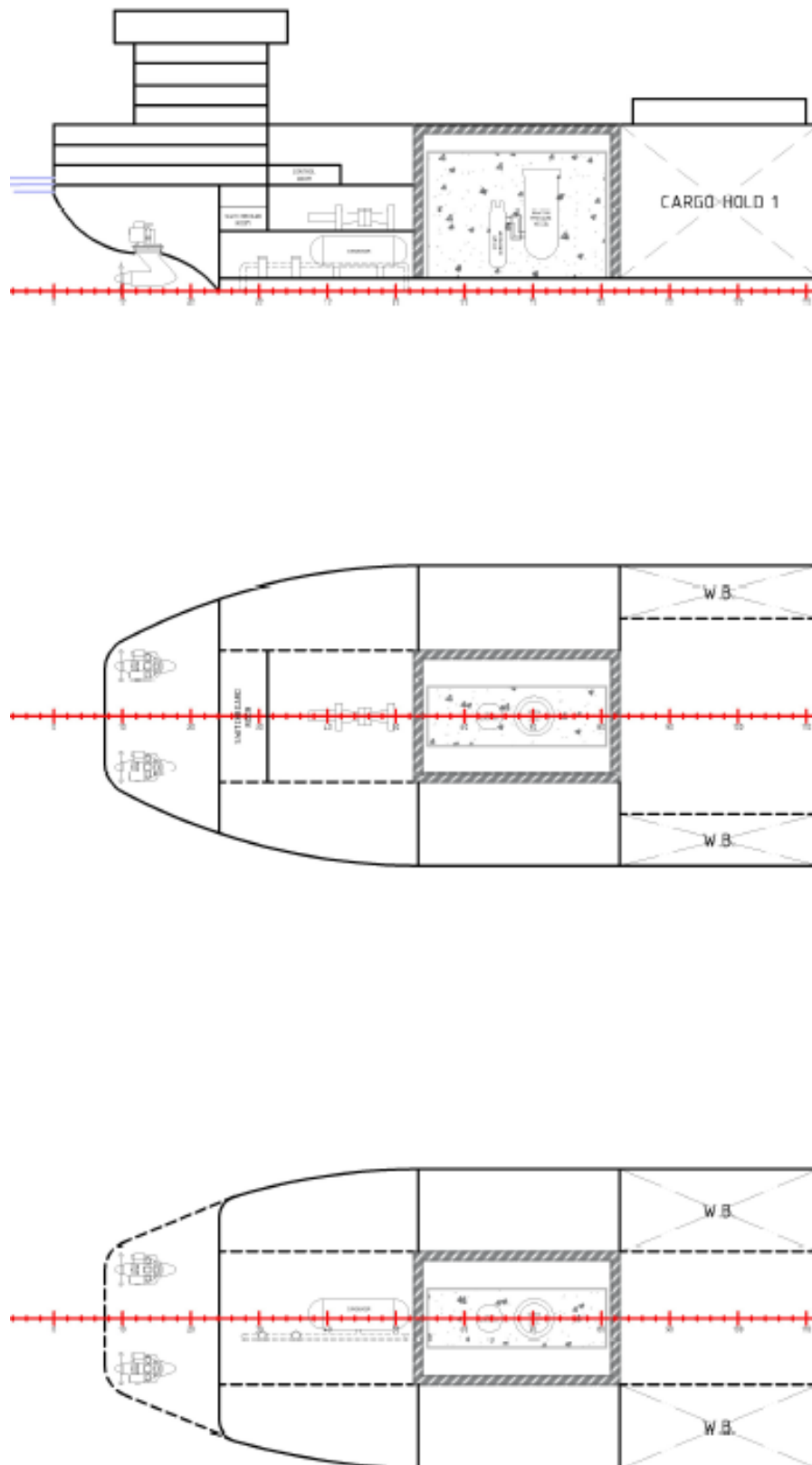
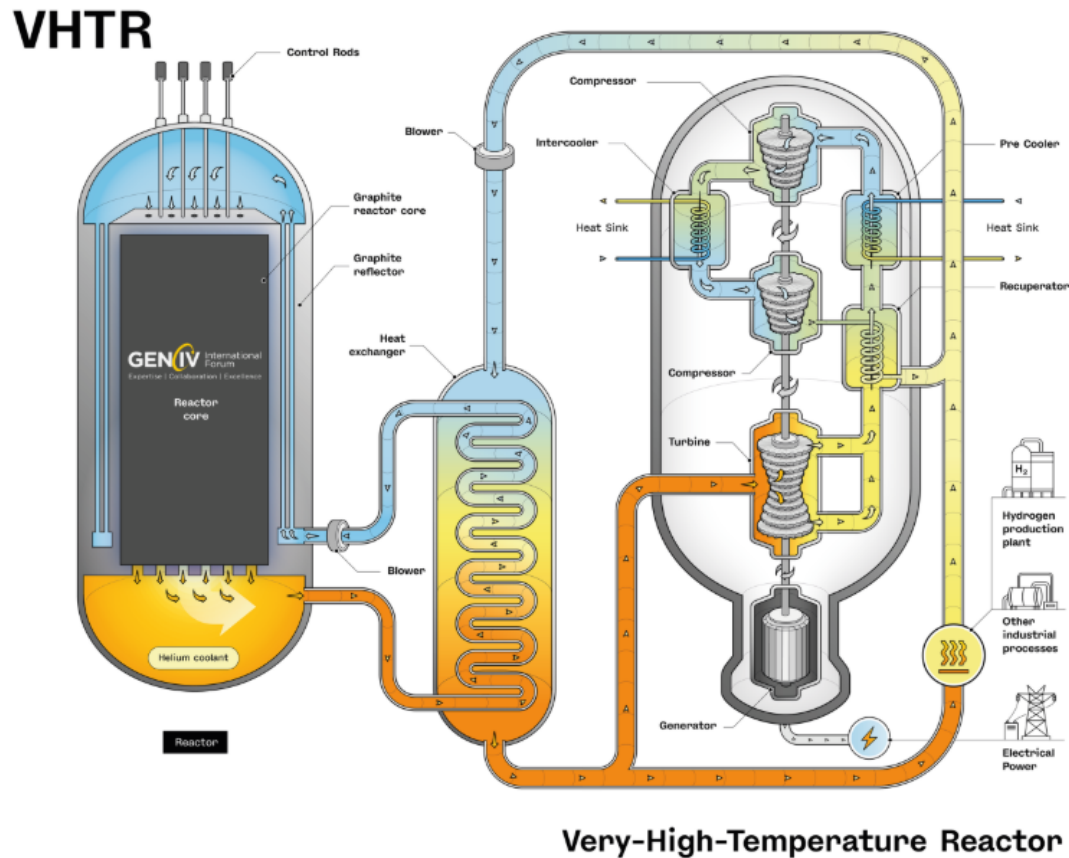
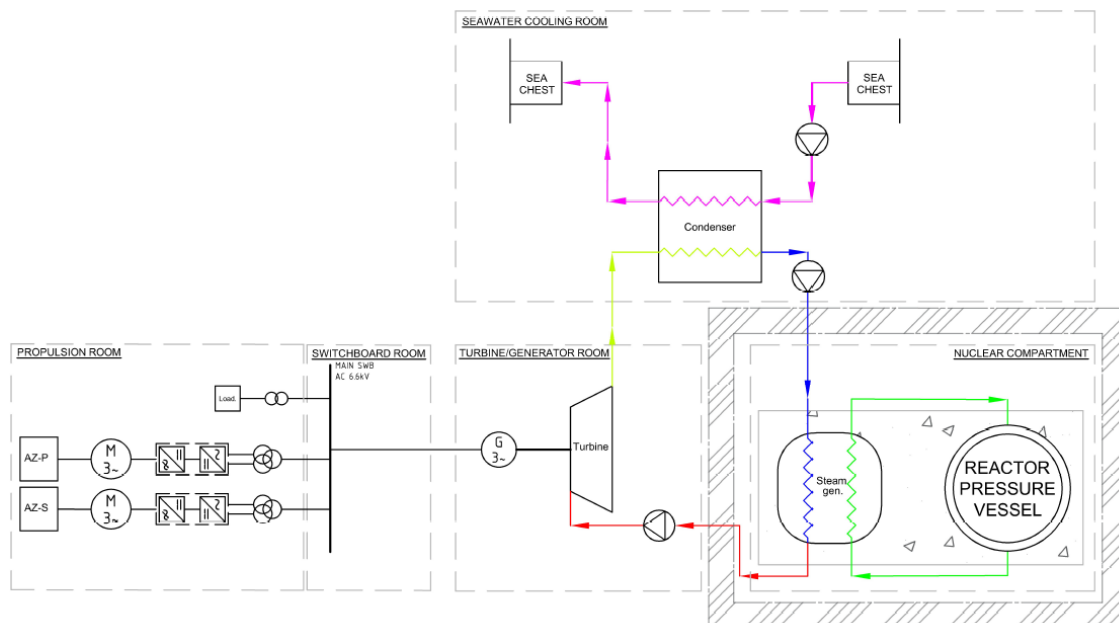


Figure 6.1: Reference REV0 vessel arrangements used to define the machinery space locations for the risk assessment.



(a) Conceptual land based (v)HTGR energy conversion arrangement used as the basis for the reference power system design [49].



(b) REV0 nuclear island arrangement

Figure 6.2: Reference nuclear reactor and REV0 principal system interfaces for the risk assessment.

Propulsion availability remains important because loss of maneuverability may increase exposure to collision, grounding, or severe weather. However, reactor safety has priority over continued propulsion. The propulsion system must not prevent reactor shutdown or safe removal of decay heat [50].

6.2.2. Defence-in-Depth (DiD) objective

The design is assessed against the five levels of DiD introduced in Chapter 5. The objective is not only to count the number of barriers. The assessment also considers whether the barriers perform different functions and remain sufficiently independent.

Redundancy alone is not considered sufficient evidence of independence. Two components may be functionally redundant but remain vulnerable to the same initiating event if they share a compartment, cooling source, control system, or ventilation path [51, 52].

6.2.3. As Low As Reasonably Practicable (ALARP) objective

The ALARP principle is used to support the review of whether further concept level risk reduction is reasonably practicable. Scenarios that remain within the tolerable risk region after existing safeguards are examined for additional design measures that could reduce risk further.

A formal ALARP demonstration would require more detailed quantitative evidence and consideration of factors such as cost, reliability, weight, maintainability, and operational impact [34, 35, 39, 53]. These are outside the scope of the present concept level study. ALARP is therefore applied as a guiding design principle rather than as a formal demonstration of risk acceptability.

6.3. Assessment scope, constraints and assumptions

This section defines the conditions under which the risk assessment is applied. The design constraints identify the limitations on ship integration, the assessment scope defines the systems and hazards included in the study, and the assumptions establish how incomplete concept level information is treated consistently.

6.3.1. Ship design constraints

In this study, a design constraint is a physical or operational limitation that restricts how the nuclear installation can be integrated into the vessel. The constraints considered are available machinery space volume, equipment and shielding mass, cargo capacity, stability, structural arrangement, accessibility, and the need to segregate systems.

These constraints are relevant to barrier independence. Redundant equipment requires sufficient physical separation to prevent a single local failure from disabling all available safety provisions. For example, two seawater pumps may provide functional redundancy, but their independence is reduced if both are located within the same floodable compartment. Similar considerations apply to electrical distribution, emergency power, cable routing, ventilation, and isolation functions.

6.3.2. Assessment scope and system boundaries

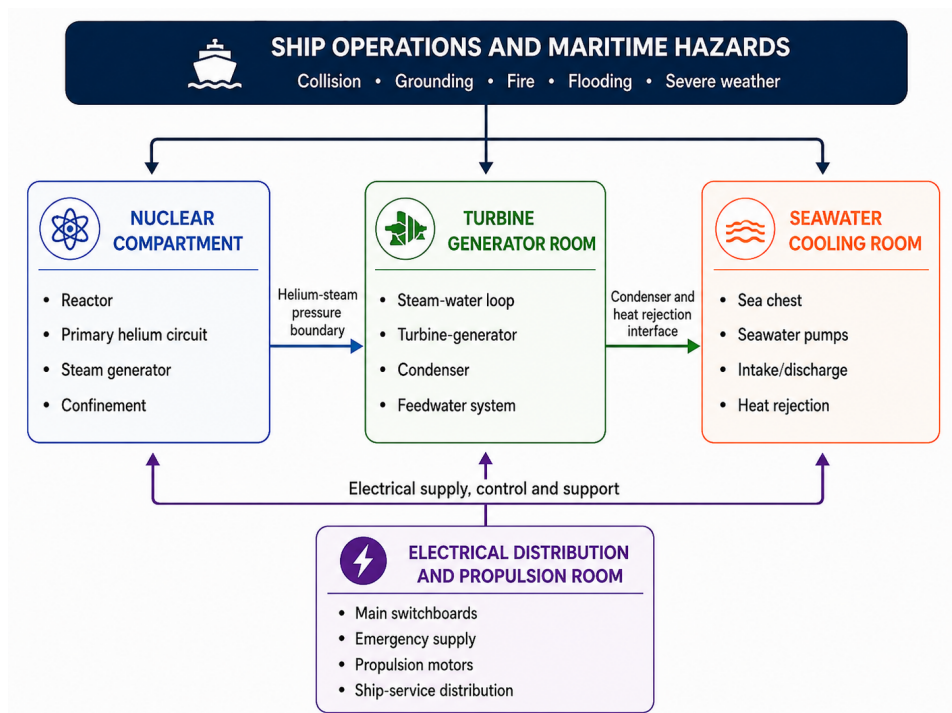
The assessment is organized into five functional nodes representing the nuclear compartment, turbine-generator room, seawater cooling room, electrical distribution and propulsion, and ship level interfaces of the reference vessel. The node structure supports the HAZID by allowing both local failures and cross-system escalation to be considered within one assessment.

The five nodes are defined in Table 6.3, while their functional and physical interfaces are illustrated in Figure 6.3.

Table 6.3: Functional nodes used in the HAZID.

Node	Assessment area	Main systems and functions
1	Nuclear compartment	Reactor, primary helium circuit, steam generator, reactor shutdown systems, confinement functions, and associated monitoring.
2	Turbine-generator room	Steam-water power conversion circuit, turbine-generator, condenser interface, feedwater system, and pressure control functions.
3	Seawater cooling room	Sea chest, seawater pumps, condenser cooling circuit, seawater piping, intake and overboard discharge.
4	Electrical distribution and propulsion	Main and emergency electrical supply, switchboards, ship-service distribution, propulsion motors, and electrical support to safety systems.
5	Ship operations and maritime interfaces	Ship level operational and external interfaces through which maritime events may challenge the plant and supporting systems.

Figure 6.3 shows the main assessment logic. The nuclear compartment, turbine-generator room, and seawater cooling room form the energy transfer path, while electrical distribution provides a shared supporting function across these systems. Maritime hazards may challenge several nodes simultaneously. The HAZID node structure was selected to preserve these interfaces and common dependencies during the assessment.

**Figure 6.3:** Functional HAZID nodes and their principal system interfaces.

The nodes define the systems and functions being assessed. They are not themselves hazard categories. Hazards are applied across the relevant nodes during the HAZID and include abnormal pressure and temperature, loss of flow or inventory, leakage and rupture, loss of heat rejection, loss of electrical power, control failure, fire, flooding, collision, grounding, severe weather, contamination spread, and radioactive release.

The node boundaries follow the energy transfer, electrical, and structural interfaces of the reference vessel. This allows failures at one interface to be traced into other systems where escalation is credible.

The assessment remains at concept design level. Detailed reactor physics and thermal hydraulic calculations, radiological consequence modeling, component level probabilistic reliability analysis, structural collision calculations, security assessment, human reliability analysis, port emergency planning, re-fueling operations, decommissioning, and formal cost effectiveness analysis are outside the detailed scope.

These exclusions define the limits of the conclusions that can be drawn from the assessment and identify areas requiring more detailed analysis during later design stages.

6.3.3. Assessment assumptions

The assumptions presented in Table 6.4 were applied to maintain a consistent basis across the HAZID and Bow-tie analyses.

Table 6.4: Main assumptions used in the risk assessment

Subject	Assessment assumption
Design maturity	The vessel is assessed at concept design level. General arrangement drawings and simplified system design are available, but detailed piping and instrumentation diagrams, cable schedules, equipment specifications, and reliability data are not available.
Reactor shutdown	The reactor is assumed to shutdown following a valid trip signal. Failure to trip is considered separately where relevant.
Passive heat removal	Passive HTGR decay heat removal capability is credited following the loss of active cooling, provided that the passive heat transfer path and ultimate heat sink remain available and are not impaired by the initiating event.
System boundaries	The primary helium, steam-water, and seawater circuits are treated as separate fluid systems. Leakage or rupture at an interface between these systems is assessed where it may result in loss of inventory, cross-system transfer, or release to the marine environment.
Electrical dependence	Pumps, active valves, ventilation equipment, instrumentation, and control systems are assumed to require electrical power unless a passive or fail safe function is specifically identified.
Marine environment	Normal ship motion, vibration, and seawater exposure are included in the design basis. Severe weather, collision, grounding, fire, and flooding are treated as initiating hazards.
Safeguard credit	A safeguard is credited in Iteration 1 only where it is shown in the baseline design, stated as part of the defined system function, or clearly identified as an existing operational control.

Passive reactor response does not remove the need for instrumentation, isolation, pressure control, confinement, electrical support, environmental monitoring, or long term heat rejection. These functions remain relevant even where the reactor core can tolerate a short term loss of forced circulation [30, 4].

6.4. Risk ranking method

Having defined the reference concept, system boundaries, and assessment assumptions, a method is required to rank the identified scenarios and compare the effect of safeguards. The HAZID therefore uses an ordinal Risk Index based on a Severity Index and a Frequency Index. The method follows the general structure of the IMO FSA approach and the qualitative risk assessment process discussed in Chapter 5 [36, 37, 41, 45].

6.4.1. Severity Index

The Severity Index ranges from S_1 to S_4 . The assessment considers potential consequences for human life and health and for the external environment. Each scenario is assessed against both consequence categories. Where the two categories result in different severity levels, the highest justified Severity Index is assigned. The categories used in the assessment are defined in Table 6.5.

Table 6.5: Definition of the Severity Index, adapted from [36].

SI	Severity	Human life and health	External environment
<i>S1</i>	Minor	Medical treatment required; absence from work between zero and three days.	Environmental recovery time between one day and one week.
<i>S2</i>	Significant	Medical treatment ashore required; absence from work of up to eight weeks.	Environmental recovery time between one week and one month.
<i>S3</i>	Severe	Major trauma, partial disability, or reduced ability to work for more than eight weeks.	Environmental recovery time between one month and one year.
<i>S4</i>	Catastrophic	Permanent disability or fatality.	Environmental recovery time greater than one year.

6.4.2. Frequency Index

The Frequency Index ranges from *F1* to *F7*. The categories are based on the IMO FSA frequency scale and are presented in Table 6.6 [36, 37].

Table 6.6: Definition of the Frequency Index [36].

FI	Frequency category	Definition	Frequency per ship-year
7	Frequent	Approximately once per month on one ship.	10
6	Frequent	Approximately once per year on one ship.	1
5	Reasonably probable	Approximately once per year in a fleet of ten ships.	10^{-1}
4	Reasonably probable	Approximately once per year in a fleet of one hundred ships.	10^{-2}
3	Remote	Approximately once per year in a fleet of one thousand ships.	10^{-3}
2	Remote	Approximately once per ten years in a fleet of one thousand ships.	10^{-4}
1	Extremely remote	Approximately once per twenty years in a fleet of five thousand ships.	10^{-5}

Validated component failure data are not available for the reference vessel. Thus, frequency assignments are comparative estimates based on the system configuration, expected equipment behavior, operating exposure, initiating causes, and engineering judgment.

The purpose of the assigned Frequency Index is to support consistent ranking and comparison between scenarios. The Frequency Index used in the HAZID is independent of the PPC classification introduced in Chapter 4. The PPC numbers represent regulatory plant condition classes, whereas F1-F7 provide an ordinal frequency scale for comparative scenario ranking.

6.4.3. Risk Index and risk categories

The Risk Index is calculated as

$$RI = FI + SI \quad (6.1)$$

where *RI* is the Risk Index, *FI* is the Frequency Index, and *SI* is the Severity Index.

The resulting risk categories are shown in Table 6.7 [36, 41].

The terms likelihood and frequency refer to the same horizontal dimension of the risk matrix (Figure A.3). The term Frequency Index is used in the HAZID tables because it is consistent with the adopted IMO scale [36].

6.4.4. Initial and residual risk

Two risk states are recorded during the first design iteration. Initial risk is assessed before crediting existing safeguards. Residual risk is assessed after the documented safeguards have been considered.

Table 6.7: Risk Index categories used in the HAZID

Risk Index	Risk category	Required treatment
2–4	Low	Broadly acceptable, subject to normal control and accepted engineering practice.
5–6	Medium	Tolerable only after safeguard review and ALARP-oriented assessment.
7–8	High	Additional risk reduction or design modification is required, followed by ALARP-oriented reassessment.
9–11	Extreme	Intolerable without major risk reduction.

The initial risk represents the credible escalation potential of the scenario without protective measures. This prevents effective safeguards from hiding the inherent hazard associated with the equipment, energy source, or process.

The residual risk represents the scenario after the existing safeguards have been applied. Any reduction in the residual Risk Index must be linked to a defined safeguard and is represented through a reduction in the Frequency Index of the stated consequence pathway.

6.4.5. Safeguard classification

Safeguards are classified as passive, active, or procedural. Passive safeguards perform their function through physical design, material properties, structural separation, pressure boundaries, or natural circulation. Active safeguards require detection, control logic, power, or mechanical actuation. Procedural safeguards depend on inspection, maintenance, operating instructions, emergency procedures, or crew action [28, 4, 54].

The classification is used to examine barrier diversity and independence. Several active barriers connected to the same switchboard do not provide the same degree of independence as a combination of passive, active, and procedural measures [51, 52].

6.4.6. DiD assignment

Each safeguard represented in the Bow-tie diagrams is assigned a DiD level (Table 5.1) according to its main function. A monitoring system that detects abnormal pressure normally supports Level 2. An isolation valve that limits a design basis leakage event may support Level 3. A filtered confinement discharge arrangement used to control a severe release may support Level 4. Emergency evacuation and off site consequence management support Level 5 [28, 4].

The same type of equipment may support different levels depending on its role, location, independence, and position in the accident sequence.

6.5. Design iteration and evaluation structure

Three design revisions are used to represent the development of the reference vessel: REV0, REVA, and REVB. These design revisions are separate from the initial and residual risk states defined in Section 6.4.4.

REV0 represents the initial concept and the starting point of the first design iteration. REVA represents the developed configuration after the first iteration safeguards are incorporated. The remaining weaknesses identified in the REVA assessment are then translated into design recommendations and implemented in REVB.

6.5.1. REV0: Initial concept

REV0 represents the initial vessel and nuclear island concept and provides the starting point for the first design iteration. The REV0 nuclear island and general arrangement drawings are provided in Figures

B.1 & B.2.

6.5.2. REVA: First design iteration configuration

REVA represents the vessel configuration resulting from the first design iteration. It incorporates the safeguards and arrangement features developed during this iteration and represents the resulting first iteration configuration.

The remaining safeguard limitations, barrier dependencies, insufficient segregation, and missing mitigation functions identified during the first iteration provide the basis for the design recommendations developed in Chapter 8.

6.5.3. REVB: Safety driven second iteration

REVB represents the second design iteration and incorporates the recommendations derived from the REVA assessment. These measures modify the vessel arrangement or supporting system design where the first iteration identified safeguard limitations, dependencies, or insufficient mitigation.

The HAZID scenarios affected by these changes are then reassessed, and the corresponding Bow-tie barriers are updated. This allows the effect of the design recommendations to be evaluated separately from the safeguards already present in REVA.

The REVB nuclear island and general arrangement drawings are provided in Figures B.5 & B.6.

6.5.4. Traceability between assessment and design

Traceability is maintained from the HAZID scenarios and Bow-tie findings to the corresponding design recommendations and revised risk rankings. Each recommendation can be linked to the safeguard limitation or escalation pathway that motivated it and to the design change implemented in REVB.

This structure allows the effect of the risk assessment on the vessel design to be followed explicitly from hazard identification through design modification and reassessment.

6.6. Chapter 6 Conclusion

A consistent concept level assessment basis was established by defining the reference vessel design, the system interfaces, the applicable safety objectives, and the assumptions and boundaries used throughout the study. The vessel was divided into functional assessment nodes so that both local failures and cross-system dependencies could be represented consistently within the HAZID. The separation between design revisions and risk states is also defined explicitly. REV0 represents the initial concept and starting point of the first design iteration, REVA represents the resulting first iteration configuration, and REVB represents the subsequent second design iteration. This assessment basis is applied in Chapter 7 through the HAZID and Bow-tie analyses.

This page is left blank intentionally.

7

Risk Assessment and First Design Iteration

How can a structured risk based methodology be applied to assess safety events and identify safeguard limitations?

This chapter applies the assessment basis established in Chapter 6 to the first design iteration of the reference vessel. A HAZID is used to identify and rank safety scenarios across the vessel, after which Bow-tie analysis examines selected accident pathways, barrier performance, and DiD in greater detail. The assessment is conducted at concept design level to identify safeguard limitations and the system or arrangement weaknesses requiring further development.

7.1. Application sequence for the first design iteration

The first design iteration assesses the REV0 vessel configuration established in Chapter 6 and results in the developed REVA configuration. For each HAZID scenario, initial risk is assessed before crediting safeguards, while residual risk is assessed after the first iteration safeguards are considered.

The HAZID results were then used as the input to the Bow-tie stage. Related scenarios were reviewed to identify recurring loss of control conditions to which several causes and consequences converged. Three representative top events were selected from this review. The associated causes, consequences, safeguards, and scenario references were then transferred into Bow-tie structures.

The Bow-tie analysis examined the position, function, and independence of the barriers associated with each selected top event. It was used to determine how the events could escalate, whether the available preventive and mitigative barriers provided sufficiently independent protection, and where weaknesses remained within the DiD structure. The resulting barrier and escalation path findings formed the technical input to the second design iteration developed in Chapter 8.

The applied sequence is summarized in Figure 7.1:

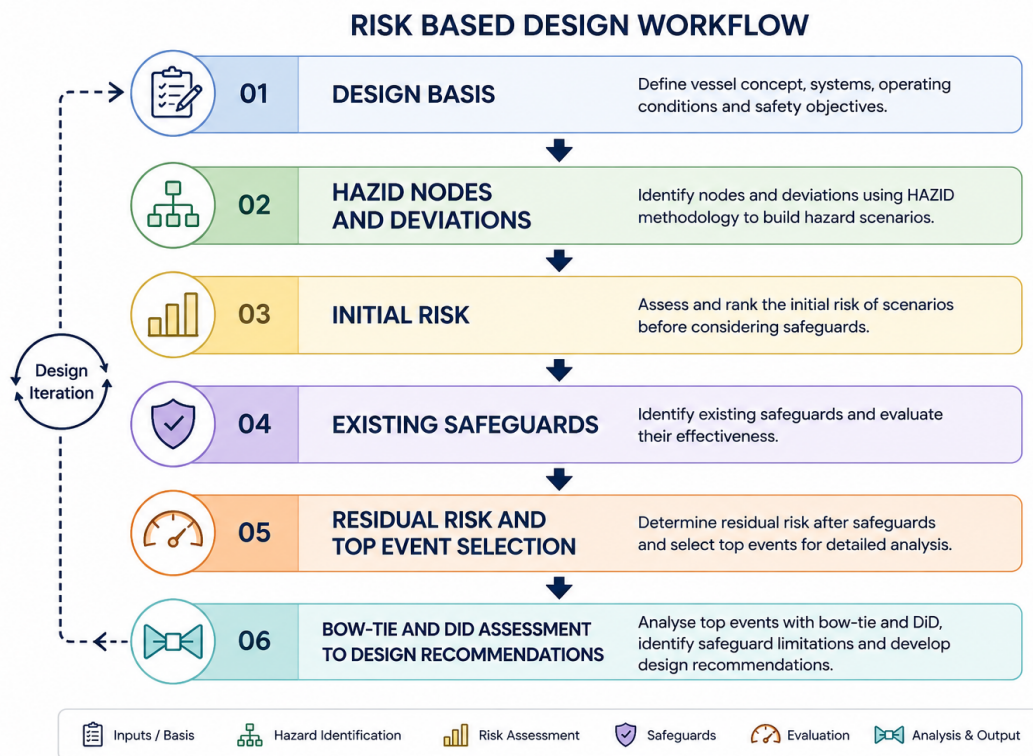


Figure 7.1: Applied risk based design workflow used in the first design iteration.

The two analytical methods therefore performed different but connected functions. The HAZID provided broad scenario coverage, comparative risk ranking, and the source information for the selected top events. The Bow-tie analysis used that information to examine accident progression and barrier performance in greater depth. The Bow-tie stage was a focused continuation of the HAZID, rather than a separate or independent assessment.

7.2. HAZID application

This section describes how the assessment basis established in Chapter 6 was converted into a structured HAZID register. The application proceeded from the definition of functional nodes and system boundaries to the selection of deviations, construction of scenarios, assignment of initial risk, assessment of existing safeguards, and processing of the resulting data. Together, these steps produced the broad scenario set and risk-ranking basis required for the subsequent Bow-tie analysis.

7.2.1. Node and boundary definition

The HAZID was divided into the five functional nodes defined in Section 6.3.2. These covered the nuclear compartment, turbine-generator room, seawater cooling room, electrical distribution and propulsion room, and ship operations and maritime hazards.

The node boundaries followed the main pressure, energy transfer, electrical, and structural interfaces of the reference design, as described in Sections 6.1 & 6.3.2. This allowed local failures and cross-system escalation to be treated within one register. For example, a steam generator tube failure is initiated at the boundary between the primary helium circuit and the steam-water circuit. Loss of seawater cooling begins in the heat rejection system but may lead to condenser failure, turbine trip, loss of generation, and reactor shutdown demand. Loss of electrical distribution may affect equipment in all machinery spaces. The boundaries were defined functionally rather than at component level, so that scenario construction could remain consistent with the concept stage assessment scope.

7.2.2. Guidewords and deviations

A consistent set of deviations was applied across the plant nodes. The deviations covered abnormal pressure, temperature, flow, inventory, structural integrity, electrical supply, control response, and contamination. Additional deviations were used for the ship operations node to cover collision, grounding, fire, flooding, severe weather, abnormal motion, and loss of maneuverability.

The use of common deviations across the machinery nodes allowed similar failures to be compared between systems. Loss of flow, for example, was examined in the primary helium circuit, steam-water circuit, seawater circuit, and supporting electrical systems. The physical causes and consequences differ between these systems, but the common deviation supports a systematic review.

The HAZID remained broader than a component level HAZOP. The analysis did not examine every valve, instrument, or pipe section separately. It focused on failures that could affect major system functions, safety boundaries, heat removal, electrical support, confinement, or vessel operation. This is consistent with the qualitative and concept stage emphasis adopted in Chapter 5, where HAZID is identified as an early hazard discovery tool rather than a component level operability study.

7.2.3. Scenario construction

Each HAZID scenario was constructed from a deviation, one or more initiating causes, the resulting consequences, and the applicable safeguards. Causes were written to identify a credible physical, mechanical, electrical, operational, or external initiating mechanism. Consequences were developed beyond the immediate local effect where further escalation was credible.

For example, loss of seawater flow was not limited to loss of pump performance. The consequence sequence also considered condenser pressure increase, turbine trip, loss of electrical generation, loss of propulsion, and reactor shutdown demand. Similarly, primary helium leakage was developed from pressure boundary failure through helium inventory loss, reactor compartment contamination, pressure effects, radiological exposure, and possible release management. These escalation paths reflect the representative accident scenarios and hazard categories established in Chapter 4.

Repeated causes and consequences were cross-referenced within the HAZID rather than rewritten in full for every related scenario. The cross-references maintained consistency between linked rows while avoiding multiple descriptions of the same escalation mechanism. Each cause, safeguard, and consequence retained a unique reference number for connection to the Bow-tie diagrams in Appendix D, ensuring traceability between the qualitative register and the barrier based analysis.

7.2.4. Initial risk assessment

Initial risk was assigned before crediting any safeguards. The Severity Index and Frequency Index defined in Section 6.4 were applied to each scenario, and the initial Risk Index was calculated using Equation 6.1. The index structure and frequency bands were adapted from the IMO FSA Guidelines and qualitative risk assessment guidance [36, 41], in line with the concept stage focus of the study.

The initial severity represented the credible consequence if the scenario progressed without effective prevention or mitigation. The initial frequency represented the estimated frequency of the initiating condition and progression before the listed safeguards were credited. These assignments were based on comparative engineering judgment rather than fully quantified probabilistic data, as recognized in Chapter 5.

The use of an unmitigated initial score was important because it preserved the distinction between the inherent hazard and the performance of the safeguards. A low residual risk could therefore be traced to effective risk reduction rather than interpreted as evidence that the initial hazard was minor. This approach is consistent with ALARP-oriented decision making, in which risk reduction measures are judged against the underlying hazard rather than the already mitigated risk picture.

7.2.5. Existing safeguard assessment

Existing safeguards were credited only where they were present in the initial design basis, stated as part of the defined reactor or ship system, or included as an explicit baseline assumption. These safeguards were incorporated within the first design iteration leading from REV0 to REVA. This follows the qualitative HAZID workflow recommended by the MTF, in which unmitigated consequences are

assessed before protective measures are considered [41]. Measures introduced during the second design iteration in Chapter 8 were not credited here, so that the effect of baseline safeguards and the effect of design recommendations remained distinguishable.

The safeguard review considered the function of each measure, its position in the accident pathway, and its dependence on other systems. Safeguards were credited by considering their effect on the frequency of the stated consequence pathway. The Severity Index assigned to the consequence was retained, since the consequence itself remained the same, safeguards instead reduced the estimated frequency with which that consequence would be reached.

Preventive safeguards reduce the frequency of progression toward the hazardous event, while mitigative safeguards reduce the frequency with which the top event progresses to the stated consequence. This distinction allows preventive and mitigative functions to be represented consistently without changing the defined severity of the consequence.

A listed safeguard did not automatically result in a lower residual risk score. A reduction in the Frequency Index was assigned only where the safeguard provided a credible preventive or mitigative function within the scenario pathway. Safeguards that improved detection, monitoring, or recovery but did not provide sufficient justification for a change in the ordinal frequency score were recorded without changing the residual Risk Index.

The safeguards were also classified as passive, active, or procedural. This classification supported the later assessment of diversity and independence, in line with DiD principles and barrier based Bow-tie analysis. Several active safeguards supplied by the same switchboard, located in the same compartment, or dependent on the same detection system were not treated as fully independent barriers, since a single initiating event could impair multiple provisions simultaneously. This aligns with common cause failure guidance and the DiD requirement that different levels should remain sufficiently independent.

7.2.6. Data processing and visualization

The HAZID register was developed in OpenPHA software and exported for post processing. The exported data were processed to generate risk matrices, scenario summaries, and comparison dashboards for the initial and residual risk states.

The processing method retained the original HAZID scenario references. Cross-referenced causes and consequences were resolved for reporting, while the original links remained available for traceability. Scenario rows were counted once in the global risk summary, including where a cause or consequence referred to another HAZID entry.

The resulting outputs included the full risk matrix before safeguards, the full risk matrix after existing safeguards, and separate summaries for scenarios later affected by design recommendations. The full HAZID register and detailed outputs are provided in Appendix C, which forms the primary traceability record for the first iteration assessment.

7.3. First iteration HAZID results

The HAZID application produced a wide risk picture covering the five functional assessment nodes. The results are presented in three stages. First, the initial distribution shows the credible risk before safeguards are credited. Second, the residual distribution shows the effect of the existing safeguards represented in REVA. Finally, the combined results are interpreted to identify the system interfaces and escalation events requiring more detailed pathway analysis.

7.3.1. Initial risk picture

The completed HAZID contained 95 scenario rows across the five assessment nodes. No scenario fell within the Extreme-risk category (RI 9–11). Eleven scenarios were classified as High, 65 as Medium, and 19 as Low, as summarized in Table 7.1.

The initial distribution contained 76 Medium- or High-risk scenarios, all of which required review of the available safeguards and associated accident pathways.

The High-risk group included scenarios associated with primary pressure boundary failure, inter-loop

Table 7.1: Initial HAZID risk distribution before existing safeguards.

Result	Initial condition
Number of scenario rows	95
Extreme-risk scenarios	0
High-risk scenarios	11
Medium-risk scenarios	65
Low-risk scenarios	19

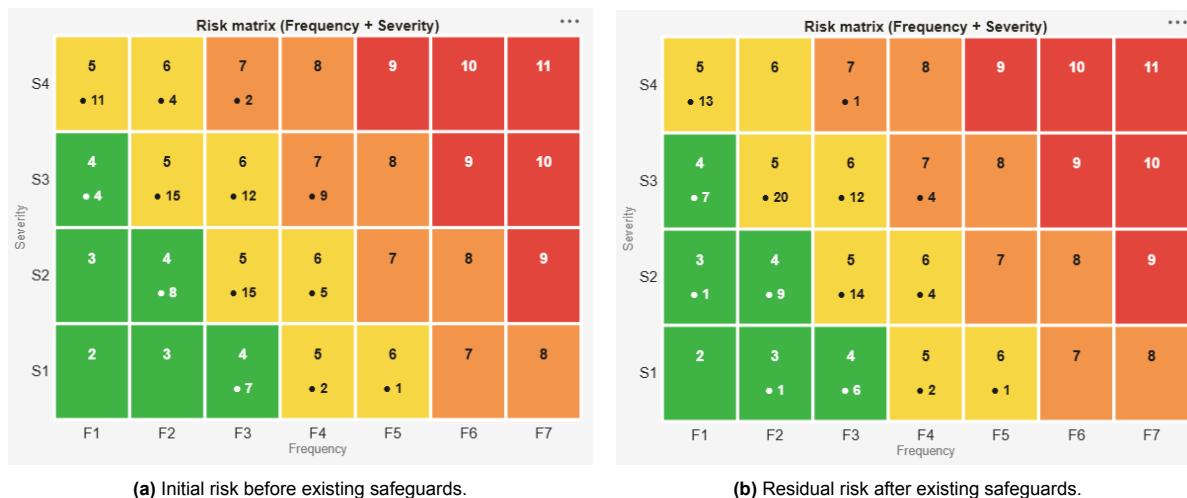
leakage, loss of heat rejection, loss of electrical support, and failures capable of producing several linked consequences. Their importance was determined by the combination of their risk ranking and their ability to affect multiple safety functions, in line with the DiD interpretation adopted in Chapter 5.

7.3.2. Risk picture after existing safeguards

After the existing safeguards were credited, the number of High-risk scenarios decreased from 11 to five, while the number of Low-risk scenarios increased from 19 to 24. The number of Medium-risk scenarios changed from 65 to 66 because several High-risk scenarios moved into the Medium category while a smaller number of Medium-risk scenarios moved into the Low category.

The dataset contained explicit after-safeguard scores for 29 scenario rows. Of these, 18 received a lower Risk Index and 11 retained their initial score. The remaining 66 rows retained their initial values because no complete after safeguard Frequency and Severity score was assigned.

Figure 7.2 compares the global risk distribution before and after crediting the existing safeguards. The reduction from 11 to five High-risk scenarios shows that the existing safeguards provide meaningful risk reduction. However, Medium risk remains the dominant category and five High-risk scenarios remain, indicating the need for further examination of the associated escalation pathways and barrier structure.

**Figure 7.2:** Global HAZID risk distribution before and after crediting the existing safeguards.

The residual distribution therefore supports two conclusions. First, existing safeguards provide risk reduction and should be retained in the design basis. Second, the global risk matrix does not show whether the remaining risk is caused by missing barriers, dependent barriers, inadequate mitigation, or weak recovery arrangements. Detailed pathway analysis using the Bow-tie structures in Appendix D was required to answer this question.

7.3.3. Interpretation of the HAZID results

The residual HAZID did not identify one isolated component as the dominant safety concern. Instead, the higher-risk and interconnected scenarios showed that the main vulnerabilities were associated with loss of important system boundaries between separate ship systems.

Three recurring escalation mechanisms were significant. The first concerns loss of primary helium circuit pressure boundary integrity. The associated HAZID entries include primary helium leakage and pressure loss, reduced helium inventory affecting core cooling, radiological exposure, and loss of propulsion. For example, scenario 1.2.1.2 was initially ranked at RI 5 and reduced to RI 4 after existing safeguards, while the loss of propulsion pathway in 1.2.1.8 remained at RI 6. These results show that loss of the primary pressure boundary can develop beyond a local pipe or component failure and affect cooling, confinement, personnel protection, and vessel operation.

The second concerns loss of steam generator tube integrity. The relevant scenarios cover both primary helium transfer into the steam-water circuit and reverse water or steam ingress into the primary helium circuit. The latter sequence included moisture ingress and graphite oxidation, corrosion or oxidation of reactor materials, combustible gas accumulation, and fire or overpressure. In particular, scenario 1.2.3.2 had an initial RI of 7 before being reduced to RI 4 by the existing safeguards. The steam generator therefore represents an important interface through which pressure, fluid, and potentially radioactive contamination may propagate between the nuclear and conventional sides of the plant.

The third concerns loss of ship service electrical power. This pathway was represented by several linked scenarios covering main switchboard failure, turbine generator trip, electrical room fire and flooding, loss of maneuverability, loss of reactor control and shutdown support, and loss of safe reactor recovery capability. Several of these scenarios had initial Risk Indices of 7 and remained at RI 5-6 after existing safeguards. Unlike the first two events, this is not a loss of a physical fluid boundary. Its significance arises from the number of systems that depend on electrical distribution, so that a single electrical failure can simultaneously affect propulsion, monitoring, control, cooling support, isolation, and recovery functions.

These three mechanisms therefore represent different but complementary challenges, loss of a primary nuclear boundary, loss of an interface between nuclear and conventional systems, and loss of a shared supporting function. Their selection for detailed Bow-tie analysis was based on the combination of risk ranking, recurring or linked HAZID scenarios, potential accident escalation, and the number of safety functions affected, rather than on Risk Index alone.

7.4. Selection of representative top events for Bow-tie analysis

The HAZID provides a broad comparison of individual scenarios, but the risk ranking alone does not show how several initiating causes may converge on the same loss-of-control event or how that event may subsequently develop through multiple consequence pathways. Bow-tie analysis was therefore used to examine the three recurring escalation mechanisms identified in Section 7.3.3.

The selected top events were required to represent a recurring HAZID finding, affect one or more safety-significant functions, involve meaningful accident escalation, and provide a useful basis for examining barrier performance and ship design implications. The resulting three top events are summarized in Table 7.2.

Taken together, the selected top events represent three complementary forms of vulnerability within the reference vessel. Loss of primary helium circuit pressure boundary integrity represents failure of a nuclear side pressure and confinement boundary. Loss of steam generator tube integrity represents pressure and contamination transfer across the interface between the primary helium circuit and the steam-water power conversion system. Loss of ship service electrical power represents failure of a shared supporting function required by several preventive, mitigative, monitoring, and recovery systems.

7.5. Bow-tie construction and assessment

Following selection of the three representative top events, the corresponding HAZID information was reorganized into Bow-tie structures. The purpose was to move beyond ordinal risk ranking and examine how each event could escalate and which barriers interrupt the sequence. The following subsections define the diagram structure, explain the traceability to the HAZID, classify the represented barriers, and describe how their contribution to DiD was assessed.

Table 7.2: Top events selected for Bow-tie analysis

Top event	Safety theme	Selection basis
Loss of primary helium circuit pressure boundary integrity	Primary confinement	Selected because multiple initiating scenarios in the HAZID converge on the same loss of integrity event. It represents helium inventory loss, degradation of the primary pressure boundary, reactor compartment contamination, and the need for controlled release management.
Loss of steam generator tube integrity	Inter-loop transfer	Selected because it was identified as the most severe of the examined top events in terms of credible consequence development. It represents pressure and contamination transfer between the primary helium circuit and the steam-water power conversion circuit.
Loss of ship service electrical power	Supporting system dependency	Selected because it was associated with the largest number of related entries in the HAZID register. It represents the dependence of propulsion, monitoring, control, cooling, ventilation, isolation, and recovery functions on electrical distribution.

7.5.1. Bow-tie structure

Each Bow-tie was developed from the corresponding HAZID entries. The top event was placed at the center of the diagram. Initiating causes were positioned on the left, and consequences were positioned on the right.

Preventive barriers were placed between each initiating cause and the top event. Mitigative barriers were placed between the top event and the associated consequences. Where an event developed through several intermediate consequences, the barriers were placed at the relevant stage of the escalation sequence rather than grouped at the beginning or end of the branch.

The diagrams represent accident progression pathways. The purpose was to show how an event could continue if the applicable barriers failed or were unavailable.

Figure 7.3 provides a representative example of the simplified Bow-tie structure. It shows how the initiating causes identified in the HAZID converge on a selected top event and how the event may subsequently develop into different consequence pathways. The complete Bow-ties, including the individual safeguards, HAZID references, risk information, barrier classifications, and DiD assignments, are provided in Appendix D.

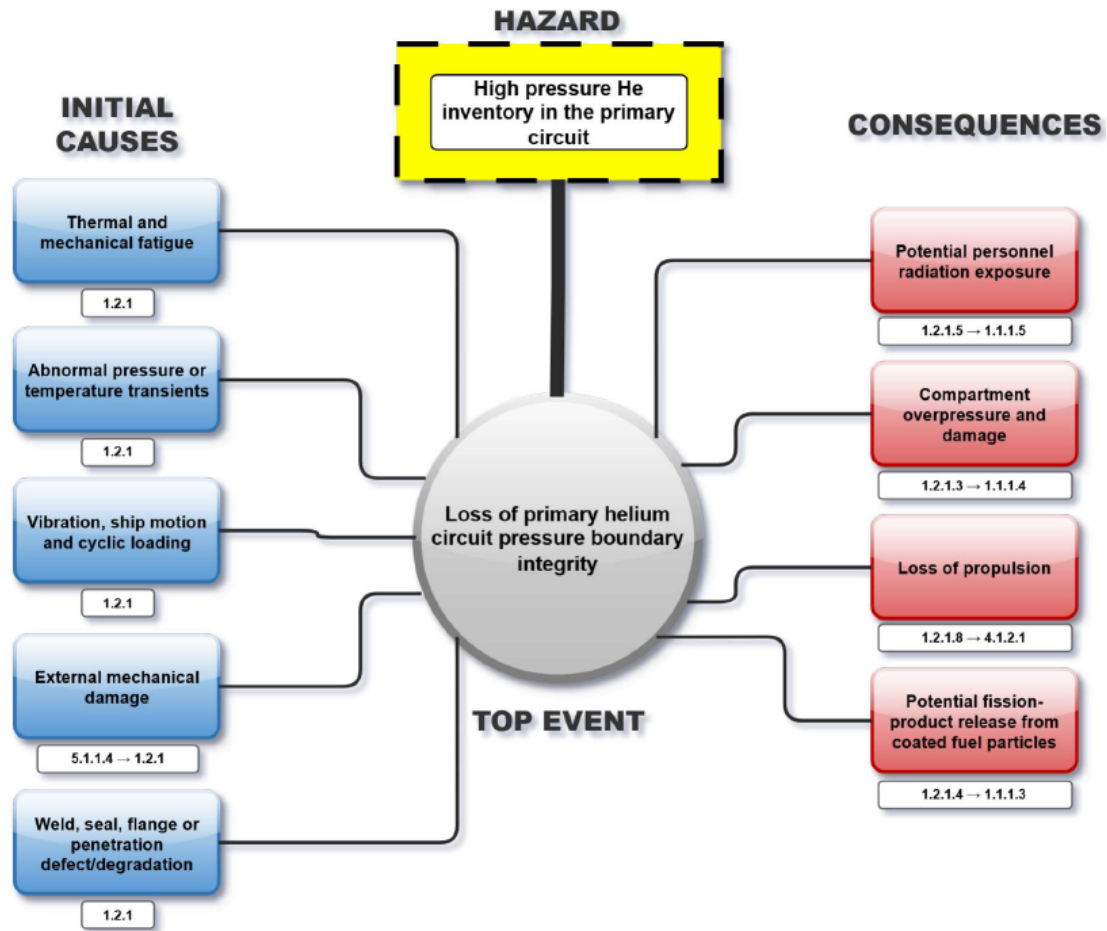


Figure 7.3: Simplified first iteration Bow-tie for loss of primary helium circuit pressure boundary integrity, showing the principal initiating causes and consequence pathways derived from the HAZID.

7.5.2. HAZID traceability

Causes, consequences, and safeguards in the Bow-ties were linked to their HAZID reference numbers. The reference structure allowed each branch to be traced back to the source scenario and risk ranking.

Where several HAZID scenarios represented the same physical barrier function, their safeguard references were grouped at the same barrier position. Where one consequence continued into another HAZID scenario, the corresponding reference was shown as a linked progression.

The extended Bow-ties retained the complete cause, consequence, safeguard, risk, and DiD information. Simplified Bow-ties were also produced for communication purposes. The extended diagrams formed the analytical basis of the study, as documented in Appendix D.

7.5.3. Barrier classification

Two complementary classifications are used for the barriers represented in the Bow-ties. The first describes how a barrier performs its function: passive, active, or procedural. The second describes its position in the accident pathway: preventive or mitigative.

Passive barriers perform their function through inherent physical characteristics or fixed design features without requiring powered actuation or crew action. Examples include structural separation, shielding, pressure boundaries, and passive heat-removal characteristics.

Active barriers require detection, control logic, electrical power, or mechanical actuation to perform

their intended function. Examples include automatic isolation valves, protection systems, powered ventilation isolation, emergency generators, and monitoring systems.

Procedural barriers depend primarily on human or organizational action. Examples include inspection and maintenance, operating limits, abnormal operating procedures, and emergency response actions.

Preventive barriers act before the top event and reduce the frequency with which it is reached, whereas mitigative barriers act after the top event and reduce the frequency with which the event progresses to a stated consequence. A barrier may therefore be, for example, both active and preventive or passive and mitigative.

7.5.4. DiD assessment

Each barrier was assigned a DiD level according to its function in the accident pathway. The assessment examined whether each branch contained sufficient prevention, detection, accident control, severe condition mitigation, and emergency response provisions. [28, 4]

The DiD review did not assume that the presence of barriers from several levels automatically provided adequate protection. Barrier independence and common dependencies were also considered. A detection system, automatic isolation valve, and powered ventilation damper may appear as three separate barriers but remain vulnerable to one loss of electrical supply.

The Bow-tie review showed that DiD Levels 1-3 were generally represented through equipment design, inspection, monitoring, reactor protection, isolation, and pressure-relief functions.

Level 4 was represented less consistently. In this study, Level 4 refers to the control of severe plant conditions, including measures intended to prevent further accident progression and to mitigate the consequences of a severe accident after the principal design basis protection has been challenged. Typical Level 4 functions may therefore include controlled confinement, dedicated release management, severe-condition isolation, and other complementary mitigation measures.

Several first-iteration pathways lacked such explicitly defined mitigation and instead relied mainly on the preceding Levels 1-3 or on general emergency response provisions.

7.6. Bow-tie results and escalation path analysis

The following sections present the three selected Bow-ties and examine the principal escalation pathways, existing barriers, and safeguard limitations identified during the first design iteration.

7.6.1. Loss of primary helium circuit pressure boundary integrity

The first Bow-tie examines loss of primary helium circuit pressure boundary integrity. The primary helium circuit is the main pressure retaining boundary of the reactor coolant system, and its failure may therefore lead directly to loss of coolant inventory, degradation of core cooling conditions, and release of potentially contaminated helium into the nuclear compartment.

Credible initiating causes include material fatigue, pressure or temperature transients, vibration, ship motion loading, mechanical impact, weld degradation, seal failure, and manufacturing defects. Preventive barriers include pressure boundary design margins, qualified materials, inspection and maintenance, operating limits, pressure monitoring, leak detection, and vibration monitoring. These measures reduce the probability of boundary failure but do not eliminate the need to manage the release once integrity has been lost.

The representative Bow-tie introduced in Figure 7.3 corresponds to this top event. The detailed version in Appendix D contains the individual safeguards and HAZID references used for the assessment.

Following the top event, helium may leak into the nuclear compartment. The immediate response depends on the size and location of the failure. A small leak may first be detected through pressure, inventory, radiation, or gas monitoring systems, whereas a larger rupture may cause rapid depressurization, loss of forced helium circulation, and an increase in reactor compartment pressure.

Because the released helium may contain radioactive contamination from the primary circuit, the event may escalate from a coolant inventory loss scenario to a confinement and radiological control event.

Further consequences may include reactor trip, loss of electrical generation and propulsion, increased radiation levels, compartment overpressure, personnel exposure, and potential release from the vessel if confinement is not maintained [20, 30, 50].

Existing mitigative functions include reactor shutdown, isolation of the affected circuit where possible, pressure relief, passive decay heat removal characteristics, ventilation isolation, radiological monitoring, emergency electrical supply, and emergency procedures [13, 24, 4].

The detailed Bow-tie in Figure D.1 shows that the preventive side of the top event contains several defined measures, including pressure boundary design, inspection and maintenance, operating limits, pressure monitoring, leak detection, and vibration monitoring. On the consequence side, the available measures rely mainly on reactor shutdown, isolation, compartment confinement, radiological monitoring, pressure relief, and emergency response.

The main residual weakness was therefore associated with management of the released helium inventory after loss of pressure boundary integrity. In particular, the first iteration design did not define a dedicated route for the controlled handling, monitoring, treatment, and discharge of potentially contaminated helium or relief flow. This gap provided the basis for the release-management recommendation introduced in the second design iteration.

7.6.2. Loss of steam generator tube integrity

The second Bow-tie examines the loss of steam generator tube integrity. The steam generator forms the pressure and contamination boundary between the primary helium circuit and the steam and water circuit. Failure of this boundary may therefore affect both the nuclear heat transfer system and the conventional power conversion plant.

Credible initiating causes include thermal fatigue, differential thermal expansion, corrosion or erosion, vibration, pressure cycling, material defects, weld degradation, manufacturing or installation defects, and loading associated with ship motion. Preventive barriers include qualified materials and design margins, manufacturing quality control, inspection and non destructive testing, pressure and temperature monitoring, leak detection, maintenance, operating limits, and secondary side isolation capability [13, 24].

The principal threats, preventive barriers, top event, mitigative barriers, and consequence groups identified during the first design iteration are summarized in Figure 7.4.

Following loss of tube integrity, the direction of inter-loop transfer depends on the local pressure conditions. Primary helium may enter the steam and water circuit, while water or steam may enter the primary helium circuit under a reversed pressure differential. The top event therefore creates an inter-loop transfer pathway rather than a failure confined to one system or compartment.

Helium transfer to the secondary circuit may contaminate downstream equipment, increase radiation levels, and create pressure control and discharge management requirements. Water or steam ingress into the primary helium circuit may degrade heat transfer, alter primary system pressure, challenge reactor operation, and require reactor shutdown and isolation of the affected steam generator.

The existing mitigative barriers include leak and pressure differential detection, automatic reactor trip, primary and secondary side isolation, pressure relief, feedwater isolation and level control, shutdown of the power conversion system, passive reactor heat removal, ventilation and isolation procedures [24, 30].

The detailed Bow-tie in Figure D.2 shows that several barriers are available to detect and isolate a steam generator tube failure, including leak and pressure differential detection, reactor trip, primary and secondary isolation, pressure relief, and feedwater isolation. However, these measures do not by themselves control the subsequent handling of a mixed helium and steam inventory once inter-loop transfer has occurred.

The principal residual issue was therefore the management of this inventory after the confinement had failed. Potentially contaminated helium or steam must be depressurized, confined, monitored, and routed to a controlled location. A pressure relief function alone is not a radiological barrier where contamination of the relieved inventory is credible. The discharge destination, isolation capability, monitor-

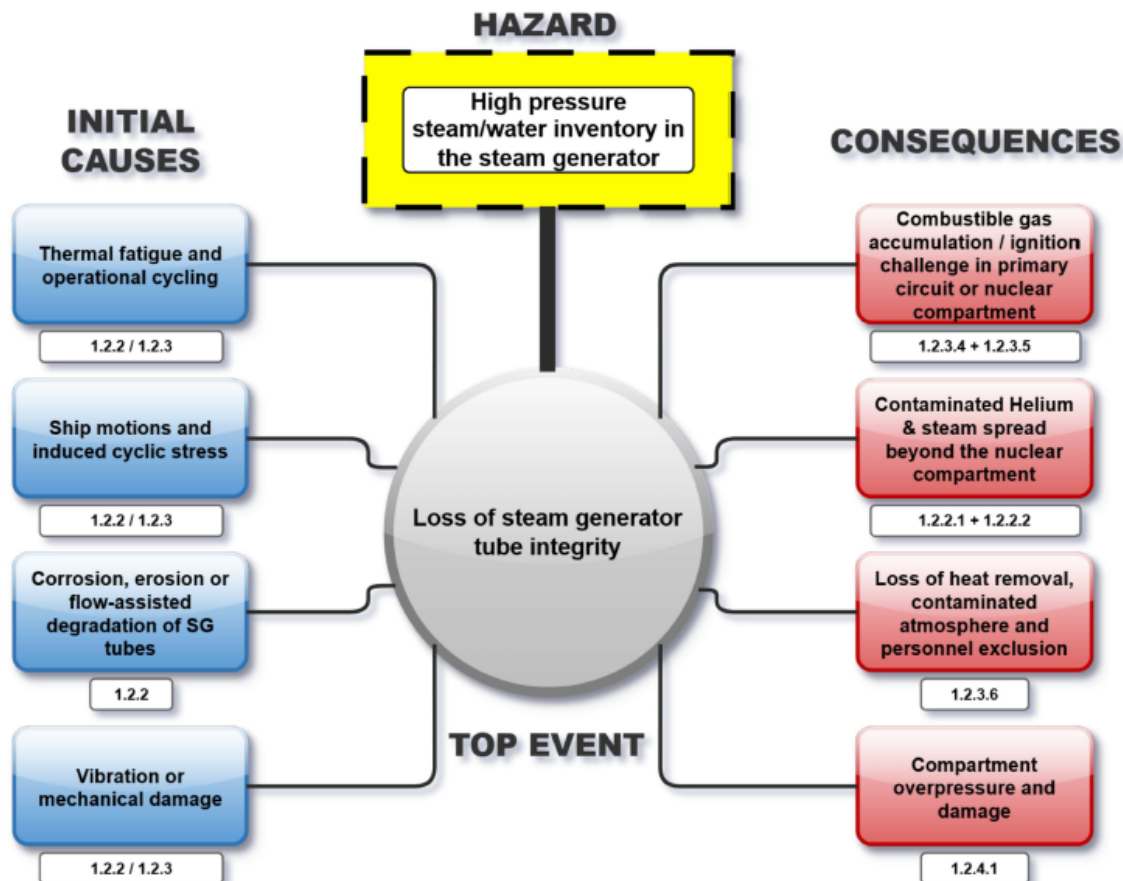


Figure 7.4: Simplified first iteration Bow-tie for loss of steam generator tube integrity, showing the principal initiating causes and consequence pathways derived from the HAZID.

ing arrangement, and treatment of the released inventory must therefore form part of the overall safety function.

The analysis also identified a downstream relationship with the turbine and condenser. Loss of condenser performance or an increase in turbine side back pressure may further challenge the steam and water circuit when the normal heat rejection pathway is unavailable. Pressure protection must therefore remain effective independently of normal condenser operation.

Several barriers in this pathway depend on electrical power, instrumentation, control, and actuation. A common loss of these supporting functions could simultaneously disable detection, isolation, pressure control, ventilation, and monitoring. The third Bow-tie consequently examines loss of ship service electrical power as a shared dependency across multiple safety functions.

7.6.3. Loss of ship service electrical power

The third Bow-tie examines loss of ship service electrical power. Unlike the two pressure boundary events, electrical power is a shared supporting function required by multiple preventive and mitigative systems. Its loss may therefore affect several nuclear and ship safety functions simultaneously.

Credible initiating causes include turbine generator trip, generator fault, main switchboard fault, cable damage, protection system failure, electrical room fire, electrical room flooding, and loss of a supporting cooling or control service. Preventive measures include generator and switchboard protection, equipment maintenance, operating limits, fault detection, automatic bus transfer, cable protection, fire detection, and flood protection.

These measures reduce the likelihood of a complete loss of electrical distribution. Their effectiveness may nevertheless be limited where normal and emergency distribution functions share a switchboard, compartment, or supporting service.

The principal threats, preventive barriers, top event, mitigative barriers, and consequence groups identified during the first design iteration are summarized in Figure 7.5.

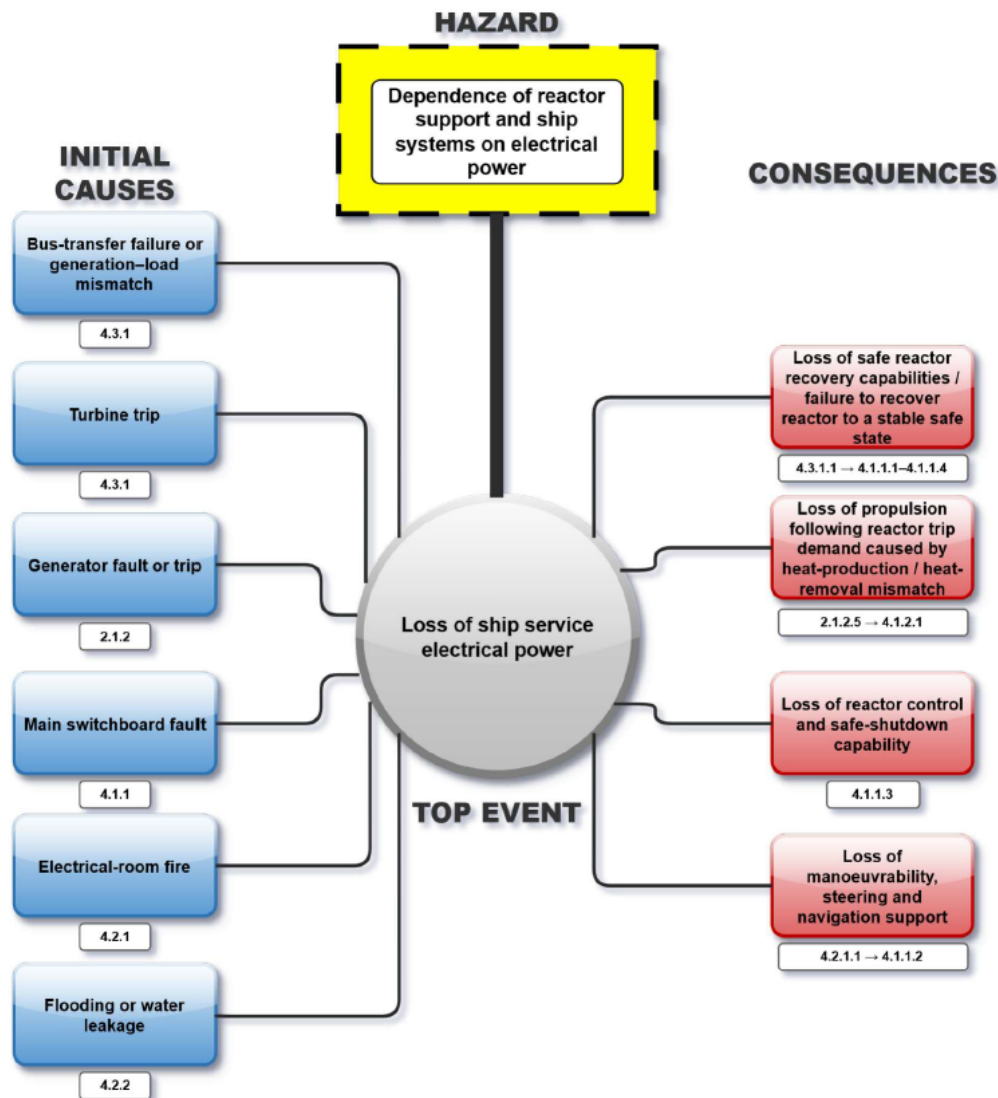


Figure 7.5: Simplified first iteration Bow-tie for loss of ship service electrical power, showing the principal initiating causes and consequence pathways derived from the HAZID.

Following the top event, propulsion and maneuvering capability may be lost. Pumps, ventilation fans, monitoring equipment, control systems, communications, lighting, and electrically actuated valves may also become unavailable. Loss of ship service power may therefore affect both safe vessel operation and the ability to monitor, shut down, isolate, cool, and recover the nuclear plant [20, 50].

Battery backed direct current supplies provide immediate, short duration power for reactor protection, essential instrumentation and control, and selected actuation functions. The emergency diesel generator provides longer duration support following successful start, connection, and transfer of the required loads. Emergency procedures support load shedding, blackout response, restoration, and control of the vessel during the recovery period [43, 55].

The detailed Bow-tie in Figure D.3 shows that the response to loss of ship service power relies on

battery backed supplies, emergency generation, transfer functions, and the distribution paths connecting these sources to the required loads. The presence of an emergency generator therefore does not by itself provide an independent barrier if the normal and emergency supplies share a switchboard, compartment, cable route, or control function.

This dependency was the principal residual weakness identified in the electrical power pathway. A main switchboard fault, fire, or flooding event could remove the normal electrical supply while also preventing the emergency source from reaching the required loads. Greater physical and functional segregation of the normal and emergency distribution paths was therefore required to preserve reactor shutdown, monitoring, isolation, cooling, communication, and recovery functions following a switchboard or compartment level event.

The first iteration assessment therefore indicated a need for greater physical and functional segregation of the normal and emergency electrical distribution paths. A protected emergency distribution function is required to preserve reactor shutdown, monitoring, isolation, cooling, communication, and recovery loads following a switchboard level or compartment level event.

7.6.4. Cross-cutting barrier findings

Although the three Bow-ties represent different top events, they produced several common findings. These are summarized in Table 7.3.

Table 7.3: Main findings from the first iteration Bow-tie assessment

Finding	Technical issue	Design implication
Shared supporting services	Several active barriers depend on common electrical distribution, control, ventilation, or cooling functions.	Redundancy must include physical and functional segregation.
Incomplete release handling	Pressure relief may control equipment pressure without controlling contamination spread or discharge location.	Relief paths require confinement, monitoring, isolation, and controlled routing.
Heat rejection dependency	Loss of seawater cooling can affect the condenser, turbine-generator, electrical generation, and plant recovery.	Heat rejection functions require redundancy and separation.
Weak Level 4 mitigation	Several branches rely on general emergency response after engineered isolation or relief barriers are challenged.	Additional severe condition mitigation should be defined in the ship design.
Environmental interface	Seawater discharge creates a potential route from machinery systems to the external environment.	Abnormal discharge conditions require detection and isolation.

The Bow-ties also showed that a barrier may perform its local equipment function without fully controlling the wider accident sequence. A relief valve can protect a pipe from overpressure while transferring the hazard to another compartment or discharge point. An emergency generator can produce power while the required distribution path remains unavailable. A duplicated pump can provide redundancy while both units remain vulnerable to the same flooding event.

This pathway level interpretation is the principal analytical contribution of the Bow-tie stage. It shows that the presence of individual safeguards is not sufficient where their supporting services, physical location, discharge route, or response function leave the wider escalation sequence uncontrolled. The resulting cross-cutting weaknesses form the basis of the first iteration findings summarized in Section 7.7.

7.7. Synthesis of first iteration findings

The first design iteration produced two complementary forms of evidence. The HAZID established the broad risk picture across the five functional nodes and showed the effect of the safeguards represented in REVA. The Bow-tie analysis then examined selected pathways in greater detail and identified

escalation mechanisms and barrier limitations that were not visible from the risk rankings alone.

At the global level, the reduction in the number of High-risk scenarios and the movement of scenarios towards lower risk categories demonstrate that the existing safeguards provide meaningful risk reduction. However, the residual distribution remained dominated by Medium-risk scenarios, while five scenarios remained within the High-risk category. The first iteration therefore showed that the presence of safeguards and a reduction in the overall risk distribution did not, by themselves, demonstrate that the complete accident pathways were adequately controlled.

At pathway level, the Bow-tie assessment showed that the principal weaknesses were associated with the independence, physical arrangement, and wider function of the barriers rather than only with their number. As summarized in Table 7.3, the recurring issues concerned shared supporting services, incomplete handling of potentially contaminated relief flow, dependence on the seawater heat rejection path, limited representation of DiD Level 4 mitigation, and insufficient monitoring and isolation at the seawater discharge interface.

The combined findings therefore indicate that the principal opportunities for further risk reduction lie in the vessel and system design. Redundant equipment must be supported by sufficiently segregated compartments, distribution paths, and supporting services. Pressure relief functions must control not only equipment pressure but also the subsequent location and handling of released inventory. Heat rejection and electrical support functions must remain available following local compartment or distribution failures. Additional mitigation must also be provided where preventive and design basis accident control barriers have already been challenged. These findings form the technical basis for the second design iteration.

7.8. Implementation of the first design iteration

The findings and safeguards identified during the first design iteration were incorporated into the reference vessel to develop the REVA configuration from the initial REV0 concept. The resulting changes are visible in the nuclear island arrangement, where the relevant safety functions and safeguards are represented explicitly.

Figures 7.6 & 7.7 compare the REV0 and REVA nuclear island and general arrangements, and illustrate the development introduced during the first design iteration. Full size drawings of the individual design revisions are provided in Appendix B.

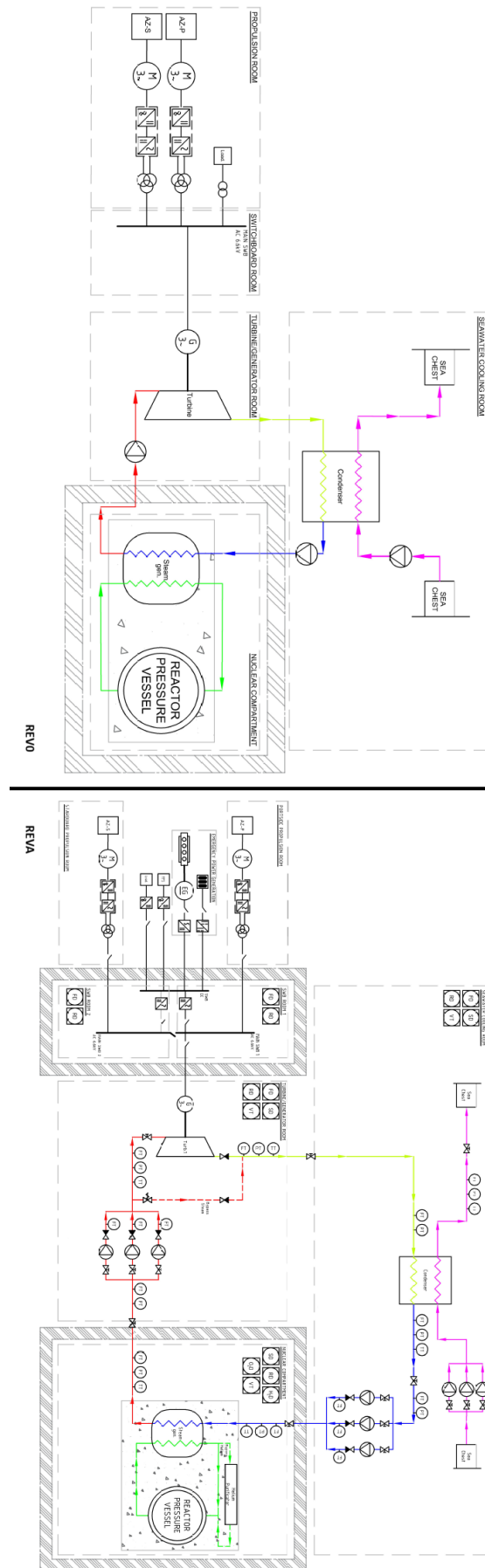


Figure 7.6: Comparison of the REV0 and REVA nuclear island arrangements.

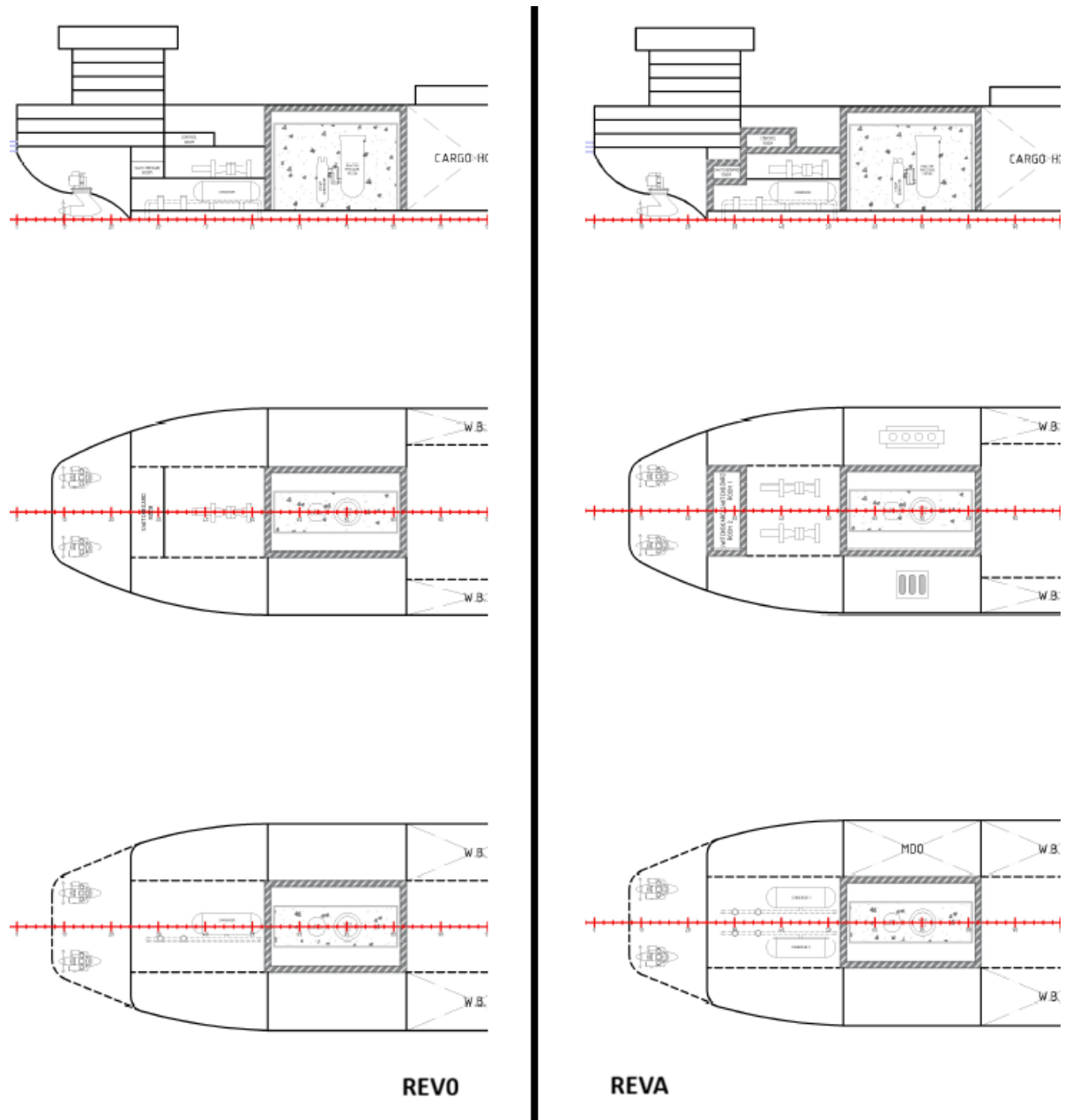
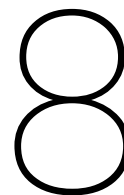


Figure 7.7: Comparison of the REV0 and REVA general arrangements.

7.9. Chapter 7 Conclusion

A structured risk based methodology can assess concept level safety events by combining the broad scenario coverage and comparative risk ranking of HAZID with the pathway and barrier analysis provided by Bow-ties. Applied to the reference vessel, the HAZID showed that the existing safeguards reduced the overall risk picture but left residual Medium- and High-risk scenarios requiring further examination. The Bow-tie analysis then revealed that the limitations concerned barrier dependence, insufficient segregation, incomplete control of potentially contaminated releases, vulnerability of supporting electrical and heat rejection functions, and limited DiD Level 4 mitigation. These findings provide the assessment basis from which Chapter 8 develops and evaluates the corresponding design recommendations.



Design Recommendations and Second Design Iteration

What design and safety recommendations follow from the risk assessment of the selected safety events?

This chapter translates the safeguard limitations and escalation path findings identified in Chapter 7 into concept level design recommendations. The recommendations are implemented in REVB, linked to the affected HAZID scenarios and Bow-tie branches, and evaluated through risk reassessment and their contribution to DiD. The objective is to determine how the identified weaknesses can be addressed through changes to the vessel arrangement, system design, and operating philosophy.

8.1. Translation of assessment findings into design recommendations

Section 6.5 defined the roles of REV0, REVA, and REVB within the overall design iteration structure. The purpose of the present section is not to redefine those design states, but to explain how the findings from the first iteration assessment were translated into the design recommendations implemented in REVB.

The recommendation development process began with the residual risk and Bow-tie findings presented in Chapter 7. The risk matrix identified the scenarios requiring further review, while the Bow-tie analysis showed how the associated events could progress from initiating causes, through the selected top events, to intermediate and final consequences. This provided the basis for identifying where additional preventive or mitigative functions were required and where those functions should act within the accident pathway.

A recommendation was developed where the escalation path review identified one or more of the following conditions:

- dependence on a single system train;
- several barriers dependent on the same supporting service;
- functional redundancy without sufficient physical or functional segregation;
- uncontrolled transfer of pressure or potentially contaminated inventory;
- incomplete representation of DiD Level 4 mitigation;
- an external discharge pathway without sufficient monitoring and isolation; or
- potential personnel exposure during abnormal nuclear compartment conditions or necessary intervention.

As defined in Section 6.5, the design recommendations are treated separately from the safeguards already present in REVA. They are introduced only in REVB so that their contribution can be evaluated independently during the second design iteration.

Figure 8.1 shows how the first iteration findings are converted into design changes and subsequently reassessed. Residual HAZID results and Bow-tie findings are first reviewed to identify a specific safeguard or design weakness. A corresponding design recommendation is then defined and implemented in REVB. The recommendation is linked only to the HAZID scenarios and Bow-tie branches that it directly affects, after which those scenarios are reassessed and the resulting change in risk and DiD is evaluated.

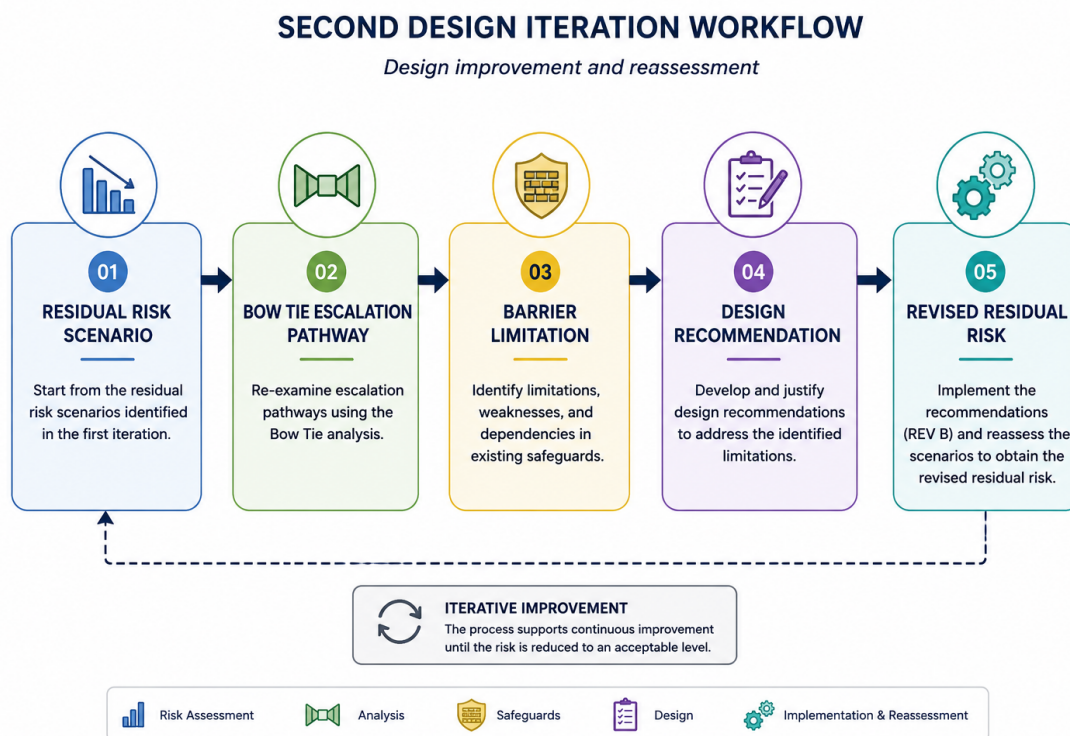


Figure 8.1: Second iteration workflow showing how first iteration findings are translated into REVB design changes and reassessed.

The purpose of this sequence is to preserve traceability. Each REVB modification must originate from an identified first iteration weakness and its assessed effect must be limited to the scenarios that the modification can credibly influence.

The design changes were assessed according to their intended safety function rather than only their physical form. For example, a pressure relief valve is not sufficient as a complete recommendation if it only protects equipment from overpressure while transferring contaminated fluid to an uncontrolled location. The associated pipe routing, collection volume, monitoring, isolation, and final discharge arrangement also form part of the barrier function.

The same principle applies to personnel protection within the nuclear compartment. Designating the compartment as normally unmanned does not prevent a pressure boundary failure, control the quantity of released material, or replace engineered confinement and isolation. The operating philosophy must be supported by remote monitoring and control, authorization controlled access, and defined arrangements for necessary manned intervention.

The second iteration does not treat the recommendations as isolated equipment additions. Each recommendation is defined as a safety function comprising the necessary equipment, physical arrangement,

supporting services, monitoring, control, and discharge or recovery path. Section 8.2 summarizes the resulting recommendations before the following sections explain their design logic.

8.2. Design recommendations

The six recommendations and their relationship to the first iteration findings are summarized in Table 8.1.

Table 8.1: Design recommendations derived from the first iteration assessment

Ref.	Recommendation	Barrier limitation addressed	Primary pathway
REC-1	Segregated seawater cooling and condensing trains	Loss of one cooling train may remove condenser heat rejection and cause turbine trip, loss of generation, and reactor shutdown demand.	Seawater cooling and power conversion
REC-2	Controlled relief handling through the cofferdam and monitored vent mast discharge	Potentially contaminated helium or helium-steam mixtures may be relieved without a complete confinement and discharge management path.	Primary helium and steam generator release pathways
REC-3	Controlled turbine side pressure relief arrangement	Condenser failure or loss of cooling may cause back pressure downstream of the turbine and challenge the steam-water circuit.	Steam generator, turbine, and condenser pathway
REC-4	Segregated main switchboard rooms and a protected emergency switchboard	A switchboard fault, fire, or flooding event may affect both the main distribution system and the connection of emergency power.	Ship service electrical power
REC-5	Seawater discharge monitoring and discharge side isolation	Leakage into the seawater circuit may create an unmonitored release path to the external environment.	Seawater cooling and environmental interface
REC-6	Normally unmanned nuclear compartment with remote monitoring and controlled manned intervention	Personnel may be exposed if they are present within, or required to enter, the nuclear compartment following a helium, steam, contamination, or atmospheric hazard.	Primary helium, steam generator, and nuclear compartment intervention pathways

The recommendations should not be considered as six independent equipment additions. REC-1 and REC-5 address the availability and environmental integrity of the seawater system. REC-2 and REC-3 address pressure relief and management of fluids for which radioactive contamination may be credible. REC-4 supports the continued operation of active barriers included in the other recommendations. REC-6 addresses personnel protection by establishing a normally unmanned nuclear compartment operating philosophy supported by remote monitoring, controlled access, and defined arrangements for necessary manned intervention.

The order of the following sections reflects the system dependencies identified in the Bow-ties. REC-1 first addresses the continued availability of heat rejection. REC-2 and REC-3 then address the management of pressure and potentially contaminated relief flow. REC-4 addresses the electrical support required by active monitoring, isolation, cooling, and recovery functions. REC-5 controls the interface between the onboard cooling system and the external marine environment. REC-6 then addresses nuclear compartment occupancy and intervention where remote operation is insufficient and personnel access becomes necessary.

8.2.1. REC-1: Segregated seawater cooling and condensing trains

First iteration finding

The first iteration assessment identified the seawater cooling system as a common support function for the condenser and power conversion plant. Loss of seawater flow can increase condenser pressure, trip the turbine generator, remove normal electrical generation, and create reactor shutdown demand. Thus, the event can progress beyond the seawater cooling room and affect propulsion, ship service power, and nuclear plant recovery.

The baseline arrangement contained seawater pumping and condenser functions, but it did not provide sufficient evidence that a single equipment or compartment failure would leave an independent heat rejection path available. Duplication without physical separation would not resolve this weakness because fire, flooding, electrical failure, or local structural damage could affect both trains.

Recommended arrangement

REC-1 introduces two functionally and physically segregated seawater cooling and condensing trains. Each train is intended to provide a defined heat rejection function using its own pumping, isolation, piping, and condenser side equipment. The two trains should be separated within the ship arrangement and should not depend on one local electrical distribution point.

The recommendation does not require both trains to provide full propulsion power following every failure. The requirement is that failure of one train does not remove all available condenser cooling and does not prevent the plant from reaching a controlled shutdown condition.

Safety function and DiD contribution

REC-1 is primarily an active and arrangement based recommendation. The pumps and isolation valves are active components, while physical segregation and separate routing provide passive protection against common cause failure.

The recommendation strengthens DiD Level 3 by maintaining an engineered heat rejection function following a single failure or local accident. Its principal DiD assignment is summarized in Table 8.4. It also supports Level 4 where one segregated train remains available after a wider equipment or compartment level event and provides a means of preventing further plant escalation.

It reduces the estimated frequency of consequences associated with complete loss of heat rejection. It does not remove the initiating causes of pump failure, fouling, blockage, or hull damage. Its function is to prevent one such failure from developing into complete loss of the condenser cooling function. Its effect on the affected HAZID scenarios is presented in Figure E.1. The segregation of the seawater cooling and condensing trains is visible in the overall REVA-REVB arrangement comparison shown in Figure 8.6.

8.2.2. REC-2: Controlled handling of potentially contaminated relief flow

First iteration finding

The primary helium and steam generator Bow-ties identified a weakness after loss of pressure boundary integrity. Existing pressure relief devices can protect equipment against unacceptable pressure, but pressure protection alone does not provide complete control of radioactive contamination.

A primary helium leak may release contaminated helium into the nuclear compartment. A steam generator tube failure may produce a helium-steam mixture or transfer contamination to the steam-water circuit. If the affected system is relieved without a defined handling arrangement, the relief function may transfer the hazard from the equipment to another compartment, ventilation system, or external discharge point.

The first iteration design included isolation and pressure relief functions but did not define a complete route for collecting, monitoring, confining, and discharging potentially contaminated relief flow.

Recommended arrangement

REC-2 routes relevant relief flows to a controlled handling arrangement associated with the cofferdam surrounding the nuclear compartment. The cofferdam is used as a separated handling or collection volume rather than allowing direct discharge into an occupied machinery space.

Potentially contaminated helium, steam, or mixed relief flow is routed through a defined and protected relief path. The arrangement includes suitable isolation, pressure and leakage monitoring, radiation monitoring, drainage or collection provisions, and treatment or filtration where required by the credible source term and physical condition of the relieved inventory.

The controlled relief path is connected to a monitored vent mast or equivalent elevated discharge point. Before discharge, the relieved inventory should be monitored and, where required by the source term and fluid condition, filtered, treated, or retained until controlled discharge is permitted.

The detailed sizing, filtration performance, pressure capacity, drainage requirements, and radiological release criteria are outside the scope of the concept design.

Safety function and DiD contribution

The recommendation contains passive and active elements. The cofferdam boundary, pressure relief path, and protected routing are passive barriers. Isolation valves, pressure monitoring, leakage detection, radiation monitoring, treatment or filtration equipment, and controlled vent actuation are active barriers.

REC-2 mainly strengthens DiD Level 4. It is intended to limit contamination spread and manage a release after the primary pressure boundary or steam generator boundary has already failed. Its principal DiD assignment is summarized in Table 8.4. Detection and isolation functions within the arrangement also contribute to Levels 2 and 3.

The recommendation reduces consequence severity by limiting the spread of contaminated fluid and avoiding uncontrolled discharge into machinery or accommodation spaces. It may also reduce escalation frequency where rapid detection and isolation prevent a small release from developing into a larger compartment or external release event. Its effect on the affected HAZID scenarios is presented in Figure E.1. The implementation of the controlled relief routing in REVB is shown in Figure 8.2.

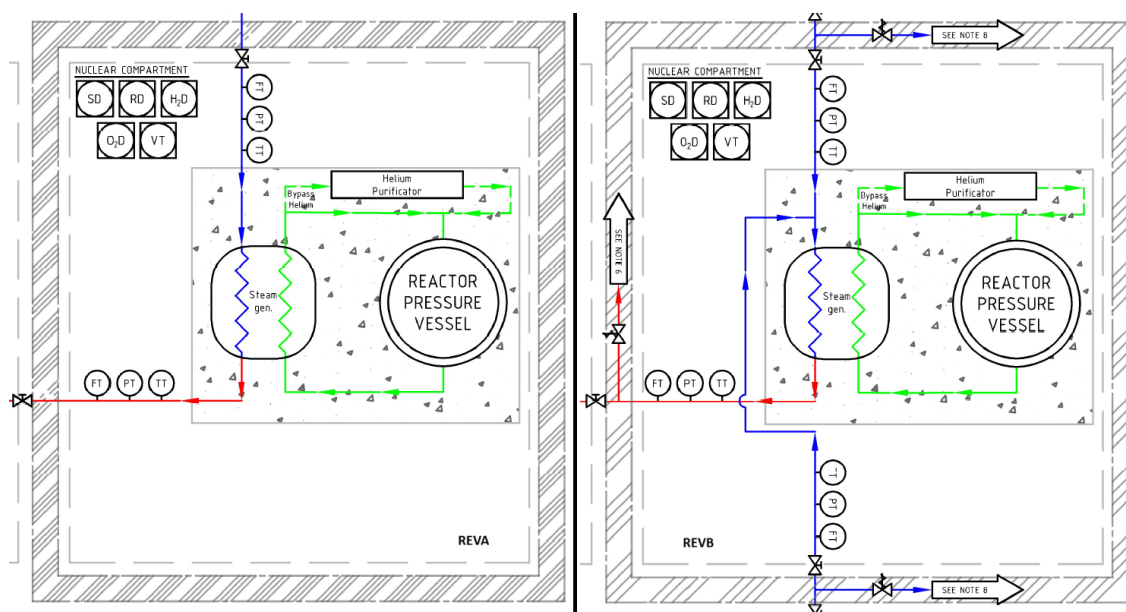


Figure 8.2: Comparison of the REVA and REVB nuclear compartment arrangements showing the controlled relief routing introduced in the second design iteration.

8.2.3. REC-3: Controlled turbine side pressure relief

First iteration finding

The steam generator escalation pathway identified a pressure control requirement downstream of the turbine. Loss of condenser performance, loss of seawater cooling, or blockage of the exhaust path can increase turbine exhaust pressure and challenge the steam-water circuit.

The normal turbine and condenser arrangement assumes that steam can expand through the turbine and condense at low pressure. When condenser cooling is unavailable, this pressure relationship may no longer be maintained. The resulting back pressure can trip the turbine and may challenge downstream piping or equipment. [30, 4]

A further concern is that the steam-water circuit may contain radioactive contamination following a steam generator tube failure. A conventional turbine side relief route may become a potential radiological discharge path during a combined or consequential event.

Recommended arrangement

REC-3 introduces a turbine side pressure relief or controlled dump function downstream of the turbine. The arrangement protects the turbine and associated steam-water equipment against unacceptable back pressure when the condenser or its cooling function is unavailable.

The discharge should not be routed directly to an uncontrolled machinery space location. Where contamination of the steam-water inventory is credible, the relieved flow should be directed to a controlled collection, condensing, or relief-handling system.

The relief function must be coordinated with turbine trip, steam isolation, feedwater isolation, reactor trip, and the controlled relief arrangement introduced under REC-2. This coordination prevents one pressure control action from creating a separate uncontrolled release pathway.

Safety function and DiD contribution

REC-3 is primarily an active mitigative barrier because it requires pressure detection and valve actuation. The associated pressure rated piping and protected discharge route provide passive support.

The recommendation strengthens DiD Level 3 by controlling an abnormal pressure condition following condenser or cooling failure. Its principal DiD assignment is summarized in Table 8.4. Where the relieved inventory may be contaminated and is routed to controlled handling, the recommendation also contributes to Level 4 consequence mitigation.

The recommendation mainly reduces the severity of turbine and steam-water circuit overpressure consequences. It may also reduce the probability of secondary pipe rupture by providing a defined relief path before equipment pressure limits are exceeded. Its effect on the affected HAZID scenarios is presented in Figure E.1. Figure 8.3 shows the additional turbine side pressure relief provision introduced in REVB.

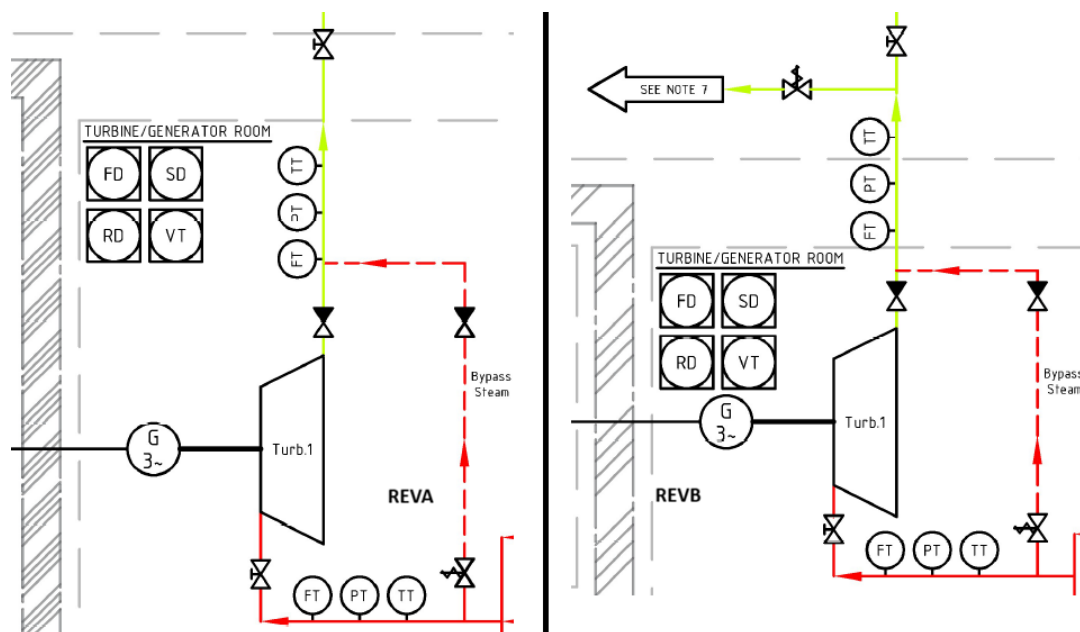


Figure 8.3: Comparison of the REVA and REVB turbine-generator arrangements showing the additional turbine side pressure relief provision introduced in REVB.

8.2.4. REC-4: Segregated electrical distribution

First iteration finding

The loss of ship service power Bow-tie showed that emergency generation alone does not ensure recovery. An emergency generator may remain available while the switchboard, cable route, or distribution compartment required to supply the essential loads has been damaged.

Main switchboard faults, electrical fires, flooding, cable damage, and bus transfer failures may affect several electrical functions at the same time. If the main and emergency supplies depend on one room or one distribution path, the arrangement contains common cause failures.

This issue is important because electrical distribution supports monitoring, reactor protection, valve actuation, ventilation, communications, lighting, cooling support, and recovery actions. Loss of distribution can weaken barriers in all three Bow-ties.

Recommended arrangement

REC-4 separates the main electrical distribution between two segregated main switchboard rooms and introduces a dedicated emergency switchboard in a protected location. Essential safety and recovery loads are supplied through distribution paths that do not all pass through one switchboard room.

The emergency switchboard is connected to the emergency diesel generator and the required battery backed supply. The battery system provides immediate continuity for reactor protection, instrumentation, control, communication, and selected actuators during the period between loss of the main supply and connection of longer duration emergency generation.

Safety function and DiD contribution

REC-4 combines active electrical equipment with passive segregation. The switchboards, transfer devices, batteries, and emergency generator are active barriers. Separate rooms, protected boundaries, and segregated cable routes provide passive protection.

The recommendation strengthens DiD Level 3 by preserving engineered accident control and safe shutdown functions following loss of normal power. It also supports Level 4 because the emergency distribution system remains available to operate monitoring, isolation, confinement, and release management equipment during more severe conditions. Its principal DiD assignment is summarized in Table 8.4.

The recommendation reduces the estimated frequency of complete loss of essential electrical supply. It does not prevent all generator or switchboard faults, but it reduces the probability that one fault disables all normal and emergency distribution functions. Its effect on the affected HAZID scenarios is presented in Figure E.1. The resulting segregation of the electrical distribution is shown in Figure 8.4.

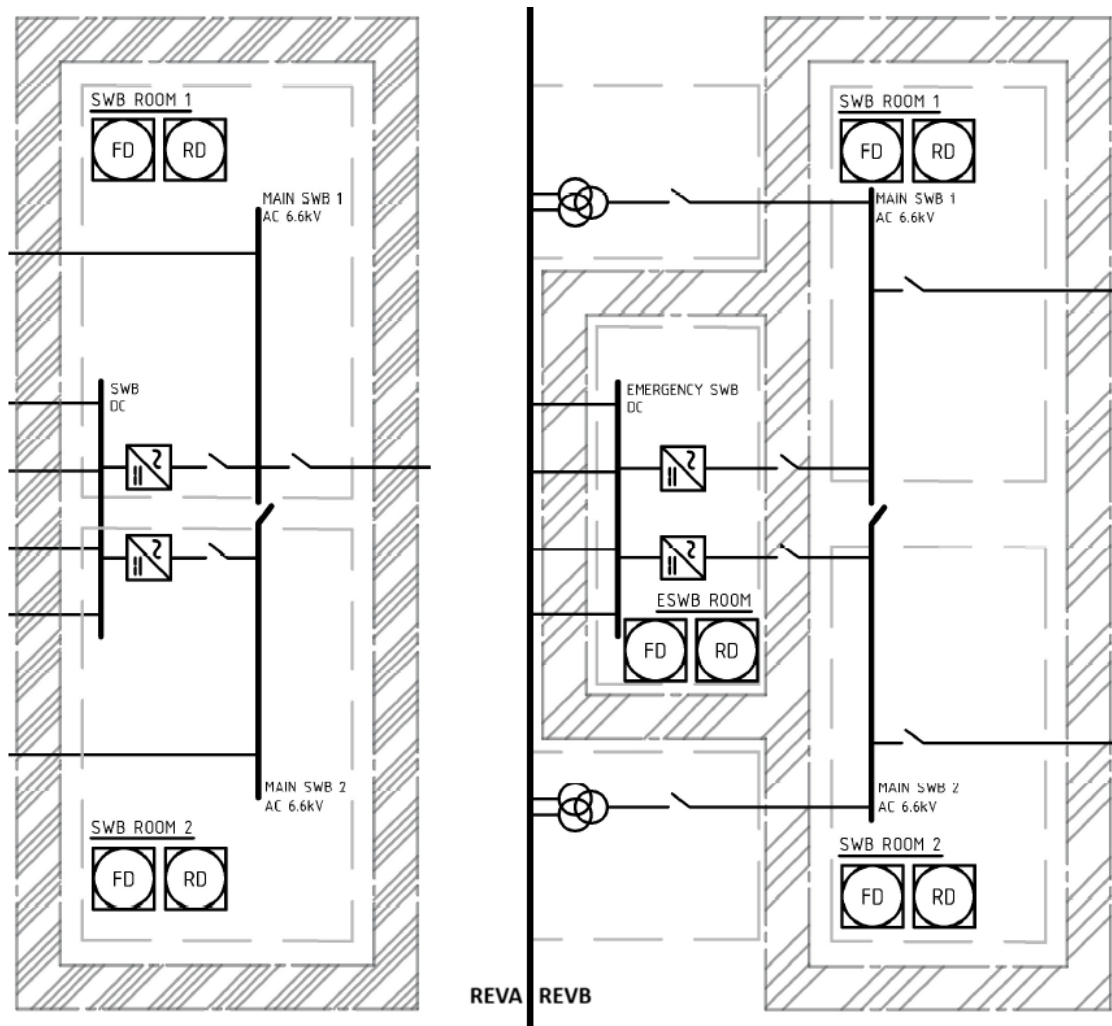


Figure 8.4: Comparison of the REVA and REVB electrical distribution arrangements showing the increased physical and functional segregation introduced in the second design iteration.

8.2.5. REC-5: Seawater discharge monitoring and isolation

First iteration finding

The seawater cooling system forms a direct interface between the machinery plant and the external environment. A failure of the condenser or another heat transfer boundary may allow steam-water inventory or contamination to enter the seawater circuit.

The baseline discharge arrangement did not provide a sufficiently explicit means of detecting an abnormal discharge and isolating the overboard path. Continued seawater pumping under such conditions could transport the released inventory outside the vessel.

The external discharge consequence may remain limited where the transferred inventory is not contaminated. However, following an inter-loop leakage event or another pressure boundary failure, radioactive contamination cannot be excluded without monitoring.

Recommended arrangement

REC-5 introduces monitoring of the seawater discharge and an isolation valve on the discharge side of the seawater circuit. The monitoring function is intended to identify abnormal conditions before continued discharge results in a larger environmental release.

The final monitoring parameters would depend on the detailed system design. They may include radiation, conductivity, temperature, pressure, or other indicators capable of identifying leakage across the relevant heat transfer boundary.

The discharge isolation valve should be remotely operable and should move to the required safe position following a confirmed abnormal condition or loss of control power. Closure of the discharge path must be coordinated with pump trip and isolation of the affected cooling train to avoid unacceptable system pressure.

Where REC-1 provides two segregated cooling trains, REC-5 should allow the affected train to be isolated without unnecessarily removing the unaffected train.

Safety function and DiD contribution

REC-5 consists mainly of active monitoring and isolation equipment. The separated discharge routing and pressure boundary provide passive support.

The monitoring function contributes to DiD Level 2 by detecting an abnormal plant condition. Isolation of the affected discharge path contributes to Level 3 by controlling the event within the design basis. Where the function limits a credible radioactive release to the marine environment, it also supports Level 4 mitigation. Its principal DiD assignment is summarized in Table 8.4.

The recommendation mainly reduces consequence severity by limiting the duration and quantity of an abnormal discharge. It may also reduce escalation frequency by allowing the affected cooling train to be isolated before contamination spreads through a larger part of the seawater system. Its effect on the affected HAZID scenarios is presented in Figure E.1. The additional discharge monitoring and isolation provision is shown in Figure 8.5.

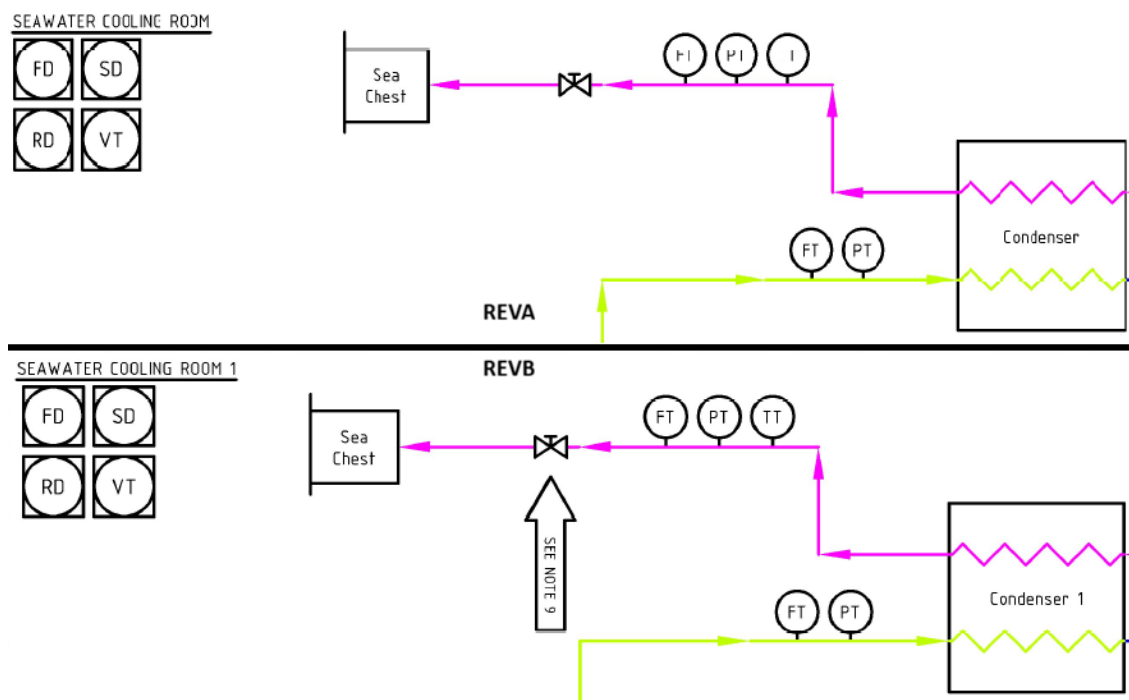


Figure 8.5: Comparison of the REVA and REVB seawater cooling arrangements showing the additional discharge monitoring and isolation provision introduced in REVB.

8.2.6. REC-6: Normally unmanned nuclear compartment and controlled manned intervention

First iteration finding

The primary helium and steam generator Bow-ties identified accident pathways in which helium, steam, or radioactive contamination may enter the nuclear compartment. Existing monitoring, isolation, and ventilation functions provide detection and support accident control, but the potential personnel consequence also depends on whether crew members are present in the compartment or are required to enter.

The first iteration design included controlled access and radiological monitoring but did not establish a complete nuclear compartment occupancy philosophy. It also did not define the conditions, protective measures, and response arrangements required for exceptional manned intervention following an abnormal condition.

Without a defined occupancy and intervention philosophy, personnel may be exposed to radiation, airborne contamination, oxygen deficient conditions, elevated temperature, pressure, steam, or helium during an accident or subsequent activity.

Recommended arrangement

REC-6 designates the nuclear compartment as normally unmanned whenever the reactor or primary helium system is in operation. Normal plant operation, surveillance, and condition monitoring should be performed remotely from a continuously attended control station.

Permanent monitoring should be provided for radiation, airborne contamination, helium concentration, oxygen concentration, pressure, temperature, and fire conditions, as applicable to the final compartment arrangement. Abnormal indications should generate alarms at the control station and support the remote actuation of reactor shutdown, system isolation, ventilation isolation, and compartment confinement functions where required.

Access to the nuclear compartment should be authorization controlled and interlocked against defined unsafe radiation or atmospheric conditions. Personnel entry should only be permitted where necessary and after the NPP has been placed in an appropriate safe state.

Any necessary manned intervention should follow a documented controlled entry and safe response procedure. The procedure should define system isolation and depressurization where practicable, independent pre-entry radiation and atmosphere surveys, continuous monitoring during entry, personal dosimetry, appropriate personal protective and respiratory equipment, communication with the control station, standby support, occupancy limits, escape routes, withdrawal criteria, and emergency extraction arrangements.

REC-6 does not remove the need for physical access for inspection, maintenance, testing, or recovery. Instead, it establishes the conditions under which access may occur and ensures that routine reactor operation does not depend on continuous personnel presence within the nuclear compartment.

Safety function and DiD contribution

REC-6 is primarily a mitigative and operational control measure. The normally unmanned operating philosophy does not reduce the frequency of the initiating plant event, but it reduces the likelihood that personnel are present when such an event occurs and therefore reduces the frequency of the personnel exposure pathway. Remote monitoring, alarms, and access interlocks provide active barriers, while entry authorization, dosimetry, protective equipment, communication, standby support, and controlled entry procedures provide procedural barriers.

The recommendation mainly contributes to DiD Level 4 by limiting personnel exposure and supporting controlled accident management following a significant plant or confinement event. Continuous monitoring also contributes to Level 2 by detecting abnormal compartment conditions, while access control, system isolation, and controlled intervention support Level 3 accident control. Its principal DiD assignment is summarized in Table 8.4.

REC-6 was linked to the applicable personnel exposure and intervention scenarios as an additional barrier. Although the normally unmanned philosophy reduces the likelihood of personnel being exposed following an abnormal event, the concept level assessment does not provide sufficient evidence to justify a specific reduction in the ordinal Frequency Index. No independent risk score reduction was therefore credited solely to REC-6.

8.3. Implementation in the second design iteration

The preceding sections defined the required safety functions and arrangement principles for the second design iteration. REVB represents the physical and operational design response to the first iteration assessment. The revised arrangement contains segregated cooling and condensing functions, controlled

relief flow routing, additional turbine side pressure relief capability, segregated electrical distribution, monitored seawater discharge isolation, and a normally unmanned nuclear compartment supported by remote monitoring, access control, and controlled manned intervention. The resulting design changes are shown in Figures 8.6 & 8.7. Full size versions of the design drawings are provided in Appendix B.

The comparison shows that the recommendations were implemented as changes to the vessel arrangement rather than remaining only as actions in the HAZID. The REVB nuclear island arrangement makes the segregated cooling and condensing functions, controlled relief routing, and supporting isolation and monitoring provisions more explicit. The revised general arrangement also reflects the segregation of electrical distribution and the supporting arrangement changes required by the second design iteration.

The main differences between REVA and REVB are summarized in Table 8.2. Each recommendation was also entered into the affected HAZID scenarios, and the corresponding Bow-tie barriers were updated. The complete second iteration traceability record is provided in Appendix E. Figure E.1 summarizes the affected HAZID scenarios and their risk development, while Figures E.2, E.3 & E.4 present the updated Bow-ties.

Table 8.2: Main safety related differences between REVA and REVB

Design function	REVA condition	REVB development
Seawater heat rejection	Cooling and condenser functions represented without sufficient evidence of train segregation.	Two segregated cooling and condensing trains with independent isolation and distribution principles.
Relief flow management	Pressure relief represented mainly as local equipment protection.	Controlled relief routing through a separated handling volume, with monitoring, isolation, treatment where required, and controlled vent mast discharge.
Turbine back pressure protection	Normal turbine and condenser pressure control functions represented.	Additional downstream relief or dump function for condenser failure and cooling loss conditions.
Electrical distribution	Main and emergency generation represented, but distribution independence not sufficiently explicit.	Segregated main switchboard rooms, protected emergency switchboard, and separated essential distribution.
Seawater environmental interface	Overboard discharge represented without explicit abnormal condition isolation.	Discharge monitoring and discharge side isolation of the affected cooling train.
Nuclear compartment occupancy and intervention	Controlled access and monitoring represented, but no complete occupancy or intervention philosophy defined.	Normally unmanned during reactor and primary helium system operation, with remote monitoring and control, access interlocks, controlled entry authorization, and defined arrangements for necessary manned intervention.

Each recommendation was also entered into the affected HAZID scenarios. The revised scenario record contains the recommendation reference, the affected risk parameter where a reassessment was justified, and the residual risk after the recommendation. The corresponding Bow-tie barriers were updated to show their preventive or mitigative position and their DiD contribution.

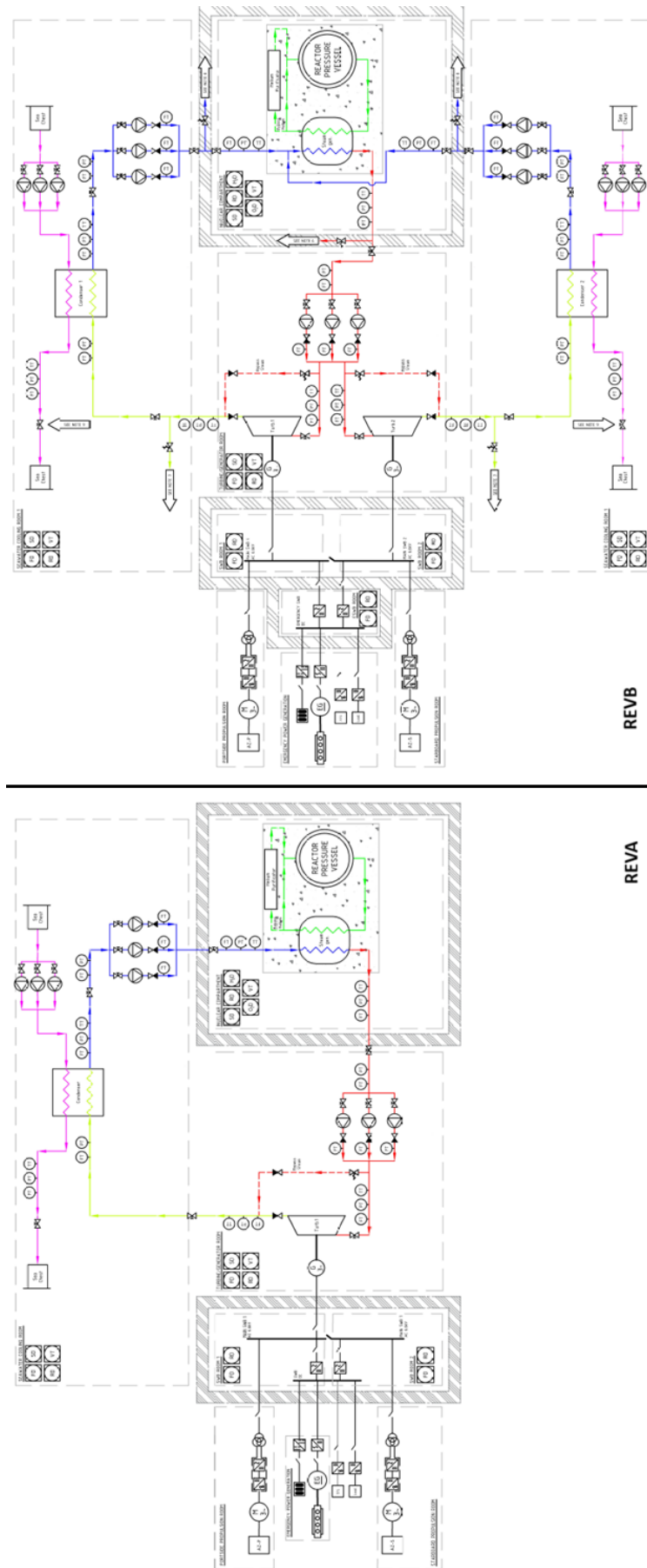


Figure 8.6: Comparison of the REVA and REVB nuclear island arrangements.

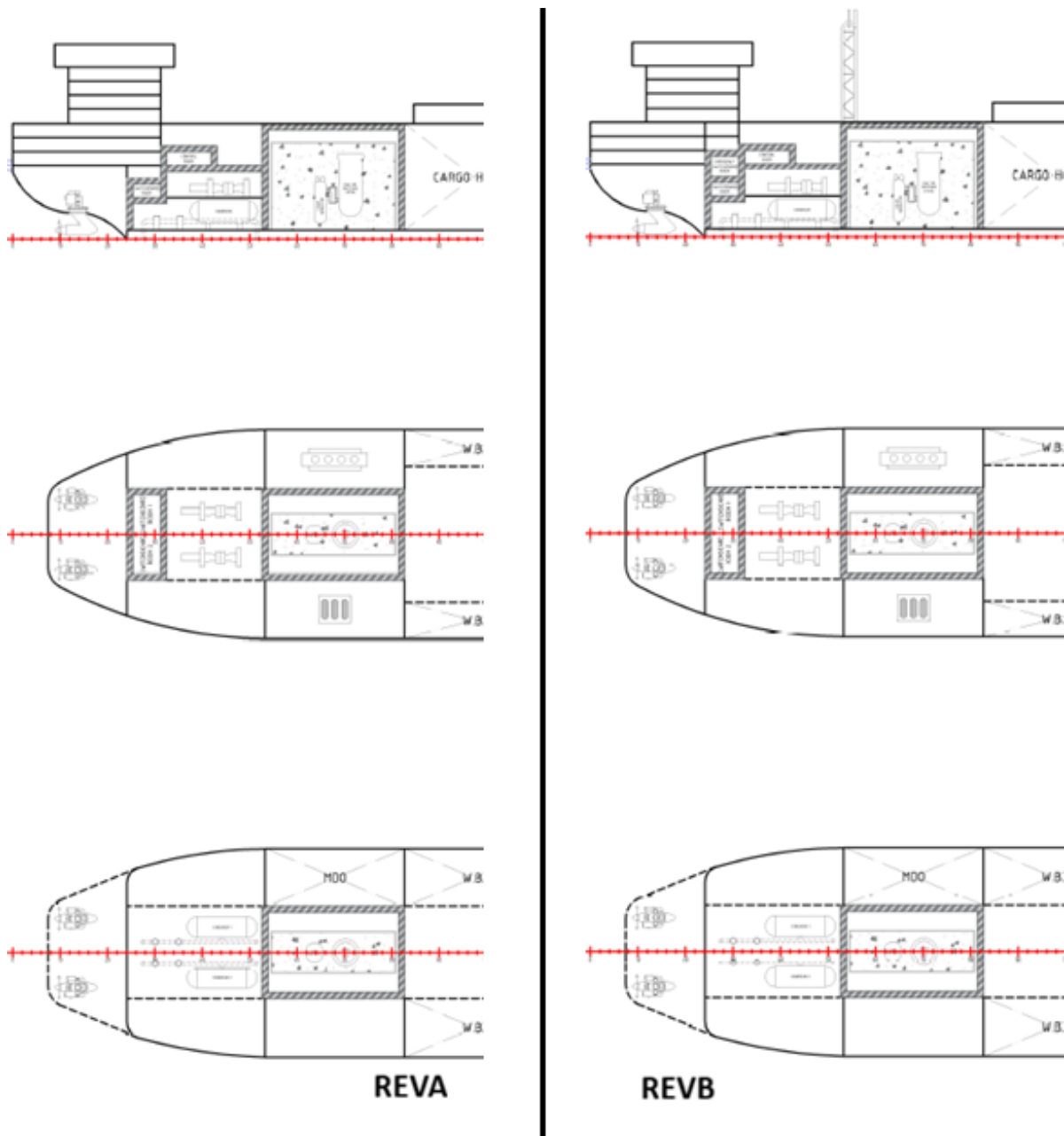


Figure 8.7: Comparison of the REVA and REVB general arrangements.

8.4. Second iteration assessment results

The second iteration assessment examines the effect of the design recommendations on the scenarios to which they are directly applicable. The complete HAZID was not reassessed, because several scenarios were unaffected by the proposed changes. Instead, a recommendation subset was established through traceable links between each recommendation, its originating first iteration finding, the relevant HAZID scenarios, and the associated Bow-tie branches.

8.4.1. Selection of scenarios affected by the recommendations

Implementation in REVB does not imply that every HAZID scenario benefits from every recommendation. To avoid overstating the effect of the second iteration, each recommendation was applied only to scenarios in which it interrupted a credible cause to consequence pathway or strengthened an applicable barrier function.

A total of 20 scenario rows were included in the recommendation subset. These scenarios were associated mainly with loss of heat rejection, condenser and turbine pressure effects, primary or inter-loop release management, electrical distribution dependency, abnormal seawater discharge, and personnel exposure or intervention within the nuclear compartment.

The inclusion of REC-6 expanded the recommendation subset to include the applicable nuclear compartment personnel exposure and intervention scenarios. A lower residual score was assigned only where the complete set of applicable recommendations provided sufficient justification within the adopted assessment method.

The 20 affected scenarios were assessed in three distinct states:

1. Initial risk before any safeguards were credited;
2. Residual risk after the existing REVA safeguards;
3. Residual risk after both the existing safeguards and the applicable REVB recommendations.

This separation distinguishes the contribution of the baseline safeguards from the additional contribution of the second design iteration. It also prevents the REVB recommendations from being treated as features of the first iteration design.

With the recommendation subset and comparison states defined, Section 8.4.2 evaluates the resulting change in risk distribution and Risk Index.

8.4.2. Risk reassessment after design recommendations

The reassessment examines whether the recommendations provide a measurable change within the adopted ordinal ranking method. The results are considered from three perspectives: the distribution of the affected scenarios across the risk categories, the change in their sum of scenario Risk Indices, and the number of scenarios for which the recommendations justify a lower residual score. Because the indices are ordinal rather than probabilistic, the results are interpreted as comparative evidence of design improvement rather than as a quantified change in absolute accident risk.

Recommendation subset risk distribution

Before safeguards were credited, the 20 affected scenarios contained four High-risk, 11 Medium-risk, and five Low-risk scenarios. The sum of scenario Risk Indices for the subset was 108.

After the existing safeguards were applied, all four High-risk scenarios moved into the Medium category. The resulting distribution contained 15 Medium-risk and five Low-risk scenarios. The sum of scenario Risk Indices reduced to 99.

After the design recommendations were applied, the number of Medium-risk scenarios reduced from 15 to six, while the number of Low-risk scenarios increased from five to 14. No High- or Extreme-risk scenarios remained in the recommendation subset. The sum of scenario Risk Indices reduced to 86.

Table 8.3: Risk development for the scenarios affected by design recommendations

Result	Initial	After existing safeguards	After recommendations
Scenario rows	20	20	20
Sum of scenario Risk Indices	108	99	86
Extreme-risk scenarios	0	0	0
High-risk scenarios	4	0	0
Medium-risk scenarios	11	15	6
Low-risk scenarios	5	5	14

Figure 8.8 illustrates the progressive change in the risk distribution of the 20 scenarios affected by the design recommendations. Existing safeguards removed the four High-risk scenarios but left Medium risk as the dominant category. Following implementation of the recommendations, nine scenarios

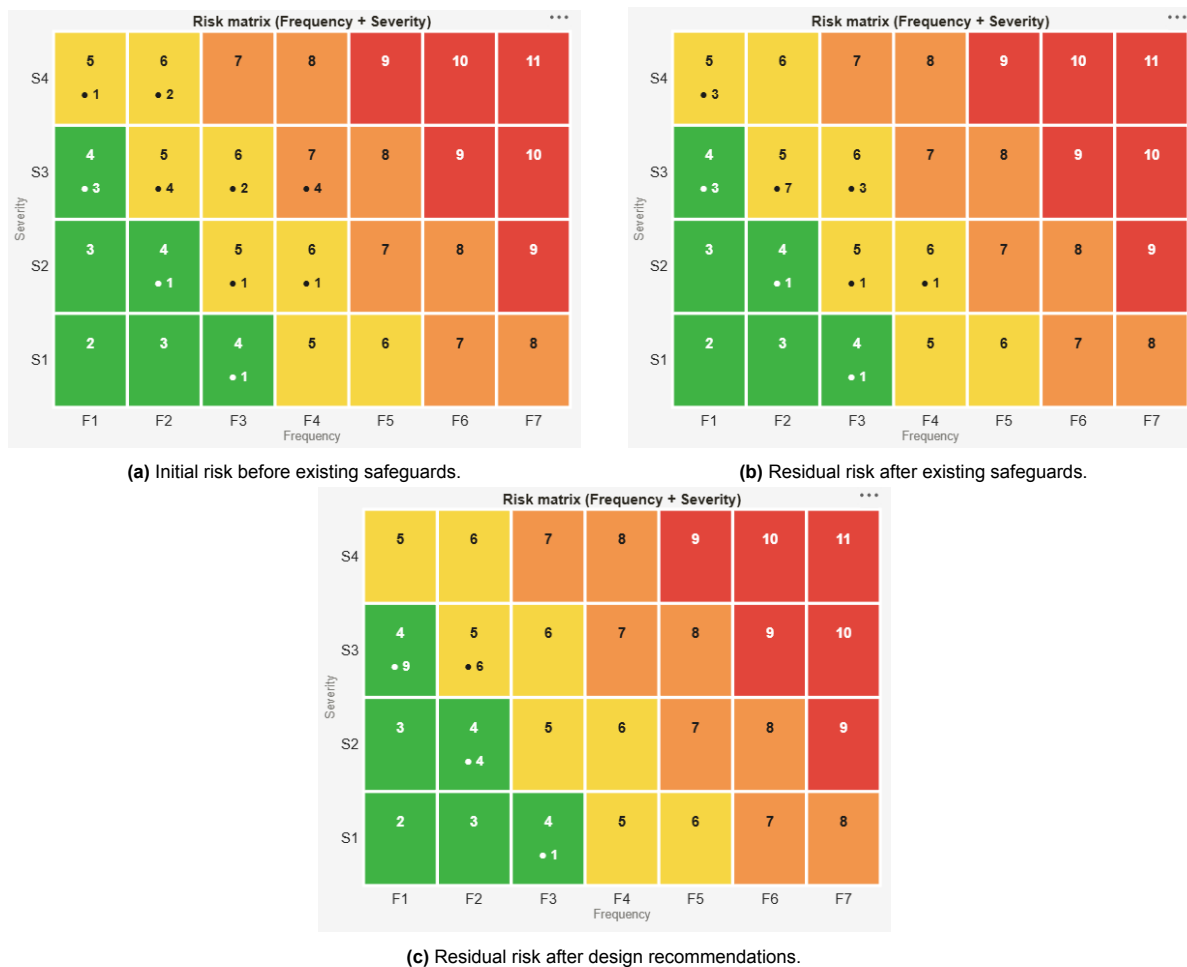


Figure 8.8: Risk matrix development for the scenarios affected by the design recommendations across the three assessment states.

moved from Medium to Low risk, leaving six Medium-risk and 14 Low-risk scenarios. Thus, the comparison separates the contribution of the existing safeguards from the additional risk reduction provided by REVB.

The six scenarios that remained in the Medium category demonstrate that the recommendations did not produce a uniform reduction across the complete subset. This includes scenarios for which the recommendations strengthened the barrier arrangement but did not provide sufficient evidence to justify a lower ordinal Frequency or Severity Index.

Risk index reduction

The existing safeguards reduced the subset Risk Index from 108 to 99, corresponding to a reduction of nine points. The design recommendations then reduced the index by a further 13 points, from 99 to 86. The total reduction between the initial and final assessment states was therefore 22 points.

These changes should be interpreted as an ordinal comparison within the adopted risk ranking method rather than as a quantified reduction in accident probability. The Risk Index is formed by adding categorical Severity and Frequency Indices. Consequently, the reduction in the sum of scenario Risk Indices demonstrates a systematic movement towards lower ranked scenarios but does not represent a directly measurable reduction in physical risk.

Effectiveness across the affected scenarios

Eleven of the 20 affected scenario rows received a lower residual Risk Index after the design recommendations were applied. The remaining nine scenarios retained their previous score because the

recommendations either improved barrier quality without crossing an ordinal scoring boundary or did not provide sufficient evidence to reduce the assigned Severity or Frequency Index. An unchanged score therefore indicates that no additional ordinal risk reduction was demonstrated, rather than that the recommendation provides no safety benefit.

The strongest change is visible in the movement from Medium to Low risk. Existing safeguards removed the High-risk cases but left Medium risk as the dominant category. The recommendations changed this distribution by providing additional isolation, segregation, release handling, monitoring, and personnel protection functions. Nine scenarios moved from Medium to Low risk, while two additional scenarios received a lower Risk Index without changing risk category.

The remaining six Medium-risk scenarios require further review during detailed design. Their presence does not indicate that the recommendations are ineffective. It indicates that concept level measures alone do not provide sufficient evidence to classify every affected scenario as Low risk. This distinction is particularly relevant to REC-6, which strengthens personnel protection and accident management but was not assigned an independent ordinal risk reduction solely on the basis of the normally unmanned operating philosophy.

8.4.3. Effect on Defence-in-Depth (DiD)

The first iteration Bow-ties showed that DiD Levels 1 to 3 were generally represented by equipment design, inspection, monitoring, reactor protection, isolation, and pressure relief. Level 4 mitigation was less explicit, particularly for contaminated relief flow, personnel protection during abnormal nuclear compartment conditions, and wider escalation following failure of the principal pressure boundary.

The second iteration improves the DiD structure in four ways. First, it adds independence to existing accident control functions. The segregated cooling trains and electrical distribution reduce the probability that one local event removes all available trains.

Second, it adds explicit mitigation after loss of a principal boundary or function. Controlled relief routing, monitored discharge, treatment or retention where required, and vent mast handling remain relevant after a leak or pressure boundary failure has occurred. These measures therefore provide a clearer Level 4 function.

Third, it improves detection and isolation at the environmental interface. Seawater discharge monitoring identifies abnormal conditions, while the discharge side valve limits continued release.

Fourth, it strengthens personnel protection and accident management within the nuclear compartment. The normally unmanned operating philosophy reduces routine personnel presence during reactor and primary helium system operation. Remote monitoring, access control, and controlled manned intervention provide additional protection where abnormal radiation, contamination, helium, oxygen, pressure, temperature, or fire conditions are present. These measures principally support Level 4 mitigation, while their monitoring and isolation functions also contribute to Levels 2 and 3.

The level assignment identifies the principal function of each recommendation. Some recommendations include several components that support different levels. For example, REC-5 contains a monitoring function associated with Level 2 and an isolation function associated with Levels 3 or 4. Similarly, REC-6 principally supports Level 4 personnel protection and accident management, while remote monitoring contributes to Level 2 and access control, isolation, and controlled intervention support Level 3.

The second iteration does not establish that every DiD level is fully independent under all accident conditions. Detailed independence assessment would require equipment location, cable routing, environmental qualification, power supply design, remote monitoring reliability, access-control logic, and failure response data. The concept level results show that the main first iteration gaps have been addressed in the system design and operating philosophy.

The DiD assessment establishes how the recommendations strengthen prevention, accident control, and mitigation. A separate question is whether the second iteration represents a systematic search for further practicable risk reduction. This is considered through the ALARP-oriented evaluation in Section 8.4.4.

Table 8.4: Principal Defence-in-Depth (DiD) contribution of the recommendations

Ref.	Main safety function	Main DiD level	Contribution
REC-1	Maintain heat rejection following train failure	Level 3	Provides an alternative engineered cooling and condensing path and reduces common cause dependency.
REC-2	Confine and control potentially contaminated relief flow	Level 4	Limits contamination spread after loss of a pressure boundary and provides controlled release management.
REC-3	Control turbine and steam-water back pressure	Levels 3-4	Protects equipment during condenser failure and controls relief where contamination is credible.
REC-4	Preserve essential electrical distribution	Level 3	Maintains shutdown, monitoring, isolation, and recovery loads following a switchboard or room level event.
REC-5	Detect and isolate abnormal seawater discharge	Levels 2-4	Detects leakage, isolates the environmental release path, and limits the quantity discharged.
REC-6	Limit personnel exposure and support controlled nuclear-compartment intervention	Level 4	Reduces routine personnel presence, supports remote accident monitoring, and establishes controlled access and intervention following an abnormal condition.

8.4.4. ALARP-oriented evaluation

The design recommendations were developed for scenarios that remained relevant after the existing safeguards had been considered. This is consistent with an ALARP-oriented process because further risk reduction was examined rather than accepting the first residual risk result without additional review [36, 39].

The recommendations provide defined safety functions and can be traced to identified escalation pathways. Their implementation also results in a lower risk ranking for most affected scenarios. For the remaining scenarios, the recommendations strengthen the barrier arrangement without providing sufficient concept level evidence to justify a lower ordinal Severity or Frequency Index. These findings support the argument that reasonably identifiable concept level risk reduction measures were considered and applied without overstating the demonstrated reduction.

However, the study does not provide a complete formal ALARP demonstration. No detailed cost effectiveness assessment was performed, and the study does not quantify the cost, weight, maintenance burden, reliability, or operational effect of each recommendation. This includes the operational and reliability implications of remote monitoring, access control, and controlled manned intervention associated with the normally unmanned nuclear compartment. It is therefore not possible to demonstrate that every additional risk reduction option beyond REVB would be grossly disproportionate to its safety benefit [36, 39].

The conclusion that can be supported is that the method produced an ALARP-oriented design development process. It identified residual risks, examined further practicable measures, implemented relevant recommendations, and reassessed the affected scenarios. Where the available evidence did not justify a lower ordinal risk ranking, the existing score was retained. Formal acceptance would require additional quantitative reliability analysis, consequence assessment, design verification, operational assessment, and cost effectiveness evaluation.

The ALARP-oriented evaluation therefore concerns the design development process rather than formal proof of risk tolerability. Having established this boundary, the next section evaluates whether the combined HAZID and Bow-tie methodology performed the functions for which it was selected.

8.5. Evaluation and discussion

Section 8.2 - 8.4 presented the recommendations, their implementation in REVB, and the resulting reassessment. This section does not repeat those individual design changes or risk results. Instead, it considers what can be learned from the application of the methodology beyond the specific recommendations.

First, the combined HAZID, Bow-tie, DiD, and FSA-informed approach is evaluated against the method-selection criteria defined in Chapter 5. The recurring findings are then used to derive broader ship design implications, before the limitations of the second design iteration are discussed.

8.5.1. Evaluation of the combined methodology

The combined methodology was assessed against the five selection criteria defined in Section 5.3. The results are summarized in Table 8.5.

Table 8.5: Evaluation of the applied methodology against the selection criteria

Criterion	Requirement	Observed performance
C-1	Suitability for concept design assessment	The HAZID and Bow-ties were developed using general arrangements, system functions, operating principles, and main interfaces without requiring detailed component design.
C-2	Ability to reveal common cause failure and false redundancy	The Bow-ties identified common electrical, cooling, compartment, discharge, and operational dependencies that were not clear from the risk matrix.
C-3	Ability to examine layered barrier performance	Preventive and mitigative barriers were positioned along each escalation branch and classified by function and DiD level.
C-4	Ability to produce ship integration measures	The assessment produced six recommendations that were implemented in REVB and linked to specific arrangement, system, and operating philosophy changes.
C-5	Limited dependence on quantified reliability data	The assessment produced comparative risk and barrier findings without requiring component level failure probabilities, although this limits the strength of the final risk claim.

The HAZID was effective for establishing broad hazard coverage and identifying where further assessment was required, but its tabular structure provided limited visibility of complete escalation pathways and safeguard dependencies. The Bow-tie analysis complemented the HAZID by making these pathways and barrier relationships explicit.

A principal strength of the combined methodology was its traceability. Identified HAZID scenarios and Bow-tie barrier weaknesses could be linked to specific recommendations, which were subsequently implemented and reassessed in REVB as described in Section 8.2 - 8.4. This demonstrates that the assessment outputs could be translated into design action rather than remaining only as qualitative risk findings.

The methodology also showed that resulting recommendations need not be limited to equipment changes. REC-6, for example, represents an operating and personnel protection philosophy supported by remote monitoring, access control, and controlled intervention arrangements.

The method remains dependent on engineering judgment. Severity and Frequency Indices are ordinal estimates, barrier effectiveness is not supported by validated failure data, and the Bow-ties do not quantify complete accident-sequence probabilities. The results should therefore be used for concept development and prioritization rather than as a licensing level risk demonstration.

8.5.2. General ship design implications

Although the recommendations were derived from specific HAZID scenarios and Bow-tie branches, their significance is not limited to the reference vessel. Together, they reveal wider principles for inte-

grating nuclear safety functions into a commercial ship arrangement and operating philosophy.

The assessment indicates that the safety of a nuclear powered commercial vessel cannot be addressed only through reactor equipment. Several important risk controls are ship integration measures involving compartment arrangement, electrical distribution, seawater systems, pipe routing, discharge control, remote monitoring, and personnel access arrangements.

Physical segregation is a central requirement. Redundant equipment should not be considered independent where it remains vulnerable to one fire, flooding event, switchboard fault, cable-route failure, or structural impact. The location and routing of the systems are therefore part of their safety classification.

Pressure relief must be assessed as a complete pathway. The design must consider not only whether pressure can be reduced, but also where the relieved fluid is routed, whether radioactive contamination is credible, how leakage is detected, whether treatment or retention is required, and how the final discharge is controlled.

Supporting systems must be included in the nuclear safety assessment. Electrical distribution, seawater cooling, ventilation, monitoring, and control systems determine whether reactor shutdown, isolation, confinement, and accident management functions remain available after a shipboard event.

Environmental interfaces require explicit isolation. Systems connected to overboard discharge, ventilation outlets, drains, or other external paths should include monitoring and control appropriate to the possible source term.

An explicit occupancy and intervention philosophy is also required for compartments containing primary nuclear systems. Where continuous personnel presence is not necessary, the nuclear compartment should be normally unmanned during reactor and primary helium system operation. Normal surveillance and control should be performed remotely, while access should be authorization controlled and restricted where radiation or atmospheric conditions are unsafe.

Necessary manned intervention should be treated as a defined safety function rather than as an improvised operational response. The design should therefore support pre-entry radiation and atmosphere surveys, continuous monitoring, personal dosimetry, suitable protective equipment, communication, standby support, occupancy limits, escape routes, withdrawal criteria, and emergency extraction arrangements. This operating philosophy complements, but does not replace, engineered pressure-boundary integrity, confinement, isolation, and controlled release management.

8.5.3. Limitations of the second iteration

The second design iteration demonstrates how findings from the first iteration assessment can be converted into traceable changes to the vessel arrangement, system design, and operating philosophy. It does not, however, verify the detailed performance, reliability, or regulatory acceptability of the recommended measures.

The recommendations define required safety functions and concept-level arrangement principles. Their implementation in REVb shows where segregation, controlled relief handling, environmental isolation, remote monitoring, and personnel protection provisions should be introduced. The revised risk rankings therefore represent a comparative assessment of the expected effect of these measures rather than quantified proof of their effectiveness.

In particular, the second iteration does not verify cooling capacity, relief system sizing, emergency power endurance, structural resistance, radiological consequences, instrumentation reliability, human performance, or the effectiveness of controlled manned intervention. It also does not demonstrate that the recommendations satisfy class, flag State, nuclear regulatory, or port State acceptance criteria.

Within these boundaries, the second iteration is sufficient to demonstrate the intended thesis contribution: a traceable process through which concept-level risk assessment findings inform ship design and operating-philosophy development. The wider methodological limitations and the corresponding recommendations for further work are discussed in Section 9.2.

8.6. Chapter 8 Conclusion

The risk assessment produced six recommendations addressing the main weaknesses identified in the selected top-events: segregated heat rejection trains, controlled handling of potentially contaminated relief flow, turbine side pressure protection, segregated electrical distribution, seawater discharge monitoring and isolation, and a normally unmanned nuclear compartment supported by remote monitoring and controlled intervention. Their implementation in REVB strengthened barrier independence, introduced more explicit DiD Level 4 mitigation, and reduced the residual risk of the affected scenario set. The results show that the assessment findings can be translated into traceable changes to ship arrangement, system design, and operating philosophy, although detailed engineering verification would still be required before design acceptance.

9

Conclusion

This chapter brings together the findings from the literature review, risk assessment, and two design iterations to answer the main research question. The conclusions focus on how the applied risk based design process identified safety dependencies and how these findings influenced the vessel arrangement and supporting system design. The resulting design considerations are followed by the main limitations of the study, recommendations for further work, and a personal reflection on the research process.

9.1. Conclusions

9.1.1. Summary and Answer to the Main Research Question

The literature review established that the safety of a nuclear powered commercial vessel cannot be assessed by considering the reactor independently from the ship. Fundamental nuclear safety functions such as reactivity control, heat removal, and confinement depend on shipboard electrical power, cooling, ventilation, monitoring, structural protection, and emergency support. At the same time, maritime hazards may challenge several of these functions simultaneously. Existing requirements across the nuclear, maritime, and classification domains provide relevant safety principles, but remain fragmented and do not form a complete modern framework for nuclear powered commercial vessels.

The methodological review showed that no single risk assessment method was sufficient for the objectives of the reference design. HAZID provided broad hazard identification and comparative risk ranking, while Bow-tie analysis provided greater insight into accident progression, barrier placement, and dependencies between safeguards. Combined within an FSA-informed structure, the methods provided a traceable way of moving from hazard identification and risk assessment towards risk control options and design development.

Application of the methodology showed that risk ranking is useful for identifying where further attention is required, but does not by itself explain why a safety pathway remains vulnerable. The Bow-tie assessment showed that important weaknesses were often associated not only with missing safeguards, but also with dependencies between apparently separate barriers. Nominal redundancy was therefore not necessarily equivalent to effective DiD where systems remained exposed to electrical supplies, supporting services, compartment hazards, or other common cause failures. The effectiveness of the safety design depends on the function, independence, and position of the barriers within the complete accident pathway.

The second design iteration demonstrated that these findings can be translated into identifiable ship design changes and subsequently reassessed. The resulting recommendations addressed weaknesses in system segregation, pressure and release management, electrical distribution, environmental isolation, monitoring, arrangement, and personnel intervention. The principal lesson is that risk assessment should not be treated only as a verification activity after the design has been developed, but as an input to the development and refinement of the ship itself.

The main research question was:

‘How can risk based design be applied to the safety assessment for nuclear powered commercial vessels, and what ship design implications follow from this approach?’

Risk based design can be applied to nuclear powered commercial vessels through an iterative concept level process that identifies and ranks hazards, examines accident escalation and barrier performance, translates identified safety weaknesses into ship design modifications, and reassesses the resulting design to progressively improve the integration and independence of nuclear and maritime safety functions.

This conclusion is supported by the successive application of the methodology to the reference vessel and the resulting development from REV0 to REVA and subsequently to REVB.

9.1.2. Design considerations derived from this study

Although the recommendations developed in this research are specific to the reference vessel, they also support several broader concept level design considerations for nuclear powered commercial vessels. These considerations are derived from the present study and should not be interpreted as prescriptive design requirements.

1. Treat nuclear safety as a ship integration requirement.

Reactor shutdown, heat removal, confinement, monitoring, and recovery depend on shipboard electrical, cooling, ventilation, structural, and control systems. These systems should therefore be integrated into the design from the earliest stage rather than added after the general arrangement has been fixed.

2. Demonstrate independence rather than assuming it from redundancy.

Duplicated pumps, switchboards, cables, valves, or cooling trains do not provide independent protection if they remain vulnerable to the same fire, flooding event, structural damage, compartment failure, or supporting service. Redundancy should therefore be supported by physical separation, independent routing, functional segregation, and protected emergency supplies.

3. Assess barriers as complete safety functions.

The effectiveness of a barrier should be assessed across its complete functional chain. For example, pressure relief should include detection, actuation, routing, confinement, monitoring, isolation, treatment or retention where required, and controlled discharge. Similarly, emergency power should include the source, switchboard, cabling, distribution route, and connection to the required loads.

4. Protect common supporting services and environmental interfaces.

Electrical distribution, heat rejection, ventilation, instrumentation, and control may support several preventive and mitigative barriers simultaneously. Their failure can therefore affect multiple accident pathways. Systems connected to the sea or atmosphere should also provide suitable detection, monitoring, isolation, and controlled handling where contamination is credible.

5. Assess DiD along accident pathways.

DiD should not be demonstrated only by counting safeguards. Each representative pathway should be examined to determine whether prevention, detection, accident control, severe condition mitigation, and emergency response are sufficiently represented. Attention should be given to explicit Level 4 measures after the isolation or protection systems have been challenged.

6. Establish a defined occupancy and intervention philosophy.

Compartments containing primary nuclear systems should be normally unmanned where continuous personnel presence is not required. Normal operation and surveillance should be supported by remote monitoring and control, while access should be authorization controlled and restricted where radiation or atmospheric conditions are unsafe. Necessary manned intervention should be supported by pre-entry surveys, continuous monitoring, personal dosimetry, suitable protective equipment, communication, standby support, occupancy limits, escape routes, withdrawal

criteria, and emergency extraction arrangements. This operating philosophy should complement, rather than replace, engineered confinement, isolation, and controlled release functions.

These guidelines indicate that a nuclear powered commercial vessel must be developed as an integrated nuclear and maritime safety system. The design priorities are therefore the independence of safety functions, the completeness of barrier pathways, the protection of supporting services, the control of interfaces through which an accident could propagate within or beyond the vessel, and the protection of personnel through remote operation and controlled intervention.

9.2. Research limitations and recommendations for further work

This research was carried out at concept design level with limited system detail and reliability data. The methodology was therefore intended to identify important hazards, dependencies, and design weaknesses rather than provide a complete safety case. The main areas for further work concern validation of the methodology, development towards quantitative assessment, verification of the proposed design measures, and inclusion of operational and regulatory aspects.

Further development of the methodology

The HAZID, risk ranking, and Bow-tie analyses required engineering judgment. This was relevant when defining scenarios, crediting safeguards, assigning DiD levels, and selecting the top events for more detailed analysis. The assessment was performed as an individual research project rather than through the multidisciplinary workshop process normally used in industry.

A useful next step would therefore be to repeat the assessment with a multidisciplinary team including nuclear, marine, electrical, operational, and human factors specialists. This would test whether the same important scenarios, dependencies, and design weaknesses are identified and would provide a stronger basis for the assigned risk rankings and safeguard credit.

The transition from HAZID to Bow-tie analysis could also be formalized further. In this study, top events were selected using risk ranking, recurring scenarios, accident escalation potential, and the number of safety functions affected. Future work could develop clearer selection criteria so that the process can be applied more consistently to other vessel concepts.

A further point for future work is the scalability of the combined methodology. The use of HAZID, Bow-tie analysis, and an FSA-informed decision structure provided complementary information in the present study, but the process may become increasingly resource intensive as the number of systems, hazards, and accident pathways increases. Future studies should examine whether the full combination of methods is required for every part of the assessment. This could be tested by applying the methods to specific hazards or systems and comparing the resulting findings. Where one method provides the same relevant safety and design insights without loss of important information, a more focused assessment approach may be sufficient. This would help determine where the combined methodology provides added value and where a simpler method could be used instead.

The same applies to safeguard assessment. More explicit criteria could be developed for when a safeguard may reduce the Frequency Index, how common dependencies should be treated, and when apparently redundant barriers can be considered sufficiently independent.

Finally, the methodology should be applied to other vessel types, reactor technologies, and power conversion arrangements. This would show which parts of the process are generally applicable and which design conclusions are specific to the reference vessel used in this thesis.

Development towards quantitative assessment

The risk ranking used in this study was qualitative and ordinal. The Severity and Frequency Indices supported comparison between scenarios and design states but do not represent calculated accident frequencies or consequences.

The three Bow-ties could be developed further using FTA and ETA, supported by validated reliability data, and common cause failure modeling.

This would provide a natural next stage for the methodology, qualitative methods could continue to

be used for broad hazard identification and design development, while selected risk pathways are developed quantitatively when sufficient design information becomes available.

Verification of the design recommendations

The recommendations developed in Chapter 8 were assessed according to their intended safety function rather than through detailed engineering calculations. Their implementation in REVB therefore demonstrates how risk findings can influence the vessel design, but it does not prove that the proposed systems will meet all required safety performance criteria.

Further design work should verify the segregated cooling arrangements, pressure relief and contamination management systems, electrical distribution, emergency power supply, seawater discharge monitoring, and remote monitoring and access arrangements. This would require system calculations, equipment specifications, control logic, structural assessment, and radiological analysis.

Regulatory and operational development

The study does not constitute a formal ALARP demonstration. Cost effectiveness was not evaluated, and the methodology was not reviewed by maritime or nuclear authorities.

Future work should therefore examine how the proposed process could fit within an approval and safety case framework. Review by class societies, flag Administrations, nuclear regulators, reactor vendors, operators, and port authorities would help determine what additional evidence is required at later design stages.

Human and organizational factors should also receive greater attention as the concept develops. Staffing, training, alarm management, maintenance, emergency decision making, and communication with shore based support may become important parts of the accident response and should be included in later applications of the methodology.

Overall, the next stage of the research should focus on making the methodology more repeatable, less dependent on individual judgment, and suitable for progressively more detailed analysis. The main value of the present study is the traceable link from hazard identification to barrier assessment, design change, and reassessment. Future work can build on this process as the vessel design and available safety evidence become more mature.

9.3. Personal Reflection

Completing this thesis was not a linear process. Throughout the research, I gradually became aware of several mistakes in the way I had initially defined, structured, and executed the work. Some of these mistakes could be corrected as my understanding improved. Others had already influenced later decisions and therefore had to be accepted and managed because returning to the beginning was no longer realistic within the available time. This was sometimes frustrating, but it became one of the most valuable lessons of the project. Research does not always progress through a sequence of correct decisions. It also involves recognizing the consequences of earlier choices, understanding which aspects can still be improved, and continuing in a transparent and defensible manner when complete correction is no longer possible.

Looking back, I can now identify several alternative approaches that could have been used to address the research question. With the knowledge I gained during the project, I would probably not follow exactly the same path if I were beginning the research again. The scope could have been narrowed earlier, the assessment boundaries could have been defined more precisely from the beginning, and greater emphasis could have been placed on validating the methodology before expanding the HAZID and Bow-tie analyses. However, this judgment is only possible because I completed the process and experienced its difficulties. The path followed was personally challenging and at times overwhelming, but it forced me to develop knowledge across nuclear safety, ship design, risk assessment, and system integration.

The final results may be less conclusive than I originally hoped. The research does not demonstrate that the reference vessel is safe, nor does it validate the proposed methodology as a complete safety assessment framework. Instead, it demonstrates a structured way of moving from hazard identification

to escalation path analysis, design recommendations, and reassessment. I believe that this process has potential, but its potential cannot be established convincingly through one individual MSc project. A much stronger test would require a multidisciplinary team to apply the methodology collectively and determine how far it can be developed.

Such a team should include, at minimum, expertise in naval architecture, nuclear engineering, electrical systems, thermal hydraulics, radiological protection, human factors, ship operation, risk analysis, and regulatory assessment. Each specialist would be able to challenge assumptions that may appear reasonable from the perspective of another discipline but are incomplete or technically unrealistic. Repeating the process through structured workshops would also provide stronger validation of the identified hazards, risk rankings, safeguards, and design recommendations. I therefore see this thesis less as a finished framework and more as a possible starting structure that should be tested, criticized, and refined by people with different areas of expertise.

Before starting the thesis, my perception of nuclear power was strongly influenced by the way nuclear technology is commonly presented in the news and in society. Growing up, words such as nuclear, radiation, and atomic were usually associated with catastrophic accidents, weapons, contamination, and large scale destruction. I therefore expected the greatest difficulty in nuclear shipping to be the technical challenge of designing a power plant that could remain safe at sea.

The research changed this perception. Nuclear systems clearly introduce serious hazards, and their potential consequences demand exceptional engineering discipline. However, I no longer believe that constructing a technically safe nuclear powered vessel will necessarily be the greatest obstacle. The more difficult challenge may be convincing regulators, port authorities, operators, seafarers, and the general public that such a vessel is sufficiently safe to operate within normal commercial society. Technical safety and perceived safety are not the same. A vessel may satisfy demanding engineering criteria, but commercial operation would remain impossible without public trust, regulatory legitimacy, port access, institutional responsibility, and confidence in emergency preparedness.

This does not mean that public concern should simply be dismissed as irrational. Nuclear technology carries consequences that justify scrutiny. Public confidence must therefore be earned through transparency, independent review, operational evidence, clear communication, and credible responsibility for the full life cycle of the technology. In my opinion, the burden lies on the designers and operators to demonstrate safety in a form that can be understood and trusted, rather than expecting society to accept technical claims without sufficient evidence.

My view of nuclear power as a possible contributor to maritime decarbonization has nevertheless become more positive. Nuclear energy is one of several zero carbon energy options with the potential to support future shipping, particularly for vessels requiring high power, long endurance, and limited dependence on frequent refueling. At the same time, describing it as promising does not mean that it is ready for widespread commercial implementation. Substantial research remains necessary in areas including reactor integration, accident response, regulation, port operation, waste management, decommissioning, economics, and public acceptance.

During the literature review, I also developed the impression that the publicly available information represents only part of the knowledge that may exist in this field. Nuclear technology has considerable strategic, commercial, and security significance. It is therefore possible that relevant industrial, governmental, or military research remains confidential, commercially restricted, or classified. This is a personal interpretation rather than a conclusion demonstrated by the present research. Nevertheless, the limited availability of detailed information affected the project and reinforced the importance of distinguishing between knowledge that does not exist and knowledge that is simply inaccessible to an individual researcher.

This idea also led me to reflect on the relationship between knowledge, technological capability, and power. Friedrich Nietzsche wrote:

“What is good? All that heightens the feeling of power, the will to power, power itself in man. What is bad? All that proceeds from weakness. What is happiness? The feeling that power increases—that a resistance is overcome. Not contentment, but more power; not peace at

all, but war.”

— Friedrich Nietzsche

I do not interpret this quotation as an endorsement of conflict or as an argument for pursuing nuclear technology without restraint. Instead, I relate it to the human desire to overcome limitations, increase knowledge, and confront challenges that initially appear beyond our capabilities. Nuclear energy is perhaps one of the clearest examples of this tension. It demonstrates humanity’s ability to understand and control an extraordinary source of energy, but it also demonstrates how technological power creates an equally significant responsibility. The ability to develop a technology does not automatically justify its application. Its use must be accompanied by ethical judgment, appropriate regulation, transparency, and an understanding of the consequences if that power is mismanaged.

The quotation also reflects my personal experience during the thesis. The satisfaction I gained from the project did not come from reaching a simple or fully conclusive answer. It came from gradually overcoming the resistance created by unfamiliar technical subjects, incomplete information, methodological difficulties, and mistakes made during the research process. In this sense, the thesis increased my capability as an engineer. However, it also taught me that engineering strength should not be understood only as the ability to create increasingly powerful systems. It should also include the discipline to recognize uncertainty, acknowledge limitations, question one’s own decisions, and apply technological capability responsibly.

The most important personal lesson from the project concerns teamwork. Attempting to develop the vessel concept, HAZID, Bow-ties, risk ranking system, design recommendations, and design iterations largely as one integrated individual exercise made the scale of multidisciplinary engineering very clear. Working independently gave me ownership of the complete process and forced me to understand the connections between its different parts. However, it also limited the depth with which each part could be examined and increased the possibility that assumptions or inconsistencies would remain unchallenged.

I now understand more clearly that teamwork is not only a means of dividing workload. Its greater value lies in combining different perspectives. A reactor engineer, naval architect, electrical engineer, ship operator, and safety analyst will not interpret the same accident pathway in exactly the same way. These differences can reveal missing hazards, unrealistic safeguards, hidden dependencies, and practical constraints that one person may overlook. A capable team can therefore progress not only faster, but also more critically and with stronger technical confidence.

For this reason, my principal recommendation to future students undertaking similarly broad research is to seek multidisciplinary collaboration as early as possible. Even when the thesis itself must remain an individual submission, the research process can benefit greatly from structured discussions, expert workshops, peer review, and regular challenge from people with different technical backgrounds. The aim should not be to eliminate disagreement, but to use disagreement to test the quality of the analysis.

Ultimately, this thesis taught me that meaningful engineering progress often comes from overcoming uncertainty, revising earlier beliefs, and continuing despite imperfect decisions. The achievement is not that every decision made during the research was correct. It is that the process allowed me to recognize where the work was weak, understand why those weaknesses developed, and identify how a stronger future study could address them. The thesis has therefore changed both my perception of nuclear shipping and my understanding of myself as an engineer. I leave the project more convinced of the potential of nuclear propulsion, but also more aware that real progress will depend on technical humility, multidisciplinary cooperation, transparent evidence, and the ability to earn public trust.

References

1. Ministerie van Economische Zaken en Klimaat, Ministerie van Infrastructuur en Waterstaat, Ministerie van Financiën, Ministerie van Buitenlandse Zaken, and Ministerie van Defensie. No guts, no Hollands Glorie! - sectoragenda maritieme maakindustrie. Den Haag, 2023 Oct 26. Available from: <https://open.overheid.nl/documenten/700c6d90-4922-4ad5-ab4c-448853015fee/file>
2. European Commission. Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions: The European Green Deal. COM(2019) 640 final. 2019 Dec 11. Available from: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2019:640:FIN>
3. International Maritime Organization. Code of Safety for Nuclear Merchant Ships. Assembly resolution A.491(XII). London: International Maritime Organization, 1981 Nov 19. Available from: <https://wwwcdn.imo.org/localresources/en/KnowledgeCentre/IndexofIMOResolutions/AssemblyDocuments/A.491%2812%29.pdf>
4. European Atomic Energy Community, Food and Agriculture Organization of the United Nations, International Atomic Energy Agency, International Labour Organization, International Maritime Organization, OECD Nuclear Energy Agency, Pan American Health Organization, United Nations Environment Programme, and World Health Organization. Fundamental Safety Principles. SF-1. Safety Fundamentals. Vienna: International Atomic Energy Agency, 2006
5. Lloyd's Register. Navigating nuclear energy in maritime. Research report. 2025 Oct 16. Available from: <https://www.lr.org/en/knowledge/research-reports/2025/navigating-nuclear-energy-in-maritime/>
6. American Bureau of Shipping. Requirements for Nuclear Power Systems for Marine and Offshore Applications. Spring, TX, 2024 Oct. Available from: https://ww2.eagle.org/content/dam/eagle/rules-and-guides/current/special_service/346-requirements-for-nuclear-power-systems-for-marine-and-offshore-applications-2024/346-nuclear-power-systems-reqts-oct24.pdf
7. DNV. Maritime nuclear propulsion: Technologies, commercial viability, and regulatory challenges for nuclear-powered vessels. White paper. Høvik, Norway, 2025 Oct 21. Available from: <https://www.dnv.com/maritime/publications/maritime-nuclear-propulsion-download/>
8. Russian Maritime Register of Shipping. Rules for the Classification and Construction of Nuclear Ships and Floating Facilities. ND No. 2-020101-168-E. St. Petersburg, 2022. Available from: <https://lk.rs-class.org/regbook/getDocument2?d=431C510B-642D-490B-AF53-2686C73C122D&f=&type=rules3>
9. Houtkoop KCF. Nuclear reactors for marine propulsion and power generation systems. Marine Technology, Marine Engineering. Master's thesis. Delft: Delft University of Technology, 2022 Jul 6. Available from: <https://resolver.tudelft.nl/uuid:fb44c464-6936-4ec6-96b1-52333ff799e3>
10. De Sanctis E, Monti S, and Ripani M. Energy from Nuclear Fission: An Introduction. Undergraduate Lecture Notes in Physics. Cham: Springer International Publishing, 2016. DOI: 10.1007/978-3-319-30651-3. Available from: <https://link.springer.com/book/10.1007/978-3-319-30651-3>
11. Journée D. Helium bubbling in a Molten Salt Fast Reactor: A flotation process. Master's thesis. Delft: Delft University of Technology, 2014 Jan. Available from: https://www.janleenkloosterman.nl/reports/thesis_journee_2014.pdf

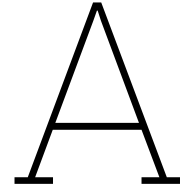
12. Bays SE, Abou Jaoude A, and Borlodon G. Reactor Fundamentals Handbook. INL/EXT-19-53301-Rev000. OSTI ID: 1615634. Idaho Falls, ID: Idaho National Laboratory, 2019 Apr 1. DOI: 10.2172/1615634. Available from: <https://www.osti.gov/biblio/1615634>
13. International Atomic Energy Agency. Design of the Reactor Core for Nuclear Power Plants. Specific Safety Guide SSG-52. STI/PUB/1859. Vienna, 2019. Available from: https://www-pub.iaea.org/MTCD/Publications/PDF/PUB1859_web.pdf
14. Japan Atomic Energy Agency. Evaluation of Thermal Properties of High Burnup MOX Fuel for LWRs - Thermal Conductivity Change in MOX Pellets Due to Long-Term Use -. JAEA R&D Review 2010, Section 6-2. 2010. Available from: https://rdreview.jaea.go.jp/review_en/2010/e2010_6_2.html
15. U.S. Nuclear Regulatory Commission. Pressurized Water Reactors. 2023 Feb 9. Available from: <https://www.nrc.gov/reactors/power/pwrs>
16. American Bureau of Shipping. Pathways to a Low Carbon Future: Floating Nuclear Power Plant. White paper. In partnership with Herbert Engineering Corporation. Spring, TX, 2024. Available from: <https://ww2.eagle.org/content/dam/eagle/publications/whitepapers/pathways-to-low-carbon-fnpp.pdf>
17. OECD Nuclear Energy Agency. Investing in Trust: Nuclear Regulators and the Public. Workshop proceedings NEA#3062. Workshop proceedings, Paris, France, 29 November–1 December 2000. Paris, 2001 May 16. Available from: <https://www.oecd-neo.org/upload/docs/application/pdf/2019-12/3062-investing-in-trust.pdf>
18. International Atomic Energy Agency. Small Modular Reactors: Advances in SMR Developments 2024. IAEA/PAT/008. Vienna, 2024. DOI: 10.61092/iaea.3o4h-svum. Available from: https://www-pub.iaea.org/MTCD/Publications/PDF/p15790-PUB9062_web.pdf
19. The Merchant Shipping (Nuclear Ships) Regulations 2022. SI 2022/1169. Laid before Parliament 2022-11-16; in force 2022-12-08. 2022 Nov 15. Available from: <https://www.legislation.gov.uk/ukxi/2022/1169>
20. Valiaveedu A, Edmonds N, and Izurieta J. Nuclear Ship Safety Handbook. MIT Maritime Consortium, 2025 Sep. Available from: <https://hdl.handle.net/1721.1/163117>
21. Holbert KE. A Review of Maritime Nuclear Reactor Systems. Journal of Nuclear Engineering. 2025 Feb 5; 6:5. DOI: 10.3390/jne6010005. Available from: <https://www.mdpi.com/2673-4362/6/1/5>
22. Yoo YH, Jeong HK, Park W, Kim SH, and Jeong YH. Study on the seawater cooled PRHRS of a nuclear propulsion ship with the upper heat exchanger for driving force and the seawater heat exchanger as an ultimate heat sink. International Journal of Naval Architecture and Ocean Engineering. 2024; 16:100588. DOI: 10.1016/j.ijnaoe.2024.100588. Available from: <https://www.sciencedirect.com/science/article/pii/S2092678224000074>
23. Yoo S, Lee W, and Lee KY. A Conceptual Design of Supercritical CO₂ Brayton Cycle for a Small Modular Molten Salt Reactor. *Transactions of the Korean Nuclear Society Spring Meeting*. May 18–20, 2022. Korean Nuclear Society. Jeju, Korea, 2022 May. Available from: https://www.kns.org/files/pre_paper/47/22S-366-%EC%9C%A0%EC%84%B1%ED%98%84.pdf
24. International Atomic Energy Agency. Safety of Nuclear Power Plants: Design. SSR-2/1 (Rev. 1). Vienna, 2016. Available from: <https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1715web-46541668.pdf>
25. International Atomic Energy Agency. Design of Electrical Power Systems for Nuclear Power Plants. Specific Safety Guide SSG-34. Vienna, 2016. Available from: <https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1673web-53477409.pdf>
26. International Atomic Energy Agency. Safety of Nuclear Power Plants: Design. Specific Safety Requirements SSR-2/1 (Rev. 1). Vienna, 2016. Available from: <https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1715web-46541668.pdf>
27. OECD Nuclear Energy Agency. Defence in Depth of Electrical Systems and Grid Interaction. Tech. rep. CSNI-R-2009-10. Paris, 2009. Available from: <https://www.oecd-neo.org/upload/docs/application/pdf/2021-03/csni-r2009-10.pdf>

28. International Atomic Energy Agency. Application of the Principle of Defence in Depth in Nuclear Safety to Small Modular Reactors: Addendum to INSAG-10. 28. STI/PUB/2094. Vienna, 2024. DOI: 10.61092/iaea.w9s3-1k5y. Available from: https://www-pub.iaea.org/MTCD/Publications/PDF/p15676-PUB2094_web.pdf
29. International Atomic Energy Agency. Radiation Protection and Safety of Radiation Sources: International Basic Safety Standards. GSR Part 3. STI/PUB/1578. Co-sponsored by EC/Euratom, FAO, ILO, OECD/NEA, PAHO, UNEP and WHO. Vienna, 2014. DOI: 10.61092/iaea.u2pu-60vm. Available from: <https://www.iaea.org/publications/8930/radiation-protection-and-safety-of-radiation-sources-international-basic-safety-standards>
30. International Atomic Energy Agency. Radiation Protection Aspects of Design for Nuclear Power Plants. Specific Safety Guide SSG-90. STI/PUB/2078. Vienna, 2024. DOI: 10.61092/iaea.jc6f-diaa. Available from: https://www-pub.iaea.org/MTCD/Publications/PDF/p15554-PUB2078_web.pdf
31. International Atomic Energy Agency. Environmental and Source Monitoring for Purposes of Radiation Protection. Safety Guide RS-G-1.8. Vienna, 2005. Available from: https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1216_web.pdf
32. International Maritime Organization. International Code for the Safe Carriage of Packaged Irradiated Nuclear Fuel, Plutonium and High-Level Radioactive Wastes on Board Ships (INF Code). MSC.88(71). Effective 2001-01-01; as amended. London, 1999 May 27
33. International Maritime Organization. SOLAS: Consolidated Edition, 2024. London: International Maritime Organization, 2024 Sep. DOI: 10.62454/KH110E
34. International Atomic Energy Agency. Safety Assessment for Facilities and Activities. General Safety Requirements GSR Part 4 (Rev. 1). STI/PUB/1714. Vienna, 2016. Available from: <https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1714web-7976998.pdf>
35. Office for Nuclear Regulation. Safety Assessment Principles for Nuclear Facilities. Version Revision 1. 2020 Jan. Available from: <https://www.onr.org.uk/media/pobf24xm/saps2014.pdf>
36. International Maritime Organization. Revised Guidelines for Formal Safety Assessment (FSA) for Use in the IMO Rule-Making Process. MSC-MEPC.2/Circ.12/Rev.2. London, 2018 Apr 9. Available from: <https://wwwcdn.imo.org/localresources/en/OurWork/HumanElement/Documents/MS-C-MEPC.2-Circ.12-Rev.2-20-Revised-Guidelines-For-Formal-Safety-Assessment-28Fsa-29For-20Use-In-20The-20Imo-20Rule-Making-20Proces...-20-28Secretariat-29.pdf>
37. Simmons DC, Dauwe R, Gowland R, Gyenes Z, King AG, Riedstra D, and Schneiderbauer S. Qualitative and quantitative approaches to risk assessment. *Science for disaster risk management 2017: knowing better and losing less*. Ed. by Poljanšek K, Marín Ferrer M, De Groeve T, and Clark I. EUR 28034 EN. Luxembourg: Publications Office of the European Union, 2017. Chap. 2.1. DOI: 10.2788/688605. Available from: https://drmkc.jrc.ec.europa.eu/portals/0/Knowledge/ScienceforDRM/ch02/ch02_subch0201.pdf
38. International Maritime Organization. Guidelines for the Approval of Alternatives and Equivalents as Provided for in Various IMO Instruments. MSC.1/Circ.1455. Accessible copy via Netherlands Regulatory Framework (NeRF) – Maritime. London, 2013 Jun 24. Available from: https://puc.overheid.nl/nsi/doc/PUC_2017_14/
39. Risktec Solutions Limited. So What is ALARP? RISKworld newsletter article Issue 4. Autumn 2003. 2003. Available from: <https://risktec.tuv.com/wp-content/uploads/2018/09/so-what-is-alarp.pdf>
40. Kim K, Kang H, and Kim Y. Risk assessment for natural gas hydrate carriers: a hazard identification (HAZID) study. *Energies*. 2015 Apr 20; 8:3142–64. DOI: 10.3390/en8043142. Available from: <https://www.mdpi.com/1996-1073/8/4/3142>

41. Diacakis M, Damianidou Y, Sakai R, Yoshida Y, Pedersen OHK, Moon KT, Ramli H, Lee R, and Rygh BM. Guidelines for conducting qualitative risk assessments for alternative-fuelled ships: HAZID and HAZOP. Guidelines. Report dated October 2025; published on MTF website 2025-11-12. Maritime Technologies Forum, 2025 Oct. Available from: https://www.maritimetechnologiesforum.com/documents/202511_MTF_Guidelines_for_conducting_qualitative_risk_assessments.pdf
42. U.S. Army Corps of Engineers, Institute for Water Resources. Risk Assessment - Quantitative Methods. Training module. 2018 Jul. Available from: https://www.iwr.usace.army.mil/Portals/70/docs/risk/Risk_Assessment_Quantitative_Methods_dft.pdf
43. International Atomic Energy Agency. Deterministic Safety Analysis for Nuclear Power Plants. Specific Safety Guide SSG-2 (Rev. 1). STI/PUB/1851. Vienna, 2019. Available from: https://www-pub.iaea.org/MTCD/Publications/PDF/PUB1851_web.pdf
44. International Atomic Energy Agency. Probabilistic safety assessment. Basic Professional Training Course on Nuclear Safety, Module VII, v1.0. 2015 May. Available from: <https://gnssn.iaea.org/main/bptc/BPTC%20Module%20Documents/Module07%20Probabilistic%20safety%20assessment.pdf>
45. American Bureau of Shipping. Guidance Notes on Risk Assessment Applications for the Marine and Offshore Industries. Guidance Notes. Spring, TX, 2020 May. Available from: https://ww2.eagle.org/content/dam/eagle/rules-and-guides/current/other/97_riskassessapplmari neandoffshoreandg/risk-assessment-gn-may20.pdf
46. Ruijter A de and Guldenmund F. The bowtie method: A review. Safety Science. 2016; 88:211–8. DOI: 10.1016/j.ssci.2016.03.001. Available from: <https://www.sciencedirect.com/science/article/abs/pii/S0925753516300078>
47. American Bureau of Shipping. Guidance Notes on Failure Mode and Effects Analysis (FMEA) for Classification. Guidance Notes. Spring, TX, 2015 May. Available from: https://ww2.eagle.org/content/dam/eagle/rules-and-guides/current/design_and_analysis/215_fmea/FMEA_GN_e-Mar18.pdf
48. U.S. Department of Defense. Military Standard: Procedures for Performing a Failure Mode, Effects and Criticality Analysis. MIL-STD-1629A. Canceled 1998-08-04. Washington, DC, 1980 Nov 24. Available from: https://quicksearch.dla.mil/qsDocDetails.aspx?ident_number=37027
49. Generation IV International Forum. Very High Temperature Reactor (VHTR). Available from: https://www.gen-4.org/gif/jcms/c_40801/very-high-temperature-reactor-vhtr
50. European Maritime Safety Agency. Potential use of nuclear power for shipping. Technical report. Lisbon, Portugal, 2024 Dec 5. Available from: <https://www.emsa.europa.eu/publications/item/5366-potential-use-of-nuclear-power-for-shipping.html>
51. Mosleh A, Rasmuson DM, and Marshall FM. Guidelines on Modeling Common-Cause Failures in Probabilistic Risk Assessment. NUREG/CR-5485. Idaho Falls, ID: Idaho National Engineering and Environmental Laboratory, 1998 Nov. Available from: https://nrc.nrel.gov/publicdocs/CCF/NUREGCR-5485_Guidelines%20on%20Modeling%20Common-Cause%20Failures%20in%20PRA.pdf
52. International Atomic Energy Agency. Case Study on the Use of PSA Methods: Determining Safety Importance of Systems and Components at Nuclear Power Plants. IAEA-TECDOC-590. Vienna, 1991. Available from: <https://www.iaea.org/publications/846/case-study-on-the-use-of-psa-methods-determining-safety-importance-of-systems-and-components-at-nuclear-power-plants>
53. Drouin M, Gilbertson A, Parry G, Lehner J, Martinez-Guridi G, LaChance J, and Wheeler T. Guidance on the Treatment of Uncertainties Associated with PRAs in Risk-Informed Decisionmaking. NUREG staff report NUREG-1855. Version Revision 1. Washington, DC: Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 2017 Mar. Available from: <https://www.nrc.gov/reading-rm/doc-collections/nuregs/staff/sr1855/r1/index.html>
54. International Atomic Energy Agency. Safety Culture. STI/PUB/882. INSAG-4; IAEA Safety Series No. 75-INSAG-4. Vienna, 1991. Available from: <https://www.iaea.org/publications/3753/safety-culture>

55. International Atomic Energy Agency. Safety of Nuclear Power Plants: Commissioning and Operation. Specific Safety Requirements SSR-2/2 (Rev. 1). Vienna, 2016. Available from: <https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1716web-18398071.pdf>
56. World Nuclear Association. Generation IV Nuclear Reactors. 2025 Nov 21. Available from: <https://world-nuclear.org/information-library/nuclear-power-reactors/other/generation-iv-nuclear-reactors>

This page is left blank intentionally.



Supplementary Literature and Method Material

Table A.1: Civilian nuclear powered vessels. [9]

Vessel	Country	Vessel type	Reactor type	Installed power (MW _{th})	Operating period
<i>Savannah</i>	USA	General cargo ship	Babcock&Wilcox PWR	1 × 74	1962–1972
<i>Otto Hahn</i>	Germany	General cargo ship	Babcock&Wilcox Int. Atom. GmbH PWR	1 × 38	1968–1979
<i>Mutsu</i>	Japan	General cargo ship	Mitsubishi PWR	1 × 36	1974–1992
<i>Sevmorput</i>	USSR / Russia	Cargo (LASH/container)	KLT-40 PWR	1 × 135	1988–2007 2016–pres.
<i>Lenin</i>	USSR	Icebreaker	OK-900 PWR	2 × 171	1959–1989
<i>Arktika</i> (1975)	USSR / Russia	Icebreaker	OK-900A PWR	2 × 171	1975–2008
<i>Sibir</i> (1977)	USSR / Russia	Icebreaker	OK-900A PWR	2 × 171	1977–1992
<i>Rossiya</i>	USSR / Russia	Icebreaker	OK-900A PWR	2 × 171	1985–2013
<i>Sovetskiy Soyuz</i>	USSR / Russia	Icebreaker	OK-900A PWR	2 × 171	1989–2014
<i>Taymyr</i>	USSR / Russia	Icebreaker	KLT-40M PWR	1 × 171	1989–pres.
<i>Vaygach</i>	USSR / Russia	Icebreaker	KLT-40M PWR	1 × 171	1990–pres.
<i>Yamal</i>	Russia	Icebreaker	OK-900A PWR	2 × 171	1993–pres.
<i>50 Let Pobedy</i>	Russia	Icebreaker	OK-900A PWR	2 × 171	2007–pres.
<i>Arktika</i> (2020)	Russia	Icebreaker	RITM-200 PWR	2 × 175	2020–pres.
<i>Sibir</i> (2021)	Russia	Icebreaker	RITM-200 PWR	2 × 175	2021–pres.
<i>Ural</i>	Russia	Icebreaker	RITM-200 PWR	2 × 175	2022–pres.
<i>Yakutia</i>	Russia	Icebreaker	RITM-200 PWR	2 × 175	2024–pres.

Table A.2: Key characteristics of advanced reactor concepts [9], [56].

	PWR	(v)HTGR, Pebble bed*	(v)HTGR, Prismatic*	SFR	LFR	GFR	MSR
Coolant	Light water	Helium	Helium	Liquid sodium	Liquid lead or Pb–Bi	Helium	Molten salt (fuel and/or coolant)
Neutron spectrum	Thermal	Thermal	Thermal	Fast	Fast	Fast	Thermal/Fast
Fuel type	U/Pu/Th	U/Pu/Th	U/Pu/Th	U/Pu/Th	U/Pu/Th	U/Pu/Th	U/Pu/Th
Refueling	Offline	Online	Offline	Offline	Offline	Offline	Online/ Offline
Refueling cycle (low end)	1.5–2 y	1.5–2 y	1.5–2 y	1.5–2 y	1.5–2 y	1.5–2 y	1.5–2 y
Refueling cycle (high end)	7–8 y	Continuous	1.5–2 y	Lifetime (20+ y)	Lifetime (20+ y)	Lifetime (20+ y)	Lifetime/ Continuous
Passive safety	+	+	+	+	+	O	+
Active safety	+	+	+	+	+	+	+

Table A.3: PSA levels: scope, modelling focus, and typical outputs [44].

Level	Primary focus	Typical outputs (examples)
Level 1	Accident sequence modeling up to core damage.	Core damage frequency, dominant sequences and cut-sets; importance measures; insights into design and operational weaknesses.
Level 2	Post-core-damage progression, containment and confinement performance, and source term categories.	Containment failure modes; source term exceedance distributions; Large early release frequency.
Level 3	Off-site consequence analysis conditional on source terms, leading to public risk measures.	Probabilistic consequence metrics (population dose, health, and economic endpoints); risk vs criteria; evaluation of emergency measures.

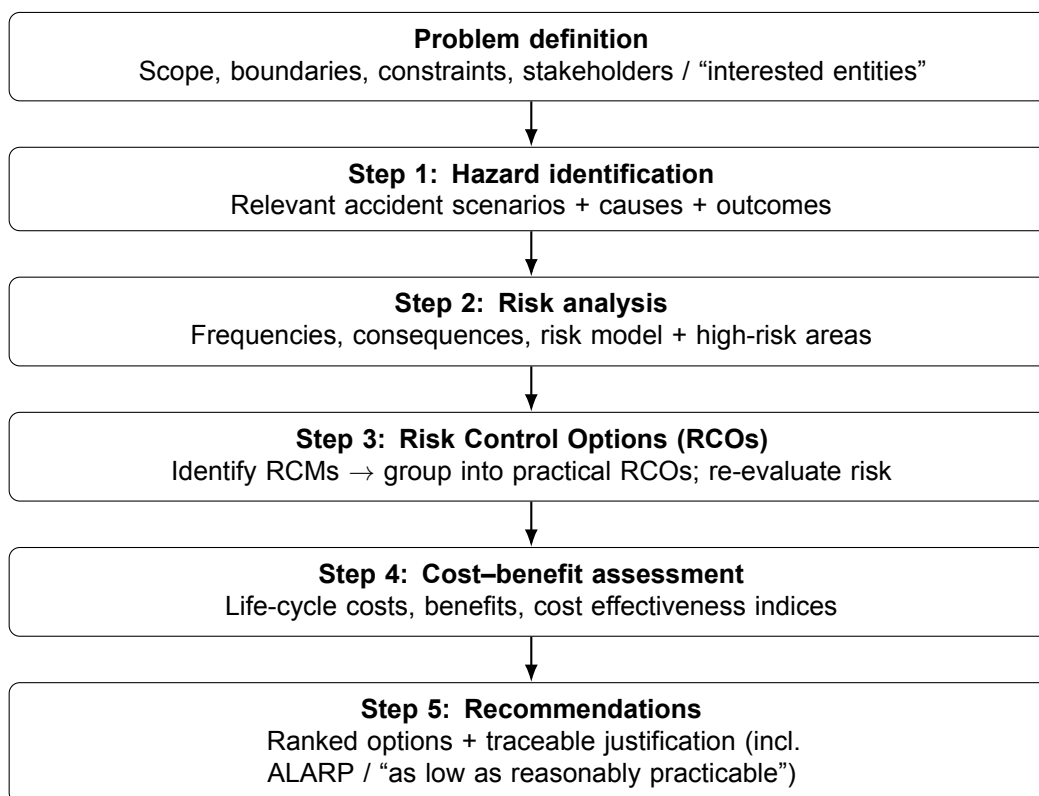


Figure A.1: FSA process structure per IMO FSA Guidelines [36]

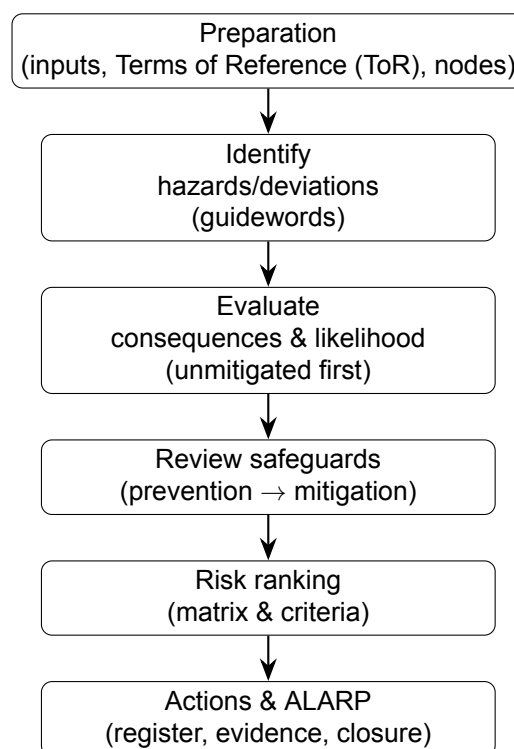


Figure A.2: Standardized QIRA workflow used in HAZID & HAZOP workshops [41].

Risk matrix (Frequency + Severity)

Severity	S4 — Catastrophic	5	6	7	8	9	10	11
	S3 — Severe	4	5	6	7	8	9	10
	S2 — Significant	3	4	5	6	7	8	9
	S1 — Minor	2	3	4	5	6	7	8
		F1	F2	F3	F4	F5	F6	F7
		Extremely remote		Remote		Reasonably probable		Frequent
		Frequency						

Figure A.3: Risk matrix structure and indexing used for HAZID & HAZOP with frequency categories Extremely remote (1) to Frequent (7), adapted from [41].

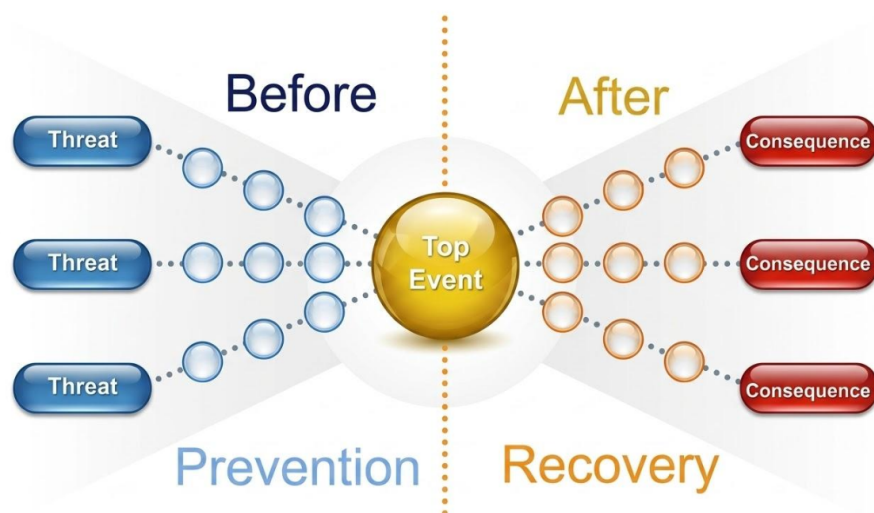


Figure A.4: Generic Bow-tie structure.

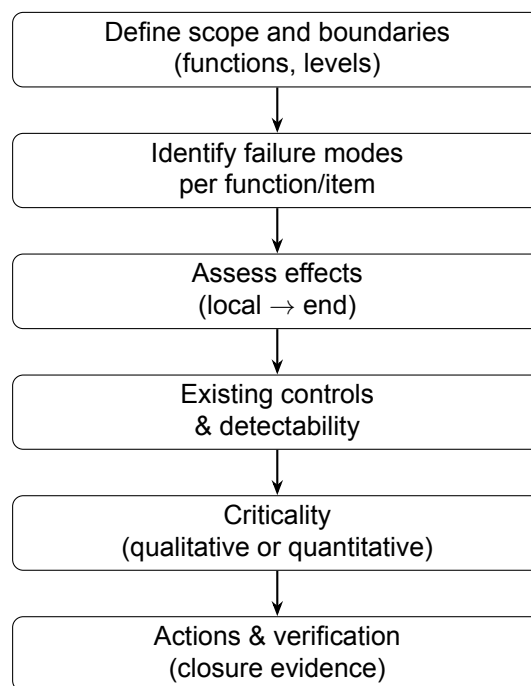


Figure A.5: Typical FMEA & FMECA workflow. [47], [48]

Table A.4: Bow-tie layout notation and symbol explanation

Symbol / notation	Meaning
Cause / threat box	Initiating cause or threat that may lead to the top event if not controlled by preventive barriers.
Top-event box	Central undesired event selected from the HAZID for bow-tie analysis. It represents the loss of control point between causes and consequences.
Consequence box	Outcome that may occur after the top event. Consequences may represent initial, secondary, or final escalation outcomes.
Preventive barrier	Existing safeguard placed between a cause and the top event. Its function is to prevent the top event from occurring or reduce the likelihood of escalation.
Mitigative barrier	Existing safeguard placed after the top event. Its function is to reduce the severity or limit the escalation of consequences.
Active barrier	Safeguard requiring detection, actuation, control logic, powered equipment, or operator-enabled system response to perform its function.
Passive barrier	Safeguard that performs its function through inherent design, physical separation, layout, material properties, structural containment, or thermal inertia without active actuation.
Procedural barrier	Safeguard based on operational procedures, inspection, maintenance, emergency response, access control, or human action.

Symbol / notation	Meaning
Solid arrow from cause to top event	Accident progression pathway showing how an initiating cause can escalate towards the top event.
Solid arrow from top event to consequence	Consequence pathway showing how the top event can lead to an adverse outcome.
Barrier placed across an arrow	Point at which an existing safeguard interrupts, prevents, controls, or mitigates the accident progression pathway.
S-number, e.g. S14	Safeguard reference number linked to the corresponding safeguard entry in the HAZID.
Slash between safeguard references, e.g. S28/S54	More than one safeguard contributes to the same barrier function or is represented at the same point in the bow-tie pathway.
Cause reference number	Reference number linking the bow-tie cause to the corresponding HAZID cause entry.
Consequence reference number	Reference number linking the bow-tie consequence to the corresponding HAZID consequence entry.
Reference arrow in a cause or consequence label, e.g. 1.2.1.1 → 1.2.2.1	Traceability notation showing that one HAZID entry escalates into, continues as, or is represented by another linked HAZID entry.
Multiple consequence references, e.g. 1.2.2.1 + 1.2.2.2	The same bow-tie consequence box represents more than one HAZID consequence entry.
I-number	Initial risk ranking before accounting for existing safeguards.
R-number	Residual risk ranking after accounting for existing safeguards in Iteration 1.
DiD 1	Defence-in-Depth Level 1: prevention of abnormal operation and failures through conservative design, quality, and normal operating controls.
DiD 2	Defence-in-Depth Level 2: control of abnormal operation and detection of failures through monitoring, alarms, control systems, and protective functions.
DiD 3	Defence-in-Depth Level 3: control of accidents within the design basis using safety systems and engineered safety functions.
DiD 4	Defence-in-Depth Level 4: control of severe conditions and prevention of further escalation through additional mitigation measures.
DiD 5	Defence-in-Depth Level 5: emergency response, evacuation, radiological protection, and consequence management measures.

Reference Design and Drawing Revisions

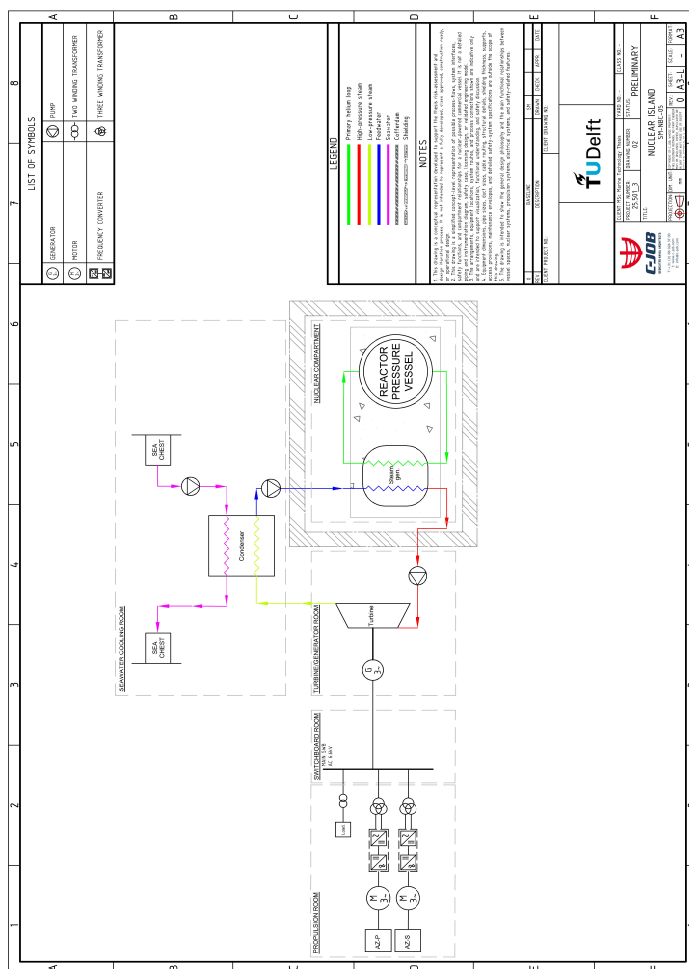


Figure B.1: Reference design drawing of nuclear island

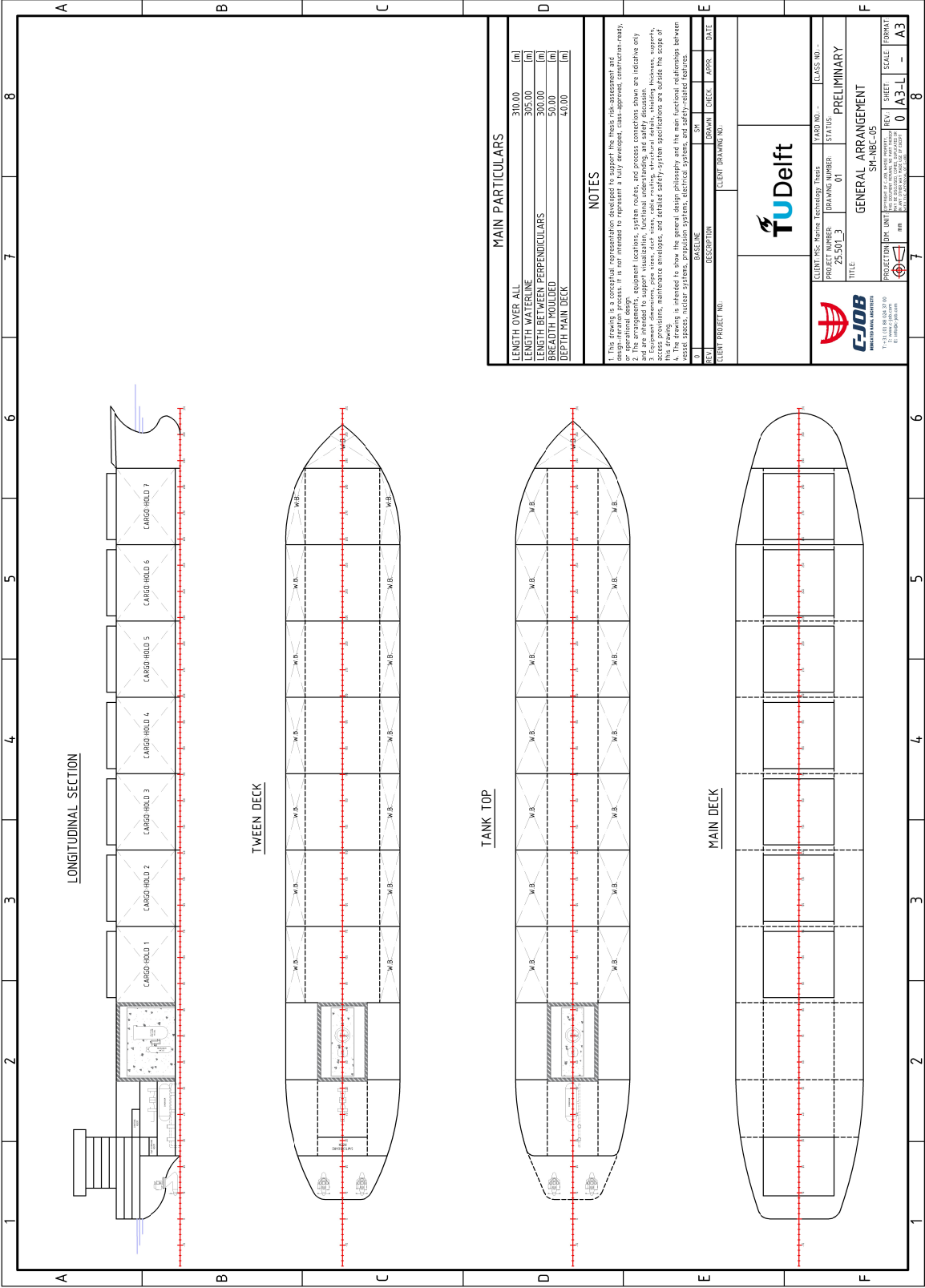


Figure B.2: Reference design drawing of general arrangement

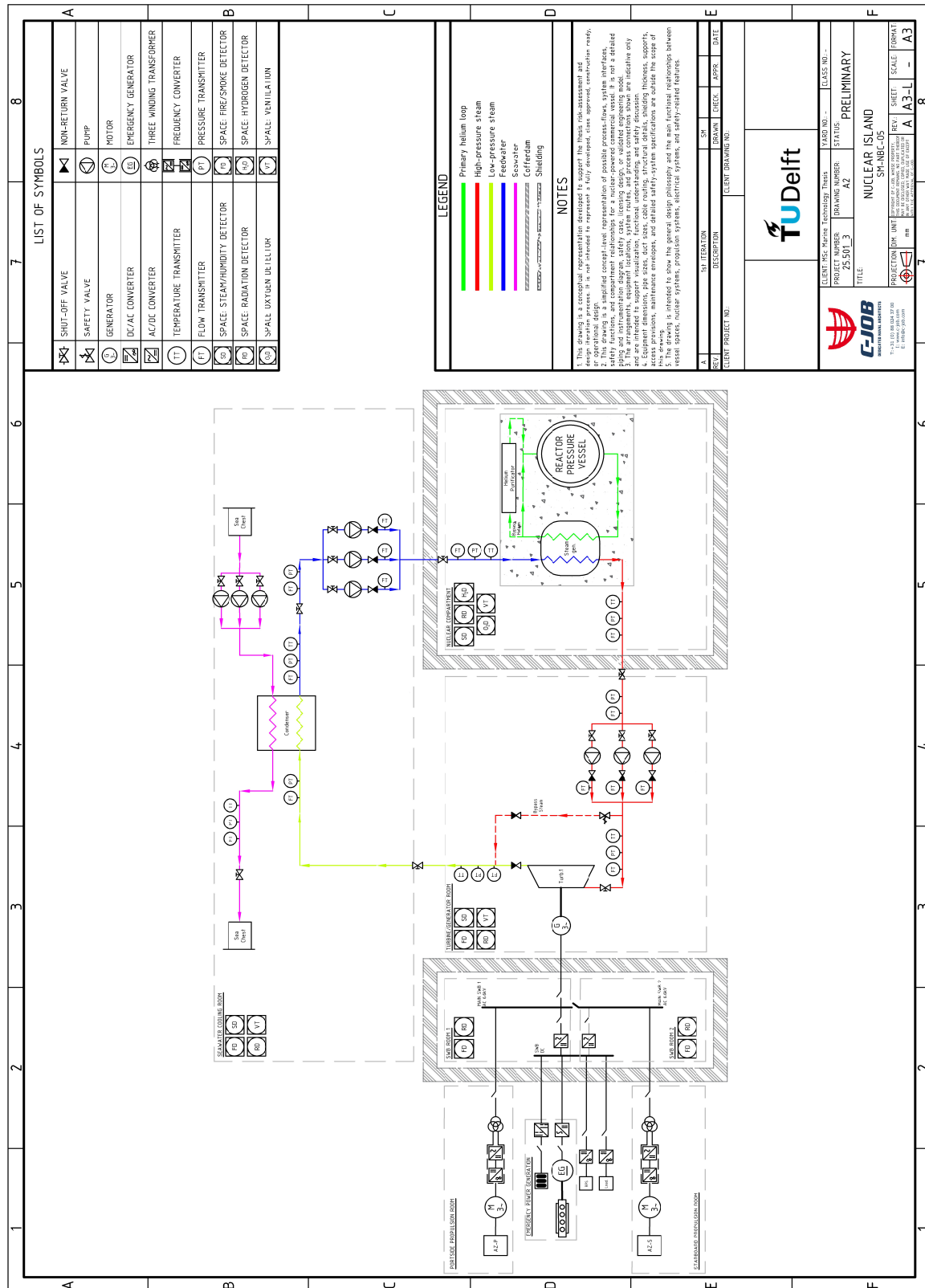


Figure B.3: First iteration design drawing of nuclear island

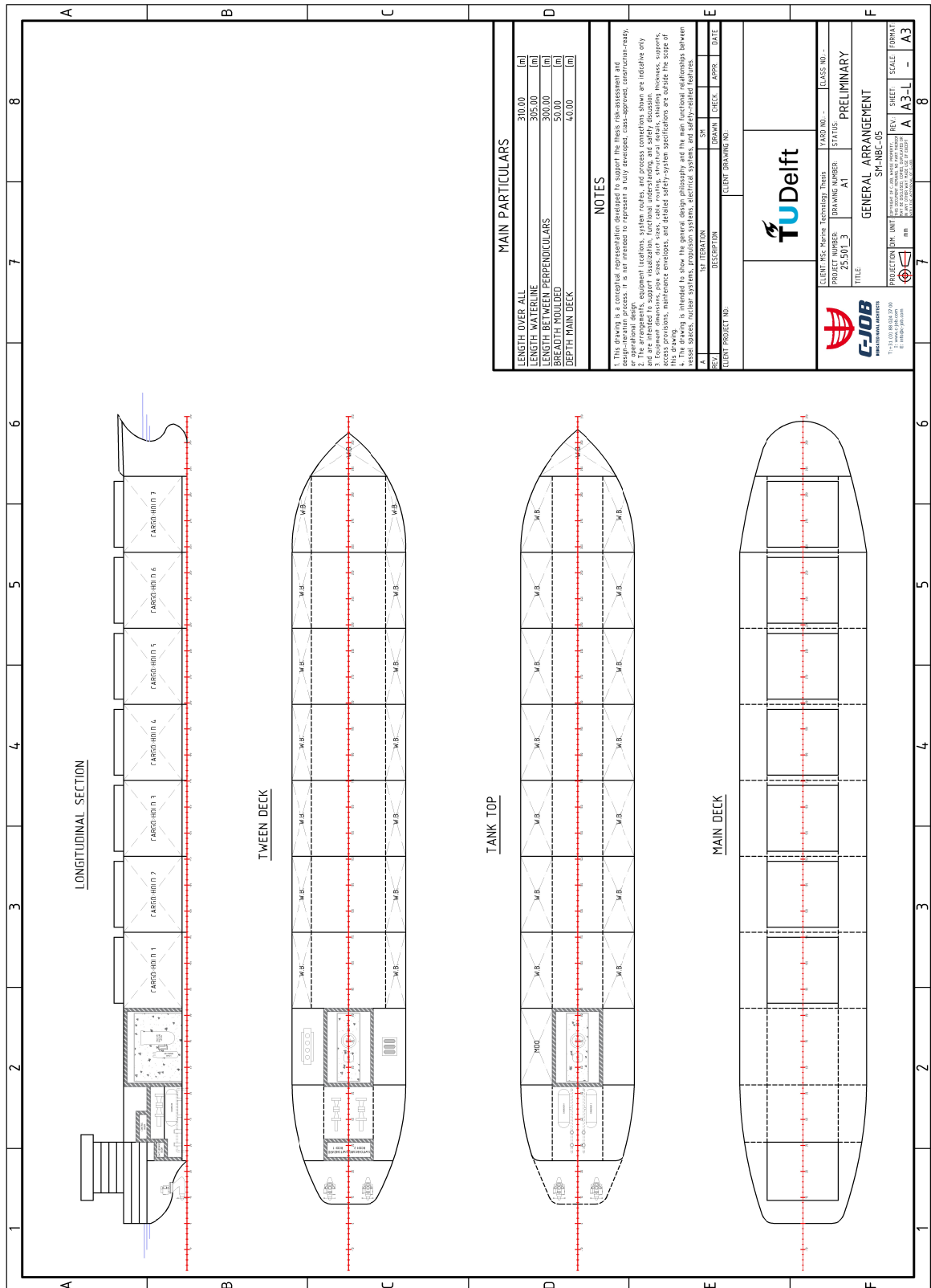


Figure B.4: First iteration design drawing of general arrangement

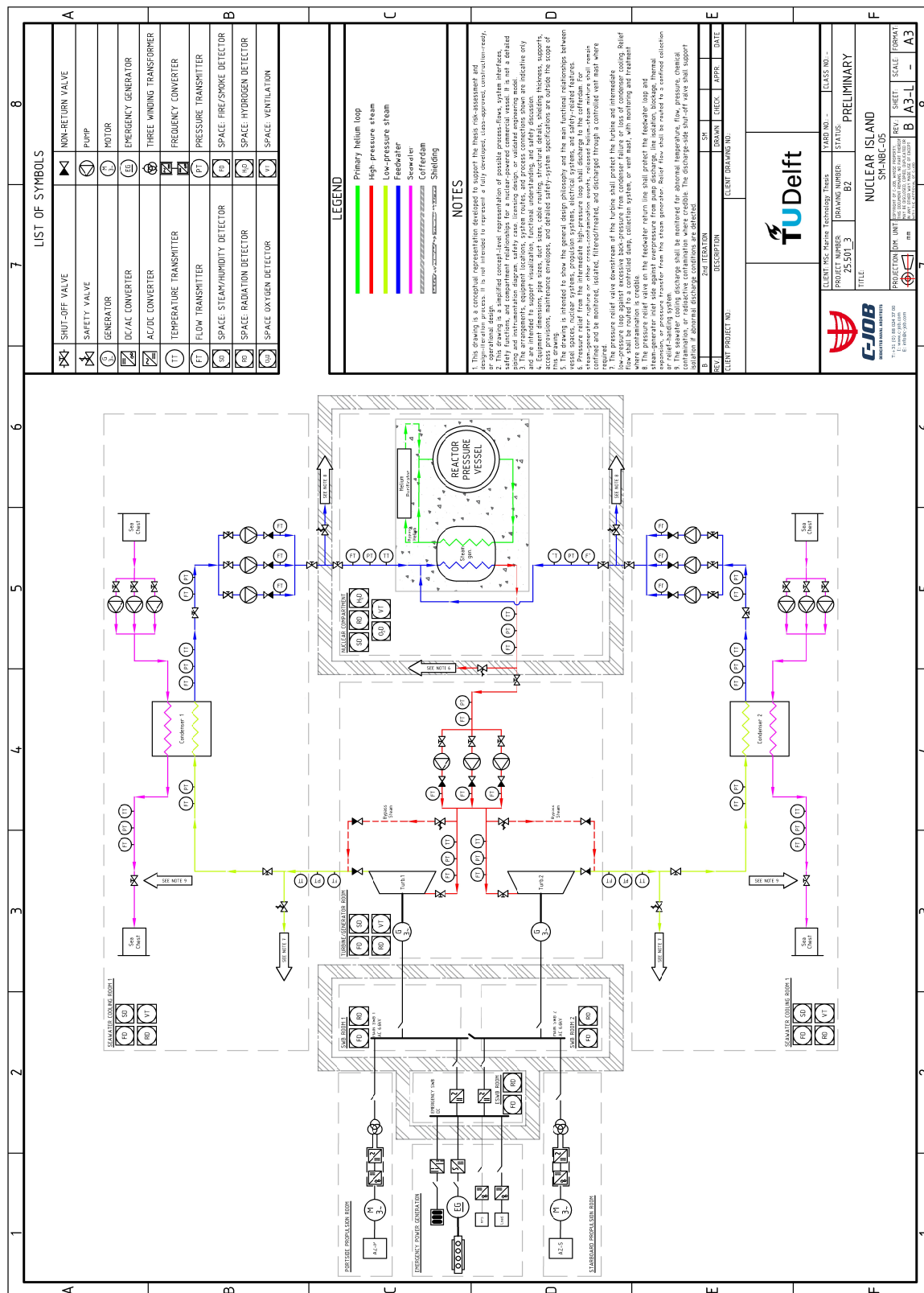


Figure B.5: Final design drawing of nuclear island

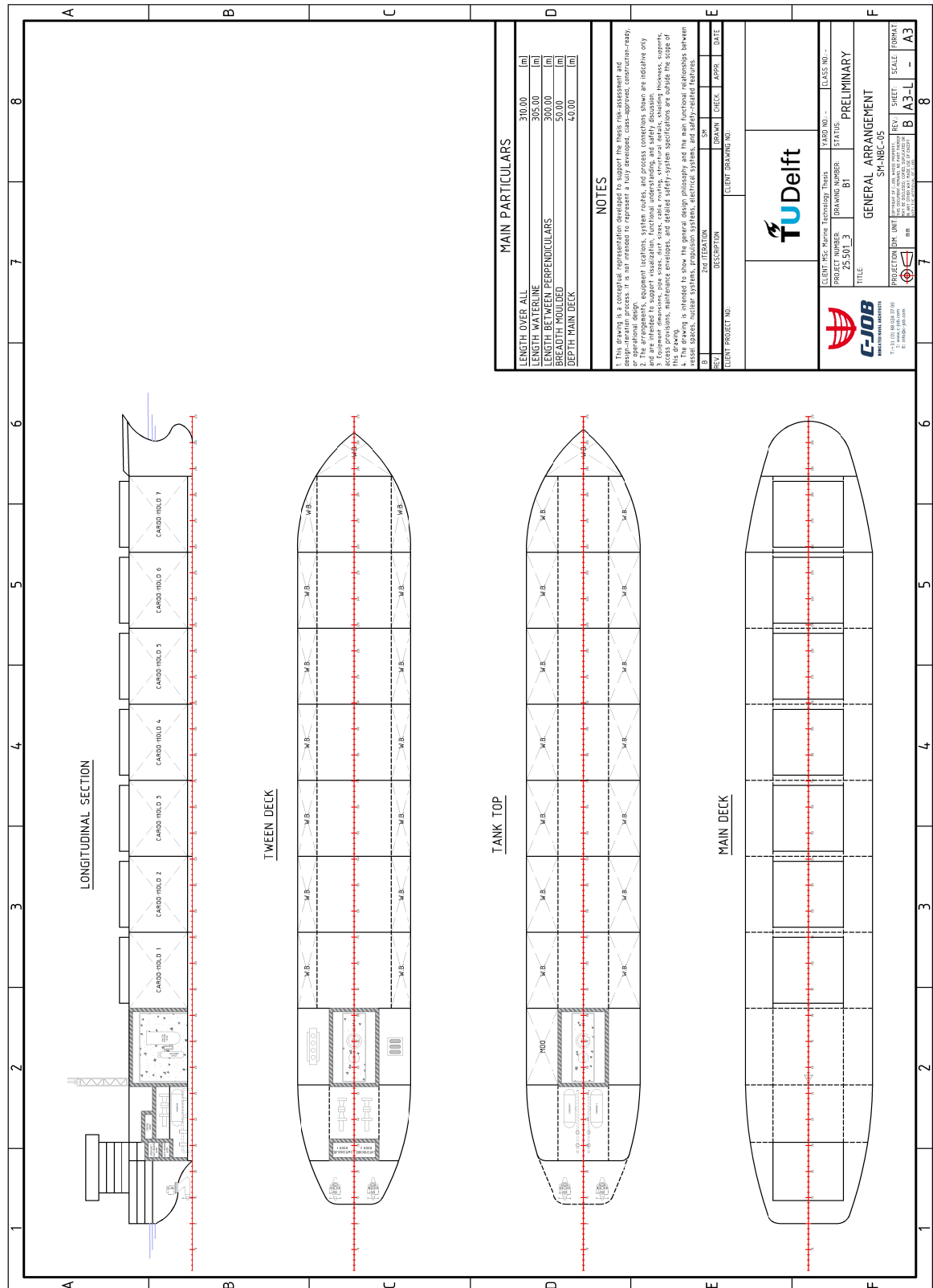


Figure B.6: Final design drawing of general arrangement

C

HAZID Register first iteration

C.1. Node 1: Nuclear compartment

Deviation	Causes		Consequences	CAT	S Before Safeguards	L Before Safeguards	MR Before Safeguards	Safeguards		Type	1	2	3	4	5	6	7	8	9	10		
	Cause	Consequence	Safeguard																			
1.1 Functional performance failure	1.1.1 Uncommanded positive reactivity insertion caused by control-rod withdrawal error, rod drive malfunction, or incorrect reactor protection demand signal.	1.1.1.1 Core power increases above the demanded level and fuel, moderator, and primary helium temperatures begin to rise.																				
		1.1.1.2 Primary helium outlet temperature and loop pressure increase, impairing thermal and pressure stress on the reactor vessel, steam-generator primary side, piping, valves, seals, and penetrations.																				
		1.1.1.3 If the transient is not arrested, automatic reactor trip and decay heat-removal demand occur. Failure of these functions can lead to excessive fuel temperatures and potential fission-product release from cooled fuel particles.	S	4	2	6		34 Active residual heat-removal cooling systems	Active													
									35 Primary helium circulator forced-circulation capability	Active												
									47 Primary pressure-boundary leak detection	Active												
									15 Protective trips for transients exceeding design limits	Active												
									29 EDO restores essential auxiliaries, steering, navigation and communications power	Active												
									28 Segregated ship-service electrical distribution	Passive												
									54 Redundant ship-service electrical distribution pathways sections	Passive												
									2 Passive reactor heat-removal and decay-heat management systems	Passive												
									42 Personnel evacuation and muster procedures	Procedural												
									12 Emergency radiation protection and down-control procedures	Procedural												
									43 Radiological exposure-response and recovery arrangements	Procedural												
									47 Primary pressure-boundary leak detection	Active												
									15 Protective trips for transients exceeding design limits	Active												
									11 Remote-operated isolation and shut-off valves	Active												
									49 Nuclear-compartment isolation capability	Active												
									14 HVAC isolation and filtered ventilation for contaminated compartments	Active												
									2 Passive reactor heat-removal and decay-heat management systems	Passive												
									42 Personnel evacuation and muster procedures	Procedural												
									12 Emergency radiation protection and down-control procedures	Procedural												
									43 Radiological exposure-response and recovery arrangements	Procedural												
								47 Primary pressure-boundary leak detection	Active													
								15 Protective trips for transients exceeding design limits	Active													
								11 Remote-operated isolation and shut-off valves	Active													
								49 Nuclear-compartment isolation capability	Active													
								14 HVAC isolation and filtered ventilation for contaminated compartments	Active													
								4 Airside monitoring and radiological release detection in supervised areas	Active													
								42 Personnel evacuation and muster procedures	Procedural													
								12 Emergency radiation protection and down-control procedures	Procedural													
								43 Radiological exposure-response and recovery arrangements	Procedural													
			1.1.1.6 See consequence 4.1.1.1	S	3	2	5															
			1.1.1.7 A severe unmitigated sequence can require reactor shutdown, compartment isolation, emergency response, and potential off-ship radiological release control.	S	4	1	5															
			1.1.1.8 See consequence 4.1.2.1	S	3	2	5															
			1.1.2.1 Core power falls below the required level and primary helium temperature decreases.																			
		1.1.2.2 Steam generator heat input decreases, steam production falls, and turbine generator output is reduced.																				
		1.1.2.3 See consequence 4.1.1.1																				
		1.1.2.4 Rapid condenser or regulated power cycling impairs thermal stress on the reactor vessel, steam generator, and connected primary components.	S	1	3	4																
		1.1.2.5 See consequence 4.1.2.1																				
		1.1.3.1 Operators or automatic control systems under-estimate reactor power or primary-loop temperature.																				
		1.1.3.2 Control-rod insertion, trip demand, or heat-removal response is delayed or insufficient.	S	2	2	4																
		1.1.3.3 See cause 1.1.1																				
		1.1.3.4 See consequence 1.1.1.4																				
		1.1.3.5 See consequence 1.1.1.5																				

[illegible]

1.2.1 Primary helium piping crack, weld defect, seal failure, flange leakage, or penetration failure caused by fatigue, thermal cycling, manufacturing defect, vibration, or ship-motion loads.	1.2.1.3 See consequence 1.1.1.4	S	3	3	6	14 HVAC isolation and filtered ventilation for contaminated compartments	Active	3	2	5
						2 Passive reactor heat-removal and decay-heat management systems	Passive			
						42 Personnel evacuation and muster procedures	Procedural			
						12 Emergency radiation-protection and dose-control procedures	Procedural			
						43 Radiological exposure-response and recovery arrangements	Procedural			
	1.2.1.4 See consequence 1.1.1.3	S	4	2	6	34 Active residual-heat-removal cooling systems	Active	4	1	5
						35 Primary helium circulator forced-circulation capability	Active			
						47 Primary pressure-boundary leak detection	Active			
						15 Protective trips for transients exceeding design limits	Active			
						29 EDG restores essential auxiliaries, steering, navigation and communications power	Active			
						28 Segregated ship-service electrical distribution	Passive			
						54 Redundant ship-service electrical distribution paths/bus sections	Passive			
						2 Passive reactor heat-removal and decay-heat management systems	Passive			
						42 Personnel evacuation and muster procedures	Procedural			
						12 Emergency radiation-protection and dose-control procedures	Procedural			
						43 Radiological exposure-response and recovery arrangements	Procedural			
	1.2.1.5 See consequence 1.1.1.5	S	3	2	5	47 Primary pressure-boundary leak detection	Active	3	2	5
						15 Protective trips for transients exceeding design limits	Active			
						11 Remote-operated isolation and shut-off valves	Active			
						49 Nuclear-compartment isolation capability	Active			
						14 HVAC isolation and filtered ventilation for contaminated compartments	Active			
						4 Area radiation monitoring and radiological release detection in supervised areas	Active			
						42 Personnel evacuation and muster procedures	Procedural			
						12 Emergency radiation-protection and dose-control procedures	Procedural			
						43 Radiological exposure-response and recovery arrangements	Procedural			
	1.2.1.6 See consequence 4.1.1.1									
	1.2.1.7 See consequence 1.1.1.7									
	1.2.1.8 See consequence 4.1.2.1	S	3	3	6	34 Active residual-heat-removal cooling systems	Active	3	3	6
						35 Primary helium circulator forced-circulation capability	Active			
						47 Primary pressure-boundary leak detection	Active			
						15 Protective trips for transients exceeding design limits	Active			
						29 EDG restores essential auxiliaries, steering, navigation and communications power	Active			
						28 Segregated ship-service electrical distribution	Passive			
						54 Redundant ship-service electrical distribution paths/bus sections	Passive			
						42 Personnel evacuation and muster procedures	Procedural			
						12 Emergency radiation-protection and dose-control procedures	Procedural			
						43 Radiological exposure-response and recovery arrangements	Procedural			
	1.2.1.9 Personnel present in the nuclear compartment, or entering before compartment conditions are independently verified, may be exposed to elevated radiation, airborne contamination, helium-induced oxygen deficiency, or other hazardous atmospheric conditions.	S	3	3	6	47 Primary pressure-boundary leak detection	Active	3	2	5
						11 Remote-operated isolation and shut-off valves	Active			
						49 Nuclear-compartment isolation capability	Active			
						14 HVAC isolation and filtered ventilation for contaminated compartments	Active			
						4 Area radiation monitoring and radiological release detection in supervised areas	Active			
						5 Controlled-access procedures for supervised/radiological areas	Procedural			
						42 Personnel evacuation and muster procedures	Procedural			
						12 Emergency radiation-protection and dose-control procedures	Procedural			
						43 Radiological exposure-response and recovery arrangements	Procedural			
						36 Steam-generator elevation/layout limiting liquid-water migration to the reactor	Passive			
						22 Steam-generator tube material selection, tube-support design, corrosion allowance, and fatigue margin	Passive			

1.2 Boundary or compartment integrity failure	1.2.2 Steam-generator tube leakage from primary helium to secondary steam/water side due to tube cracking, corrosion, thermal fatigue, vibration, manufacturing defect, or differential-pressure loading.	1.2.2.1 Radioactive or activated primary helium enters the intermediate steam/water circuit through the failed tube boundary.	S	2	2	4	51 Steam-generator tube inspection, maintenance, and integrity-management programme 52 Steam-generator pressure-differential control 9 Moisture, pressure, and chemistry detection for steam/water ingress into the primary helium circuit 65 Operator response to process alarms and abnormal indications 24 Automatic detection of steam-generator/intermediate-loop abnormal conditions 53 Automatic protective actuation for steam-generator/intermediate-loop abnormal conditions 1 Reactor protection system and emergency shutdown actuation (ESD) 6 Secondary emergency shutdown 10 Primary helium purification and contamination-removal system 26 Primary and intermediate-loop isolation 11 Remote-operated isolation and shut-off valves	Procedural Active Active Procedural Active Active Active Active Active Active	2	2	4
		1.2.2.2 Contamination can be transported with steam to the turbine, condenser, drains, and non-nuclear machinery spaces.	S	3	2	5	36 Steam-generator elevation/layout limiting liquid-water migration to the reactor 22 Steam-generator tube material selection, tube-support design, corrosion allowance, and fatigue margin 51 Steam-generator tube inspection, maintenance, and integrity-management programme 52 Steam-generator pressure-differential control 9 Moisture, pressure, and chemistry detection for steam/water ingress into the primary helium circuit 65 Operator response to process alarms and abnormal indications 24 Automatic detection of steam-generator/intermediate-loop abnormal conditions 53 Automatic protective actuation for steam-generator/intermediate-loop abnormal conditions 1 Reactor protection system and emergency shutdown actuation (ESD) 6 Secondary emergency shutdown 10 Primary helium purification and contamination-removal system 26 Primary and intermediate-loop isolation 11 Remote-operated isolation and shut-off valves 25 Feedwater and steam-line isolation 50 Isolation of the steam-generator/intermediate cooling train 3 Pressure-relief and overpressure-protection devices 8 Primary and secondary pressure-control system 14 HVAC isolation and filtered ventilation for contaminated compartments 42 Personnel evacuation and muster procedures 12 Emergency radiation-protection and dose-control procedures 43 Radiological exposure-response and recovery arrangements	Passive Passive Procedural Active Active Procedural Active Active Active Active Active Active Active Active Procedural Procedural Procedural	3	2	5
		1.2.2.3 See consequence 1.2.1.1									
		1.2.2.4 See consequence 1.2.1.2									
		1.2.2.5 If isolation is delayed, contaminated condensate or steam can create personnel exposure, equipment contamination, and possible contaminated liquid discharge management issues.	S	3	1	4			3	1	4
	1.2.3.1 Water or steam enters the primary helium circuit and is transported toward hot graphite and core structures.		S	2	3	5	22 Steam-generator tube material selection, tube-support design, corrosion allowance, and fatigue margin 23 Feedwater/helium chemistry-control programme 51 Steam-generator tube inspection, maintenance, and integrity-management programme 52 Steam-generator pressure-differential control	Passive Procedural Procedural Active	2	1	3
		1.2.3.2 Moisture ingress degrades helium purity and can promote graphite oxidation and steam-carbon reactions producing hydrogen and carbon monoxide.	S	4	3	7	9 Moisture, pressure, and chemistry detection for steam/water ingress into the primary helium circuit 24 Automatic detection of steam-generator/intermediate-loop abnormal conditions 53 Automatic protective actuation for steam-generator/intermediate-loop abnormal conditions 25 Feedwater and steam-line isolation 26 Primary and intermediate-loop isolation 10 Primary helium purification and contamination-removal system	Active Active Active Active Active Active	3	1	4

							13 Control-room alarms for inconsistent or abnormal process indications	Active											
							65 Operator response to process alarms and abnormal indications	Procedural											
							1 Reactor protection system and emergency shutdown actuation (ESD)	Active											
							1.2.3.3 Fuel, graphite, and metallic components may experience corrosion, oxidation, thermal stress, or local damage.	S				4	2	6	6 Secondary emergency shutdown	Active	3	1	4
															2 Passive reactor heat-removal and decay-heat management systems	Passive			
															11 Remote-operated isolation and shut-off valves	Active			
															8 Primary and secondary pressure-control system	Active			
							1.2.3.4 Combustible gases can accumulate in the primary circuit or nuclear compartment if released and mixed with air.	S				4	2	6	17 Hydrogen/carbon-monoxide detection and alarm	Active	3	1	4
															44 Nitrogen-inerted reactor-compartment atmosphere	Passive			
															45 Ignition-source control provisions in the reactor compartment	Procedural			
															26 Primary and intermediate-loop isolation	Active			
															14 HVAC isolation and filtered ventilation for contaminated compartments	Active			
															36 Steam-generator elevation/layout limiting liquid-water migration to the reactor	Passive			
															37 TRISO fuel-particle radionuclide retention capability	Passive			
															38 Graphite reflector/core thermal inertia limiting rapid temperature escalation	Passive			
															22 Steam-generator tube material selection, tube-support design, corrosion allowance, and fatigue margin	Passive			
															51 Steam-generator tube inspection, maintenance, and integrity-management programme	Procedural			
															52 Steam-generator pressure-differential control	Active			
															9 Moisture, pressure, and chemistry detection for steam/water ingress into the primary helium circuit	Active			
															65 Operator response to process alarms and abnormal indications	Procedural			
															24 Automatic detection of steam-generator/intermediate-loop abnormal conditions	Active			
															53 Automatic protective actuation for steam-generator/intermediate-loop abnormal conditions	Active			
															1 Reactor protection system and emergency shutdown actuation (ESD)	Active			
															6 Secondary emergency shutdown	Active			
															10 Primary helium purification and contamination-removal system	Active			
															11 Remote-operated isolation and shut-off valves	Active			
															3 Pressure-relief and overpressure-protection devices	Active			
							8 Primary and secondary pressure-control system	Active											
							2 Passive reactor heat-removal and decay-heat management systems	Passive											
							42 Personnel evacuation and muster procedures	Procedural											
							12 Emergency radiation-protection and dose-control procedures	Procedural											
							43 Radiological exposure-response and recovery arrangements	Procedural											
							1.2.3 Steam-generator tube leakage from intermediate water/steam to primary helium side during abnormal pressure reversal, shutdown condition, water hammer, tube rupture, or failed isolation.								17 Hydrogen/carbon-monoxide detection and alarm	Active			
44 Nitrogen-inerted reactor-compartment atmosphere	Passive																		
45 Ignition-source control provisions in the reactor compartment	Procedural																		
16 Fire detection, alarm, and fixed fire-suppression system	Active																		
3 Pressure-relief and overpressure-protection devices	Active																		
41 Filtered release path for overpressure events	Passive																		
20 Nuclear-compartment confinement boundary	Passive																		
49 Nuclear-compartment isolation capability	Active																		
14 HVAC isolation and filtered ventilation for contaminated compartments	Active																		
36 Steam-generator elevation/layout limiting liquid-water migration to the reactor	Passive																		
37 TRISO fuel-particle radionuclide retention capability	Passive																		
38 Graphite reflector/core thermal inertia limiting rapid temperature escalation	Passive																		
22 Steam-generator tube material selection, tube-support design, corrosion allowance, and fatigue margin	Passive																		
51 Steam-generator tube inspection, maintenance, and integrity-management programme	Procedural																		
52 Steam-generator pressure-differential control	Active																		
1.2.3.5 If ignition occurs after air ingress or compartment release, fire or explosion can damage safety-related equipment and	S	4	1	5			4	1	5										

1.2.4 Steam-generator external shell, nozzle, or connected secondary-side pipe rupture releasing water or steam into the nuclear compartment.	1.2.3.6 The sequence can escalate to reactor shutdown, loss of heat removal, contaminated atmosphere, personnel exclusion, and emergency release-control actions.	S	4	1	5	9 Moisture, pressure, and chemistry detection for steam/water ingress into the primary helium circuit	Active	4	1	5								
						65 Operator response to process alarms and abnormal indications	Procedural											
						24 Automatic detection of steam-generator/intermediate-loop abnormal conditions	Active											
						53 Automatic protective actuation for steam-generator/intermediate-loop abnormal conditions	Active											
						1 Reactor protection system and emergency shutdown actuation (ESD)	Active											
						6 Secondary emergency shutdown	Active											
						10 Primary helium purification and contamination-removal system	Active											
						26 Primary and intermediate-loop isolation	Active											
						11 Remote-operated isolation and shut-off valves	Active											
						8 Primary and secondary pressure-control system	Active											
						2 Passive reactor heat-removal and decay-heat management systems	Passive											
						42 Personnel evacuation and muster procedures	Procedural											
						12 Emergency radiation-protection and dose-control procedures	Procedural											
						43 Radiological exposure-response and recovery arrangements	Procedural											
	1.2.3.6 The sequence can escalate to reactor shutdown, loss of heat removal, contaminated atmosphere, personnel exclusion, and emergency release-control actions.	S	4	1	5	22 Steam-generator tube material selection, tube-support design, corrosion allowance, and fatigue margin	Passive	4	1	5								
						51 Steam-generator tube inspection, maintenance, and integrity-management programme	Procedural											
						52 Steam-generator pressure-differential control	Active											
						9 Moisture, pressure, and chemistry detection for steam/water ingress into the primary helium circuit	Active											
						65 Operator response to process alarms and abnormal indications	Procedural											
						24 Automatic detection of steam-generator/intermediate-loop abnormal conditions	Active											
						53 Automatic protective actuation for steam-generator/intermediate-loop abnormal conditions	Active											
						26 Primary and intermediate-loop isolation	Active											
						11 Remote-operated isolation and shut-off valves	Active											
						25 Feedwater and steam-line isolation	Active											
						50 Isolation of the steam-generator/intermediate cooling train	Active											
						29 EDG restores essential auxiliaries, steering, navigation and communications power	Active											
						28 Segregated ship-service electrical distribution	Passive											
						54 Redundant ship-service electrical distribution paths/bus sections	Passive											
	42 Personnel evacuation and muster procedures	Procedural																
	12 Emergency radiation-protection and dose-control procedures	Procedural																
	43 Radiological exposure-response and recovery arrangements	Procedural																
	1.2.4.1 Hot water or steam is released into the nuclear compartment, increasing temperature, humidity, and pressure.	S	4	1	5	26 Primary and intermediate-loop isolation	Active	4	1	5								
						11 Remote-operated isolation and shut-off valves	Active											
25 Feedwater and steam-line isolation						Active												
50 Isolation of the steam-generator/intermediate cooling train						Active												
14 HVAC isolation and filtered ventilation for contaminated compartments						Active												
49 Nuclear-compartment isolation capability						Active												
2 Passive reactor heat-removal and decay-heat management systems						Passive												
42 Personnel evacuation and muster procedures						Procedural												
12 Emergency radiation-protection and dose-control procedures						Procedural												
43 Radiological exposure-response and recovery arrangements						Procedural												
1.2.4.2 Flooding or steam impingement can damage instrumentation, electrical equipment, insulation, and local access routes.																2		
1.2.4.3 Active cooling, monitoring, or isolation equipment in the compartment may become unavailable.																		
1.2.4.4 If water contacts contaminated surfaces or leaked primary helium, contaminated liquid waste can be generated.						S	3				2	5				3	2	5
1.2.4.5 Progressive flooding can challenge watertight boundaries, vessel stability, and needs for emergency response.						S	3				1	4				3	1	4

C.2. Node 2: Turbine-generator room

[illegible]

		2.2.2.6 Flooding, hot surfaces, and electrical-equipment exposure can create room-habitability and fire hazards.	S	3	3	6			3	3	6
2.3 Operating condition and plant-state mismatch	2.3.1 Rapid propulsion load step during manoeuvring, bypass, or generator response capability.	2.3.1.1 The turbine-generator demand changes faster than the steam cycle can stabilise.									
		2.3.1.2 Turbine overspeed, underspeed, vibration, or generator protection demand may occur.									
		2.3.1.3 Steam bypass, turbine trip, or generator trip is initiated to protect equipment.									
		2.3.1.4 See cause 1.3.1									
		2.3.1.5 Critical manoeuvring capability is degraded, increasing collision or grounding risk.	S	3	4	7			3	4	7
		2.3.1.6 See consequence 4.1.1.1	S	3	4	7			3	4	7
		2.3.1.7 See consequence 4.1.2.1	S	3	4	7			3	4	7

C.3. Node 3: Seawater cooling room

Deviation	Causes		Consequences								
	Cause	Consequence	CAT	S Before Safeguards	L Before Safeguards	RR Before Safeguards	Safeguards Safeguard	Type	S	L	RR
3.1 Functional performance failure	3.1.1 Sea chest or strainer blockage caused by marine growth, debris, or ice.	3.1.1.1 Seawater suction pressure falls and flow to the condenser decreases progressively.									
		3.1.1.2 Condenser heat-rejection capacity is reduced and condenser pressure rises.									
		3.1.1.3 Turbine back-pressure increases, turbine efficiency falls, and turbine trip may occur.	S	2	4	6			2	4	6
		3.1.1.4 The steam cycle loses effective heat rejection, causing unstable steam-generator operation and reactor power reduction or trip demand.									
		3.1.1.5 See consequence 4.1.1.1	S	2	3	5			2	3	5
		3.1.1.6 If blockage also affects decay heat removal support and room cooling margins may be reduced.								2	
		3.1.1.7 See consequence 4.1.2.1	S	2	3	5			2	3	5
	3.1.2 Seawater pump mechanical or electrical failure caused by motor trip, bearing seizure, impeller damage, control fault, or loss of electrical supply.	3.1.2.1 Seawater flow to the condenser and essential coolers decreases or stops abruptly.									
		3.1.2.2 See consequence 3.1.1.2									
		3.1.2.3 See consequence 3.1.1.3									
		3.1.2.4 See consequence 3.1.1.4									
		3.1.2.5 See consequence 4.1.1.1									
		3.1.2.6 See consequence 3.1.1.6									
		3.1.2.7 See consequence 4.1.2.1									
	3.1.3 Essential cooling or feedwater-support function lost because seawater cooling is unavailable, common electrical support is lost.	3.1.3.1 Heat rejection from dependent coolers or feedwater-support equipment is reduced.									
		3.1.3.2 See cause 1.1.6									
		3.1.3.3 See consequence 1.1.6.2									
		3.1.3.4 See consequence 4.1.1.1									
		3.1.3.5 See consequence 1.1.1.7									
		3.1.3.6 See consequence 4.1.2.1									
3.2 Boundary or compartment integrity failure	3.2.1 Seawater pipe, expansion joint, valve, or hull penetration leakage caused by corrosion, erosion, vibration, impact, poor maintenance, or joint failure.	3.2.1.1 Seawater leaks into the seawater cooling room.									
		3.2.1.2 Flooding damages pumps, motors, instrumentation, local controls, and access routes.	S	3	2	5			3	2	5
		3.2.1.3 Loss of seawater cooling reduces condenser and essential-cooler heat rejection.	S	2	2	4			2	2	4
		3.2.1.4 Flooding may spread to adjacent spaces if watertight boundaries or drainage are ineffective.	S	3	2	5			3	2	5
		3.2.1.5 Progressive flooding can affect electrical distribution, propulsion support, vessel stability, and emergency response access.	S	3	1	4			3	1	4
		3.2.1.6 A severe uncontrolled flood can contribute to loss of essential cooling and risk of vessel loss.	S	4	1	5			4	1	5
		3.2.1.7 See consequence 4.1.1.1	S	4	1	5			4	1	5
		3.2.1.8 See consequence 4.1.2.1	S	4	1	5			4	1	5
	3.2.2 Sea chest structural failure under collision, or grounding.	3.2.2.1 The sea chest or hull opening loses integrity and uncontrolled seawater ingress enters the hull.									
		3.2.2.2 Rapid flooding of the seawater room occurs and may exceed drainage or isolation capacity.	S	3	2	5			3	2	5
		3.2.2.3 See consequence 3.2.1.3									
		3.2.2.4 See consequence 3.2.1.4									
		3.2.2.5 See consequence 3.2.1.5									
		3.2.2.6 See consequence 3.2.1.6									
		3.2.2.7 See consequence 4.1.1.1									
		3.2.2.8 See consequence 4.1.2.1									
	3.2.3 Condenser tube leakage from seawater side to condensate side caused by tube corrosion, erosion, vibration, fouling, or differential-pressure transient.	3.2.3.1 Seawater contaminates condensate with chlorides, dissolved solids, and biological material.									
		3.2.3.2 Contaminated feedwater is returned to the steam generator, causing scaling, corrosion, and degraded heat transfer.	S	1	3	4			1	3	4</

C.4. Node 4: Electrical distribution and propulsion room

Deviation	Causes		Consequences				Safeguards		S	L	RR
	Cause	Consequence	CAT	S Before Safeguards	L Before Safeguards	RR Before Safeguards	Safeguard	Type			
4.1 Functional performance failure	4.1.1 Main switchboard fault caused by loose connection, overload, cooling failure, or maintenance error.	4.1.1.1 Loss of ship-service electrical power.	S	3	4	7	27 Electrical protection relays, circuit breakers, and selective fault isolation	Active	3	3	6
							28 Segregated ship-service electrical distribution	Passive			
							54 Redundant ship-service electrical distribution paths/bus sections	Passive			
							29 EDG restores essential auxiliaries, steering, navigation and communications power	Active			
							39 Ship-service generator maintenance and inspection programme	Procedural			
							64 Ship-service generator condition monitoring	Active			
							40 Battery-backed essential control and instrumentation power supply	Active			
							55 Automatic bus transfer and load-shedding logic	Active			
							56 Transfer to emergency power and essential-load prioritisation procedure	Procedural			
		4.1.1.2 Loss of manoeuvrability, steering and navigation support.	S	2	4	6	40 Battery-backed essential control and instrumentation power supply	Active	2	3	5
							56 Transfer to emergency power and essential-load prioritisation procedure	Procedural			
							29 EDG restores essential auxiliaries, steering, navigation and communications power	Active			
							42 Personnel evacuation and muster procedures	Procedural			
							12 Emergency radiation-protection and dose-control procedures	Procedural			
							43 Radiological exposure-response and recovery arrangements	Procedural			
							28 Segregated ship-service electrical distribution	Passive			
							54 Redundant ship-service electrical distribution paths/bus sections	Passive			
		4.1.1.3 Loss of reactor control and safe-shutdown capability.	S	3	4	7	40 Battery-backed essential control and instrumentation power supply	Active	3	3	6
							27 Electrical protection relays, circuit breakers, and selective fault isolation	Active			
							29 EDG restores essential auxiliaries, steering, navigation and communications power	Active			
							55 Automatic bus transfer and load-shedding logic	Active			
							56 Transfer to emergency power and essential-load prioritisation procedure	Procedural			
							2 Passive reactor heat-removal and decay-heat management systems	Passive			
							1 Reactor protection system and emergency shutdown actuation (ESD)	Active			
							6 Secondary emergency shutdown	Active			
							42 Personnel evacuation and muster procedures	Procedural			
							12 Emergency radiation-protection and dose-control procedures	Procedural			
							43 Radiological exposure-response and recovery arrangements	Procedural			
							28 Segregated ship-service electrical distribution	Passive			
							54 Redundant ship-service electrical distribution paths/bus sections	Passive			
		4.1.1.4 Loss of safe reactor recovery capabilities	S	3	4	7	40 Battery-backed essential control and instrumentation power supply	Active	3	2	5
							56 Transfer to emergency power and essential-load prioritisation procedure	Procedural			
							29 EDG restores essential auxiliaries, steering, navigation and communications power	Active			
							42 Personnel evacuation and muster procedures	Procedural			
							12 Emergency radiation-protection and dose-control procedures	Procedural			
							43 Radiological exposure-response and recovery arrangements	Procedural			
							28 Segregated ship-service electrical distribution	Passive			
							54 Redundant ship-service electrical distribution paths/bus sections	Passive			
		4.1.2 Propulsion converter, drive, transformer, or motor fault caused by cooling loss overload, or control-system failure.	S	3	4	7	2 Passive reactor heat-removal and decay-heat management systems	Passive	3	4	7
							1 Reactor protection system and emergency shutdown actuation (ESD)	Active			
							6 Secondary emergency shutdown	Active			
							30 Electrical-room fire detection and alarm	Active			
							57 Automatic electrical fault isolation in electrical rooms	Active			
							58 Fixed fire-suppression system for electrical rooms	Active			
							31 Fire-resistant cable routing	Passive			
							59 Fire segregation between electrical zones/divisions	Passive			

4.2 Boundary or compartment integrity failure	4.2.1 Cable fire, switchboard fire, or transformer fire caused by overload, poor termination, or cooling failure.	4.2.1.1 See consequence 4.1.1.2	S	3	3	6	60 Physical separation of redundant electrical divisions	Passive	3	2	5
							28 Segregated ship-service electrical distribution	Passive			
							54 Redundant ship-service electrical distribution paths/bus sections	Passive			
							39 Ship-service generator maintenance and inspection programme	Procedural			
							64 Ship-service generator condition monitoring	Active			
							40 Battery-backed essential control and instrumentation power supply	Active			
							29 EDG restores essential auxiliaries, steering, navigation and communications power	Active			
	4.2.2 Flooding, water leak, ventilation failure, or loss of HVAC in the electrical room causing moisture ingress, overheating, or loss of room environmental control.	4.2.2.1 See consequence 4.1.1.1	S	3	3	6	56 Transfer to emergency power and essential-load prioritisation procedure	Procedural	3	2	5
							32 Watertight segregation for electrical rooms	Passive			
							61 Electrical-room leak/flood detection	Active			
							62 Electrical-room drainage provisions	Passive			
							33 Redundant ventilation and cooling for electrical equipment	Active			
							63 Environmental monitoring for electrical equipment	Active			
							28 Segregated ship-service electrical distribution	Passive			
							54 Redundant ship-service electrical distribution paths/bus sections	Passive			
							40 Battery-backed essential control and instrumentation power supply	Active			
							29 EDG restores essential auxiliaries, steering, navigation and communications power	Active			
							56 Transfer to emergency power and essential-load prioritisation procedure	Procedural			
4.3 Operating condition and plant-state mismatch	4.3.1 Turbine trip, generator trip, bus-transfer failure, or rapid propulsion-load rejection causes a mismatch between generation, distribution, and propulsion demand.	4.3.1.1 See cause 4.1.1 and downstream consequences 4.1.1.1-4.1.1.4.	S	3	4	7	29 EDG restores essential auxiliaries, steering, navigation and communications power	Active	3	3	6
							28 Segregated ship-service electrical distribution	Passive			
							54 Redundant ship-service electrical distribution paths/bus sections	Passive			
							39 Ship-service generator maintenance and inspection programme	Procedural			
							64 Ship-service generator condition monitoring	Active			
							40 Battery-backed essential control and instrumentation power supply	Active			
							27 Electrical protection relays, circuit breakers, and selective fault isolation	Active			
							55 Automatic bus transfer and load-shedding logic	Active			
							56 Transfer to emergency power and essential-load prioritisation procedure	Procedural			
		4.3.1.2 See consequence 4.1.2.1	S	3	4	7	29 EDG restores essential auxiliaries, steering, navigation and communications power	Active	3	3	6
							28 Segregated ship-service electrical distribution	Passive			
							54 Redundant ship-service electrical distribution paths/bus sections	Passive			
							39 Ship-service generator maintenance and inspection programme	Procedural			
							64 Ship-service generator condition monitoring	Active			

C.5. Node 5: Ship operations and maritime hazards

Deviation	Causes		Consequences									
	Cause	Consequence	CAT	S Before Safeguards	L Before Safeguards	RR Before Safeguards	Safeguards	Type	S	L	RR	
		Safeguard										
5.1 Maritime impact or external fire and explosion	5.1.1 Collision with another vessel near the protected machinery or nuclear-compartment region due to navigation error, loss of propulsion, or poor visibility.	5.1.1.1 Local hull deformation occurs and watertight boundaries, cable routes, seawater systems, or protected compartment boundaries may be damaged.	S	3	3	6			3	3	6	
		5.1.1.2 See cause 3.2.1										
		5.1.1.3 See cause 4.2.1										
		5.1.1.4 See cause 1.2.1										
		5.1.1.5 See cause 1.2.2										
		5.1.1.6 See cause 2.2.1										
		5.1.1.7 See consequence 3.2.1.3	S	2	3	5			2	3	5	
		5.1.1.8 See consequence 4.1.1.1										
		5.1.1.9 See cause 5.3.2										
		5.1.1.10 A severe sequence can escalate to vessel abandonment, salvage intervention, exclusion area, and potential vessel loss.	S	4	1	5			4	1	5	
	5.1.2 Grounding in shallow water caused by navigation error, propulsion loss, extreme weather, charting error, or emergency manoeuvre.	5.1.1.11 See consequence 4.1.2.1	S	2	3	5			2	3	5	
		5.1.2.1 Bottom plating, double-bottom tanks, sea chests, and hull penetrations can be damaged.	S	3	3	6			3	3	6	
		5.1.2.2 See cause 3.2.2										
		5.1.2.3 See consequence 3.2.1.3										
		5.1.2.4 See consequence 1.1.1.3										
		5.1.2.5 See consequence 3.2.1.5										
		5.1.2.6 See consequence 3.2.1.6										
		5.1.2.7 See cause 5.3.2										
		5.1.2.8 A severe grounding can require evacuation, salvage, environmental response, and long-term recovery operations.	S	4	1	5			4	1	5	
		5.1.2.9 See consequence 4.1.1.1										
		5.1.2.10 See consequence 4.1.2.1										
5.2 Natural and environmental hazards	5.2.1 Severe weather event with extreme sea state, storm, green-water loading, heavy rolling/pitching/heaving, or slamming beyond normal operating assumptions.	5.2.1.1 Dynamic loads and accelerations act on hull structure, pipe supports, reactor and machinery foundations, electrical equipment, and seawater intakes.										
		5.2.1.2 See cause 3.1.2										
		5.2.1.3 Ship motions can challenge operator performance, maintenance access, and automatic control stability.										
		5.2.1.4 See consequence 4.1.1.1										
		5.2.1.5 See consequence 3.1.1.4										
		5.2.1.6 The vessel may enter a degraded navigation condition with increased collision, grounding, or emergency-response difficulty.	S	3	3	6			3	3	6	
		5.2.1.7 See consequence 4.1.2.1										
	5.2.2 Extreme ambient seawater temperature, ice, biofouling, or abnormal coastal water condition outside the heat-rejection design basis.	5.2.2.1 The available temperature difference across the condenser and coolers is reduced or seawater flow is physically restricted.										
		5.2.2.2 See consequence 3.1.1.2										
		5.2.2.3 See consequence 3.1.1.3										
		5.2.2.4 See consequence 3.1.1.4										
		5.2.2.5 See consequence 3.1.1.6										
		5.2.2.6 The vessel may require route change, port refuge, or emergency cooling restoration.	S	3	3	6			3	3	6	
		5.2.2.7 See consequence 4.1.2.1	S	3	3	6			3	3	6	
5.3 Failure of off-ship release control or environmental protection	5.3.1 Radioactive material release path not isolated or monitored because discharge monitoring fails, or contaminated floodwater is pumped overboard.	5.3.1.1 Radioactive material enters a liquid or airborne discharge pathway from a contaminated compartment, secondary circuit, condenser discharge, drain, or floodwater route.										
		5.3.1.2 Onboard personnel and responders may be exposed during access, pumping, isolation, sampling, or decontamination activities.	S	3	2	5			3	2	5	
		5.3.1.3 Contaminated water, steam, or airborne material can move beyond the vessel boundary if isolation or filtration is ineffective.	S	3	2	5			3	2	5	
		5.3.1.4 A major uncontrolled release can lead to exclusion zones, reputational impact, operational shutdown, and vessel recovery or disposal decisions.	S	4	1	5			4	1	5	

[illegible]

C.6. Existing safeguard catalogue

Safeguard	Type	Category	Reference
1 Reactor protection system and emergency shutdown actuation (ESD)	Active	Active	1.2.1.2
			1.2.2.1
			1.2.2.2
			1.2.3.3
			1.2.3.4
			1.2.3.5
			2.1.2.5
			4.1.1.3
2 Passive reactor heat-removal and decay-heat management systems	Passive	Passive	4.1.1.4
			1.1.1.3
			1.1.1.4
			1.2.1.2
			1.2.1.3
			1.2.1.4
			1.2.3.3
			1.2.3.4
			1.2.3.5
			1.2.4.1
3 Pressure-relief and overpressure-protection devices	Active	Active	2.1.2.5
			4.1.1.3
			4.1.1.4
4 Area radiation monitoring and radiological release detection in supervised areas	Active	Active	1.2.2.2
			1.2.3.4
			1.2.3.5
5 Controlled-access procedures for supervised/radiological areas	Active	Active	1.1.1.5
			1.2.1.5
			1.2.1.9
6 Secondary emergency shutdown	Procedural	Procedural	1.2.1.9
			1.2.1.2
			1.2.2.1
			1.2.2.2
			1.2.3.3
			1.2.3.4
			1.2.3.5
			2.1.2.5
7 Redundant safety instrumentation with 2-out-of-3 voting logic	Active	Active	4.1.1.3
			4.1.1.4
			1.2.1.1
			1.2.1.1
8 Primary and secondary pressure-control system	Active	Active	1.2.2.2
			1.2.3.3
			1.2.3.4
			1.2.3.5
9 Moisture, pressure, and chemistry detection for steam/water ingress into the primary helium circuit	Active	Active	1.2.2.1
			1.2.2.2
			1.2.3.2
			1.2.3.4

10 Primary helium purification and contamination-removal system	Active	Active	1.2.3.5
			1.2.3.6
			1.2.2.1
			1.2.2.2
			1.2.3.2
11 Remote-operated isolation and shut-off valves	Active	Active	1.2.3.4
			1.2.3.5
			1.1.1.4
			1.1.1.5
			1.2.1.3
			1.2.1.5
			1.2.1.9
			1.2.2.1
			1.2.2.2
			1.2.3.3
			1.2.3.4
			1.2.3.5
12 Emergency radiation-protection and dose-control procedures	Procedural	Procedural	1.2.3.6
			1.2.4.1
			1.1.1.3
			1.1.1.4
			1.1.1.5
			1.2.1.3
			1.2.1.4
			1.2.1.5
			1.2.1.8
			1.2.1.9
			1.2.2.2
			1.2.3.4
			1.2.3.5
			1.2.3.6
			1.2.4.1
13 Control-room alarms for inconsistent or abnormal process indications	Active	Active	2.1.2.5
			4.1.1.2
14 HVAC isolation and filtered ventilation for contaminated compartments	Active	Active	4.1.1.3
			4.1.1.4
			1.2.3.2
			1.1.1.4
			1.1.1.5
			1.2.1.3
			1.2.1.5
			1.2.1.9
			1.2.2.2
			1.2.3.4
			1.2.3.5
			1.2.4.1
			1.1.1.3
			1.1.1.4
			1.1.1.5

15 Protective trips for transients exceeding design limits	Active	Active	1.2.1.1
			1.2.1.3
			1.2.1.4
			1.2.1.5
			1.2.1.8
16 Fire detection, alarm, and fixed fire-suppression system	Active	Active	1.2.3.5
17 Hydrogen/carbon-monoxide detection and alarm	Active	Active	1.2.3.4
			1.2.3.5
18 Qualified primary pressure-boundary design and material selection	Passive	Passive	1.2.1.1
19 Primary pressure-boundary in-service inspection and maintenance programme	Procedural	Procedural	1.2.1.1
20 Nuclear-compartment confinement boundary	Passive	Passive	1.2.3.5
21 Controlled shutdown of the steam-generator/intermediate cooling train	Active	Active	1.2.1.2
22 Steam-generator tube material selection, tube-support design, corrosion allowance, and fatigue margin	Passive	Passive	1.2.2.1
			1.2.2.2
			1.2.3.1
			1.2.3.4
			1.2.3.5
23 Feedwater/helium chemistry-control programme	Procedural	Procedural	1.2.3.6
			1.2.3.1
			1.2.2.1
			1.2.2.2
			1.2.3.2
24 Automatic detection of steam-generator/intermediate-loop abnormal conditions	Active	Active	1.2.3.4
			1.2.3.5
			1.2.3.6
			1.2.2.2
			1.2.3.2
25 Feedwater and steam-line isolation	Active	Active	1.2.3.6
			1.2.4.1
			1.2.2.1
			1.2.2.2
			1.2.3.2
26 Primary and intermediate-loop isolation	Active	Active	1.2.3.4
			1.2.3.5
			1.2.3.6
			1.2.4.1
			2.1.2.5
27 Electrical protection relays, circuit breakers, and selective fault isolation	Active	Active	4.1.1.1
			4.1.1.3
			4.3.1.1
			1.1.1.3
			1.2.1.4
			1.2.1.8
			1.2.3.6

28 Segregated ship-service electrical distribution	Passive	Passive	4.1.1.1
			4.1.1.2
			4.1.1.3
			4.1.1.4
			4.2.1.1
			4.2.2.1
			4.3.1.1
29 EDG restores essential auxiliaries, steering, navigation and communications power	Active	Active	4.3.1.2
			1.1.1.3
			1.2.1.4
			1.2.1.8
			1.2.3.6
			2.1.2.5
			4.1.1.1
			4.1.1.2
			4.1.1.3
			4.1.1.4
			4.2.1.1
			4.2.2.1
			4.3.1.1
			4.3.1.2
30 Electrical-room fire detection and alarm	Active	Active	4.2.1.1
31 Fire-resistant cable routing	Passive	Passive	4.2.1.1
32 Watertight segregation for electrical rooms	Passive	Passive	4.2.2.1
33 Redundant ventilation and cooling for electrical equipment	Active	Active	4.2.2.1
34 Active residual-heat-removal cooling systems	Active	Active	1.1.1.3
			1.2.1.2
			1.2.1.4
			1.2.1.8
35 Primary helium circulator forced-circulation capability	Active	Active	1.1.1.3
			1.2.1.2
			1.2.1.4
			1.2.1.8
36 Steam-generator elevation/layout limiting liquid-water migration to the reactor	Passive	Passive	1.2.2.1
			1.2.2.2
			1.2.3.4
			1.2.3.5
37 TRISO fuel-particle radionuclide retention capability	Passive	Passive	1.2.3.4
			1.2.3.5
38 Graphite reflector/core thermal inertia limiting rapid temperature escalation	Passive	Passive	1.2.3.4
			1.2.3.5
39 Ship-service generator maintenance and inspection programme	Procedural	Procedural	2.1.2.1
			2.1.2.2
			2.1.2.5
			4.1.1.1
			4.2.1.1
			4.3.1.1
			4.3.1.2

40 Battery-backed essential control and instrumentation power supply	Active	Active	2.1.2.2
			2.1.2.5
			4.1.1.1
			4.1.1.2
			4.1.1.3
			4.1.1.4
			4.2.1.1
			4.2.2.1
			4.3.1.1
41 Filtered release path for overpressure events	Passive	Passive	1.2.3.5
42 Personnel evacuation and muster procedures	Procedural	Procedural	1.1.1.3
			1.1.1.4
			1.1.1.5
			1.2.1.3
			1.2.1.4
			1.2.1.5
			1.2.1.8
			1.2.1.9
			1.2.2.2
			1.2.3.4
			1.2.3.5
			1.2.3.6
			1.2.4.1
			2.1.2.5
			4.1.1.2
43 Radiological exposure-response and recovery arrangements	Procedural	Procedural	4.1.1.3
			4.1.1.4
			1.1.1.3
			1.1.1.4
			1.1.1.5
			1.2.1.3
			1.2.1.4
			1.2.1.5
			1.2.1.8
			1.2.1.9
			1.2.2.2
			1.2.3.4
			1.2.3.5
			1.2.3.6
			1.2.4.1
44 Nitrogen-inerted reactor-compartment atmosphere	Passive	Passive	2.1.2.5
			4.1.1.2
45 Ignition-source control provisions in the reactor compartment	Procedural	Procedural	4.1.1.3
			4.1.1.4
			1.2.3.4
			1.2.3.5

46 Primary pressure-boundary fabrication quality assurance, pressure testing, and leak-tightness verification	Procedural	Procedural	1.2.1.1
47 Primary pressure-boundary leak detection	Active	Active	1.1.1.3
			1.1.1.4
			1.1.1.5
			1.2.1.1
			1.2.1.3
			1.2.1.4
			1.2.1.5
48 Primary pressure-boundary vibration and pressure monitoring	Active	Active	1.2.1.8
			1.2.1.9
			1.2.1.1
49 Nuclear-compartment isolation capability	Active	Active	1.1.1.4
			1.1.1.5
			1.2.1.3
			1.2.1.5
			1.2.1.9
			1.2.3.5
			1.2.4.1
50 Isolation of the steam-generator/intermediate cooling train	Active	Active	1.2.1.2
			1.2.2.2
			1.2.3.6
			1.2.4.1
51 Steam-generator tube inspection, maintenance, and integrity-management programme	Procedural	Procedural	1.2.2.1
			1.2.2.2
			1.2.3.1
			1.2.3.4
			1.2.3.5
			1.2.3.6
52 Steam-generator pressure-differential control	Active	Active	1.2.2.1
			1.2.2.2
			1.2.3.1
			1.2.3.4
			1.2.3.5
			1.2.3.6
53 Automatic protective actuation for steam-generator/intermediate-loop abnormal conditions	Active	Active	1.2.2.1
			1.2.2.2
			1.2.3.2
			1.2.3.4
			1.2.3.5
			1.2.3.6
54 Redundant ship-service electrical distribution paths/bus sections	Passive	Passive	1.1.1.3
			1.2.1.4
			1.2.1.8
			1.2.3.6
			4.1.1.1
			4.1.1.2
			4.1.1.3

			4.1.1.4
			4.2.1.1
			4.2.2.1
			4.3.1.1
			4.3.1.2
55 Automatic bus transfer and load-shedding logic	Active	Active	2.1.2.5
			4.1.1.1
			4.1.1.3
			4.3.1.1
56 Transfer to emergency power and essential-load prioritisation procedure	Procedural	Procedural	2.1.2.5
			4.1.1.1
			4.1.1.2
			4.1.1.3
			4.1.1.4
			4.2.1.1
57 Automatic electrical fault isolation in electrical rooms	Active	Active	4.2.2.1
			4.3.1.1
58 Fixed fire-suppression system for electrical rooms	Active	Active	4.2.1.1
59 Fire segregation between electrical zones/divisions	Passive	Passive	4.2.1.1
60 Physical separation of redundant electrical divisions	Passive	Passive	4.2.1.1
61 Electrical-room leak/flood detection	Active	Active	4.2.2.1
62 Electrical-room drainage provisions	Passive	Passive	4.2.2.1
63 Environmental monitoring for electrical equipment	Active	Active	4.2.2.1
64 Ship-service generator condition monitoring	Active	Active	2.1.2.1
			2.1.2.2
			2.1.2.5
			4.1.1.1
			4.2.1.1
			4.3.1.1
65 Operator response to process alarms and abnormal indications	Procedural	Procedural	4.3.1.2
			1.2.2.1
			1.2.2.2
			1.2.3.2
			1.2.3.4
			1.2.3.5
			1.2.3.6

D

First Iteration Bow-tie Analysis

D.1. Loss of primary helium circuit pressure boundary integrity, detailed Bow-tie

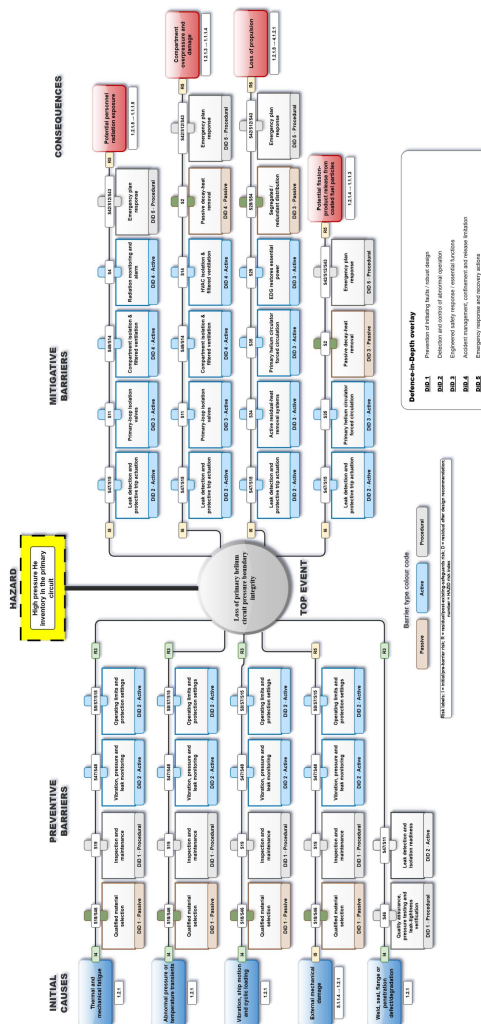


Figure D.1: Detailed first iteration Bow-tie for loss of primary helium circuit pressure boundary integrity.

D.2. Loss of steam generator tube integrity, detailed Bow-tie

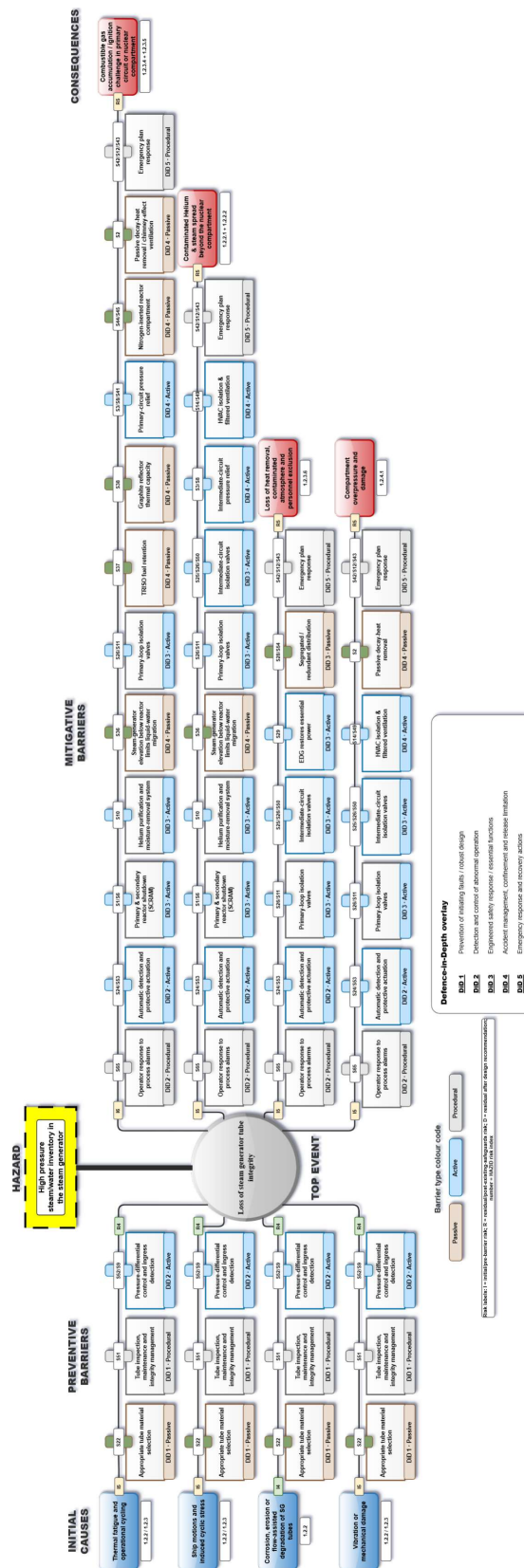


Figure D.2: Detailed first iteration Bow-tie for loss of steam generator tube integrity.

D.3. Loss of ship service electrical power, detailed Bow-tie

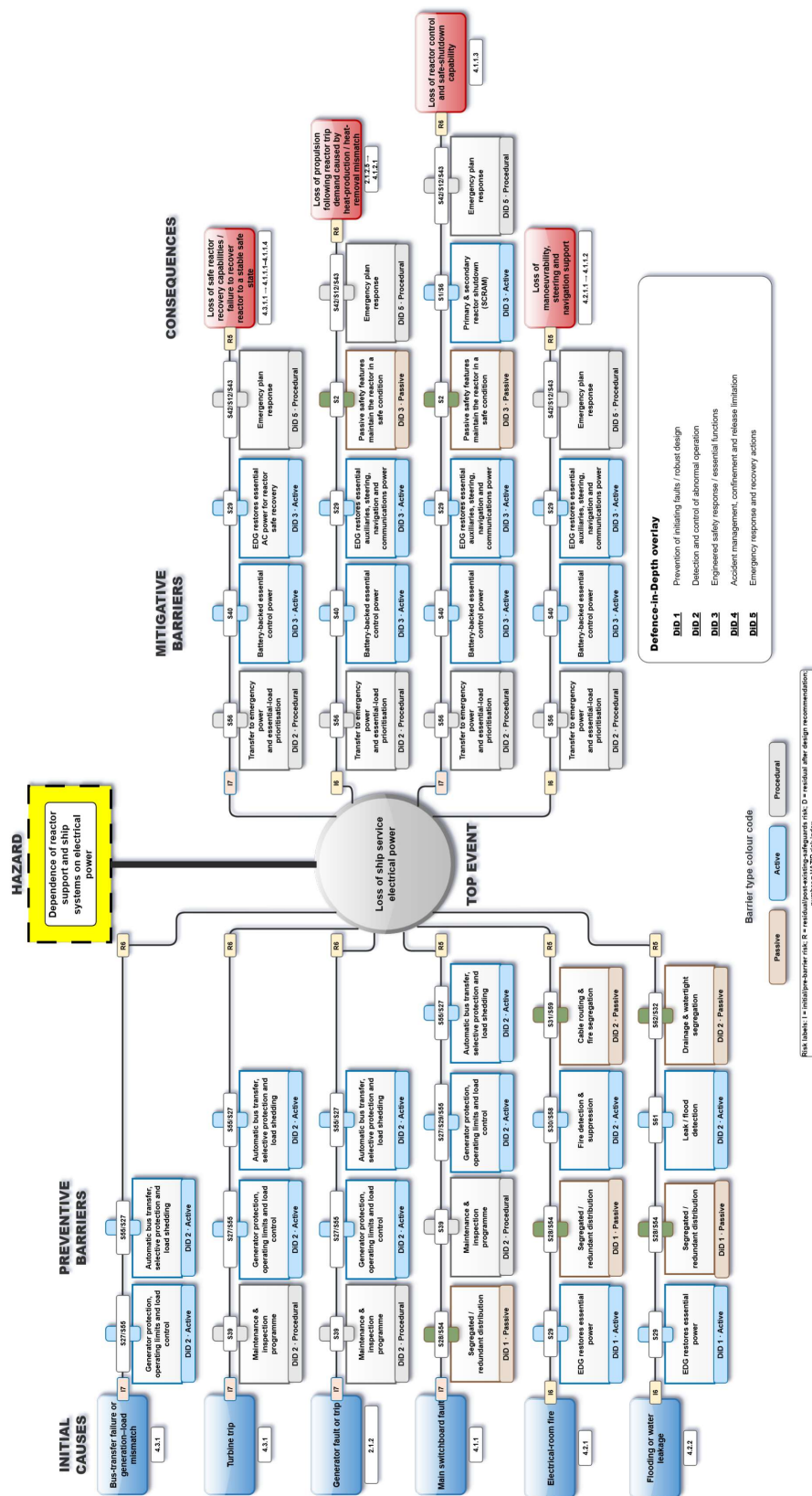


Figure D.3: Detailed first iteration Bow-tie for loss of ship service electrical power.

This page is left blank intentionally.

E

Design Recommendation Traceability and Second Iteration Results

E.1. Design recommendation traceability and affected scenarios

PHA Recommendation	Referenced Locations										
	Reference	CAT	S Before Safeguards	L Before Safeguards	RR Before Safeguards	S	L	RR	S After Recommendations	L After Recommendations	RR After Recommendations
1 REC 1 - REV B design change: provide two independent, segregated seawater cooling and condensing trains (Seawater Cooling Room 1 and 2, with dedicated sea chests, seawater pumps, and condensers 1 and 2) so that loss of one train does not result in total loss of condenser/essential-cooler heat rejection.	3.1.1.3	S	2	4	6	2	4	6	2	2	4
	3.2.1.3	S	2	2	4	2	2	4	2	2	4
	4.1.1.4	S	3	4	7	3	2	5	3	1	4
	4.3.1.1	S	3	4	7	3	3	6	3	1	4
2 REC 2 - REV B design change (Notes 6, 8 & 10): route contaminated or potentially contaminated pressure-relief flows from the intermediate high pressure loop and feedwater/steam generator boundary to a confined cofferdam or relief handling. Released helium steam or fluid shall be confined, monitored, isolated, filtered/treated, and discharged through a controlled vent mast where required.	1.1.1.3	S	4	2	6	4	1	5	3	1	4
	1.1.1.4	S	3	2	5	3	2	5	3	2	5
	1.2.1.3	S	3	3	6	3	2	5	3	2	5
	1.2.1.4	S	4	2	6	4	1	5	3	1	4
	1.2.2.2	S	3	2	5	3	2	5	2	2	4
	1.2.3.6	S	4	1	5	4	1	5	3	1	4
	5.3.1.3	S	3	2	5	3	2	5	3	1	4
3 REC 3 - REV B design change (Note 7): install a pressure-relief valve downstream of the turbine to protect the turbine and intermediate low pressure loop against excessive back-pressure from condenser failure or loss of condenser cooling. Relief flow shall be routed to a controlled dump, collection system, or vent mast, with monitoring and treatment where contamination is credible.	2.1.1.3	S	1	3	4	1	3	4	1	3	4
	2.1.3.3	S	2	3	5	2	3	5	2	2	4
4 REC 4 - REV B design change: provide two segregated main switchboard rooms and a dedicated, segregated Emergency Switchboard (ESWB) in a fire- and flood-rated room with independent detection, to preserve emergency distribution and reactor safe-shutdown power following main switchboard or compartment hazards.	4.1.1.1	S	3	4	7	3	3	6	3	2	5
	4.1.1.3	S	3	4	7	3	3	6	3	2	5
	4.1.1.4	S	3	4	7	3	2	5	3	1	4
	4.3.1.1	S	3	4	7	3	3	6	3	1	4
5 REC 5 - REV B design change (Note 9): monitor the seawater cooling discharge for abnormal temperature, flow, pressure, chemical or radioactive contamination, and provide a discharge-side shut-off valve to isolate the seawater discharge path on abnormal indication.	3.2.4.2	S	3	1	4	3	1	4	3	1	4
	5.3.1.3	S	3	2	5	3	2	5	3	1	4
6 REC 6 - REV B design change: designate the nuclear compartment as normally unmanned whenever the reactor or primary helium system is in operation. Provide remote operation and continuous monitoring of radiation, airborne contamination, helium and oxygen concentration, pressure, temperature, and fire conditions from a continuously attended control station. Access shall be authorization-controlled and interlocked against unsafe conditions..	1.1.5.2	S	3	2	5	3	2	5	3	2	5
	1.2.1.9	S	3	3	6	3	2	5	3	2	5
	1.2.2.5	S	3	1	4	3	1	4	3	1	4
	1.2.3.6	S	4	1	5	4	1	5	3	1	4
	1.2.4.5	S	3	1	4	3	1	4	3	1	4

Figure E.1: HAZID scenarios affected by the design recommendations and their risk ranking development across the three assessment states.

E.2.1. Loss of primary helium circuit pressure boundary integrity

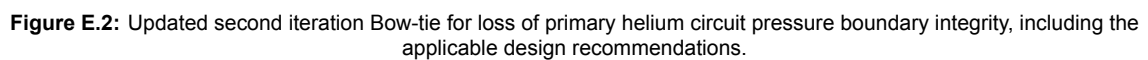


Figure E.3: Updated second iteration Bow-tie for loss of steam generator tube integrity, including the applicable design recommendations.

E.2.3. Loss of ship service electrical power

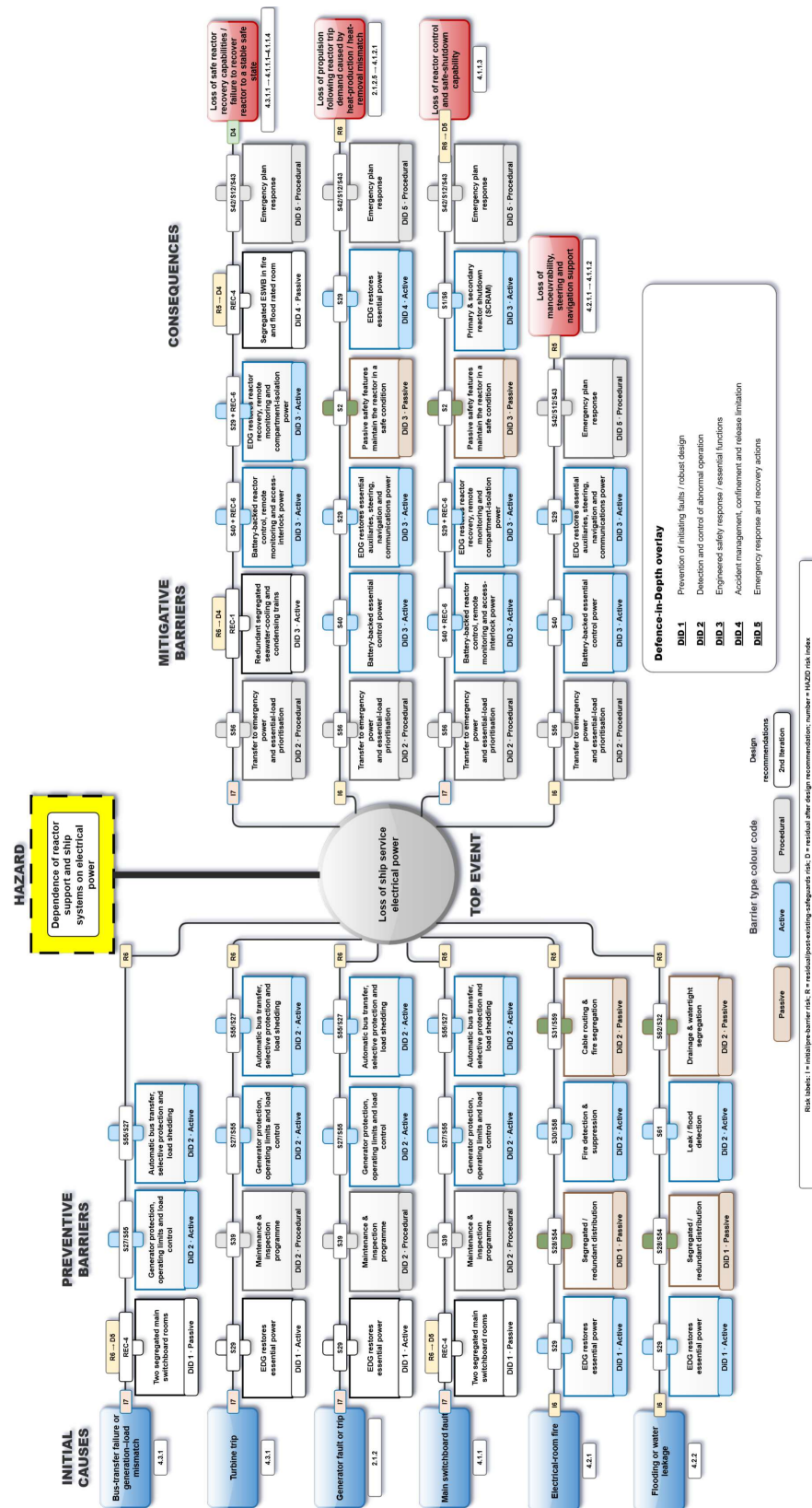


Figure E.4: Updated second iteration Bow-tie for loss of ship service electrical power, including the applicable design recommendations.

